



Active IQ Unified Manager のドキュメント

Active IQ Unified Manager 9.12

NetApp
December 18, 2023

目次

Active IQ Unified Manager のドキュメント	1
リリースノート	2
はじめに	3
VMwareのインストールのクイックスタート手順	3
Linux インストールのクイックスタート手順	4
Windows インストールのクイックスタート手順	5
VMware vSphere システムに Unified Manager をインストールします	7
Active IQ Unified Manager の概要	7
Unified Manager をインストールするための要件	8
Unified Manager ソフトウェアのインストール、アップグレード、削除を行います	16
Linux システムに Unified Manager をインストールします	26
Active IQ Unified Manager の概要	26
Unified Manager をインストールするための要件	27
Unified Manager ソフトウェアのインストール、アップグレード、削除を行います	36
Windows システムに Unified Manager をインストールする	57
Active IQ Unified Manager の概要	57
Unified Manager をインストールするための要件	58
Unified Manager ソフトウェアのインストール、アップグレード、削除を行います	66
設定タスクと管理タスクを実行	77
Active IQ Unified Manager を設定しています	77
Unified Manager のバックアップを設定しています	97
機能設定の管理	97
メンテナンスコンソールを使用する	101
ユーザアクセスの管理	115
SAML 認証の設定を管理する	122
認証の管理	129
セキュリティ証明書の管理	136
ストレージを監視および管理する	143
Active IQ Unified Manager の概要	143
ユーザインターフェイスの概要	146
ダッシュボードからクラスタを監視および管理する	153
クラスタの管理	164
VMware 仮想インフラを監視する	170
ワークロードのプロビジョニングと管理	179
MetroCluster 構成を管理および監視する	195
クォータの管理	203
トラブルシューティング	210
イベントとアラートの管理	218
イベントの管理	218

アラートの管理	317
スクリプトの管理	331
クラスタのパフォーマンスを監視および管理する	344
Active IQ Unified Manager によるパフォーマンス監視の概要	344
Unified Manager の GUI で実行するパフォーマンスワークフロー	348
ダッシュボードからのクラスタパフォーマンスの監視	357
Workload Analyzer を使用したワークロードのトラブルシューティング	359
パフォーマンスクラスタランディングページからのクラスタパフォーマンスの監視	362
パフォーマンスインベントリページを使用したパフォーマンスの監視	368
パフォーマンスエクスプローラページを使用したパフォーマンスの監視	378
QoS ポリシーグループ情報を使用したパフォーマンスの管理	399
パフォーマンス容量と使用可能な IOPS の情報を使用してパフォーマンスを管理する	405
ノードフェイルオーバープランの概要と使用方法ページ	413
データを収集してワークロードのパフォーマンスを監視	417
パフォーマンスイベントとアラートの概要	425
パフォーマンスしきい値の管理	436
パフォーマンスイベントを分析しています	447
パフォーマンスイベントを解決しています	462
Unified Manager サーバと外部データプロバイダ間の接続の設定	478
クラスタヘルスを監視および管理する	483
Active IQ Unified Manager の健全性監視の概要	483
クラスタおよびクラスタオブジェクトの健全性を管理および監視する	486
Unified Manager の一般的な健全性関連のワークフローとタスク	500
データを保護、リストア	634
保護関係の作成、監視、およびトラブルシューティング	634
保護関係を管理および監視する	647
カスタムレポートを生成	727
Unified Manager のレポート機能	727
レポートの操作	732
レポートのスケジュール設定	740
サンプルのカスタムレポート	745
Microsoft Excel レポートの例	763
REST API を使用してストレージを管理できます	775
Active IQ Unified Manager REST APIの使用を開始する	775
Active IQ Unified Manager での REST API へのアクセスおよび認証	779
Unified Manager REST API	789
ストレージ管理のための一般的なAPIワークフロー	823
法的通知	858
著作権	858
商標	858
特許	858

プライバシーポリシー	858
オープンソース	858

Active IQ Unified Manager のドキュメント

リリースノート

Active IQ Unified Manager 9.12の新機能、制限事項、および既知の問題の概要を示します。

詳細については、を参照してください "[Active IQ Unified Manager リリースノート](#)"。

はじめに

VMwareのインストールのクイックスタート手順

はダウンロードできます .tar ルート証明書を含むファイル README ファイル、および OVA ファイルを作成し、Unified Managerを仮想アプライアンスとして導入します。

システム要件

- オペレーティングシステム：VMware ESXi 6.5、6.7、および7.0.x
- RAM ： 12GB
- CPU ：合計 9572MHz
- 空きディスクスペース： 5GB （シンプロビジョニング）、 152GB （シックプロビジョニング）

システム要件の詳細については、を参照してください "[Unified Manager をインストールするための要件](#)" および "[互換性マトリックス](#)"。

Active IQ Unified Manager をインストールしています

インストーラをダウンロードします。

1. をダウンロードします .tar ルート証明書を含むファイル README ファイル、および OVA ファイル。
2. vSphere Client からアクセス可能なローカルまたはネットワークのディレクトリにファイルを保存します。
3. をダウンロードしたディレクトリ .tar ファイルで、を入力します `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz` コマンドを実行します+必要なを押します OVA ファイル、ルート証明書、および README ファイルがターゲットディレクトリに解凍されます。

整合性を検証

の整合性を検証できます OVA で説明した手順に従ってファイルを作成します README ファイル。

Unified Manager をインストールします

1. vSphere Client で、 * File > Deploy OVF Template * をクリックします。
2. OVA ファイルを探し、ウィザードを使用して ESXi サーバに仮想アプライアンスを導入します。
3. [詳細の確認]ページの[発行元]セクションで、メッセージを確認します Entrust Code Signing - OVCS2 (Trusted certificate) ダウンロードしたの整合性を確認します OVA ファイル。をクリックしてください `Entrust Code Signing - OVCS2 (Invalid certificate)` をクリックして、VMware vCenter Serverを7.0U3E以降のバージョンにアップグレードします。
4. [テンプレートのカスタマイズ]ページの[プロパティ]タブで、実行するインストールのタイプに応じて、必要に応じてフィールドに入力します。
 - 静的設定の場合は、すべてのフィールドに必要な情報を入力します。[* Secondary DNS* （セカンダリ DNS *）] フィールドへの情報の追加は不要です。

- IPv4 を使用する DHCP の場合、どのフィールドにも情報を追加しないでください。
- IPv6 を使用する DHCP の場合は、[Enable Auto IPv6 addressing] チェックボックスをオンにします。他のフィールドには情報を追加しないでください。

5. VM の電源をオンにします。
6. [コンソール] タブをクリックして、最初の起動プロセスを表示します。
7. タイムゾーンを設定します。
8. Unified Manager のメンテナンスユーザの名前とパスワードを入力します。

インストールの完了時に、Unified Manager Web UI に接続するための情報が表示されます。

Linux インストールのクイックスタート手順

インストールパッケージをダウンロードして、Red Hat Enterprise LinuxまたはCentOSの物理プラットフォームまたは仮想プラットフォームにUnified Managerをインストールできます。

システム要件

- オペレーティングシステム：Red Hat Enterprise Linuxバージョン7.xおよび8.0から8.6、またはx86_64アーキテクチャに基づくCentOSバージョン7.x。OSインストーラの* Software Selection *オプションから「Server with GUI」ベース環境を使用してインストールします
- RAM：12 GB、CPU：合計 9572MHz
- 空きディスクスペース：100GBのディスクスペースがに表示されます /opt/netapp/data ディレクトリ。ルートパーティション内で50GB。別途マウントする必要があります /opt および /var/log ディレクトリに移動する場合は、を確認します /opt 15 GB、 /var/log には16GB、およびが搭載されています /tmp に10GBの空きスペースがあります。

システム要件の詳細および製品をセキュリティ保護されたサイトにインストールする方法については、を参照してください "[Unified Manager をインストールするための要件](#)" および "[互換性マトリックス](#)"。

Active IQ Unified Manager をインストールしています

インストーラをダウンロードします。

1. をダウンロードします ActiveIQUnifiedManager-<version>.zip インストールパッケージとコード署名証明書 (.pem) およびデジタル署名 (.sig) 。
2. インストールファイルをダウンロードしたディレクトリで、次のコマンドを実行します。

```
# unzip ActiveIQUnifiedManager-<version>.zip
```

整合性を検証

次のコマンドを実行して、インストーラパッケージの整合性を確認します。

- を実行します openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem >

<public_key_file_name> コード署名証明書から公開鍵を使用してファイルを作成するには、次の手順を実行します。

- を実行します `openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip` インストーラパッケージの署名を確認します。

リポジトリの構成を確認する

Red Hat Enterprise Linux リポジトリまたは CentOS リポジトリを設定する手順はサイトによって異なります。を使用できます `pre_install_check.sh` インストールパッケージに含まれるスクリプトで、オペレーティングシステムの構成を確認します。システムがインターネットに接続されている場合は、Red Hat Enterprise Linux リポジトリまたは CentOS リポジトリのセットアップ手順が自動的に表示されます。

```
# sudo ./pre_install_check.sh
```

Unified Manager をインストールします

Unified Managerでは、を使用します `yum` ソフトウェアおよび依存ソフトウェアをインストールするユーティリティ。Red Hat Enterprise Linux または CentOS にはさまざまなイメージがインストールされるため、インストールするパッケージはイメージに含まれるソフトウェアによって異なります。。 `yum` インストールに使用する依存ソフトウェアパッケージは、ユーティリティによって決定されます。依存するソフトウェアパッケージの詳細については、を参照してください "[Linux ソフトウェアとインストールの要件](#)"。

Unified Managerをインストールするには、rootユーザとして、またはを使用して、次のコマンドを実行します `sudo` インストールファイルを解凍したディレクトリで、次の手順を実行します。

```
# yum install netapp-um<version>.x86_64.rpm
```

または

```
% sudo yum install netapp-um<version>.x86_64.rpm
```

インストールの完了時に、Unified Manager Web UI に接続するための情報が表示されます。Web UIに接続できない場合は、を参照してください `README` ポート443の制限の詳細については、ソフトウェアにパッケージ化されたファイルを参照してください。

Windows インストールのクイックスタート手順

インストールパッケージをダウンロードしてUnified Managerをインストールすることで、データストレージの容量、可用性、パフォーマンス、保護の問題を監視してトラブルシューティングすることができます。

システム要件

- オペレーティングシステム
 - Microsoft Windows Server 2019 Standard EditionおよびDatacenter Edition
 - Microsoft Windows Server 2022 Standard EditionおよびDatacenter Edition

Unified Manager は、以下の言語で 64 ビットの Windows オペレーティングシステムでサポートされ

ています。

- 英語
- 日本語
- 簡体字中国語

- RAM : 12GB
- CPU : 合計 9572MHz
- 空きディスクスペース: インストールディレクトリ用に 100GB、MySQL データディレクトリ用に 50GB のディスクスペースが必要です

システム要件の詳細については、を参照してください ["Unified Manager をインストールするための要件"](#) および ["互換性マトリックス"](#)。

Active IQ Unified Manager をインストールしています

インストーラをダウンロードします。

1. をダウンロードします ActiveIQUnifiedManager-<version>.exe インストールパッケージ:
2. インストールファイルをターゲットシステムのディレクトリにコピーします。

Unified Manager をインストールします

Unified Manager をインストールするには、Microsoft .NET 4.5.2 以降のバージョンがインストールされている必要があります。インストールプロセスの一環として、Unified Manager は必要に応じて他のサードパーティパッケージをインストールします。依存するソフトウェアパッケージの詳細については、を参照してください ["Windows ソフトウェアとインストールの要件"](#)。

1. デフォルトのローカル管理者アカウントで Windows にログインします。
2. インストールファイルをダウンロードしたディレクトリで、Unified Manager の実行ファイル（.exe ファイル）を右クリックし、管理者として実行します。
3. プロンプトが表示されたら、ユーザ名とパスワードを入力して Unified Manager のメンテナンスユーザを作成します。
4. データベース接続ウィザードで、MySQL の root パスワードを入力します。
5. 画面の指示に従ってインストールを完了します。
6. インストールの完了時に * Finish * をクリックすると、Unified Manager Web UI が表示されます。

VMware vSphere システムに Unified Manager をインストールします

Active IQ Unified Manager の概要

Active IQ Unified Manager（旧 OnCommand Unified Manager）を使用すると、ONTAP ストレージシステムの健全性とパフォーマンスを 1 つのインターフェイスから監視および管理できます。Unified Manager は、Linux サーバや Windows サーバに導入できるほか、VMware ホストに仮想アプライアンスとして導入することもできます。

インストールの完了後、管理対象のクラスタを追加すると、Unified Manager のグラフィカルインターフェイスに、監視対象ストレージシステムの容量、可用性、保護、パフォーマンスのステータスが表示されます。

- 関連情報 *

["NetApp Interoperability Matrix Tool で確認できます"](#)

Unified Manager サーバの機能

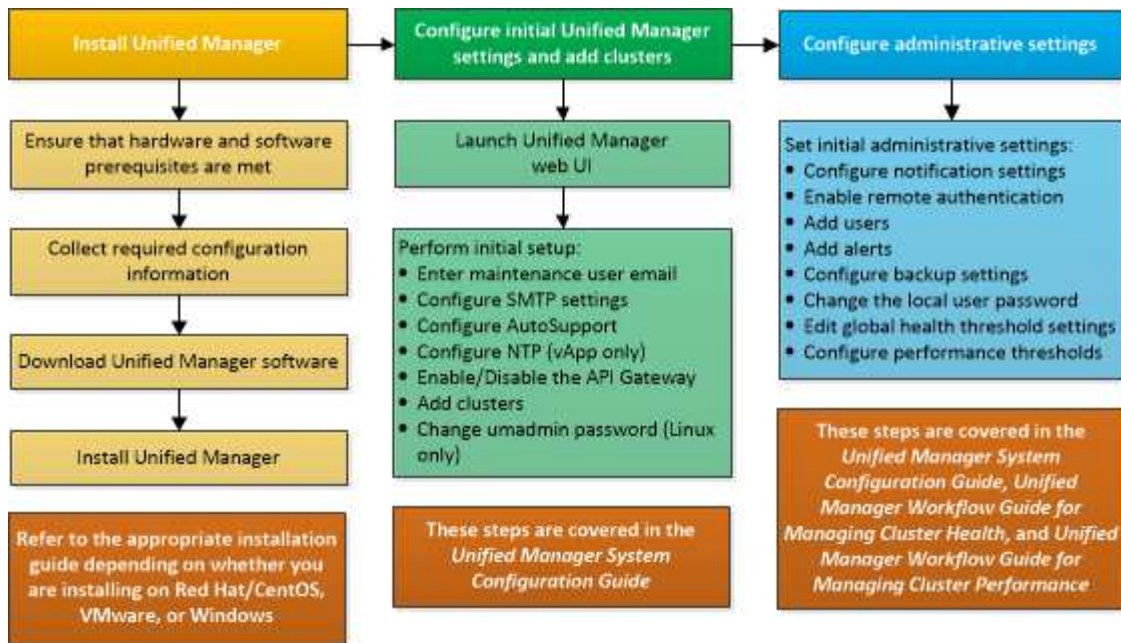
Unified Manager サーバインフラは、データ収集ユニット、データベース、アプリケーションサーバで構成され、検出、監視、ロールベースアクセス制御（RBAC）、監査、ロギングなどのインフラサービスを提供します。

Unified Manager は、クラスタの情報を収集してデータベースにデータを格納し、そのデータを分析してクラスタに問題がないかどうかを確認します。

インストール手順の概要

以下は、Unified Manager を使用する前に必要なインストール作業のワークフローです。

ここでは、次のワークフローに示されている各項目について説明します。



Unified Manager をインストールするための要件

インストールプロセスを開始する前に、Unified Manager をインストールするサーバがソフトウェア、ハードウェア、CPU、およびメモリの所定の要件を満たしていることを確認してください。

ネットアップは、Unified Manager アプリケーションコードの変更をサポートしていません。Unified Manager サーバにセキュリティ対策を適用する必要がある場合は、Unified Manager がインストールされているオペレーティングシステムに変更を加える必要があります。

Unified Manager サーバへのセキュリティ対策の適用の詳細については、ナレッジベースの記事を参照してください。

["Data ONTAP for clustered Active IQ Unified Manager に適用されるセキュリティ対策のサポート性"](#)

- 関連情報 *

詳細については、を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#)

仮想インフラおよびハードウェアシステムの要件

仮想インフラまたは物理システムに Unified Manager をインストールする場合、メモリ、CPU、およびディスクスペースの最小要件を満たす必要があります。

次の表に、メモリ、CPU、およびディスクスペースの各リソースについて、推奨される値を示します。これらは、Unified Manager が許容されるパフォーマンスレベルを達成することが確認されている値です。

ハードウェア構成	推奨設定
RAM	12GB （最小要件は 8GB ）

ハードウェア構成	推奨設定
プロセッサ	CPU × 4
CPU サイクル容量	合計 9572MHz（最小要件は 9572MHz）
空きディスク容量	<ul style="list-style-type: none"> • 5GB（シンプロビジョニング） • 152GB（シックプロビジョニング）

Unified Manager はメモリの少ないシステムにもインストールできますが、推奨される 12GB の RAM があれば最適なパフォーマンスが保証されるだけでなく、拡張時にクラスタやストレージオブジェクトの追加にも対応できます。Unified Manager を導入する VM にはメモリの上限などを設定しないでください。また、ソフトウェアがシステムで割り当てられているメモリを利用できなくなる機能（バレーニングなど）は有効にしないでください。

また、1 つの Unified Manager インスタンスで監視できるノードの数には上限があり、この上限を超える場合は 2 つ目の Unified Manager インスタンスをインストールする必要があります。詳細については、[を参照してください](#) **"Unified Manager ベストプラクティスガイド"**。

メモリページのスワッピングは、システムや管理アプリケーションのパフォーマンスに悪影響を及ぼします。CPU リソースがホスト全体で競合して使用できなくなると、パフォーマンスが低下する可能性があります。

専用使用の要件

Unified Manager をインストールする物理システムまたは仮想システムは、他のアプリケーションとは共有せず、Unified Manager 専用にする必要があります。他のアプリケーションにシステムリソースが消費されることで、Unified Manager のパフォーマンスが大幅に低下する可能性があります。

バックアップ用のスペース要件

Unified Manager のバックアップとリストア機能を使用する場合は、「data」ディレクトリまたはディスクに 150GB のスペースがあるように追加の容量を割り当ててください。バックアップはローカルにもリモートにも保存できますが、Unified Manager ホストシステムとは別の、150GB 以上のスペースがあるリモートの場所に保存することを推奨します。

ホスト接続の要件

Unified Manager をインストールする物理システムまたは仮想システムは、問題なく設定できるように設定する必要があります ping ホスト自体のホスト名です。IPv6 構成の場合は、確認する必要があります ping6 これで Unified Manager を正しくインストールできるようになります。

製品の Web UI には、ホスト名（またはホストの IP アドレス）を使用してアクセスできます。導入時に静的 IP アドレスを使用してネットワークを設定した場合は、指定したネットワークホストの名前を使用します。DHCP を使用してネットワークを設定した場合は、DNS からホスト名を取得します。

完全修飾ドメイン名（FQDN）または IP アドレスの代わりに短縮名を使用した Unified Manager へのアクセスをユーザに許可する場合は、短縮名が有効な FQDN に解決されるようにネットワークを設定する必要があります。

VMware ソフトウェアとインストールの要件

Unified Manager をインストールする VMware vSphere システムには、特定のバージョンのオペレーティングシステムとサポートソフトウェアが必要です。

オペレーティングシステムソフトウェア

サポートされる VMware ESXi のバージョンは次のとおりです。

- ESXi 6.5、6.7、および7.0.x



VMware vSphereシステム上のUnified Manager OVAは、内部でDebian OS 11 (bustle) を実行します。サポート対象のバージョンのESXiサーバでサポートされる仮想マシンハードウェアのバージョンについては、VMwareのドキュメントを参照してください。

サポートされる vSphere のバージョンは次のとおりです。

- VMware vCenter Server 6.5、6.7、および7.0.x

サポートされている ESXi のバージョンの最新のリストについては、Interoperability Matrix を参照してください。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

仮想アプライアンスが正しく動作するには、VMware ESXi サーバの時刻が NTP サーバの時刻と同じである必要があります。VMware ESXi サーバの時刻を NTP サーバの時刻と同期すると、時刻に関する障害は発生しなくなります。

インストールの要件

Unified Manager 仮想アプライアンスでは、VMware High Availability がサポートされます。

ONTAP ソフトウェアを実行しているストレージシステムに NFS データストアを導入する場合は、NetApp NFS Plug-in for VMware VAAI を使用してシックプロビジョニングを使用します。

リソースが十分でないために高可用性に対応した環境を使用して展開に失敗した場合は、仮想マシンの再起動優先度を無効にし、ホスト隔離時の対応をオンにしたままにすることで、クラスタ機能仮想マシンオプションを変更する必要があります。



Unified Manager のインストールまたはアップグレード時に、必要なサードパーティ製ソフトウェアおよびセキュリティパッチが VMware vSphere システムに自動的にインストールまたはアップグレードされます。これらのコンポーネントは Unified Manager のインストールプロセスとアップグレードプロセスで制御されるため、サードパーティコンポーネントのスタンドアロンインストールやアップグレードを実行しないでください。

サポートされているブラウザ

Unified Manager Web UI にアクセスするには、サポートされているブラウザを使用します。

サポートされているブラウザとバージョンは Interoperability Matrix で確認できます。

すべてのブラウザで、ポップアップブロックを無効にすることでソフトウェアの機能が正しく表示されます。

アイデンティティプロバイダ（IdP）でユーザを認証できるように Unified Manager で SAML 認証を設定する場合は、IdP でサポートされるブラウザのリストも確認してください。

プロトコルとポートの要件

このポートとプロトコルを使用して、Unified Manager サーバは管理対象のストレージシステム、サーバ、その他のコンポーネントと通信します。

Unified Manager サーバへの接続

通常的环境では、Unified Manager Web UI への接続に常にデフォルトのポートが使用されるため、ポート番号を指定する必要はありません。たとえば、Unified Managerは常にデフォルトのポートで実行されるため、と入力できます `https://<host>` ではなく `https://<host>:443`。

Unified Manager サーバでは、次のインターフェイスにアクセスする際に特定のプロトコルを使用します。

インターフェイス	プロトコル	ポート	説明
Unified Manager Web UI	HTTP	80	Unified Manager Web UI へのアクセスに使用され、自動的にセキュアポート 443 にリダイレクトされます。
Unified Manager Web UI および API を使用するプログラム	HTTPS	443	Unified Manager Web UI へのセキュアなアクセスと API 呼び出しに使用されます。API 呼び出しは HTTPS でしか実行できません。
メンテナンスコンソール	SSH/SFTP	22	メンテナンスコンソールにアクセスしてサポートバンドルを取得する際に使用されます。
Linux コマンドライン	SSH/SFTP	22	Red Hat Enterprise Linux または CentOS のコマンドラインにアクセスしてサポートバンドルを取得する際に使用されます。

インターフェイス	プロトコル	ポート	説明
syslog	UDP	514	ONTAP システムからのサブスクリプションベースの EMS メッセージにアクセスし、メッセージに基づいてイベントを作成する際に使用されます。
REST	HTTPS	ポート 1	認証された ONTAP システムからの REST API ベースのリアルタイムの EMS イベントにアクセスする際に使用されます。



MySQL のデフォルトのポート 3306 は、VMware vSphere システムに Unified Manager をインストールする際に localhost にのみ使用できます。これは、前の構成を維持したままのアップグレードシナリオには影響しません。この設定は変更可能で、を使用して他のホストから接続を利用できるようにすることができます Control access to MySQL port 3306 メンテナンスコンソールのオプション。詳細については、を参照してください ["その他のメニューオプション"](#)。HTTP 通信と HTTPS 通信に使用されるポート（ポート 80 と 443）は、Unified Manager メンテナンスコンソールを使用して変更できます。詳細については、を参照してください ["メンテナンスコンソールのメニュー"](#)。

Unified Manager サーバからの接続

ファイアウォールの設定で、Unified Manager サーバと管理対象のストレージシステム、サーバ、その他のコンポーネントの間の通信に使用するポートを開くように設定する必要があります。ポートが開いていない場合、通信は失敗します。

環境に応じて、Unified Manager サーバから特定の接続先への接続に使用するポートとプロトコルを変更することもできます。

Unified Manager サーバは、次のプロトコルとポートを使用して、管理対象のストレージシステム、サーバ、その他のコンポーネントに接続します。

宛先	プロトコル	ポート	説明
ストレージシステム	HTTPS	443 tcp	<p>ストレージシステムの監視と管理に使用されます。</p> <div>  <p>このポートや他のポートを使用して VMware vCenter Server または ESXi サーバに接続する場合は、そのポートが使用可能で、保護されたサイトで接続可能であることを確認してください。</p> </div>
ストレージシステム	NDMP	10000 TCP	特定の Snapshot リストア処理に使用されます。
AutoSupport サーバ	HTTPS	443	AutoSupport 情報の送信に使用されます。この機能を実行するには、インターネットアクセスが必要です。
認証サーバ	LDAP	389	認証要求、およびユーザとグループの検索要求に使用されます。
LDAPS	636	セキュアな LDAP 通信に使用されます。	メールサーバ
SMTP	25	アラート通知 E メールを送信に使用されます。	SNMP トラップの送信元
SNMPv1 または SNMPv3	162 UDP	アラート通知 SNMP トラップの送信に使用されます	外部データプロバイダのサーバ

宛先	プロトコル	ポート	説明
TCP	2003 年	Graphite などの外部データプロバイダにパフォーマンスデータを送信します。	NTP サーバ

ワークシートへの記入

Unified Manager をインストールして設定する前に、環境に関する特定の情報を確認しておく必要があります。この情報はワークシートに記録できます。

Unified Manager のインストール情報

Unified Manager をインストールする際に必要な情報を記入します。

ソフトウェアが導入されているシステム	あなたの価値
ESXi サーバの IP アドレス	
ホストの完全修飾ドメイン名	
ホストの IP アドレス	
ネットワークマスク	
ゲートウェイの IP アドレス	
プライマリ DNS アドレス	
セカンダリ DNS アドレス	
検索ドメイン	
メンテナンスユーザのユーザ名	
メンテナンスユーザのパスワード	

Unified Manager の設定情報

インストール後に Unified Manager を設定するための情報を記入します。設定によっては省略可能な値もあります。

設定	あなたの価値
メンテナンスユーザの E メールアドレス	
NTP サーバ	
SMTP サーバのホスト名または IP アドレス	
SMTP ユーザ名	
SMTP パスワード	
SMTP ポート	25 (デフォルト値)
アラート通知の送信元 E メールアドレス	
認証サーバのホスト名または IP アドレス	
Active Directory の管理者名または LDAP のバインド識別名	
Active Directory のパスワードまたは LDAP のバインドパスワード	
認証サーバのベース識別名	
アイデンティティプロバイダ (IdP) の URL	
アイデンティティプロバイダ (IdP) のメタデータ	
SNMP トラップの送信先ホストの IP アドレス	
SNMP ポート	

クラスタ情報

Unified Manager を使用して管理するストレージシステムの情報を記入します。

クラスタ 1 / N	あなたの価値
ホスト名またはクラスタ管理 IP アドレス	

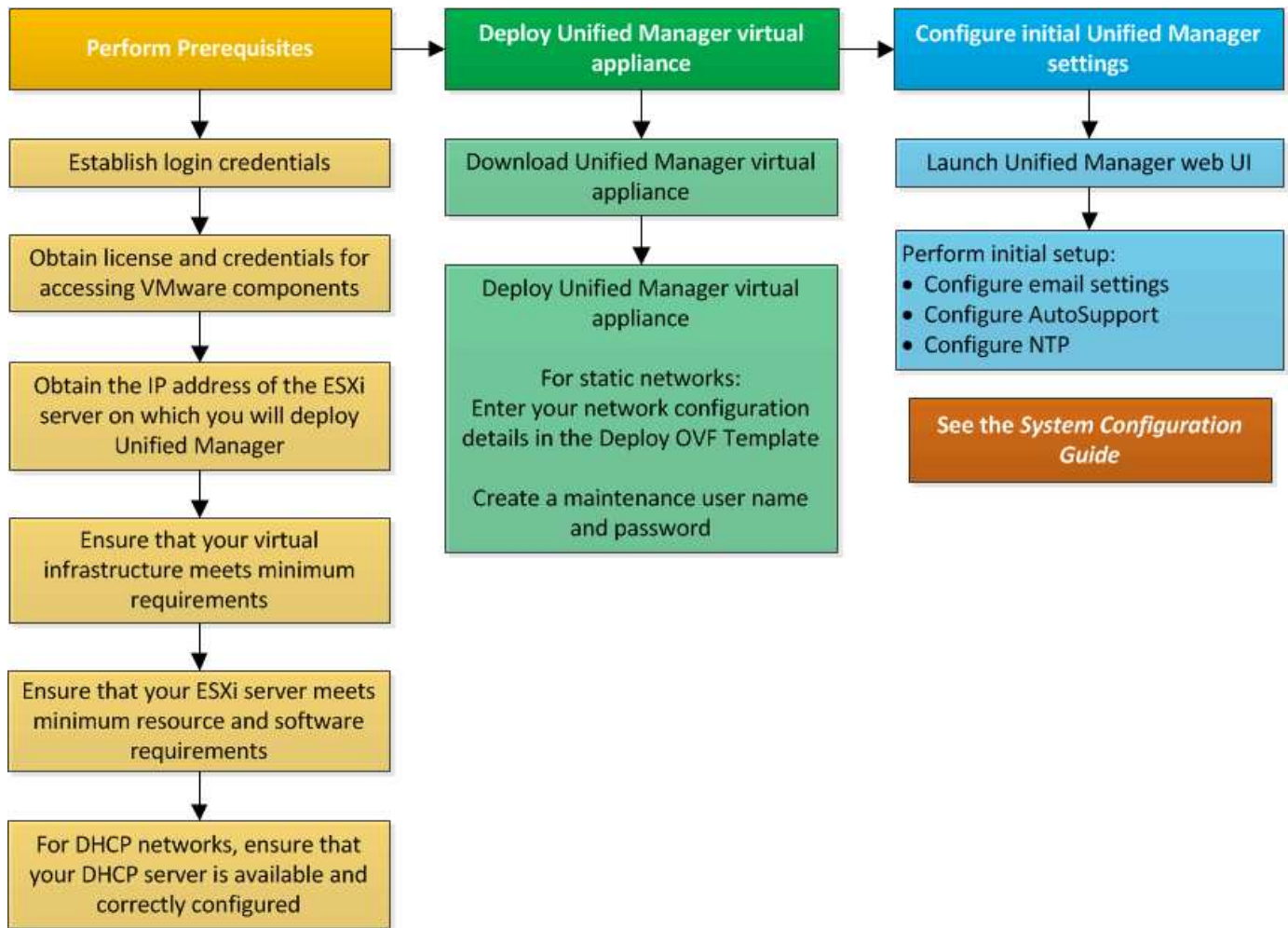
クラスタ 1 / N	あなたの価値
ONTAP 管理者のユーザ名 <div>  管理者には「admin」ロールが割り当てられている必要があります。 </div>	
ONTAP 管理者のパスワード	
プロトコル	HTTPS

Unified Manager ソフトウェアのインストール、アップグレード、削除を行います

VMware vSphereシステムで、Unified Managerのインストール、新しいバージョンへのアップグレード、またはUnified Manager仮想アプライアンス（vApp）の削除を実行できます。

導入プロセスの概要

以下は、Unified Manager を使用する前に必要な導入作業のワークフローです。



Unified Manager を導入します

Unified Manager を導入するには、ソフトウェアをダウンロードし、仮想アプライアンスを導入し、メンテナンスユーザを作成してユーザ名とパスワードを設定し、Web UI で初期セットアップを行います。

- 必要なもの *
- 導入に必要なシステム要件を確認し、満たしておく必要があります。

を参照してください "[システム要件](#)".

- 次の情報があることを確認します。
 - NetApp Support Siteのログインクレデンシャル
 - VMware vCenter Server および vSphere Web Client にアクセスするためのクレデンシャル
 - Unified Manager 仮想アプライアンスを導入する ESXi サーバの IP アドレス
 - データストアのストレージスペースやメモリ要件など、データセンターに関する詳細情報
 - IPv6 アドレスを使用する場合は、ホストで IPv6 が有効になっている必要があります。

Unified Manager は、VMware ESXi サーバに仮想アプライアンスとして導入できます。

メンテナンスコンソールには、SSH ではなく、VMware コンソールを使用してアクセスする必要があります。



Unified Manager 9.8以降では、VMware ToolsがOpen VM Toolsに置き換えられています (open-vm-tools)。VMware Toolsをインストールの一部としてインストールする必要がなくなりました。理由は、open-vm-tools は、Unified Managerインストールパッケージに含まれています。

導入と初期セットアップが完了したら、クラスタを追加するかメンテナンスコンソールで追加のネットワーク設定を行ってから、Web UI にアクセスできます。

手順

1. の手順に従います **"Unified Manager をダウンロードします"**。
2. また、の手順も実行します **"Unified Manager 仮想アプライアンスを導入します"**。

Unified Manager インストールファイルをダウンロードします

Unified Manager のインストールファイルをNetApp Support Siteからダウンロードして、Unified Manager を仮想アプライアンスとして導入します。

- 必要なもの *

NetApp Support Siteのログインクレデンシャルが必要です。

インストールファイルは、.tar ルート証明書を含むファイル、README ファイル、および OVA 仮想アプライアンス用に設定されたUnified Managerソフトウェアを含むファイル。

手順

1. NetApp Support Siteにログインし、Unified Manager のダウンロードページに移動します。

"NetApp Support Site"

2. 必要なバージョンの Unified Manager を選択し、エンドユーザライセンス契約（EULA）に同意します。
3. をダウンロードして保存します .tar File for VMware vSphereをインストールし、vSphere Clientからアクセス可能なローカルまたはネットワークのディレクトリにインストールします。
4. チェックサムを確認して、ソフトウェアが正しくダウンロードされたことを確認します。
5. をダウンロードしたディレクトリに移動します .tar ファイルを展開し、ターミナルウィンドウで次のコマンドを入力してUnified Managerのバンドルを展開します。

```
tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz
```

が必要です OVA ファイル、ルート証明書、および README Unified Managerのファイルがターゲットディレクトリに解凍されます。

6. の整合性を確認します OVA で説明した手順に従ってファイルを作成します README ファイル。

Unified Manager 仮想アプライアンスの導入

インストールファイルをダウンロードしたら、Unified Manager を仮想アプライアンスとして導入します。vSphere Web Client を使用して、ESXi サーバに仮想アプライアンスを導入します。仮想アプライアンスを導入すると、仮想マシンが作成されます。

- 必要なもの *

システム要件を確認しておく必要があります。Unified Manager仮想アプライアンスを導入する前に、必要な変更を行ってください。

を参照してください ["仮想インフラの要件"](#)。

を参照してください ["VMware ソフトウェアとインストールの要件"](#)。

Dynamic Host Configuration Protocol (DHCP ; 動的ホスト構成プロトコル) を使用する場合は、DHCP サーバが使用可能であり、DHCP と仮想マシン (VM) のネットワークアダプタの設定が正しいことを確認してください。DHCP はデフォルトで設定されています。

静的ネットワーク設定を使用する場合は、IP アドレスが同じサブネット内で重複していないこと、および適切な DNS サーバエントリが設定されていることを確認してください。

仮想アプライアンスを導入する前に、次の情報を入手します。

- VMware vCenter Server および vSphere Web Client にアクセスするためのクレデンシャル
- Unified Manager 仮想アプライアンスを導入する ESXi サーバの IP アドレス
- ストレージスペースの可用性など、データセンターに関する詳細
- DHCP を使用しない場合は、接続するネットワークデバイスの IPv4 または IPv6 アドレスを取得します。
 - ホストの完全修飾ドメイン名 (FQDN)
 - ホストの IP アドレス
 - ネットワークマスク
 - デフォルトゲートウェイの IP アドレス
 - プライマリおよびセカンダリ DNS アドレス
 - 検索ドメイン

Unified Manager 9.8以降では、VMware ToolsがOpen VM Toolsに置き換えられています *open-vm-tools*)。では、インストールプロセスの一環としてVMware Toolsをインストールする必要はありません *open-vm-tools* は、Unified Managerインストールパッケージに含まれています。

仮想アプライアンスを導入すると、HTTPS アクセス用に一意の自己署名証明書が生成されます。Unified Manager Web UI にアクセスする際に、信頼された証明書でないことを示す警告がブラウザに表示されることがあります。

Unified Manager 仮想アプライアンスでは、VMware High Availability がサポートされます。

手順

1. vSphere Client で、* File * > * Deploy OVF Template * をクリックします。

2. Deploy OVF Template ウィザードを実行して、Unified Manager 仮想アプライアンスを導入します。

[詳細の確認]ページで次の操作を行います

- Publisherセクションの詳細を確認します。メッセージ* Entrust Code Signing - OVCS2 (Trusted certificate)*は、ダウンロードされたの整合性を確認します OVA ファイル。+ 「Entrust Code Signing - OVCS2 (Invalid certificate) 」というメッセージが表示された場合は、VMware vCenter Server を7.0U3E以降のバージョンにアップグレードします。

[テンプレートのカスタマイズ]ページで、次の手順を実行

- DHCP と IPv4 アドレスを使用する場合は、すべてのフィールドを空白のままにします。
 - DHCP と IPv6 アドレスを使用する場合は '[Enable Auto IPv6 addressing] チェックボックスをオンにし' その他のフィールドはすべて空白のままにします
 - 静的なネットワーク設定を使用する場合は、このページのフィールドに値を入力します。これらの設定は導入時に適用されます。IP アドレスは、導入先のホストで一意であること、使用されていないこと、および有効な DNS エントリがあることを確認してください。
3. Unified Manager 仮想アプライアンスを ESXi サーバに導入したら、VM を右クリックして電源をオンにし、* 電源オン * を選択します。



リソースが十分でないために電源投入に失敗した場合は、リソースを追加してからインストールを再試行してください。

4. [* コンソール *] タブをクリックします。

初回ブートプロセスが完了するまでに数分かかります。

5. タイムゾーンを設定するには、VM コンソールウィンドウに表示される指示に従って、地理的な地域と都市または地域を入力します。

表示されるすべての日付情報には、管理対象デバイスのタイムゾーンの設定に関係なく、Unified Manager 用に設定されているタイムゾーンが使用されます。ストレージシステムと管理サーバで同じ NTP サーバが設定されている場合、違う時間が表示された場合でも、それぞれが表しているのは同じ時刻です。たとえば、管理サーバとは異なるタイムゾーンが設定されたデバイスを使用して Snapshot コピーを作成する場合、タイムスタンプは管理サーバの時間になります。

6. 使用可能な DHCP サービスがない場合や静的なネットワーク設定でエラーが発生した場合は、次のいずれかのオプションを選択します。

を使用する場合	操作
DHCP	<p>[DHCP の再試行 *] を選択します。DHCP を使用する場合は、正しく設定されていることを確認してください。</p> <p>DHCP 対応のネットワークを使用すると、FQDN と DNS サーバのエントリが仮想アプライアンスに自動的に割り当てられます。DHCP に DNS が適切に設定されていないと、ホスト名「UnifiedManager」が自動的に割り当てられ、セキュリティ証明書に関連付けられます。DHCP 対応のネットワークをセットアップしていない場合は、ネットワーク設定情報を手動で入力する必要があります。</p>
静的なネットワーク設定	<p>a. 「* Enter the details for static network configuration *」を選択します。</p> <p>設定プロセスが完了するまでに数分かかります。</p> <p>b. 入力した値を確認し、* Y * を選択します。</p>

7. プロンプトでメンテナンスユーザの名前を入力し、* Enter * をクリックします。

メンテナンスユーザの名前は、a~z のアルファベットのあとに、a~z または 0~9 の任意の組み合わせを使用してください。

8. プロンプトでパスワードを入力し、* Enter * をクリックします。

VM コンソールに Unified Manager Web UI の URL が表示されます。

Web UI にアクセスして Unified Manager の初期セットアップを実行できます。手順については、を参照してください ["Active IQ Unified Manager を設定しています"](#)。

Unified Manager をアップグレードする

リリース9.10または9.11からリリース9.12へのActive IQ Unified Manager のアップグレードのみが可能です。

アップグレードプロセスの実行中は、Unified Manager を使用できなくなります。実行中の処理がある場合は、Unified Manager をアップグレードする前に完了しておいてください

Unified Manager を OnCommand Workflow Automation のインスタンスとペアにして使用している環境では、両方の製品のソフトウェアで新しいバージョンを利用できる場合、2つの製品間の接続を解除してから各製品をアップグレードし、アップグレードの実行後に Workflow Automation の接続を新たにセットアップする必要があります。いずれかの製品のみをアップグレードする場合は、アップグレード後に Workflow Automation にログインし、Unified Manager からデータを取得していることを確認します。

手順

1. の手順に従います ["Unified Manager の ISO イメージをダウンロードします"](#)。
2. さらに、に記載されている手順に従います ["Unified Manager をアップグレードします"](#)。

Unified Managerバージョンでサポートされているアップグレードパス

Active IQ Unified Manager では、バージョンごとに特定のアップグレードパスがサポートされます。

すべてのバージョンのUnified Managerで、新しいバージョンへのインプレースアップグレードを実行できるわけではありません。Unified ManagerのアップグレードはN-2モデルに限定されています。つまり、アップグレードはすべてのプラットフォームの次の2つのリリースでのみ実行できます。たとえば、Unified Manager 9.10からUnified Manager 9.12へのアップグレードは、Unified Manager 9.11からのみ実行できます。

サポート対象よりも前のバージョンを実行している場合は、Unified Managerインスタンスをいずれかのサポート対象バージョンにアップグレードしてから、現在のバージョンにアップグレードする必要があります。

たとえば、インストールされているバージョンがOnCommand Unified Manager 9.5であり、最新のリリースActive IQ Unified Manager 9.12にアップグレードする場合は、一連のアップグレードを実行します。

アップグレードパスの例：

1. OnCommand Unified Manager 9.5 → Active IQ Unified Manager 9.7をアップグレードします。
2. 9.7→9.9にアップグレードします。
3. 9.→ 9.11にアップグレードします。
4. 9.11 → 9.12にアップグレードします。

アップグレードパスマトリックスの詳細については、こちらを参照してください ["ナレッジベース \(KB\) の記事を参照してください"](#)。

Unified Manager のアップグレードファイルをダウンロードしています

Unified Manager をアップグレードする前に、 Unified Manager のアップグレードファイルをNetApp Support Siteからダウンロードします。

- 必要なもの *

NetApp Support Siteのログインクレデンシャルが必要です。

手順

1. NetApp Support Siteにログインします。

["NetApp Support Site"](#)

2. VMware vSphere での Unified Manager のアップグレードのダウンロードページに移動します。
3. をダウンロードします .iso イメージをアップグレードし、vSphere Clientからアクセス可能なローカルまたはネットワークのディレクトリに保存します。
4. チェックサムを確認して、ソフトウェアが正しくダウンロードされたことを確認します。

Unified Manager 仮想アプライアンスをアップグレードします

Active IQ Unified Manager 仮想アプライアンスは、リリース9.10または9.11から9.12にアップグレードできます。

- 必要なもの *

次の点を確認します。

- NetApp Support Siteから ISO イメージのアップグレードファイルをダウンロードしておきます。
- Unified Manager をアップグレードするシステムがシステム要件とソフトウェア要件を満たしている必要があります。

を参照してください ["仮想インフラの要件"](#)。

を参照してください ["VMware ソフトウェアとインストールの要件"](#)。

- vSphere 6.5 以降を使用している場合は、VMware Remote Console（VMRC）をインストールしておきます。
- アップグレードの実行中に、パフォーマンスデータの保持期間について、以前のデフォルト設定である 13 カ月のままにするか 6 カ月に変更するかを確認するプロンプトが表示されることがあります。変更を確認すると、6 カ月を過ぎた過去のパフォーマンスデータはパージされます。
- 次の情報が必要です。
 - NetApp Support Siteのログインクレデンシャル
 - VMware vCenter Server および vSphere Web Client にアクセスするためのクレデンシャル
 - Unified Manager のメンテナンスユーザのクレデンシャル

アップグレードプロセスの実行中は、Unified Manager を使用できなくなります。実行中の処理がある場合は、Unified Manager をアップグレードする前に完了しておいてください

Workflow Automation と Unified Manager を連携させて使用している場合、Workflow Automation でホスト名を手動で更新する必要があります。

手順

1. vSphere Client で、* Home * > * Inventory * > * VMs and Templates * をクリックします。
2. Unified Manager 仮想アプライアンスがインストールされている仮想マシン（VM）を選択します。
3. Unified Manager VM が実行されている場合は、「* 概要 * > * コマンド * > * ゲストのシャットダウン *」に移動します。
4. アプリケーションと整合性のあるバックアップを作成するために、Unified Manager VM の Snapshot や クローンなどのバックアップコピーを作成します。
5. vSphere Client で、Unified Manager VM の電源をオンにします。
6. VMware Remote Console を起動します。
7. [* CDROM *] アイコンをクリックし、[* ディスクイメージファイル (.ISO)* に接続] を選択します。
8. を選択します ActiveIQUnifiedManager-<version>-virtual-update.iso [ファイル]をクリックし、[開く]をクリックします。

9. [* コンソール *] タブをクリックします。
10. Unified Manager メンテナンスコンソールにログインします。
11. メインメニューで、* アップグレード * を選択します。

アップグレードプロセスの実行中は Unified Manager を使用できなくなり、完了後に再開されることを示すメッセージが表示されます。

12. を入力します y 続行します。

仮想アプライアンスが配置されている仮想マシンをバックアップするように通知する警告が表示されます。

13. を入力します y 続行します。

アップグレードプロセスが完了して Unified Manager サービスが再起動されるまでに数分かかることがあります。

14. 任意のキーを押して続行します。

メンテナンスコンソールから自動的にログアウトされます。

15. * オプション：メンテナンスコンソールにログインし、Unified Manager のバージョンを確認します。

サポートされているWebブラウザの新しいウィンドウでWeb UIを起動し、ログインしてアップグレード後のバージョンのUnified Managerを使用できます。検出プロセスが完了するのを待ってから、UIでの作業を実行する必要があります。

Unified Manager 仮想マシンを再起動しています

Unified Manager 仮想マシン（VM）をメンテナンスコンソールから再起動することができます。新しいセキュリティ証明書を生成した場合や VM で問題が発生した場合、VM を再起動する必要があります。

- 必要なもの *
- 仮想アプライアンスの電源をオンにします。
- Unified Manager メンテナンスコンソールにメンテナンスユーザとしてログインする必要があります。

VMware * Restart Guest * オプションを使用して、vSphere から仮想マシンを再起動することもできます。

手順

1. メンテナンスコンソールで、* システム構成 * > * 仮想マシンの再起動 * を選択します。
2. ブラウザから Unified Manager Web UI を起動し、ログインします。
 - 関連情報 *

["VMware vSphere PowerCLI Cmdlets Reference : Restart-VMGuest"](#)

Unified Manager を削除しています

Unified Manager をアンインストールするには、Unified Manager ソフトウェアがインストールされている仮想マシン（VM）を削除します。

- 必要なもの *
- VMware vCenter Server と vSphere Web Client にアクセスするためのクレデンシャルが必要です。
- Unified Manager サーバから Workflow Automation サーバへのアクティブな接続をすべて終了しておく必要があります。
- 仮想マシン（VM）を削除する前に、Unified Manager サーバからすべてのクラスタ（データソース）を削除しておく必要があります。

手順

1. Unified Manager メンテナンスコンソールを使用して、Unified Manager サーバから外部のデータプロバイダへのアクティブな接続がないことを確認します。
2. vSphere Client で、* Home * > * Inventory * > * VMs and Templates * をクリックします。
3. 削除する VM を選択し、* Summary * タブをクリックします。
4. VM が実行中の場合は、**Power**>* ゲストのシャットダウン * をクリックします。
5. 削除する VM を右クリックし、* ディスクから削除 * をクリックします。

Linux システムに Unified Manager をインストールします

Active IQ Unified Manager の概要

Active IQ Unified Manager（旧 OnCommand Unified Manager）を使用すると、ONTAP ストレージシステムの健全性とパフォーマンスを 1 つのインターフェイスから監視および管理できます。Unified Managerは、LinuxサーバやWindowsサーバに導入できるほか、VMwareホストに仮想アプライアンス（vApp）として導入することもできます。

インストールの完了後、管理対象のクラスタを追加すると、Unified Manager のグラフィカルインターフェイスに、監視対象ストレージシステムの容量、可用性、保護、パフォーマンスのステータスが表示されます。

- 関連情報 *

["NetApp Interoperability Matrix Tool で確認できます"](#)

Unified Manager サーバの機能

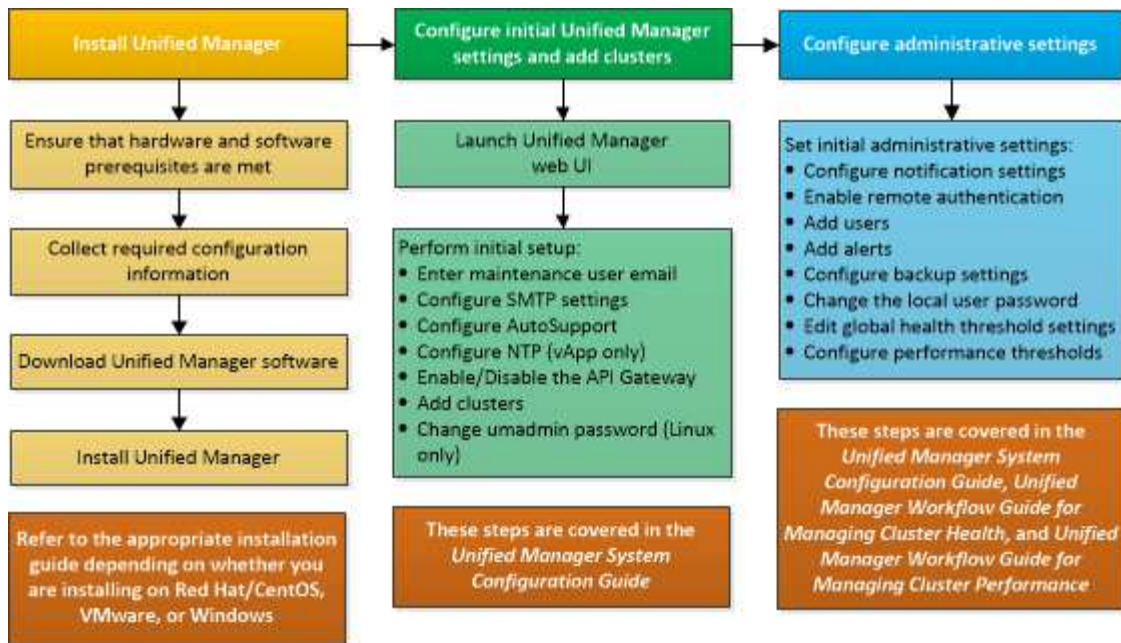
Unified Manager サーバインフラは、データ収集ユニット、データベース、アプリケーションサーバで構成され、検出、監視、ロールベースアクセス制御（RBAC）、監査、ロギングなどのインフラサービスを提供します。

Unified Manager は、クラスタの情報を収集してデータベースにデータを格納し、そのデータを分析してクラスタに問題がないかどうかを確認します。

インストール手順の概要

以下は、Unified Manager を使用する前に必要なインストール作業のワークフローです。

ここでは、次のワークフローに示されている各項目について説明します。



Unified Manager をインストールするための要件

インストールプロセスを開始する前に、Unified Manager をインストールするサーバがソフトウェア、ハードウェア、CPU、およびメモリの所定の要件を満たしていることを確認してください。

ネットアップは、Unified Manager アプリケーションコードの変更をサポートしていません。Unified Manager サーバにセキュリティ対策を適用する必要がある場合は、Unified Manager がインストールされているオペレーティングシステムに変更を加える必要があります。

Unified Manager サーバへのセキュリティ対策の適用の詳細については、ナレッジベースの記事を参照してください。

["Data ONTAP for clustered Active IQ Unified Manager に適用されるセキュリティ対策のサポート性"](#)

- 関連情報 *

["NetApp Interoperability Matrix Tool で確認できます"](#)

仮想インフラおよびハードウェアシステムの要件

仮想インフラまたは物理システムに Unified Manager をインストールする場合、メモリ、CPU、およびディスクスペースの最小要件を満たす必要があります。

次の表に、メモリ、CPU、およびディスクスペースの各リソースについて、推奨される値を示します。これらは、Unified Manager が許容されるパフォーマンスレベルを達成することが確認されている値です。

ハードウェア構成	推奨設定
RAM	12GB （最小要件は 8GB ）

ハードウェア構成	推奨設定
プロセッサ	CPU × 4
CPU サイクル容量	合計 9572MHz（最小要件は 9572MHz）
空きディスク容量	<p>150GB。割り当ては次のとおりです。</p> <ul style="list-style-type: none"> • 50GB をルートパーティションに割り当て • に100GBの空きディスクスペースが割り当てられている /opt/netapp/data ディレクトリ。LVM ドライブまたはターゲットシステムに接続された別のローカルディスクにマウントされます <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> 別途マウントする必要があります /opt および /var/log ディレクトリに移動する場合は、を確認します /opt には15GB /var/log に16GBの空きスペースがある。。 /tmp ディレクトリには10GB以上の空きスペースが必要です。</p> </div>

Unified Manager はメモリの少ないシステムにもインストールできますが、推奨される 12GB の RAM があれば最適なパフォーマンスが保証されるだけでなく、拡張時にクラスタやストレージオブジェクトの追加にも対応できます。Unified Manager を導入する VM にはメモリの上限などを設定しないでください。また、ソフトウェアがシステムで割り当てられているメモリを利用できなくなる機能（バレーニングなど）は有効にしないでください。

また、1 つの Unified Manager インスタンスで監視できるノードの数には上限があり、この上限を超える場合は 2 つ目の Unified Manager インスタンスをインストールする必要があります。詳細については、_ ベストプラクティスガイド _ を参照してください。

"テクニカルレポート 4621 : 『 Unified Manager Best Practices Guide 』 "

メモリページのスワッピングは、システムや管理アプリケーションのパフォーマンスに悪影響を及ぼします。CPU リソースがホスト全体で競合して使用できなくなると、パフォーマンスが低下する可能性があります。

専用使用の要件

Unified Manager をインストールする物理システムまたは仮想システムは、他のアプリケーションとは共有せず、Unified Manager 専用にする必要があります。他のアプリケーションにシステムリソースが消費されることで、Unified Manager のパフォーマンスが大幅に低下する可能性があります。

バックアップ用のスペース要件

Unified Manager のバックアップとリストア機能を使用する場合は、「data」ディレクトリまたはディスクに 150GB のスペースがあるように追加の容量を割り当ててください。バックアップはローカルにもリモートにも保存できますが、Unified Manager ホストシステムとは別の、150GB 以上のスペースがあるリモートの場所に保存することを推奨します。

ホスト接続の要件

Unified Managerをインストールする物理システムまたは仮想システムは、問題なく設定できるように設定する必要があります ping ホスト自体のホスト名です。IPv6構成の場合は、確認する必要があります ping6 これでUnified Managerを正しくインストールできるようになります。

製品の Web UI には、ホスト名（またはホストの IP アドレス）を使用してアクセスできます。導入時に静的 IP アドレスを使用してネットワークを設定した場合は、指定したネットワークホストの名前を使用します。DHCP を使用してネットワークを設定した場合は、DNS からホスト名を取得します。

完全修飾ドメイン名（FQDN）または IP アドレスの代わりに短縮名を使用した Unified Manager へのアクセスをユーザに許可する場合は、短縮名が有効な FQDN に解決されるようにネットワークを設定する必要があります。

Linux ソフトウェアとインストールの要件

Unified Manager をインストールする Linux システムには、特定のバージョンのオペレーティングシステムとサポートソフトウェアが必要です。

オペレーティングシステムソフトウェア

Linux システムに、次のバージョンのオペレーティングシステムとサポートソフトウェアがインストールされている必要があります。

- Red Hat Enterprise Linuxバージョン7.xおよび8.0から8.6（x86_64アーキテクチャに基づく）
- x86_64アーキテクチャに基づくCentOSバージョン7.x。CentOS ストリームはサポートされていません。

サポートされている Red Hat Enterprise Linux および CentOS のバージョンの最新のリストについては、Interoperability Matrix を参照してください。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

サードパーティ製ソフトウェア

Unified Manager は WildFly Web サーバに導入されます。WildFly 19.0.0 が Unified Manager にバンドルされて構成されています。

次のサードパーティパッケージが必要ですが、Unified Manager には含まれていません。これらのパッケージは、によって自動的にインストールされます yum 以降のセクションで説明するようにリポジトリを設定済みの場合は、インストール時にインストーラを実行します。

- MySQL Community Editionバージョン8.0.30（MySQLリポジトリから入手）。
- OpenJDKバージョン11.0.17（Red Hat Extra Enterprise Linux Serverリポジトリから入手）
- Python 3.6.x
- p7zip バージョン 16.02 以降（Red Hat Extra Packages for Enterprise Linux リポジトリから入手）



サードパーティ製ソフトウェアをアップグレードする前に、Unified Manager の実行中のインスタンスをシャットダウンする必要があります。サードパーティ製ソフトウェアのインストールが完了したら、Unified Manager を再起動できます。

ユーザ認証の要件

LinuxシステムへのUnified Managerのインストールは、rootユーザに加え、を使用してroot以外のユーザも実行できます `sudo` コマンドを実行します

インストールの要件

Red Hat Enterprise Linux または CentOS とその関連リポジトリをシステムにインストールする際のベストプラクティスは次のとおりです。別の方法でインストールまたは設定されたシステム、またはオフプレミス（クラウド）に導入されたシステムでは、追加の手順が必要になる場合があります。また、Unified Manager が適切に実行されない可能性があります。

- Red Hat のベストプラクティスに従って Red Hat Enterprise Linux または CentOS をインストールし、次のデフォルトのオプションを選択する必要があります。デフォルトのオプションでは、「GUI を使用するサーバ」ベース環境を選択します。
- Red Hat Enterprise Linux または CentOS への Unified Manager のインストール中にインストールプログラムが必要なすべてのソフトウェアにアクセスしてインストールできるように、システムには該当するリポジトリへのアクセスが必要です。
- をクリックします `yum` インストーラによるRed Hat Enterprise Linuxリポジトリで依存するソフトウェアの検索では、Red Hat Enterprise Linuxのインストール中またはインストール後に有効なRed Hatサブスクリプションを使用してシステムを登録しておく必要があります。

Red Hat Subscription Manager については、Red Hat のドキュメントを参照してください。

- 必要なサードパーティユーティリティがシステムに正しくインストールされるように、Extra Packages for Enterprise Linux （EPEL）リポジトリを有効にする必要があります。

システムで EPEL リポジトリが設定されていない場合は、リポジトリを手動でダウンロードして設定する必要があります。

を参照してください ["EPEL リポジトリを手動で設定します"](#)。

- 正しいバージョンの MySQL がインストールされていない場合は、システムに MySQL ソフトウェアが正しくインストールされるように MySQL リポジトリを有効にする必要があります。

システムで MySQL リポジトリが設定されていない場合は、リポジトリを手動でダウンロードして設定する必要があります。

を参照してください ["MySQL リポジトリを手動で設定する"](#)。

システムがインターネットにアクセスできず、インターネットに接続されたシステムからリポジトリがミラーリングされていない場合は、インストール手順に従ってシステムに必要な外部ソフトウェアを確認してください。必要なソフトウェアをインターネットに接続されたシステムにダウンロードして、をコピーします `.rpm` ファイルを、Unified Managerをインストールするシステムにインストールします。アーティファクトとパッケージをダウンロードするには、を使用する必要があります `yum install` コマンドを実行します2つのシステムで同じバージョンのオペレーティングシステムを実行していること、および該当する Red Hat Enterprise Linux バージョンまたは CentOS バージョンのサブスクリプションライセンスがあることを確認してください。



必要なサードパーティ製ソフトウェアは、ここに記載されたりリポジトリ以外からはインストールしないでください。Red Hat リポジトリからインストールされるソフトウェアは、Red Hat Enterprise Linux 用に特別に設計されたものであり、Red Hat のベストプラクティス（ディレクトリのレイアウトや権限など）に準拠しています。他の場所から入手したソフトウェアは必ずしもこれらのガイドラインに従っていないため、原因 Unified Manager のインストールに失敗したり、将来のアップグレードで原因の問題が発生したりする可能性があります。

ポート 443 の要件

Red Hat Enterprise Linux および CentOS の汎用イメージは、ポート 443 への外部アクセスをブロックする場合があります。そのため、Unified Manager のインストール後に管理者 Web UI に接続できなくなることがあります。次のコマンドを実行すると、汎用の Red Hat Enterprise Linux または CentOS システムのすべての外部ユーザとアプリケーションがポート 443 にアクセスできるようになります。

```
# firewall-cmd --zone=public --add-port=443/tcp --permanent; firewall-cmd --reload
```

Red Hat Enterprise Linux および CentOS は、「GUI を使用するサーバ」ベース環境でインストールする必要があります。このベース環境は、Unified Manager のインストール手順で使用されるコマンドを提供します。他のベース環境では、インストールを検証または完了するために追加のコマンドのインストールが必要になる場合があります。状況に応じて `firewall-cmd` を使用できない場合は、次のコマンドを実行してシステムにインストールする必要があります。

```
# sudo yum install firewalld
```

コマンドを実行する前に IT 部門に問い合わせ、セキュリティポリシーで別の手順が必要かどうかを確認してください。



CentOS および Red Hat システムでは Transparent Huge Pages（THP）を無効にします。有効にすると、特定のプロセスがメモリを大量に消費して終了した場合に原因 Unified Manager をシャットダウンできる場合があります。

サポートされているブラウザ

Unified Manager Web UI にアクセスするには、サポートされているブラウザを使用します。

サポートされているブラウザとバージョンは Interoperability Matrix で確認できます。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

すべてのブラウザで、ポップアップブロックを無効にすることでソフトウェアの機能が正しく表示されます。

アイデンティティプロバイダ（IdP）でユーザを認証できるように Unified Manager で SAML 認証を設定する場合は、IdP でサポートされるブラウザのリストも確認してください。

プロトコルとポートの要件

このポートとプロトコルを使用して、Unified Manager サーバは管理対象のストレージシステム、サーバ、その他のコンポーネントと通信します。

Unified Manager サーバへの接続

通常環境では、Unified Manager Web UI への接続に常にデフォルトのポートが使用されるため、ポート番号を指定する必要はありません。たとえば、Unified Manager は常にデフォルトのポートで実行されるため、と入力できます `https://<host>` ではなく `https://<host>:443`。

Unified Manager サーバでは、次のインターフェイスにアクセスする際に特定のプロトコルを使用します。

インターフェイス	プロトコル	ポート	説明
Unified Manager Web UI	HTTP	80	Unified Manager Web UI へのアクセスに使用され、自動的にセキュアポート 443 にリダイレクトされます。
Unified Manager Web UI および API を使用するプログラム	HTTPS	443	Unified Manager Web UI へのセキュアなアクセスと API 呼び出しに使用されます。API 呼び出しは HTTPS でしか実行できません。
メンテナンスコンソール	SSH/SFTP	22	メンテナンスコンソールにアクセスしてサポートバンドルを取得する際に使用されます。
Linux コマンドライン	SSH/SFTP	22	Red Hat Enterprise Linux または CentOS のコマンドラインにアクセスしてサポートバンドルを取得する際に使用されます。
MySQL データベース	MySQL	3306	OnCommand および OnCommand Workflow Automation API サービスから Unified Manager へのアクセスに使用されます。
syslog	UDP	514	ONTAP システムからのサブスクリプションベースの EMS メッセージにアクセスし、メッセージに基づいてイベントを作成する際に使用されます。

インターフェイス	プロトコル	ポート	説明
REST	HTTPS	ポート 1	認証された ONTAP システムからの REST API ベースのリアルタイムの EMS イベントにアクセスする際に使用されます。



MySQLのデフォルトポート3306は、LinuxシステムにUnified Managerをインストールする際にlocalhostにのみ使用できます。これは、前の構成を維持したままのアップグレードシナリオには影響しません。この設定は変更可能で、を使用して他のホストから接続を利用できるようにすることができます Control access to MySQL port 3306 メンテナンスコンソールのオプション。詳細については、を参照してください "[その他のメニューオプション](#)"。HTTP 通信と HTTPS 通信に使用されるポート（ポート 80 と 443）は、Unified Manager メンテナンスコンソールを使用して変更できます。詳細については、を参照してください "[メンテナンスコンソールのメニュー](#)"。

Unified Manager サーバからの接続

ファイアウォールの設定で、Unified Manager サーバと管理対象のストレージシステム、サーバ、その他のコンポーネントの間の通信に使用するポートを開くように設定する必要があります。ポートが開いていない場合、通信は失敗します。

環境に応じて、Unified Manager サーバから特定の接続先への接続に使用するポートとプロトコルを変更することもできます。

Unified Manager サーバは、次のプロトコルとポートを使用して、管理対象のストレージシステム、サーバ、その他のコンポーネントに接続します。

宛先	プロトコル	ポート	説明
ストレージシステム	HTTPS	443 tcp	ストレージシステムの監視と管理に使用されます。
ストレージシステム	NDMP	10000 TCP	特定の Snapshot リストア処理に使用されます。
AutoSupport サーバ	HTTPS	443	AutoSupport 情報の送信に使用されます。この機能を実行するには、インターネットアクセスが必要です。
認証サーバ	LDAP	389	認証要求、およびユーザとグループの検索要求に使用されます。

宛先	プロトコル	ポート	説明
LDAPS	636	セキュアな LDAP 通信に使用されます。	メールサーバ
SMTP	25	アラート通知 E メールを送信に使用されます。	SNMP トラップの送信元
SNMPv1 または SNMPv3	162 UDP	アラート通知 SNMP トラップの送信に使用されます	外部データプロバイダのサーバ
TCP	2003 年	Graphite などの外部データプロバイダにパフォーマンスデータを送信します。	NTP サーバ

ワークシートへの記入

Unified Manager をインストールして設定する前に、環境に関する特定の情報を確認しておく必要があります。この情報はワークシートに記録できます。

Unified Manager のインストール情報

Unified Manager をインストールする際に必要な情報を記入します。

ソフトウェアが導入されているシステム	あなたの価値
ホストの完全修飾ドメイン名	
ホストの IP アドレス	
ネットワークマスク	
ゲートウェイの IP アドレス	
プライマリ DNS アドレス	
セカンダリ DNS アドレス	
検索ドメイン	
メンテナンスユーザのユーザ名	
メンテナンスユーザのパスワード	

Unified Manager の設定情報

インストール後に Unified Manager を設定するための情報を記入します。設定によっては省略可能な値もあります。

設定	あなたの価値
メンテナンスユーザの E メールアドレス	
SMTP サーバのホスト名または IP アドレス	
SMTP ユーザ名	
SMTP パスワード	
SMTP ポート	25（デフォルト値）
アラート通知の送信元 E メールアドレス	
認証サーバのホスト名または IP アドレス	
Active Directory の管理者名または LDAP のバインド識別名	
Active Directory のパスワードまたは LDAP のバインドパスワード	
認証サーバのベース識別名	
アイデンティティプロバイダ（IdP）の URL	
アイデンティティプロバイダ（IdP）のメタデータ	
SNMP トラップの送信先ホストの IP アドレス	
SNMP ポート	

クラスタ情報

Unified Manager を使用して管理するストレージシステムの情報を記入します。

クラスタ 1 / N	あなたの価値
ホスト名またはクラスタ管理 IP アドレス	

クラスター 1 / N	あなたの価値
ONTAP 管理者のユーザ名	
 管理者には「admin」ロールが割り当てられている必要があります。	
ONTAP 管理者のパスワード	
プロトコル	HTTPS

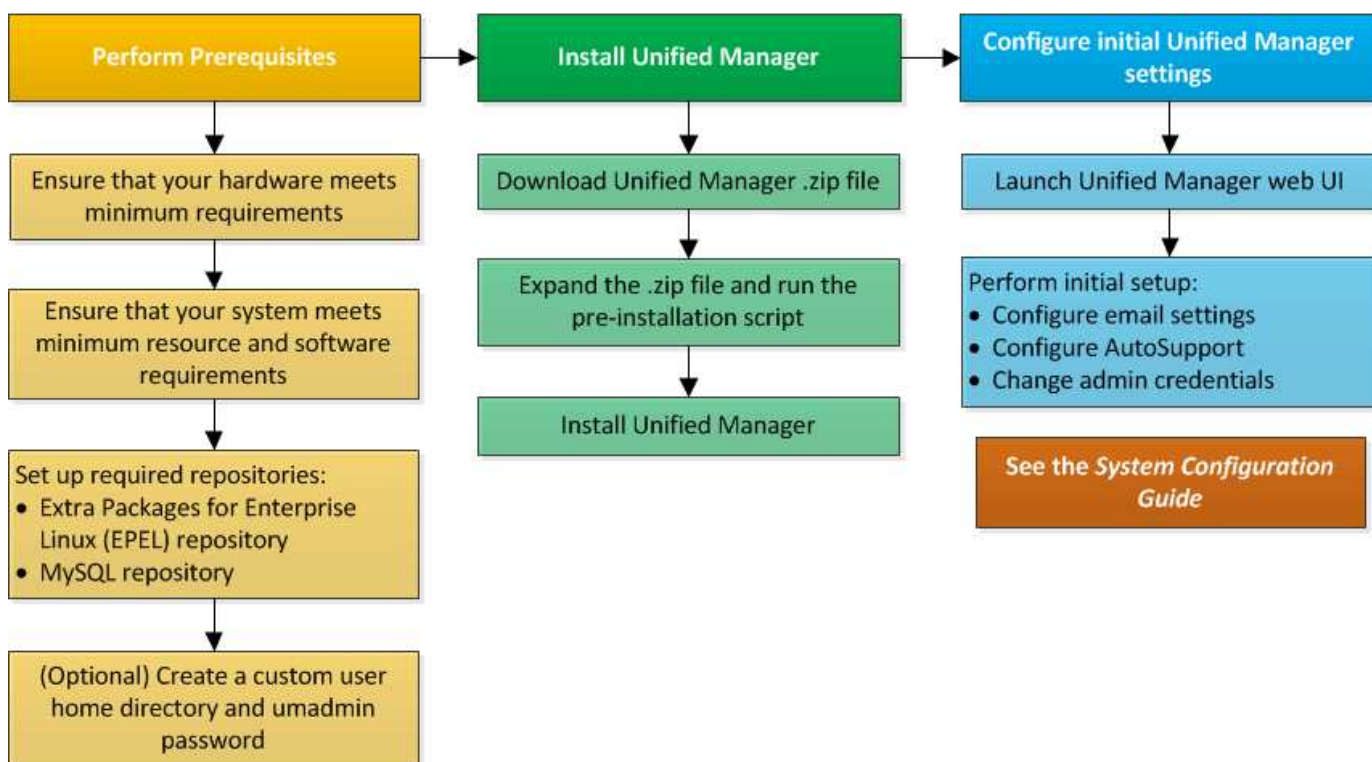
Unified Manager ソフトウェアのインストール、アップグレード、削除を行います

Linux システムで、Unified Manager ソフトウェアのインストール、新しいバージョンへのアップグレード、または Unified Manager の削除を実行できます。

Unified Manager は、Red Hat Enterprise Linux サーバまたは CentOS サーバにインストールできます。Unified Manager をインストールする Linux サーバは、物理マシンでも仮想マシンでもかまいません。仮想マシンの場合は、VMware ESXi、Microsoft Hyper-V、または Citrix XenServer で実行されているマシンを使用できます。

インストールプロセスの概要

以下は、Unified Manager を使用する前に必要なインストール作業のワークフローです。



必要なソフトウェアリポジトリをセットアップする

インストールプログラムが必要なすべてのソフトウェアをインストールできるように、特定のリポジトリへのアクセスが必要になります。

EPEL リポジトリを手動で設定します

Unified Manager をインストールするシステムが Extra Packages for Enterprise Linux (EPEL) リポジトリにアクセスできない場合、インストールが成功するためにはリポジトリを手動でダウンロードして設定する必要があります。

EPEL リポジトリは、システムにインストールする必要があるサードパーティユーティリティへのアクセスを提供します。Unified ManagerをRed Hat Enterprise LinuxとCentOSのどちらのシステムにインストールする場合もEPELリポジトリを使用します。

手順

1. インストールに対応する EPEL リポジトリをダウンロードします。Red Hat Enterprise Linux 7 の場合は、次のサイトからダウンロードしてください。

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

バージョン 8 については、次のサイトからダウンロードしてください。

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

2. EPEL リポジトリを設定します。

```
yum install epel-release-latest-<version>.noarch.rpm
```

Red Hat Enterprise Linux 8システムの場合、モジュラRPMパッケージを含む内部リポジトリがあるとします。たとえば、次のようになります。`javapackages-filesystem-<version>.module.rpm`モジュールパッケージのメタデータが同じリポジトリ内にあることを確認します。

MySQL リポジトリを手動で設定する

Unified Manager をインストールするシステムが MySQL Community Edition リポジトリにアクセスできない場合、インストールが成功するためにはリポジトリを手動でダウンロードして設定する必要があります。

MySQL リポジトリリポジトリリポジトリは、システムにインストールする必要がある MySQL ソフトウェアへのアクセスを提供します。



このタスクは、システムがインターネットに接続されていないと失敗することがあります。Unified Managerをインストールするシステムがインターネットにアクセスできない場合は、MySQLのドキュメントを参照してください。

手順

1. インストールに対応する MySQL リポジトリをダウンロードします。Red Hat Enterprise Linux 7 の場合は、次のサイトからダウンロードしてください。

```
wget http://repo.mysql.com/yum/mysql-8.0-community/el/7/x86_64/mysql80-community-release-el7-3.noarch.rpm
```

バージョン 8 については、次のサイトからダウンロードしてください。

```
wget http://repo.mysql.com/yum/mysql-8.0-community/el/8/x86_64/mysql80-community-release-el8-1.noarch.rpm
```

2. MySQL リポジトリを設定します。

```
yum install mysql80-community-release-<version>.noarch.rpm
```

Red Hat Enterprise Linux 8 システムの場合、AppStream リポジトリから提供される Java -11 openjdk、p7zip、およびその他のソフトウェアパッケージを含む内部リポジトリがある場合、AppStream リポジトリを無効にして MySQL Community Server をインストールする必要があります。次のコマンドを実行します。

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install mysql-community-server
```

キーまたはキーの不一致が見つからないというエラーが表示され、インストールが失敗した場合は、次の手順を実行してください。

- 接続されているシステムで、次のコマンドを実行して、更新されたMySQLキーをインポートします。

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-<xxxx>

for example:

rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022
```

- インターネットに接続されていないシステムでは、MySQLリポジトリファイルを更新して無効にします
gpgcheck マークで gpgcheck=0。

SELinux で NFS 共有と CIFS 共有に接続する必要がある

マウントする場合 /opt/netapp または /opt/netapp/data SELinuxを有効にしているNASデバイスまたはSANデバイスでは、いくつかの考慮事項について理解しておく必要があります。

マウントする場合 /opt/netapp または /opt/netapp/data SELinuxを有効にしている環境で、ルートファイルシステム以外の場所から、マウントされたディレクトリに正しいコンテキストを設定する必要があります。ご使用の環境で該当するシナリオについて、次の手順を実行して正しい SELinux コンテキストを設定および確認してください。

の場合の**SELinux**コンテキストの設定 /opt/netapp/data がマウントされている

をマウント済みの場合 /opt/netapp/data SELinuxの場合、システムはに設定されます Enforcing`

のSELinuxコンテキストタイプを確認してください。`/opt/netapp/data` がに設定されます。`mysql_d_b_t`を使用します。これは、データベースファイルの場所のデフォルトのコンテキスト要素です。

1. 次のコマンドを実行してコンテキストを確認します。

```
ls -dZ /opt/netapp/data
```

出力例を次に示します。

```
drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0
/opt/netapp/data
```



この出力では、コンテキストはです `default_t`。このコンテキストをに変更する必要があります `mysql_d_b_t`。

2. のマウント方法に基づいてコンテキストを設定するには、次の手順を実行します `/opt/netapp/data`。

- a. 次のコマンドを実行してコンテキストをに設定します `mysql_d_b_t` :

```
semanage fcontext -a -t mysql_d_b_t "/opt/netapp/data"
`restorecon -R -v /opt/netapp/data
```

- b. を設定している場合は `/opt/netapp/data` インチ `/etc/fstab` を編集する必要があります `/etc/fstab` ファイル。をクリックします `/opt/netapp/data/` マウントオプションで、MySQL ラベルを次のように追加します。

```
context=system_u:object_r:mysql_d_b_t:s0
```

- c. をアンマウントして再マウントします `/opt/netapp/data/` コンテキストをイネーブルにします。

- d. NFSを直接マウントした場合は、次のコマンドを実行してコンテキストをに設定します `mysql_d_b_t` :

```
mount <nfsshare>:/<mountpoint> /opt/netapp/data -o
context=system_u:object_r:mysql_d_b_t:s0
```

3. コンテキストが正しく設定されているかどうかを確認します。

```
ls -dZ /opt/netapp/data/
```

出力例を次に示します。

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysql_d_b_t:s0
/opt/netapp/data/
```

の場合のSELinuxコンテキストの設定 `/opt/netapp` がマウントされています `/opt/netapp/data/` は別途マウントすることもできます

このシナリオでは、最初のにコンテキストを設定する必要があります `/opt/netapp/data/` 前のセクションで説明したとおりです。の正しいコンテキストを設定したあと `/opt/netapp/data/`` をクリックして、親デ

ディレクトリを指定します。`/opt/netapp` SELinuxコンテキストがに設定されていない `file_t`。

手順

1. 次のコマンドを実行してコンテキストを確認します。

```
ls -dZ /opt/netapp
```

出力例を次に示します。

```
drwxr-xr-x. mysql root unconfined_u:object_r:file_t:s0 /opt/netapp
```

この出力では、コンテキストは `file_t` 変更する必要があります。次のコマンドでは、コンテキストを `usr_t` に設定しています。コンテキストは、以外の任意の値に設定できます。`file_t` セキュリティ要件に基づきます。

2. のマウント方法に応じて、次の手順を実行してコンテキストを設定します。`/opt/netapp`。

- a. 次のコマンドを実行してコンテキストを設定します。

```
semanage fcontext -a -t usr_t "/opt/netapp"
restorecon -v /opt/netapp
```

1. を設定している場合は、`/opt/netapp` インチ `etc/fstab` を編集する必要があります。`etc/fstab` ファイル。をクリックします。`/opt/netapp` マウントオプションで、MySQLラベルを次のように追加します。

```
context=system_u:object_r:usr_t:s0
```

2. をアンマウントし、再度マウントします。`/opt/netapp` コンテキストをイネーブルにします。
3. NFS を直接マウントした場合は、次のコマンドを実行してコンテキストを設定します。

```
mount <nfsshare>:/<mountpoint> /opt/netapp -o
context=system_u:object_r:usr_t:s0
```

- a. コンテキストが正しく設定されているかどうかを確認します。

```
ls -dZ /opt/netapp
```

出力例を示します

```
drwxr-xr-x. mysql root unconfined_u:object_r:usr_t:s0 /opt/netapp
```

の場合のSELinuxコンテキストの設定。`/opt/netapp` がマウントされています。`/opt/netapp/data/` は別途マウントされません。

をマウント済みの場合。`/opt/netapp` SELinuxの場合、システムはに設定されます。`Enforcing` のSELinux。

コンテキストタイプを確認してください。`/opt/netapp` がに設定されます。`mysqld_db_t`を使用します。これは、データベースファイルの場所のデフォルトのコンテキスト要素です。

手順

1. 次のコマンドを実行してコンテキストを確認します。

```
ls -dZ /opt/netapp
```

出力例を次に示します。

```
drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0 /opt/netapp
```



この出力では、コンテキストはです `default_t`。このコンテキストをに変更する必要があります `mysqld_db_t`。

2. のマウント方法に基づいてコンテキストを設定するには、次の手順を実行します `/opt/netapp`。

- a. 次のコマンドを実行してコンテキストをに設定します `mysqld_db_t`：

```
semanage fcontext -a -t mysqld_db_t "/opt/netapp"
`restorecon -R -v /opt/netapp
```

- b. を設定している場合は `/opt/netapp` インチ `/etc/fstab` を編集します。``/etc/fstab` ファイル。をクリックします `/opt/netapp/` マウントオプションで、MySQLラベルを次のように追加します。

```
context=system_u:object_r:mysqld_db_t:s0
```

- c. をアンマウントし、再度マウントします `/opt/netapp/` コンテキストをイネーブルにします。

- d. NFSを直接マウントした場合は、次のコマンドを実行してコンテキストをに設定します

```
mysqld_db_t:
mount <nfsshare>:/<mountpoint> /opt/netapp -o
context=system_u:object_r:mysqld_db_t:s0
```

3. コンテキストが正しく設定されているかどうかを確認します。

```
ls -dZ /opt/netapp/
```

出力例を次に示します。

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysqld_db_t:s0 /opt/netapp/
```

Linux システムへの Unified Manager のインストール

Unified Manager をダウンロードしてインストールする一連の手順は、インストールシナリオによって異なります。

カスタムユーザのホームディレクトリと **umadmin** のパスワードを作成しています

Unified Manager をインストールする前に、カスタムのホームディレクトリを作成し、umadmin ユーザのパスワードを独自に定義できます。このタスクはオプションですが、サイトによっては Unified Manager のデフォルトのインストール設定とは異なる設定が必要になることがあります。

- 必要なもの *
- に記載されたシステム要件を満たしている必要があります "[ハードウェアシステムの要件](#)".
- Red Hat Enterprise Linux または CentOS のシステムに root ユーザとしてログインできる必要があります。

Unified Manager のインストール時、デフォルト設定では次のタスクが実行されます。

- でumadminユーザが作成されます /home/umadmin をホームディレクトリとして指定します。
- umadmin ユーザにデフォルトのパスワード「admin」を割り当てます。

へのアクセスが制限されるインストール環境もあります '/home' の場合、インストールは失敗します。ホームディレクトリは別の場所に作成する必要があります。また、サイトによっては、パスワードの複雑さに関するルールが設定されている場合や、インストールプログラムではなくローカルの管理者が設定したパスワードが必要な場合があります。

インストール環境でデフォルトのインストール設定とは異なる設定が必要な場合は、次の手順に従って、カスタムのホームディレクトリを作成し、umadmin ユーザのパスワードを定義します。

インストール前にこの情報を定義しておけば、インストールスクリプトで設定が検出され、定義した値がデフォルトのインストール設定の代わりに使用されます。

また、Unified Managerのデフォルトのインストールでは、sudoersファイルにumadminユーザが追加されています (ocum_sudoers および ocie_sudoers) をクリックします /etc/sudoers.d/ ディレクトリ。セキュリティポリシーや一部のセキュリティ監視ツールによってこのコンテンツを環境から削除した場合は、再度追加する必要があります。Unified Manager の一部の処理では sudo 権限が必要なため、sudoers の設定を維持する必要があります。

環境内のセキュリティポリシーでは、Unified Manager メンテナンスユーザの sudo 権限を制限しないでください。制限されている権限があると、一部の Unified Manager 処理が失敗することがあります。インストールの完了後に umadmin ユーザとしてログインして、次の sudo コマンドを実行できることを確認します。

```
sudo systemctl status ocie
```

エラーが発生せずに ocie サービスの適切なステータスが返されれば問題ありません。

手順

1. サーバに root ユーザとしてログインします。
2. 「メンテナンス」という umadmin グループアカウントを作成します。

```
groupadd maintenance
```

3. メンテナンスグループの任意のホームディレクトリにユーザアカウント「umadmin」を作成します。

```
adduser --home <home_directory> -g maintenance umadmin
```

4. umadmin のパスワードを定義します。

```
passwd umadmin
```

umadmin ユーザの新しいパスワードの文字列を入力するように求められます。

Unified Manager のインストールが完了したら、umadmin ユーザのログインシェルを指定する必要があります。

Unified Manager をダウンロードしています

Unified Managerをダウンロードする必要があります。 .zip ファイルをNetApp Support Site から選択して、Unified Managerをインストールします。

- 必要なもの *

NetApp Support Siteのログインクレデンシャルが必要です。

ダウンロードする Unified Manager のインストールパッケージは、Red Hat Enterprise Linux と CentOS の両方のシステムで共通です。

手順

1. NetApp Support Siteにログインし、Unified Manager のダウンロードページに移動します。

"NetApp Support Site"

2. 必要なバージョンの Unified Manager を選択し、エンドユーザライセンス契約（EULA）に同意します。
3. Linux用のUnified Managerインストーラファイルをダウンロードし、を保存します。 .zip ファイルをターゲットシステム上のディレクトリにコピーします。



- 使用している Red Hat Enterprise Linux システムに対応した正しいバージョンのインストーラファイルをダウンロードしていることを確認してください。 Red Hat Enterprise Linux 7または8がインストールされているかどうかに基づいて、適切なバージョンのUnified Managerをダウンロードします。 .zip ファイル。
- コード署名証明書をダウンロードすることを推奨します (.pem) およびデジタル署名 (.sig) をと共に使用します。 .zip ファイル。

4. ダウンロードしたソフトウェアのチェックサムの整合性を確認します。
5. コード署名証明書とデジタル署名をダウンロードした場合は、インストーラファイルの整合性を確認できます。 インストーラファイルの整合性を確認するには、次のコマンドを使用します。
 - このコマンドは、コード署名証明書から公開鍵を使用してファイルを作成します。

```
openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem >  
<public_key_file_name>
```

- ここで、* AIQUM -RHEL-client-inter-root.pem *は、コード署名証明書を含むファイルです。
- このコマンドは、インストーラファイルの署名を検証します。

```
openssl dgst -sha256 -verify <public_key_file_name> -signature  
<signature_file_name> ActiveIQUnifiedManager-<version>.zip
```

のようなメッセージが表示されます Verified Ok インストーラファイルが安全に使用できることを確認します。

Unified Manager をインストールしています

Unified Manager は、Red Hat Enterprise Linux または CentOS の物理プラットフォームまたは仮想プラットフォームにインストールできます。

- 必要なもの *
- Unified Manager をインストールするシステムがシステムおよびソフトウェアの要件を満たしている必要があります。

を参照してください "[ハードウェアシステムの要件](#)".

を参照してください "[Linux ソフトウェアとインストールの要件](#)".

- Unified Managerをダウンロードしておく必要があります .zip ファイルをNetApp Support Site からターゲットシステムにコピーします。
- ダウンロードしたの整合性を確認しておく必要があります .zip ファイル。
- サポートされている Web ブラウザが必要です。
- ターミナルエミュレーションソフトウェアでスクロールバックが有効になっている必要があります。

Red Hat Enterprise Linux または CentOS のシステムには、必要なサポートソフトウェア（Java、MySQL、追加ユーティリティ）のすべてのバージョンがインストールされているか、必要なソフトウェアの一部のみがインストールされているか、または新たにインストールしたシステムに必要なソフトウェアがインストールされていない可能性があります。

手順

1. Unified Manager をインストールするサーバにログインします。
2. 該当するコマンドを入力し、インストールをサポートするためにターゲットシステムでインストールまたはアップグレードが必要なソフトウェアを特定します。

必要なソフトウェアと最小バージョン	ソフトウェアとバージョンを確認するコマンド
OpenJDKバージョン11.0.17	java -version
MySQL 8.0.30 Community Editionの場合	`rpm -qa
grep -i mysql`	p7zip 16.02

必要なソフトウェアと最小バージョン	ソフトウェアとバージョンを確認するコマンド
`rpm -qa`	grep p7zip`

- MySQL 8.0.30 Community Editionより前のバージョンのMySQLがインストールされている場合は、次のコマンドを入力してアンインストールします。

```
rpm -e <mysql_package_name>
```

依存関係のエラーが表示された場合は、を追加する必要があります `--nodeps` コンポーネントをアンインストールするオプション。

- インストールをダウンロードしたディレクトリに移動します `.zip` Unified Managerのバンドルをファイルして展開します。

```
unzip ActiveIQUnifiedManager-<version>.zip
```

が必要です `.rpm` Unified Managerのモジュールがターゲットディレクトリに解凍されます。

- ディレクトリに次のモジュールがあることを確認します。

```
ls *.rpm
```

```
netapp-um<version>.x86_64.rpm
```

- インストール前スクリプトを実行して、Unified Manager のインストールと競合するシステム設定やインストール済みソフトウェアがないことを確認します。

```
sudo ./pre_install_check.sh
```

インストール前スクリプトは、システムに有効なRed Hat Enterprise Linuxサブスクリプションがあるかどうか、およびシステムが必要なソフトウェアリポジトリにアクセスできるかどうかを確認します。問題が検出された場合は、Unified Manager をインストールする前に修正する必要があります。

Red Hat Enterprise Linux 8 システムの場合、JDK 11-OpenJDK、p7zip、その他のAppStream リポジトリが提供するソフトウェアパッケージを使用した内部リポジトリがある場合、AppStream リポジトリを無効にして MySQL Community Server をインストールする必要があります。次のコマンドを実行します。

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install
mysql-community-server
```

- * オプション：* システムがインターネットに接続されておらず、インストールに必要なパッケージを手動でダウンロードする必要がある場合にのみ、手順 7 を実行する必要があります。インターネットにアクセスできるシステムで、必要なすべてのパッケージがある場合は、ステップ8に進みます。システムがインターネットに接続されていない場合やRed Hat Enterprise Linuxのリポジトリを使用していない場合は、次の手順に従って、必要なパッケージが揃っているかどうかを確認し、足りないパッケージをダウンロードします。
 - Unified Managerをインストールするシステムで、使用可能なパッケージと使用できないパッケージのリストを表示します。+

```
yum install netapp-um<version>.x86_64.rpm --assumeno
```

"Installing : " セクションの項目は現在のディレクトリにあるパッケージで、 "Installing for dependencies : " セクションの項目はシステムにないパッケージです。

- b. インターネットにアクセスできるシステムで、不足しているパッケージをダウンロードします。

```
yum install <package_name> --downloadonly --downloadaddir=.
```



プラグイン「yum-plugin-downloadonly」は、Red Hat Enterprise Linux システムで常に有効になっているとは限りません。インストールせずにパッケージをダウンロードするには、この機能を有効にする必要があります。

```
yum install yum-plugin-downloadonly
```

- a. インターネットに接続されたシステムから不足しているパッケージをインストールシステムにコピーします。

8. をrootユーザとして使用するか、を使用します`sudo`を使用して、次のコマンドを実行してソフトウェアをインストールします。

```
yum install netapp-um<version>.x86_64.rpm
```

このコマンドを実行すると、.rpm パッケージ、必要な他のすべてのサポートソフトウェア、および Unified Manager ソフトウェアがインストールされます。



インストールの実行に他のコマンド（など）は使用しないでください rpm -ivh）。Unified ManagerをRed Hat Enterprise LinuxまたはCentOSのシステムに正しくインストールするには、Unified Managerのすべてのファイルと関連ファイルを特定の順序で特定のディレクトリ構造にインストールする必要があります、そのためにはによって自動的に適用されます yum install netapp-um<version>.x86_64.rpm コマンドを実行します

9. インストールメッセージの直後に表示される E メール通知は無視してください。

この E メールは最初の cron ジョブの失敗を root ユーザに通知するもので、インストールには影響しません。

10. インストールメッセージが最後まで表示されたら、メッセージを上スクロールして、Unified Manager Web UI の IP アドレスまたは URL、メンテナンスユーザの名前（umadmin）、およびデフォルトのパスワードを確認します。

次のようなメッセージが表示されます。

```
Active IQ Unified Manager installed successfully.  
Use a web browser and one of the following URL(s) to configure and  
access the Unified Manager GUI.  
https://default_ip_address/      (if using IPv4)  
https://[default_ip_address]/    (if using IPv6)  
https://fully_qualified_domain_name/
```

```
Log in to Unified Manager in a web browser by using following details:  
  username: umadmin  
  password: admin
```

11. IP アドレスまたは URL、割り当てられたユーザ名（umadmin）、および現在のパスワードをメモします。
12. Unified Manager をインストールする前にカスタムのホームディレクトリで umadmin ユーザアカウントを作成していた場合は、umadmin ユーザのログインシェルを指定する必要があります。

```
usermod -s /bin/maintenance-user-shell.sh umadmin
```

の説明に従って、Web UIにアクセスしてumadminユーザのデフォルトパスワードを変更し、Unified Managerの初期セットアップを実行します "[Active IQ Unified Manager を設定しています](#)". umadminユーザのデフォルトパスワードを変更する必要があります。

Unified Manager のインストール時に作成されるユーザ

Red Hat Enterprise Linux または CentOS に Unified Manager をインストールすると、Unified Manager とサードパーティユーティリティによって umadmin、jboss、および mysql の各ユーザが作成されます。

- * umadmin *

Unified Manager への初回ログインで使います。このユーザーには「アプリケーション管理者」ユーザーロールが割り当てられ、「メンテナンスユーザー」タイプとして設定されます。このユーザは Unified Manager によって作成されます。

- * JBoss *

JBoss ユーティリティに関連する Unified Manager サービスの実行に使います。このユーザは Unified Manager によって作成されます。

- * MySQL *

Unified Manager の MySQL データベースクエリの実行に使います。このユーザは MySQL サードパーティユーティリティによって作成されます。

Unified Manager のインストール時、これらのユーザに加え、対応するグループとして maintenance、jboss、および mysql の各グループが作成されます。maintenance グループと jboss グループは Unified Manager によって作成され、mysql グループはサードパーティユーティリティによって作成されます。



Unified Manager をインストールする前にカスタムのホームディレクトリを作成して独自の umadmin ユーザのパスワードを定義していた場合、インストール時に maintenance グループ または umadmin ユーザがもう一度作成されることはありません。

JBoss パスワードを変更しています

インストール時に設定されたインスタンス固有の JBoss パスワードをリセットできます。このセキュリティ機能によって Unified Manager のインストール設定が上書きされてしまいます。必要に応じて、パスワードをリセットすることもできます。この処理を実行すると、MySQL へのアクセス時に JBoss で使用するパスワードも変更になります。

- Unified Manager がインストールされている Red Hat Enterprise Linux または CentOS のシステムへの root ユーザアクセスが必要です。
- ネットアップが提供するサービスにアクセスする必要があります password.sh ディレクトリ内のスクリプト /opt/netapp/essentials/bin。

手順

1. システムに root ユーザとしてログインします。
2. 次のコマンドを記載された順序で入力して、Unified Manager サービスを停止します。

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

関連付けられている MySQL ソフトウェアは停止しないでください。

3. 次のコマンドを入力して、パスワードの変更プロセスを開始します。

```
/opt/netapp/essentials/bin/password.sh resetJBossPassword
```

4. プロンプトが表示されたら、新しい JBoss パスワードを入力し、確認のためにもう一度入力します。

パスワードは 8~16 文字で指定し、数字、大文字、小文字、および次の特殊文字の少なくとも 1 文字を含める必要があります。

```
!@%^*-_=[]:<>./~/~+
```

5. スクリプトが完了したら、次のコマンドを記載された順序で入力して、Unified Manager サービスを開始します。

```
systemctl start ocie
```

```
systemctl start ocieau
```

6. すべてのサービスが開始されたら、Unified Manager UI にログインできます。

Red Hat Enterprise Linux または CentOS での Unified Manager のアップグレード

新しいバージョンが利用可能になったときは、Unified Managerをアップグレードできます。

Unified Manager ソフトウェアのパッチリリースがネットアップから提供されたときは、新規リリースと同じ手順を使用してインストールします。

Unified Manager を OnCommand Workflow Automation のインスタンスとペアにして使用している環境では、両方の製品のソフトウェアで新しいバージョンを利用できる場合、2つの製品間の接続を解除してから各製品をアップグレードし、アップグレードの実行後に Workflow Automation の接続を新たにセットアップする必要があります。いずれかの製品のみをアップグレードする場合は、アップグレード後に Workflow Automation にログインし、Unified Manager からデータを取得していることを確認します。

Unified Managerバージョンでサポートされているアップグレードパス

Active IQ Unified Manager では、バージョンごとに特定のアップグレードパスがサポートされます。

すべてのバージョンのUnified Managerで、新しいバージョンへのインプレースアップグレードを実行できるわけではありません。Unified ManagerのアップグレードはN-2モデルに限定されています。つまり、アップグレードはすべてのプラットフォームの次の2つのリリースでのみ実行できます。たとえば、Unified Manager 9.10からUnified Manager 9.12へのアップグレードは、Unified Manager 9.11からのみ実行できます。

サポート対象よりも前のバージョンを実行している場合は、Unified Managerインスタンスをいずれかのサポート対象バージョンにアップグレードしてから、現在のバージョンにアップグレードする必要があります。

たとえば、インストールされているバージョンがOnCommand Unified Manager 9.5であり、最新のリリースActive IQ Unified Manager 9.12にアップグレードする場合は、一連のアップグレードを実行します。

アップグレードパスの例：

1. OnCommand Unified Manager 9.5 → Active IQ Unified Manager 9.7をアップグレードします。
2. 9.7→9.9にアップグレードします。
3. 9.→9.11にアップグレードします。
4. 9.11 → 9.12にアップグレードします。

アップグレードパスマトリックスの詳細については、こちらを参照してください ["ナレッジベース \(KB\) の記事を参照してください"](#)。

Unified Manager をアップグレードする

LinuxプラットフォームでUnified Manager 9.10または9.11から9.12にアップグレードするには、インストールファイルをダウンロードして実行します。

- 必要なもの *
- Unified Manager をアップグレードするシステムがシステム要件とソフトウェア要件を満たしている必要があります。

を参照してください ["ハードウェアシステムの要件"](#)。

を参照してください ["Linux ソフトウェアとインストールの要件"](#)。

- Red Hat Enterprise Linux Subscription Manager への登録が必要です。
- Unified Manager をアップグレードする前に、適切なバージョンの OpenJDK をインストールするか、または適切なバージョンにアップグレードする必要があります。

を参照してください ["Linux での JRE のアップグレード"](#)。

- アップグレード中に問題が使用される場合にデータが失われないようにするために、Unified Manager データベースのバックアップを作成しておく必要があります。ネットアップでは、からバックアップファイルを移動することを推奨します /opt/netapp/data ディレクトリを外部の場所に移動します。
- アップグレードの実行中に、パフォーマンスデータの保持期間について、以前のデフォルト設定である 13 カ月のままにするか 6 カ月に変更するかを確認するプロンプトが表示されることがあります。変更を確認すると、6 カ月を過ぎた過去のパフォーマンスデータはパージされます。
- アップグレードプロセスの実行中は Unified Manager を使用できなくなるため、実行中の処理がある場合は完了しておいてください。
- MySQL Community Edition は、Unified Manager のアップグレード時に自動的にアップグレードされます。システムにインストールされているMySQLのバージョンが8.0.30より前の場合は、Unified Manager のアップグレードプロセスによってMySQLが8.0.30に自動的にアップグレードされます。

手順

1. ターゲットの Red Hat Enterprise Linux サーバまたは CentOS サーバにログインします。
2. サーバに Unified Manager のバンドルをダウンロードします。

を参照してください ["Linux版Unified Managerをダウンロードしています"](#)。

3. ダウンロードしたディレクトリに移動し、Unified Manager のバンドルを展開します。

```
unzip ActiveIQUnifiedManager-<version>.zip
```

Unified Manager に必要な RPM モジュールがターゲットディレクトリに解凍されます。

4. ディレクトリに次のモジュールがあることを確認します。

```
ls *.rpm
```

```
netapp-um<version>.x86_64.rpm
```

5. インストール前スクリプトを実行して、アップグレードと競合するシステム設定やインストール済みソフトウェアがないことを確認します。

```
sudo ./pre_install_check.sh
```

インストール前スクリプトは、システムに有効なRed Hat Enterprise Linuxサブスクリプションがあるかどうか、およびシステムが必要なソフトウェアリポジトリにアクセスできるかどうかを確認します。問題が検出された場合は、修正してアップグレードを続行する必要があります。

不足しているパッケージが検出された場合は、に記載されている手順を実行します ["不足しているパッケージに対して実行する追加手順"](#)。足りないパッケージがない場合は、次の手順に進みます。

6. 次のスクリプトを使用して Unified Manager をアップグレードします。

```
upgrade.sh
```

RPM モジュールが自動的に実行され、必要なサポートソフトウェアとそれらで実行されている Unified Manager モジュールがアップグレードされます。アップグレードと競合するシステム設定やインストール済みソフトウェアがないかどうか確認されます。問題が検出された場合は、Unified Manager をアップグレードする前に修正する必要があります。Unified Manager をアップグレードする前に `_net-snmp` などのパッケージをインストールしていた場合は、MySQL の依存関係によってアップグレード中にパッケージがアンインストールされることがあります。引き続き使用するには、パッケージを手動で再度インストールする必要があります。

7. アップグレードが完了したら、メッセージを上スクロールして、Unified Manager Web UI の IP アドレスまたは URL、メンテナンスユーザの名前（umadmin）、およびデフォルトのパスワードを確認します。

次のようなメッセージが表示されます。

```
Active IQ Unified Manager upgraded successfully.  
Use a web browser and one of the following URLs to access the Unified  
Manager GUI:
```

```
https://default_ip_address/      (if using IPv4)  
https://[default_ip_address]/    (if using IPv6)  
https://fully_qualified_domain_name/
```

サポートされている Web ブラウザの新しいウィンドウに表示された IP アドレスまたは URL を入力して Unified Manager Web UI を起動し、前に設定したメンテナンスユーザの名前（umadmin）とパスワードを使用してログインします。

不足しているパッケージに対して実行する追加手順

アップグレード中にサイトで不足しているパッケージが検出された場合、またはシステムがインターネットに接続されていない場合、または Red Hat Enterprise Linux リポジトリを使用していない場合は、次の手順を実行して、必要なパッケージが揃っているかどうかを確認し、それらのパッケージをダウンロードします。



これらの手順は、メイン手順の `step_5` (ステップ 5) の後に実行する必要があります。この手順アップグレードでは Unified Manager がアップグレードされます。アップグレードのために追加の手順を実行する必要はありません。

1. 各パッケージについてその有無を表示します。

```
yum install netapp-um<version>.x86_64.rpm --assumeno
```

"Installing :" セクションの項目は現在のディレクトリにあるパッケージで、"Installing for dependencies :" セクションの項目はシステムにないパッケージです。

2. インターネットにアクセスできる別のシステムで、次のコマンドを実行して不足しているパッケージをダウンロードします。


```
yum install package_name --downloadonly --downloadaddir=.
```

パッケージは、として指定されたディレクトリにダウンロードされます --downloadaddir=。

プラグイン「yum-plugin-downloadonly」は、Red Hat Enterprise Linux システムで常に有効になっているとは限りません。インストールせずにパッケージをダウンロードするには、この機能を有効にする必要があります。

```
yum install yum-plugin-downloadonly
```

3. インストールシステムでUnified Managerのバンドルを解凍したディレクトリに、ダウンロードしたパッケージをコピーします。
4. ディレクトリをそのディレクトリに変更し、次のコマンドを実行して欠落パッケージとその依存関係をインストールします。

```
yum install *.rpm
```

5. Unified Manager サーバを起動します。次のコマンドを実行します。

```
systemctl start ocie
```

```
systemctl start ocieau
```

これでUnified Managerのアップグレードプロセスは完了です。サポートされているWebブラウザの新しいウィンドウに表示されたIPアドレスまたはURLを入力してUnified Manager Web UIを起動し、前に設定したメンテナンスマスターの名前（umadmin）とパスワードを使用してログインします。

Red Hat Enterprise Linux 7.x から 8.x へのホスト OS のアップグレード

Unified Manager がインストールされている Red Hat Enterprise Linux 7.x システムを Red Hat Enterprise Linux 8.x にアップグレードする必要がある場合は、このトピックに記載されているいずれかの手順に従う必要があります。いずれの場合も、Red Hat Enterprise Linux 7.x システムに Unified Manager のバックアップを作成し、そのバックアップを Red Hat Enterprise Linux 8.x システムにリストアする必要があります。サポートされるRed Hat Enterprise Linuxのバージョンは8.0から8.6です。

ここに記載する 2 つの方法の違いは、Unified Manager のリストア処理を新しい 8.x サーバで実行する場合と同じサーバで実行する場合です。

この作業では、Red Hat Enterprise Linux 7.x システムで Unified Manager のバックアップを作成する必要があるため、Unified Manager がオフラインになる時間が最小限になるように、アップグレードプロセス全体を実行する準備ができてからバックアップを作成します。Red Hat Enterprise Linux 7.x システムをシャットダウンしたあと、新しい Red Hat Enterprise Linux 8.x を起動するまではデータが収集されないため、その間のデータは Unified Manager UI に表示されません。

を参照してください ["バックアップとリストアの処理の管理"](#) バックアッププロセスとリストアプロセスの詳細な手順を確認する必要がある場合。

- 新しいサーバを使用したホスト OS のアップグレード *

Red Hat Enterprise Linux 8.x ソフトウェアをインストールできるスペアシステムがある場合は、Red Hat

Enterprise Linux 7.x システムが稼働している間にスペアシステムで Unified Manager のリストアを実行できるように、次の手順に従います。

1. 新しいサーバに Red Hat Enterprise Linux 8.x ソフトウェアをインストールして設定します。

を参照してください "[Linux ソフトウェアとインストールの要件](#)".

2. Red Hat Enterprise Linux 8.x システムには、既存の Red Hat Enterprise Linux 7.x システムと同じバージョンの Unified Manager ソフトウェアをインストールします。

を参照してください "[LinuxへのUnified Managerのインストール](#)".

インストールが完了しても、UI を起動したり、クラスタ、ユーザ、または認証設定を設定したりしないでください。この情報は、リストアプロセスでバックアップファイルに取り込まれます。

3. Red Hat Enterprise Linux 7.xシステムのWeb UIの管理メニューで、Unified Managerのバックアップを作成し、バックアップファイルをコピーします (.7z ファイル) とデータベースリポジトリディレクトリの内容 (/database-dumps-repo サブディレクトリ) を外部の場所に追加します。
4. Red Hat Enterprise Linux 7.x システムで、 Unified Manager をシャットダウンします。
5. Red Hat Enterprise Linux 8.xシステムで、バックアップファイルをコピーします (.7z ファイル) を外部の場所からコピーします /opt/netapp/data/ocum-backup/ およびにデータベースリポジトリファイルを追加します /database-dumps-repo のサブディレクトリ /ocum-backup ディレクトリ。
6. 次のコマンドを入力して、バックアップファイルから Unified Manager データベースをリストアします。

```
um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
```

7. Web ブラウザに IP アドレスまたは URL を入力して Unified Manager Web UI を起動し、システムにログインします。

システムが正常に動作していることを確認したら、 Red Hat Enterprise Linux 7.x システムから Unified Manager を削除できます。

- 同じサーバ上のホスト OS のアップグレード *

Red Hat Enterprise Linux 8.x ソフトウェアをインストールできるスペアシステムがない場合は、次の手順に従います。

1. Web UIの管理メニューで、Unified Managerのバックアップを作成し、バックアップファイルをコピーします (.7z ファイル) とデータベースリポジトリディレクトリの内容 (/database-dumps-repo サブディレクトリ) を外部の場所に追加します。
2. システムから Red Hat Enterprise Linux 7.x イメージを削除し、システムを完全に消去します。
3. 同じシステムに Red Hat Enterprise Linux 8.x ソフトウェアをインストールして設定します。

を参照してください "[Linux ソフトウェアとインストールの要件](#)".

4. Red Hat Enterprise Linux 8.x システムには、以前の Red Hat Enterprise Linux 7.x システムと同じバージョンの Unified Manager ソフトウェアをインストールします。

を参照してください "[LinuxへのUnified Managerのインストール](#)".

インストールが完了しても、UI を起動したり、クラスタ、ユーザ、または認証設定を設定したりしないでください。この情報は、リストアプロセスでバックアップファイルに取り込まれます。

5. バックアップファイルをコピーします (.7z ファイル) を外部の場所からにコピーします
/opt/netapp/data/ocum-backup/ およびにデータベースリポジトリファイルを追加します
/database-dumps-repo のサブディレクトリ /ocum-backup ディレクトリ。
6. 次のコマンドを入力して、バックアップファイルから Unified Manager データベースをリストアします。

```
um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
```

7. Web ブラウザに IP アドレスまたは URL を入力して Unified Manager Web UI を起動し、システムにログインします。

Unified Manager のインストール後にサードパーティ製品をアップグレードする

JRE などのサードパーティ製品が Linux システムにすでにインストールされている場合は、それらの製品をアップグレードできます。

これらのサードパーティ製品を開発する企業は、定期的にセキュリティの脆弱性を報告しています。このソフトウェアの新しいバージョンには、独自のスケジュールでアップグレードできます。

Linux での OpenJDK のアップグレード

Unified Manager がインストールされている Linux サーバで OpenJDK を新しいバージョンにアップグレードすることで、セキュリティの脆弱性に対する修正を入手できます。

- 必要なもの *

Unified Manager がインストールされている Linux システムに対する root 権限が必要です。

OpenJDK のリリースはリリースファミリー内で更新できます。たとえば、OpenJDK 11.0.14からOpenJDK 11.0.17にアップグレードできますが、OpenJDK 11からOpenJDK 12に直接更新することはできません。

手順

1. Unified Manager ホストマシンに root ユーザとしてログインします。
2. 適切なバージョンの OpenJDK （64 ビット）をターゲットシステムにダウンロードします。
3. Unified Manager のサービスを停止します。

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

4. システムに最新の OpenJDK をインストールします。
5. Unified Manager のサービスを開始します。

```
systemctl start ocie
```

```
systemctl start ocieau
```

Unified Manager を再開しています

設定を変更した場合、Unified Manager の再起動が必要になることがあります。

- 必要なもの *

Unified Manager がインストールされている Red Hat Enterprise Linux サーバまたは CentOS サーバへの root ユーザーアクセスが必要です。

手順

1. Unified Manager サービスを再起動するサーバに root ユーザーとしてログインします。
2. Unified Manager サービスと関連する MySQL ソフトウェアを次の順序で停止します。

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

```
systemctl stop mysqld
```

3. Unified Manager を次の順序で開始します。

```
systemctl start mysqld
```

```
systemctl start ocie
```

```
systemctl start ocieau
```



mysqld は、MySQLサーバの起動と停止に必要なデーモンプログラムです。

Unified Manager を削除しています

Unified Manager は、1つのコマンドで Red Hat Enterprise Linux ホストまたは CentOS ホストから停止してアンインストールできます。

- 必要なもの *
- Unified Manager を削除するサーバへの root ユーザーアクセスが必要です。
- LinuxシステムでSecurity-Enhanced Linux (SELinux) を無効にしておく必要があります。を使用して、SELinuxランタイムモードを「permissive」に変更します `setenforce 0` コマンドを実行します
- ソフトウェアを削除する前に、Unified Manager サーバからすべてのクラスタ（データソース）を削除しておく必要があります。
- MySQLポート3306を許可またはブロックするために作成されたファイアウォールルールは手動で削除する必要があります。ファイアウォールルールは自動的に削除されません。

手順

1. Unified Manager を削除するサーバに root ユーザーとしてログインします。
2. Unified Manager を停止してサーバから削除します。

```
rpm -e netapp-um
```

これにより、関連付けられているネットアップの RPM パッケージがすべて削除されます。Java、MySQL、p7zip など、前提条件のソフトウェアモジュールは削除されません。

3. * オプション：必要に応じて、Java、MySQL、p7zip などのサポートソフトウェアモジュールを削除します。

```
rpm -e p7zip mysql-community-client mysql-community-server mysql-community-common mysql-community-libs java-x.y
```

この処理が完了すると、ソフトウェアは削除されます。からのすべてのデータ /opt/netapp/data ディレクトリがに移動されます /opt/netapp/data/BACKUP アンインストール後のフォルダ。Unified Manager をアンインストールすると、Java パッケージと MySQL パッケージも削除されます。ただし、パッケージが必要でシステム上の他のアプリケーションで使用されている場合は除きます。ただし、MySQL のデータは削除されません。

カスタムの **umadmin** ユーザと **maintenance** グループを削除します

Unified Manager をインストールする前にカスタムのホームディレクトリを作成して独自の **umadmin** ユーザと **maintenance** アカウントを定義していた場合は、Unified Manager のアンインストール後にそれらを削除する必要があります。

Unified Manager の標準のアンインストール手順では、カスタムの **umadmin** ユーザと **maintenance** アカウントは削除されません。これらの項目は手動で削除する必要があります。

手順

1. Red Hat Enterprise Linux サーバに root ユーザとしてログインします。
2. **umadmin** ユーザを削除します。

```
userdel umadmin
```

3. **maintenance** グループを削除します。

```
groupdel maintenance
```

Windows システムに Unified Manager をインストールする

Active IQ Unified Manager の概要

Active IQ Unified Manager（旧 OnCommand Unified Manager）を使用すると、ONTAP ストレージシステムの健全性とパフォーマンスを 1 つのインターフェイスから監視および管理できます。Unified Manager は、Linux サーバや Windows サーバに導入できるほか、VMware ホストに仮想アプライアンスとして導入することもできます。

インストールの完了後、管理対象のクラスタを追加すると、Unified Manager のグラフィカルインターフェイスに、監視対象ストレージシステムの容量、可用性、保護、パフォーマンスのステータスが表示されます。

- 関連情報 *

["NetApp Interoperability Matrix Tool で確認できます"](#)

Unified Manager サーバの機能

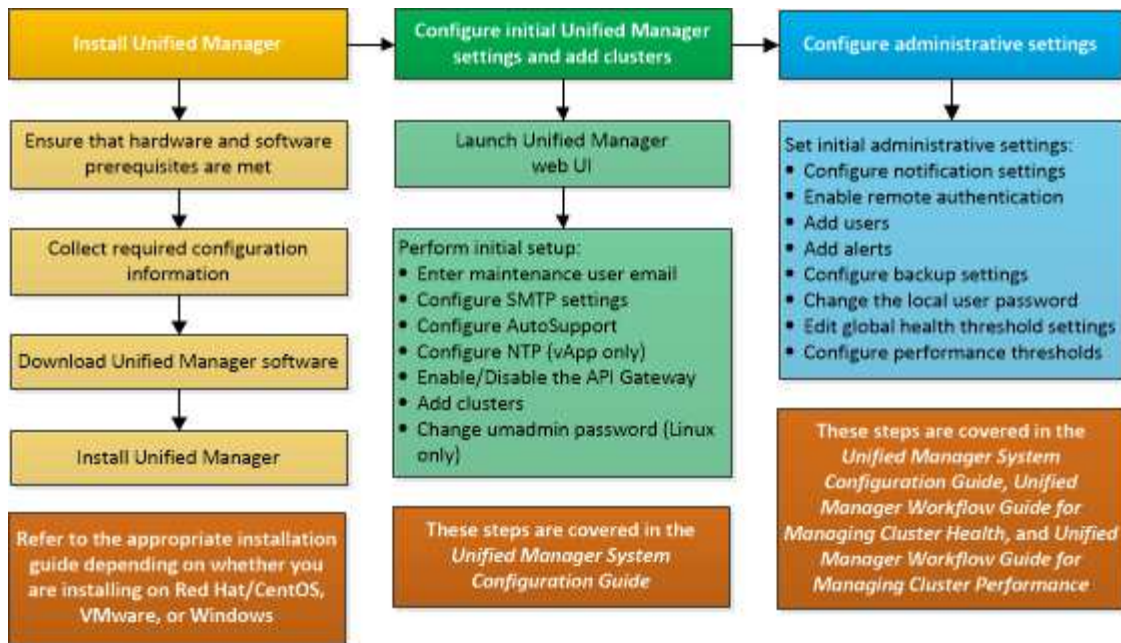
Unified Manager サーバインフラは、データ収集ユニット、データベース、アプリケーションサーバで構成され、検出、監視、ロールベースアクセス制御（RBAC）、監査、ロギングなどのインフラサービスを提供します。

Unified Manager は、クラスタの情報を収集してデータベースにデータを格納し、そのデータを分析してクラスタに問題がないかどうかを確認します。

インストール手順の概要

以下は、Unified Manager を使用する前に必要なインストール作業のワークフローです。

ここでは、次のワークフローに示されている各項目について説明します。



Unified Manager をインストールするための要件

インストールプロセスを開始する前に、Unified Manager をインストールするサーバがソフトウェア、ハードウェア、CPU、およびメモリの所定の要件を満たしていることを確認してください。

ネットアップは、Unified Manager アプリケーションコードの変更をサポートしていません。Unified Manager サーバにセキュリティ対策を適用する必要がある場合は、Unified Manager がインストールされているオペレーティングシステムに変更を加える必要があります。

Unified Manager サーバへのセキュリティ対策の適用の詳細については、ナレッジベースの記事を参照してください。

["Data ONTAP for clustered Active IQ Unified Manager に適用されるセキュリティ対策のサポート性"](#)

- 関連情報 *

["NetApp Interoperability Matrix Tool で確認できます"](#)

仮想インフラおよびハードウェアシステムの要件

仮想インフラまたは物理システムに Unified Manager をインストールする場合、メモリ、CPU、およびディスクスペースの最小要件を満たす必要があります。

次の表に、メモリ、CPU、およびディスクスペースの各リソースについて、推奨される値を示します。これらは、Unified Manager が許容されるパフォーマンスレベルを達成することが確認されている値です。

ハードウェア構成	推奨設定
RAM	12GB （最小要件は 8GB ）

ハードウェア構成	推奨設定
プロセッサ	CPU × 4
CPU サイクル容量	合計 9572MHz（最小要件は 9572MHz）
空きディスク容量	150GB。割り当ては次のとおりです。 <ul style="list-style-type: none"> • 100GB - インストールディレクトリ用 • 50GB の MySQL データディレクトリ用ディスクスペースが必要です

Unified Manager はメモリの少ないシステムにもインストールできますが、推奨される 12GB の RAM があれば最適なパフォーマンスが保証されるだけでなく、拡張時にクラスタやストレージオブジェクトの追加にも対応できます。Unified Manager を導入する VM にはメモリの上限などを設定しないでください。また、ソフトウェアがシステムで割り当てられているメモリを利用できなくなる機能（バルーニングなど）は有効にしないでください。

また、1 つの Unified Manager インスタンスで監視できるノードの数には上限があり、この上限を超える場合は 2 つ目の Unified Manager インスタンスをインストールする必要があります。詳細については、[_ ベストプラクティスガイド _](#) を参照してください。

"テクニカルレポート 4621：『Unified Manager Best Practices Guide』"

メモリページのスワッピングは、システムや管理アプリケーションのパフォーマンスに悪影響を及ぼします。CPU リソースがホスト全体で競合して使用できなくなると、パフォーマンスが低下する可能性があります。

専用使用の要件

Unified Manager をインストールする物理システムまたは仮想システムは、他のアプリケーションとは共有せず、Unified Manager 専用にする必要があります。他のアプリケーションにシステムリソースが消費されることで、Unified Manager のパフォーマンスが大幅に低下する可能性があります。

バックアップ用のスペース要件

Unified Manager のバックアップとリストア機能を使用する場合は、「data」ディレクトリまたはディスクに 150GB のスペースがあるように追加の容量を割り当ててください。バックアップはローカルにもリモートにも保存できますが、Unified Manager ホストシステムとは別の、150GB 以上のスペースがあるリモートの場所に保存することを推奨します。

ホスト接続の要件

Unified Manager をインストールする物理システムまたは仮想システムは、問題なく設定できるように設定する必要があります ping ホスト自体のホスト名です。IPv6 構成の場合は、確認する必要があります ping6 これで Unified Manager を正しくインストールできるようになります。

製品の Web UI には、ホスト名（またはホストの IP アドレス）を使用してアクセスできます。導入時に静的 IP アドレスを使用してネットワークを設定した場合は、指定したネットワークホストの名前を使用します。DHCP を使用してネットワークを設定した場合は、DNS からホスト名を取得します。

完全修飾ドメイン名（FQDN）または IP アドレスの代わりに短縮名を使用した Unified Manager へのアクセスをユーザに許可する場合は、短縮名が有効な FQDN に解決されるようにネットワークを設定する必要があります。

Windows ソフトウェアとインストールの要件

Unified Manager を Windows に正しくインストールするには、Unified Manager をインストールするシステムがソフトウェアの要件を満たしている必要があります。

オペレーティングシステムソフトウェア

Unified Managerは次のエディションのWindowsにインストールできます。

- Microsoft Windows Server 2019 Standard EditionおよびDatacenter Edition
- Microsoft Windows Server 2022 Standard EditionおよびDatacenter Edition

Unified Manager は、以下の言語で 64 ビットの Windows オペレーティングシステムでサポートされています。

- 英語
- 日本語
- 簡体字中国語

サポートされている Windows のバージョンの最新のリストについては、Interoperability Matrix を参照してください。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)



ネットアップは、Microsoft System Center Configuration Manager（SCCM）などのサードパーティツールを使用したUnified Managerのインストールをサポートしていません。

Unified Manager のみを実行する専用のサーバを用意する必要があります。他のアプリケーションをサーバにインストールしないでください。企業の規制により、アクティブなアンチウイルスソフトウェアがWindowsシステムにインストールされている可能性があります。インストールが失敗しないように、Unified Managerをインストールする前にウィルス対策ソフトウェアを無効にする必要があります。

サードパーティ製ソフトウェア

Unified Manager にバンドルされているサードパーティパッケージを次に示します。これらのサードパーティパッケージがシステムにインストールされていない場合、Unified Manager のインストール時にインストールされます。

- Microsoft Visual C++2015 再頒布可能パッケージバージョン 14.26.28720.3
- Visual Studio 2013 バージョン 12.0.40660.0 の Microsoft Visual C++ 再頒布可能パッケージ
- MySQL Community Editionバージョン8.0.30
- Python 3.11.1
- OpenJDKバージョン11.0.16

- p7zip バージョン 18.05 以降



Unified Manager 9.5 以降、OpenJDK は Unified Manager のインストールパッケージに含まれており、自動的にインストールされます。Unified Manager 9.5 以降では Oracle Java はサポートされません。

MySQL がインストールされている場合は、次の点を確認してください。

- デフォルトのポートを使用している。
- サンプルデータベースがインストールされていません。
- サービス名は「MySQL8」です。

Unified Manager は WildFly Web サーバに導入されます。WildFly 19.0.0 が Unified Manager にバンドルされて構成されています。



サードパーティ製ソフトウェアをアップグレードする前に、Unified Manager の実行中のインスタンスをシャットダウンする必要があります。サードパーティ製ソフトウェアのインストールが完了したら、Unified Manager を再起動できます。

インストールの要件

- Microsoft .NET 4.5.2 以降がインストールされている必要があります。
- 。temp インストールファイルを展開するために、ディレクトリには2GBのディスクスペースを設定する必要があります。ディレクトリが作成されたかどうかを確認するには、コマンドラインインターフェイスで次のコマンドを実行します。echo %temp%
- Unified Manager の MSI ファイルのキャッシュ用に、Windows ドライブに 2GB のディスクスペースを確保しておく必要があります。
- Unified ManagerをインストールするMicrosoft Windows Serverの完全修飾ドメイン名（FQDN）を設定し ping ホスト名とFQDNへの応答が完了しました。
- Microsoft IIS World Wide Web Publishing サービスを無効にして、ポート 80 および 443 が空いていることを確認する必要があります。
- インストール中は、「Windows Installer RDS Compatibility」のリモートデスクトップセッションホスト設定が無効になっていることを確認してください。
- UDP ポート 514 を他のサービスで使用されないように空けておく必要があります。
- Unified Managerをインストールする前に、システムのすべてのウィルス対策ソフトウェアを無効にする必要があります。インストールが完了したら、次のパスをウィルス対策スキャンから手動で除外してください。
 - Unified Managerデータディレクトリ。例：C:\ProgramData\NetApp\OnCommandAppData\
 - Unified Managerのインストールディレクトリ。例：\C:\Program Files\NetApp\
 - MySQLのデータディレクトリ。例：C:\ProgramData\MySQL\MySQLServerData

サポートされているブラウザ

Unified Manager Web UI にアクセスするには、サポートされているブラウザを使用しま

す。

サポートされているブラウザとバージョンは Interoperability Matrix で確認できます。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

すべてのブラウザで、ポップアップブロックを無効にすることでソフトウェアの機能が正しく表示されます。

アイデンティティプロバイダ（IdP）でユーザを認証できるように Unified Manager で SAML 認証を設定する場合は、IdP でサポートされるブラウザのリストも確認してください。

プロトコルとポートの要件

このポートとプロトコルを使用して、Unified Manager サーバは管理対象のストレージシステム、サーバ、その他のコンポーネントと通信します。

Unified Manager サーバへの接続

通常的环境では、Unified Manager Web UI への接続に常にデフォルトのポートが使用されるため、ポート番号を指定する必要はありません。たとえば、Unified Managerは常にデフォルトのポートで実行されるため、と入力できます `https://<host>` ではなく `https://<host>:443`。

Unified Manager サーバでは、次のインターフェイスにアクセスする際に特定のプロトコルを使用します。

インターフェイス	プロトコル	ポート	説明
Unified Manager Web UI	HTTP	80	Unified Manager Web UI へのアクセスに使用され、自動的にセキュアポート 443 にリダイレクトされます。
Unified Manager Web UI および API を使用するプログラム	HTTPS	443	Unified Manager Web UI へのセキュアなアクセスと API 呼び出しに使用されます。API 呼び出しは HTTPS でしか実行できません。
メンテナンスコンソール	SSH/SFTP	22	メンテナンスコンソールにアクセスしてサポートバンドルを取得する際に使用されます。
Linux コマンドライン	SSH/SFTP	22	Red Hat Enterprise Linux または CentOS のコマンドラインにアクセスしてサポートバンドルを取得する際に使用されます。

インターフェイス	プロトコル	ポート	説明
syslog	UDP	514	ONTAP システムからのサブスクリプションベースの EMS メッセージにアクセスし、メッセージに基づいてイベントを作成する際に使用されます。
REST	HTTPS	ポート 1	認証された ONTAP システムからの REST API ベースのリアルタイムの EMS イベントにアクセスする際に使用されます。
MySQL データベース	MySQL	3306	OnCommand および OnCommand Workflow Automation API サービスから Unified Manager へのアクセスに使用されます。



MySQLのデフォルトポート3306は、WindowsシステムにUnified Managerをインストールする際にlocalhostにのみ使用できます。これは、前の構成を維持したままのアップグレードシナリオには影響しません。この設定は変更可能で、を使用して他のホストから接続を利用できるようにすることができます Control access to MySQL port 3306 メンテナンスコンソールのオプション。詳細については、を参照してください ["その他のメニューオプション"](#)。HTTP 通信と HTTPS 通信に使用されるポート（ポート 80 と 443）は、Unified Manager メンテナンスコンソールを使用して変更できます。詳細については、を参照してください ["Active IQ Unified Manager を設定しています"](#)。

Unified Manager サーバからの接続

ファイアウォールの設定で、Unified Manager サーバと管理対象のストレージシステム、サーバ、その他のコンポーネントの間の通信に使用するポートを開くように設定する必要があります。ポートが開いていない場合、通信は失敗します。

環境に応じて、Unified Manager サーバから特定の接続先への接続に使用するポートとプロトコルを変更することもできます。

Unified Manager サーバは、次のプロトコルとポートを使用して、管理対象のストレージシステム、サーバ、その他のコンポーネントに接続します。

宛先	プロトコル	ポート	説明
ストレージシステム	HTTPS	443 tcp	ストレージシステムの監視と管理に使用されます。

宛先	プロトコル	ポート	説明
ストレージシステム	NDMP	10000 TCP	特定の Snapshot リストア処理に使用されます。
AutoSupport サーバ	HTTPS	443	AutoSupport 情報の送信に使用されます。この機能を実行するには、インターネットアクセスが必要です。
認証サーバ	LDAP	389	認証要求、およびユーザとグループの検索要求に使用されます。
LDAPS	636	セキュアな LDAP 通信に使用されます。	メールサーバ
SMTP	25	アラート通知 E メールを送信に使用されます。	SNMP トラップの送信元
SNMPv1 または SNMPv3	162 UDP	アラート通知 SNMP トラップの送信に使用されます	外部データプロバイダのサーバ
TCP	2003 年	Graphite などの外部データプロバイダにパフォーマンスデータを送信します。	NTP サーバ

ワークシートへの記入

Unified Manager をインストールして設定する前に、環境に関する特定の情報を確認しておく必要があります。この情報はワークシートに記録できます。

Unified Manager のインストール情報

Unified Manager をインストールする際に必要な情報を記入します。

ソフトウェアが導入されているシステム	あなたの価値
ホストの完全修飾ドメイン名	
ホストの IP アドレス	
ネットワークマスク	

ソフトウェアが導入されているシステム	あなたの価値
ゲートウェイの IP アドレス	
プライマリ DNS アドレス	
セカンダリ DNS アドレス	
検索ドメイン	
メンテナンスユーザのユーザ名	
メンテナンスユーザのパスワード	

Unified Manager の設定情報

インストール後に Unified Manager を設定するための情報を記入します。設定によっては省略可能な値もあります。

設定	あなたの価値
メンテナンスユーザの E メールアドレス	
SMTP サーバのホスト名または IP アドレス	
SMTP ユーザ名	
SMTP パスワード	
SMTP ポート	25 (デフォルト値)
アラート通知の送信元 E メールアドレス	
認証サーバのホスト名または IP アドレス	
Active Directory の管理者名または LDAP のバインド識別名	
Active Directory のパスワードまたは LDAP のバインドパスワード	
認証サーバのベース識別名	
アイデンティティプロバイダ (IdP) の URL	

設定	あなたの価値
アイデンティティプロバイダ（IdP）のメタデータ	
SNMP トラップの送信先ホストの IP アドレス	
SNMP ポート	

クラスタ情報

Unified Manager を使用して管理するストレージシステムの情報を記入します。

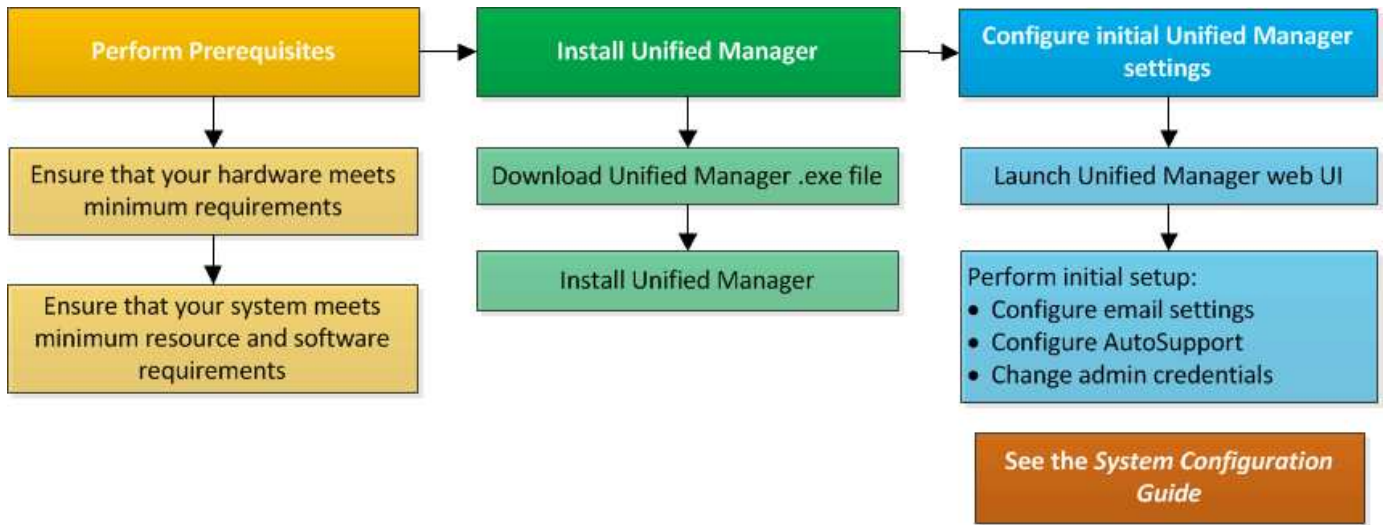
クラスタ 1 / N	あなたの価値
ホスト名またはクラスタ管理 IP アドレス	
ONTAP 管理者のユーザ名  管理者には「admin」ロールが割り当てられている必要があります。	
ONTAP 管理者のパスワード	
プロトコル	HTTPS

Unified Manager ソフトウェアのインストール、アップグレード、削除を行います

Unified Managerのインストール、新しいバージョンへのアップグレード、またはUnified Managerアプリケーションの削除を実行できます。

インストールプロセスの概要

以下は、Unified Manager を使用する前に必要なインストール作業のワークフローです。



Windows への Unified Manager のインストール

Windows で Unified Manager をダウンロードしてインストールする一連の手順を理解することが重要です。

Unified Manager をインストールしています

Unified Manager をインストールすることで、データストレージの容量、可用性、パフォーマンス、保護の問題を監視してトラブルシューティングすることができます。

- 必要なもの *
- Unified Manager をインストールするシステムがシステムおよびソフトウェアの要件を満たしている必要があります。

を参照してください "[ハードウェアシステムの要件](#)".

を参照してください "[Windows ソフトウェアとインストールの要件](#)".



Unified Manager 9.5 以降、OpenJDK はインストールパッケージに含まれており、自動的にインストールされます。Unified Manager 9.5 以降では Oracle Java はサポートされません。

- Windows の管理者権限が必要です。ユーザ名の先頭に感嘆符が付いていないことを確認してください!'. Installation of Unified Manager might fail if the user name of user running the installation begins with '!'.
- サポートされている Web ブラウザを用意しておきます。
- Unified Manager のメンテナンスユーザのパスワードは 8~20 文字で指定し、アルファベットの大文字または小文字、数字、および特殊文字を含める必要があります。
- メンテナンスユーザまたは MySQL の root ユーザのパスワードに次の特殊文字は使用できません。"'%、=<>|^\\|/ () [] ; :

次の特殊文字を使用できます。~ ! @ # \$ * - ? . [+]

1. デフォルトのローカル管理者アカウントで Windows にログインします。
2. NetApp Support Siteにログインし、 Unified Manager のダウンロードページに移動します。

"NetApp Support Site"

3. 必要なバージョンの Unified Manager を選択し、エンドユーザライセンス契約（EULA）に同意します。
4. Unified Manager Windows インストールファイルを Windows システムのターゲットディレクトリにダウンロードします。
5. インストールファイルが保存されているディレクトリに移動します。
6. Unified Manager インストーラの実行ファイル（.exe ファイル）を右クリックし、管理者として実行します。

Unified Manager により、不足しているサードパーティパッケージとインストールされているパッケージが検出されて表示されます。必要なサードパーティパッケージがシステムにインストールされていない場合、Unified Manager のインストール時にインストールされます。

7. 「* 次へ *」をクリックします。
8. ユーザ名とパスワードを入力してメンテナンスユーザを作成します。
9. データベース接続ウィザードで、MySQL の root パスワードを入力します。
10. [* 変更 *] をクリックして、Unified Manager のインストールディレクトリと MySQL のデータディレクトリの新しい場所を指定します。

インストールディレクトリを変更しない場合は、デフォルトのインストールディレクトリに Unified Manager がインストールされます。

11. 「* 次へ *」をクリックします。
12. Ready to Install Shield ウィザードで、* Install * をクリックします。
13. インストールが完了したら、「* 完了 *」をクリックします。
14. アクティブなアンチウイルスソフトウェアがWindowsシステムにインストールされている場合は、インストールの完了後にアンチウイルススキャンから次のパスを手動で除外します。

- Unified Manager データディレクトリ
- Unified Manager インストールディレクトリ
- MySQL データディレクトリ

インストールによって、複数のディレクトリが作成されます。

• インストールディレクトリ

インストール時に指定した Unified Manager のルートディレクトリです。例 C:\Program Files\NetApp\

• MySQL データディレクトリ

インストール時に指定した MySQL データベースの格納先ディレクトリです。例 C:\ProgramData\MySQL\MySQLServerData\

- Java ディレクトリ

OpenJDK がインストールされるディレクトリです。例 C:\Program Files\NetApp\JDK\

- Unified Manager のアプリケーションデータディレクトリ（ appDataDir ）

アプリケーションで生成されるすべてのデータが格納されるディレクトリです。ログ、サポートバンドル、バックアップなど、その他のすべてのデータが含まれます。例

C:\ProgramData\NetApp\OnCommandAppData\

Web UI にアクセスして Unified Manager の初期セットアップを実行できます。手順については、を参照してください ["Active IQ Unified Manager を設定しています"](#)。

Unified Manager の無人インストールを実行する

コマンドラインインターフェイスを使用して、手動操作なしで Unified Manager をインストールできます。無人インストールを実行するには、キーと値のペアの形式でパラメータを渡します。

手順

1. デフォルトのローカル管理者アカウントで Windows のコマンドラインインターフェイスにログインします。
2. Unified Manager をインストールする場所に移動し、次のいずれかを実行します。

オプション	手順
サードパーティパッケージが事前にインストールされている場合	<pre>ActiveIQUnifiedManager-x.y.exe /v"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_passw ord MAINTENANCE_USERNAME=maintenance_usern ame /qn /l*v CompletePathForLogFile"</pre> <p>• 例： *</p> <pre>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:\ProgramData\MySQL\ MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qn /l*v C:\install.log"</pre>

オプション	手順
サードパーティパッケージがインストールされていない場合	<pre>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR="Installation directory\" MYSQL_DATA_DIR="MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_passw ord MAINTENANCE_USERNAME=maintenance_usern ame /qr /l*v CompletePathForLogFile"</pre> <p>• 例： *</p> <pre>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR="C:\Program Files\NetApp\" MYSQL_DATA_DIR="C:\ProgramData\MYSQL\ MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qr /l*v C:\install.log"</pre>

。 /qr オプションを指定すると、ユーザインターフェイスが減少してQuietモードが有効になりますインストールの進捗を示す基本的なユーザインターフェイスが表示されます。入力を求められることはありません。JRE、MySQL、7zipなどのサードパーティパッケージが事前にインストールされていない場合は、を使用する必要があります /qr オプションがの場合、のインストールは失敗します /qn オプションは、サードパーティパッケージがインストールされていないサーバで使します。

。 /qn オプションを指定すると、ユーザインターフェイスのないQuietモードが有効になりますインストール中にユーザインターフェイスや詳細は表示されません。を使用しないでください /qn オプション：サードパーティパッケージがインストールされていない場合。

3. 次の URL を使用して Unified Manager Web ユーザインターフェイスにログインします。

`https://IP address`

JBoss パスワードを変更しています

インストール時に設定されたインスタンス固有の JBoss パスワードをリセットできます。このセキュリティ機能によって Unified Manager のインストール設定が上書きされてしまいます。必要に応じて、パスワードをリセットすることもできます。この処理を実行すると、MySQL へのアクセス時に JBoss で使用するパスワードも変更になります。

- 必要なもの *
- Unified Manager がインストールされている Windows システムに対する admin 権限が必要です。
- MySQL の root ユーザのパスワードが必要です。
- ネットアップが提供するサービスにアクセスできる必要があります password.bat ディレクトリ内のス

クリプト

C:\Program Files\NetApp\essentials\bin。

手順

1. Unified Manager ホストマシンに admin ユーザとしてログインします。
2. Windows サービスコンソールを使用して、次の Unified Manager サービスを停止します。
 - NetApp Active IQ 取得サービス (Ocie-au)
 - NetApp Active IQ 管理サーバサービス (Oncommandsvc)
3. を起動します password.bat パスワード変更プロセスを開始するスクリプト：

```
C:\Program Files\NetApp\essentials\bin> password.bat resetJBossPassword
```

4. プロンプトが表示されたら、MySQL root ユーザのパスワードを入力します。
5. プロンプトが表示されたら、新しい JBoss ユーザのパスワードを入力し、確認のためにもう一度入力します。

パスワードは 8~16 文字で指定し、数字、大文字、小文字、および次の特殊文字の少なくとも 1 文字を含める必要があります。

!@%^*-_=[]:<>./~/+

6. スクリプトが完了したら、Windows サービスコンソールを使用して Unified Manager サービスを開始します。
 - NetApp Active IQ 管理サーバサービス (Oncommandsvc)
 - NetApp Active IQ 取得サービス (Ocie-au)
7. すべてのサービスが開始されたら、Unified Manager UI にログインできます。

Unified Managerバージョンでサポートされているアップグレードパス

Active IQ Unified Manager では、バージョンごとに特定のアップグレードパスがサポートされます。

すべてのバージョンの Unified Manager で、新しいバージョンへのインプレースアップグレードを実行できるわけではありません。Unified Manager のアップグレードは N-2 モデルに限定されています。つまり、アップグレードはすべてのプラットフォームの次の 2 つのリリースでのみ実行できます。たとえば、Unified Manager 9.10 から Unified Manager 9.12 へのアップグレードは、Unified Manager 9.11 からのみ実行できます。

サポート対象よりも前のバージョンを実行している場合は、Unified Manager インスタンスをいずれかのサポート対象バージョンにアップグレードしてから、現在のバージョンにアップグレードする必要があります。

たとえば、インストールされているバージョンが OnCommand Unified Manager 9.5 であり、最新のリリース Active IQ Unified Manager 9.12 にアップグレードする場合は、一連のアップグレードを実行します。

アップグレードパスの例：

1. OnCommand Unified Manager 9.5 → Active IQ Unified Manager 9.7 をアップグレードします。

2. 9.7→9.9にアップグレードします。
3. 9.→9.11にアップグレードします。
4. 9.11 → 9.12にアップグレードします。

アップグレードパスマトリックスの詳細については、こちらを参照してください ["ナレッジベース \(KB\) の記事を参照してください"](#)。

Unified Manager をアップグレードする

WindowsプラットフォームでUnified Manager 9.10または9.11をダウンロードして実行すると、9.12にアップグレードできます。

- 必要なもの *
- Unified Manager をアップグレードするシステムがシステム要件とソフトウェア要件を満たしている必要があります。

を参照してください ["ハードウェアシステムの要件"](#)。

を参照してください ["Windows ソフトウェアとインストールの要件"](#)。



Unified Manager 9.5 以降、OpenJDK はインストールパッケージに含まれており、自動的にインストールされます。Unified Manager 9.5 以降では Oracle Java はサポートされません。



アップグレードを開始する前に、システムに Microsoft .NET 4.5.2 以上がインストールされていることを確認してください。

- MySQL Community Edition は、Unified Manager のアップグレード時に自動的にアップグレードされます。システムにインストールされているMySQLのバージョンが8.0.30より前の場合は、Unified Manager のアップグレードプロセスによってMySQLが8.0.30に自動的にアップグレードされます。旧バージョンのMySQLから8.0.30へのスタンドアロンアップグレードは実行しないでください。
- Windows の管理者権限が必要です。ユーザ名の先頭に感嘆符が付いていないことを確認してください!"". Installation of Unified Manager might fail if the user name of user running the installation begins with "!".
- NetApp Support Siteにログインするための有効なクレデンシャルが必要です。
- アップグレード中に問題が使用される場合にデータが失われないようにするために、Unified Manager マシンのバックアップを作成しておく必要があります。
- アップグレードを実行するための十分なディスクスペースが必要です。

インストールドライブに、データディレクトリのサイズよりも 2.5GB の使用可能なスペースが必要です。十分な空きスペースがないと、アップグレードが中止され、追加に必要なスペース量がエラーメッセージに表示されます。

- アップグレードの実行中に、パフォーマンスデータの保持期間について、以前のデフォルト設定である 13 カ月のままにするか 6 カ月に変更するかを確認するプロンプトが表示されることがあります。変更を確認すると、6 カ月を過ぎた過去のパフォーマンスデータはページされます。
- アップグレードする前に、<InstallDir>\JDK_and_MySQL Data Directory の開いているファイルまたはフォルダをすべて閉じてください。

- Windowsシステムにアクティブなウィルス対策ソフトウェアがインストールされている場合、Unified Managerのアップグレードが失敗することがあります。Unified Managerをアップグレードする前に、システムのウィルススキャンソフトウェアをすべて無効にする必要があります。

アップグレードプロセスの実行中は、Unified Manager を使用できなくなります。実行中の処理がある場合は、Unified Manager をアップグレードする前に完了しておいてください

Unified Manager を OnCommand Workflow Automation のインスタンスとペアにして使用している環境では、両方の製品のソフトウェアで新しいバージョンを利用できる場合、2つの製品間の接続を解除してから各製品をアップグレードし、アップグレードの実行後に Workflow Automation の接続を新たにセットアップする必要があります。いずれかの製品のみをアップグレードする場合は、アップグレード後に Workflow Automation にログインし、Unified Manager からデータを取得していることを確認します。

手順

1. NetApp Support Siteにログインし、Unified Manager のダウンロードページに移動します。

["NetApp Support Site"](#)。

2. 必要なバージョンの Unified Manager を選択し、エンドユーザライセンス契約（EULA）に同意します。
3. Unified Manager Windows インストールファイルを Windows システムのターゲットディレクトリにダウンロードします。
4. Unified Manager インストーラの実行ファイル（.exe ファイル）を右クリックし、管理者として実行します。

Unified Manager から次のメッセージが表示されます。

This setup will perform an upgrade of Unified Manager. Do you want to continue?

5. [はい] をクリックし、[次へ] をクリックします。
6. インストール時に設定した MySQL8 root パスワードを入力し、* Next * をクリックします。
7. サポートされているWebブラウザで新しいウィンドウでWeb UIを起動し、ログインしてアップグレード後のバージョンのUnified Managerを使用します。
8. Windowsシステムにアクティブなアンチウイルスソフトウェアがインストールされている場合は、アップグレードの完了後に、アンチウイルススキャンから次のパスを手動で除外してください。
 - Unified Manager データディレクトリ
 - Unified Manager インストールディレクトリ
 - MySQL データディレクトリ



Unified Managerのサイレントアップグレードを行う場合は、次のコマンドを実行します。
`ActiveIQUnifiedManager-<version>.exe /s /v"MYSQL_PASSWORD=<password>
/qn /l*v <system_drive>:\install.log"`

サードパーティ製品のアップグレード

JRE などのサードパーティ製品が Windows システムにインストールされている場合は、Unified Manager でそれらの製品をアップグレードできます。

これらのサードパーティ製品を開発する企業は、定期的にセキュリティの脆弱性を報告しています。このソフトウェアの新しいバージョンには、独自のスケジュールでアップグレードできます。

OpenJDK のアップグレード

Unified Manager がインストールされている Windows サーバで OpenJDK を新しいバージョンにアップグレードすることで、セキュリティの脆弱性に対する修正を入手できます。

- 必要なもの *

Unified Manager がインストールされている Windows システムに対する admin 権限が必要です。

OpenJDK のリリースはリリースファミリー内で更新できます。たとえば、OpenJDK 11.0.14からOpenJDK 11.0.16にアップグレードできますが、OpenJDK 11からOpenJDK 12に直接更新することはできません。

手順

1. Unified Manager ホストマシンに admin ユーザとしてログインします。
2. OpenJDK の適切なバージョン（64 ビット）をターゲットシステムにダウンロードします。

たとえば、をダウンロードします `openjdk-11_windows-x64_bin.zip` from <http://jdk.java.net/11/>。

3. Windows サービスコンソールを使用して、次の Unified Manager サービスを停止します。
 - NetApp Active IQ 取得サービス（Ocie-au）
 - NetApp Active IQ 管理サーバサービス（Oncommandsvc）
4. を展開します zip ファイル。
5. 作成されたからディレクトリとファイルをコピーします jdk ディレクトリ（例：jdk-11.0.16 Javaがインストールされている場所に移動します。例 C:\Program Files\NetApp\JDK\
6. Windows サービスコンソールを使用して Unified Manager サービスを開始します。
 - NetApp Active IQ 管理サーバサービス（Oncommandsvc）
 - NetApp Active IQ 取得サービス（Ocie-au）

Unified Manager を再開しています

設定を変更した場合、Unified Manager の再起動が必要になることがあります。

- 必要なもの *

Windows の管理者権限が必要です。

手順

1. デフォルトのローカル管理者アカウントで Windows にログインします。
2. Unified Manager のサービスを停止します。

方法	サービスを停止する順序
コマンドライン	a. <code>sc stop ocie-au</code> b. <code>sc stop Oncommandsvc</code>
Microsoft Service Manager の略	a. NetApp Active IQ 取得サービス (Ocic-au) b. NetApp Active IQ 管理サーバサービス (Oncommandsvc)

3. Unified Manager のサービスを開始します。

方法	サービスを開始する順序
コマンドライン	a. <code>sc start Oncommandsvc</code> b. <code>sc start ocie-au</code>
Microsoft Service Manager の略	a. NetApp Active IQ 管理サーバサービス (Oncommandsvc) b. NetApp Active IQ 取得サービス (Ocic-au)

Unified Manager をアンインストールしています

Unified Manager をアンインストールするには、プログラムと機能ウィザードを使用するか、コマンドラインインターフェイスから無人アンインストールを実行します。

- 必要なもの *
- Windows の管理者権限が必要です。
- ソフトウェアをアンインストールする前に、Unified Manager サーバからすべてのクラスタ（データソース）を削除しておく必要があります。
- MySQLポート3306を許可またはブロックするために作成されたファイアウォールルールは手動で削除する必要があります。ファイアウォールルールは自動的に削除されません。

手順

1. 次のいずれかを実行して Unified Manager をアンインストールします。
 - Unified Managerをプログラムと機能*ウィザードからアンインストールする場合は、次の手順を実行します。
 - i. [コントロールパネル > プログラムと機能 *] に移動します。
 - ii. Active IQ Unified Manager を選択し、* Uninstall * をクリックします。

- コマンドラインからUnified Managerをアンインストールする場合は、次の手順を実行します。

- i. 管理者権限でWindowsのコマンドラインにログインします。
- ii. Active IQ Unified Manager ディレクトリに移動し、次のコマンドを実行します。

```
msiexec /x {A78760DB-7EC0-4305-97DB-E4A89CDFF4E1} /qn /l*v  
%systemdrive%\UmUnInstall.log
```

サーバでユーザアカウント制御（UAC）が有効になっていて、ドメインユーザとしてログインしている場合は、コマンドラインによるアンインストールを実行する必要があります。

Unified Manager がシステムからアンインストールされます。

2. Unified Manager のアンインストール時に削除されない次のサードパーティパッケージとデータをアンインストールします。

- サードパーティパッケージ：JRE、MySQL、Microsoft Visual C# 43；2015再頒布可能パッケージ、Python、7zipで構成されます
- Unified Manager によって生成された MySQL のアプリケーションデータ
- アプリケーションログとアプリケーションデータディレクトリの内容

設定タスクと管理タスクを実行

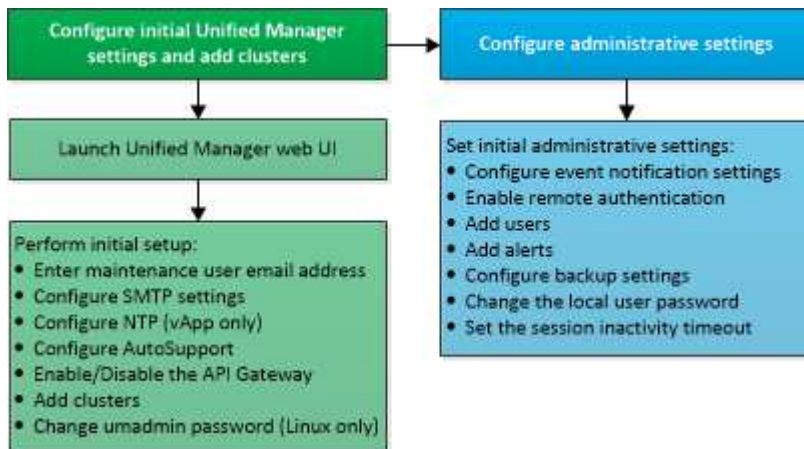
Active IQ Unified Manager を設定しています

Active IQ Unified Manager（旧 OnCommand Unified Manager）をインストールしたら、Web UI にアクセスするために初期セットアップ（初期設定ウィザード）を完了する必要があります。その後、クラスタの追加、リモート認証の設定、ユーザの追加、アラートの追加など、その他の設定作業を実行することができます。

このマニュアルに記載されている手順の一部は、Unified Manager インスタンスの初期セットアップを完了するための必須の手順です。その他の手順は、新しいインスタンスをセットアップする際に推奨される設定か、または ONTAP システムの定期的な監視を開始する前に把握しておくことが推奨される設定です。

設定手順の概要

以下は、Unified Manager を使用する前に必要な設定作業のワークフローです。



Unified Manager Web UI にアクセスします

Unified Manager をインストールしたら、ONTAP システムの監視を開始できるように、Web UI にアクセスして Unified Manager をセットアップします。

- 必要なもの *
- Web UI へのアクセスが初めての場合は、メンテナンスユーザ（Linux 環境の場合は umadmin ユーザ）としてログインする必要があります。
- 完全修飾ドメイン名（FQDN）または IP アドレスの代わりに短縮名を使用した Unified Manager へのアクセスをユーザに許可する場合は、短縮名が有効な FQDN に解決されるようにネットワークを設定する必要があります。
- 自己署名のデジタル証明書がサーバで使用されている場合、信頼されていない証明書であることを示す警告がブラウザ画面に表示されることがあります。リスクを承認してアクセスを続行するか、認証局（CA）の署名のあるデジタル証明書をインストールしてサーバを認証します。

手順

1. インストールの完了時に表示された URL を使用して、ブラウザから Unified Manager Web UI を起動します。URL は、Unified Manager サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）です。

リンクの形式は次のとおりです。https://URL。

2. メンテナンスユーザのクレデンシャルを使用して、Unified Manager Web UI にログインします。



1 時間以内に Web UI へのログインに 3 回連続して失敗すると、システムがロックアウトされ、システム管理者に連絡する必要があります。これはローカルユーザにのみ該当します。

Unified Manager Web UI の初期セットアップを実行する

Unified Manager を使用するには、NTP サーバ、メンテナンスユーザの E メールアドレス、SMTP サーバのホストなどを最初に設定し、ONTAP クラスタを追加する必要があります。

- 必要なもの *

次の作業を完了しておきます。

- インストールの完了時に表示された URL を使用して Unified Manager Web UI を起動します
- インストール時に作成したメンテナンスユーザ（Linux 環境の場合は umadmin ユーザ）の名前とパスワードを使用してログインします

Active IQ Unified Manager の Getting Started ページは、最初に Web UI にアクセスしたときにのみ表示されます。次のページは、VMware 環境の場合のものです。

≡

Active IQ Unified Manager

All ▾

Search All Storage Objects and Actions 🔍

Getting Started

1

2

3

4

5

EmailAutoSupportAPI GatewayAdd ONTAP ClustersFinish

Notifications

Configure your email server for assistance in case you forget your password.

Maintenance User Email

Emailmgo@eng.netapp.com

SMTP Server

Host Name or IP Addressemail.eng.netapp.com

Port25

User Nameadmin

Password

☐ Use STARTTLS ⓘ ☐ Use SSL ⓘ

Continue

これらのオプションをあとから変更する場合は、Unified Manager の左側のナビゲーションペインで一般オプションから選択できます。NTP 設定は VMware 専用です。この設定はあとから Unified Manager メンテナンスコンソールを使用して変更できます。

手順

1. Active IQ Unified Manager の初期セットアップページで、メンテナンスユーザの E メールアドレス、SMTP サーバのホスト名とその他の SMTP オプション、および NTP サーバ（VMware の場合のみ）を入力します。[* Continue （続行）] をクリックします。



[**Use STARTTLS ***]または[**Use SSL ***]オプションを選択した場合は、[**Continue**]ボタンをクリックすると証明書ページが表示されます。証明書の詳細を確認し、証明書を受け入れて、Web UIの初期セットアップ設定を続行します。

2. AutoSupport ページで「* Agree and Continue」をクリックして、Unified Manager から NetAppActive IQ への AutoSupport メッセージの送信を有効にします。

AutoSupport コンテンツの送信用にインターネットアクセスを提供するためにプロキシを指定する必要がある場合や、AutoSupport を無効にする場合は、Web UI から「* General * > * AutoSupport *」オプション

ョンを使用します。

3. Red HatおよびCentOSのシステムの場合、umadminユーザのパスワードをデフォルトの「admin」から独自のパスワードに変更します。
4. API ゲートウェイのセットアップページで、ONTAP REST API を使用して監視する ONTAP クラスタを Unified Manager で管理できるようにする API ゲートウェイ機能を使用するかどうかを選択します。[* Continue (続行)] をクリックします。

この設定は、Web UI の * General * > * Feature Settings * > * API Gateway * で後から有効または無効にできます。APIの詳細については、を参照してください ["Active IQ Unified Manager REST APIの使用を開始する"](#)。

5. Unified Manager で管理するクラスタを追加し、* Next * をクリックします。管理するクラスタごとに、ホスト名またはクラスタ管理 IP アドレス（IPv4 または IPv6）、ユーザ名およびパスワードクレデンシャルが必要です。ユーザには「admin」ロールが必要です。

この手順はオプションです。クラスタは、Web UI の * Storage Management * > * Cluster Setup * からあとから追加できます。

6. [概要] ページで、すべての設定が正しいことを確認し、[完了 *] をクリックします。

Getting Started ページが閉じ、Unified Manager の Dashboard ページが表示されます。

クラスタを追加する

Active IQ Unified Manager にクラスタを追加して監視することができます。たとえば、クラスタの健全性、容量、パフォーマンス、構成などの情報を取得して、発生する可能性がある問題を特定して解決できるようにすることができます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- 次の情報が必要です。

- ホスト名またはクラスタ管理 IP アドレス

ホスト名は、Unified Manager がクラスタへの接続に使用する FQDN または短縮名です。ホスト名は、クラスタ管理 IP アドレスに解決できる必要があります。

クラスタ管理 IP アドレスは、管理用 Storage Virtual Machine（SVM）のクラスタ管理 LIF である必要があります。ノード管理 LIF を使用すると処理に失敗します。

- クラスタで ONTAP バージョン 9.1 以降が実行されている必要があります。
- ONTAP 管理者のユーザ名とパスワード

このアカウントには、アプリケーションアクセスが _ontapi、console、および _http_ に設定された _admin_role_ が必要です。

- HTTPS プロトコルを使用してクラスタに接続するポート番号（通常はポート 443）
- 必要な証明書をを用意しておきます。Unified Managerでクラスタの追加時にセキュリティ証明書がインストールされます。

サーバ証明書：この証明書はUnified Managerが所有しています。デフォルトの自己署名SSL（HTTPS）証明書が生成され、Unified Managerの新規インストールが実行されます。セキュリティを強化するために、CA署名証明書にアップグレードすることを推奨します。サーバ証明書の有効期限が切れた場合は、再生成してUnified Managerを再起動し、サービスに新しい証明書を組み込む必要があります。SSL証明書の再生成の詳細については、を参照してください ["HTTPS セキュリティ証明書の生成"](#)。

相互TLS通信証明書：Unified ManagerとONTAP 間の相互TLS通信で使用されます。証明書ベースの認証は、ONTAP のバージョンに基づいてクラスタで有効になります。ONTAP バージョン9.5よりも前のバージョンを実行しているクラスタでは、証明書ベースの認証が有効になっていません。

古いバージョンのUnified ManagerをUnified Manager 9.12に更新する場合、クラスタの証明書ベースの認証は自動的に有効になりません。ただし、クラスタの詳細を変更して保存することで有効にできます。証明書の有効期限が切れた場合は、再生成して新しい証明書を組み込む必要があります。証明書の表示と再生成の詳細については、を参照してください ["クラスタを編集します"](#)。



- 証明書ベースの認証は、Web UIからクラスタを追加した場合に自動的に有効になります。メンテナンスコンソールからクラスタを追加した場合、証明書ベースの認証は有効になりません。
- クラスタで証明書ベースの認証が有効になっている場合に、Unified Managerのバックアップをサーバから作成し、ホスト名またはIPアドレスが変更された別のUnified Managerサーバにリストアすると、クラスタの監視が失敗することがあります。エラーを回避するには、クラスタの詳細を編集して保存します。クラスタの詳細の編集の詳細については、を参照してください ["クラスタを編集します"](#)。

+

クライアント証明書：ONTAP から受信したEMSメッセージの認証時に使用されます。この証明書はONTAP が所有しており、ONTAP クラスタをUnified Managerに追加する場合に必要です。有効期限が切れた証明書で Unified Manager にクラスタを追加することはできません。クライアント証明書の期限が切れている場合は、クラスタを追加する前に再生成する必要があります。ただし、追加済みのクラスタの証明書の有効期限が切れて Unified Manager で使用されている場合は、EMS メッセージが期限切れの証明書を使用して引き続き機能します。証明書の生成については、ナレッジベース（KB）の記事を参照してください ["System ManagerユーザインターフェイスでONTAP の自己署名証明書を更新する方法"](#)。

- Unified Manager サーバに十分なスペースが必要です。データベースディレクトリのスペースの使用率が90%を超えている場合、サーバにクラスタを追加することはできません。

MetroCluster 構成では、ローカルクラスタとリモートクラスタの両方を追加し、クラスタを正しく設定する必要があります。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Cluster Setup * をクリックします。
2. クラスタセットアップページで、* 追加 * をクリックします。
3. クラスタの追加ダイアログボックスで、クラスタのホスト名または IP アドレス、ユーザ名、パスワード、ポート番号など、必要な値を指定します。

クラスタ管理 IP アドレスは、IPv6 から IPv4 または IPv4 から IPv6 に変更できます。次の監視サイクルが完了すると、クラスタグリッドとクラスタ設定ページに新しい IP アドレスが反映されます。

4. [Submit（送信）] をクリックします。

5. [ホストの許可] ダイアログボックスで、[証明書の表示 *] をクリックして、クラスタに関する証明書情報を表示します。
6. 「* はい *」 をクリックします。

Unified Manager 9.12では、クラスタの詳細を保存したあと、クラスタの双方向TLS通信の証明書を確認できます。

証明書ベースの認証が有効になっていない場合、Unified Managerはクラスタが最初に追加されたときのみ証明書をチェックします。Unified Manager では、ONTAP に対する API 呼び出しごとには証明書がチェックされません。

新しいクラスタのオブジェクトがすべて検出されると、Unified Manager が過去 15 日間の履歴パフォーマンスデータの収集を開始します。これらの統計は、データの継続性収集機能を使用して収集されます。この機能では、クラスタが追加された直後から 2 週間分のクラスタのパフォーマンス情報を入手できます。データの継続性収集サイクルの完了後、デフォルトではクラスタのリアルタイムのパフォーマンスデータが 5 分ごとに収集されます。



15 日分のパフォーマンスデータを収集すると CPU に負荷がかかるため、新しいクラスタを複数追加する場合は、データの継続性収集のポーリングが同時に多数のクラスタで実行されないように、時間差をつけて追加するようにしてください。また、データの継続性収集期間に Unified Manager を再起動すると、収集が停止し、その間のデータがパフォーマンスチャートに表示されません。



エラーメッセージが表示されてクラスタを追加できない場合は、2 つのシステムのクロックが同期されておらず、Unified Manager の HTTPS 証明書の開始日がクラスタの日付よりもあとの日付になっていないかを確認してください。NTP などのサービスを使用してクロックを同期する必要があります。

• 関連情報 *

["CA 署名済みで返された HTTPS 証明書をインストールする"](#)

Unified Manager でアラート通知を送信するための設定

Unified Manager では、環境内のイベントについて警告する通知を送信するように設定することができます。通知を送信するには、Unified Manager のその他いくつかのオプションを設定する必要があります。

• 必要なもの *

アプリケーション管理者のロールが必要です。

Unified Manager を導入して初期設定を完了したら、イベントの受信に対してアラートをトリガーし、通知 E メールや SNMP トラップを生成するように環境を設定することを検討する必要があります。

手順

1. ["イベント通知を設定"](#)。

特定のイベントが発生したときにアラート通知を送信するには、SMTP サーバを設定し、アラート通知の送信元の E メールアドレスを指定する必要があります。SNMP トラップを使用する場合は、該当するオ

プシオンを選択し、必要な情報を指定します。

2. "リモート認証を有効にします"。

リモート LDAP ユーザまたは Active Directory ユーザが Unified Manager インスタンスにアクセスしてアラート通知を受信できるようにするには、リモート認証を有効にする必要があります。

3. "認証サーバを追加します"。

認証サーバを追加することで、認証サーバ内のリモートユーザが Unified Manager にアクセスできるようになります。

4. "ユーザを追加します"。

複数のタイプのローカルユーザまたはリモートユーザを追加し、特定のロールを割り当てることができます。アラートを作成する際に、アラート通知を受信するユーザを割り当てます。

5. "アラートを追加します"。

通知を送信する E メールアドレスの追加、通知を受信するユーザの追加、ネットワークの設定、環境に必要な SMTP オプションと SNMP オプションの設定が完了したら、アラートを割り当てることができます。

イベント通知を設定しています

Unified Manager では、イベントが生成されたときやユーザに割り当てられたときにアラート通知を送信するように設定することができます。アラートの送信に使用する SMTP サーバを設定したり、さまざまな通知メカニズムを設定したりできます。たとえば、アラート通知を E メールや SNMP トラップとして送信できます。

- 必要なもの *

次の情報が必要です。

- アラート通知の送信元 E メールアドレス

メール・アドレスは '送信されたアラート通知の送信元フィールドに表示されます何らかの理由で E メールを配信できない場合は、この E メールアドレスが配信不能メールの受信者としても使用されます。

- SMTP サーバのホスト名、およびサーバにアクセスするためのユーザ名とパスワード
- SNMP トラップと SNMP バージョン、アウトバウンドトラップポート、コミュニティ、およびその他の必要な SNMP 設定値を受信するトラップ送信先ホストのホスト名または IP アドレス

複数のトラップ送信先を指定するには、各ホストをカンマで区切ります。この場合、バージョンやアウトバウンドトラップポートなど、他の SNMP 設定はすべてリスト内のすべてのホストで同じでなければなりません。

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* 一般 * > * 通知 * をクリックします。
2. 通知ページで、適切な設定を行います。
 - 。注： *
 - 送信元アドレスに「 + ActiveIQUnifiedManager@localhost.com + 」というアドレスが事前に入力されている場合は、実際の作業用 E メールアドレスに変更して、すべての E メール通知が正常に配信されるようにしてください。
 - SMTP サーバのホスト名を解決できない場合は、SMTP サーバのホスト名の代わりに IP アドレス（IPv4 または IPv6）を指定できます。
3. [保存（ Save ）] をクリックします。
4. [*Use STARTTLS *]または[*Use SSL *]オプションを選択した場合は、[*Save]ボタンをクリックすると証明書ページが表示されます。証明書の詳細を確認し、証明書を受け入れて通知設定を保存します。

証明書の詳細を表示するには、[証明書の詳細を表示*]ボタンをクリックします。既存の証明書の有効期限が切れた場合は、「* STARTTLSを使用」または「* SSLを使用」チェックボックスをオフにし、通知設定を保存してから「* STARTTLSを使用*」または「SSLを使用*」チェックボックスを再度オンにして新しい証明書を表示します。

リモート認証の有効化

Unified Manager サーバが認証サーバと通信できるように、リモート認証を有効にすることができます。認証サーバのユーザが Unified Manager のグラフィカルインターフェイスにアクセスしてストレージオブジェクトとデータを管理できるようになります。

- 必要なもの *

アプリケーション管理者のロールが必要です。



Unified Manager サーバは認証サーバに直接接続する必要があります。SSSD（System Security Services Daemon）や NSLCD（Name Service LDAP Caching Daemon）などのローカルの LDAP クライアントは無効にする必要があります。

リモート認証は、Open LDAP または Active Directory のいずれかを使用して有効にすることができます。リモート認証が無効になっていると、リモートユーザは Unified Manager にアクセスできません。

リモート認証は、LDAP と LDAPS（セキュアな LDAP）でサポートされます。Unified Manager では、セキュアでない通信にはポート 389、セキュアな通信にはポート 636 がデフォルトのポートとして使用されます。



ユーザの認証に使用する証明書は、X.509 形式に準拠している必要があります。

手順

1. 左側のナビゲーションペインで、* 一般 * > * リモート認証 * をクリックします。
2. [Enable remote authentication...*] チェックボックスをオンにします。
3. [Authentication Service] フィールドで、サービスのタイプを選択し、認証サービスを設定します。

認証タイプ	入力する情報
Active Directory	<ul style="list-style-type: none"> • 認証サーバの管理者名。次のいずれかの形式で指定します。 <ul style="list-style-type: none"> ◦ domainname\username ◦ username@domainname ◦ Bind Distinguished Name（適切なLDAP表記を使用） • 管理者パスワード • ベース識別名（適切な LDAP 表記を使用）
LDAP を開きます	<ul style="list-style-type: none"> • バインド識別名（適切な LDAP 表記を使用） • バインドパスワード • ベース識別名

Active Directory ユーザの認証に時間がかかる場合やタイムアウトする場合は、認証サーバからの応答に時間がかかっている可能性があります。Unified Manager でネストされたグループのサポートを無効にすると、認証時間が短縮される可能性があります。

認証サーバに Secure Connection オプションを使用する場合、Unified Manager は Secure Sockets Layer（SSL）プロトコルを使用して認証サーバと通信します。

4. * オプション：* 認証サーバを追加し、認証をテストします。
5. [保存（Save）] をクリックします。

リモート認証でのネストされたグループの無効化

リモート認証を有効にしている場合、ネストされたグループの認証を無効にすることで、リモートからの Unified Manager への認証を個々のユーザにのみ許可し、グループのメンバーは認証されないようにすることができます。ネストされたグループを無効にすると、Active Directory 認証の応答時間を短縮できます。

- 必要なもの *
- アプリケーション管理者のロールが必要です。
- ネストされたグループの無効化は、Active Directory を使用している場合にのみ該当します

Unified Manager でネストされたグループのサポートを無効にすると、認証時間が短縮される可能性があります。ネストされたグループが無効になっている Unified Manager にリモートグループを追加した場合、Unified Manager で認証されるためには個々のユーザがそのリモートグループのメンバーである必要があります。

手順

1. 左側のナビゲーションペインで、* 一般 * > * リモート認証 * をクリックします。
2. [ネストされたグループの検索を無効にする *] チェックボックスをオンにします。

3. [保存 (Save)] をクリックします。

認証サービスをセットアップしています

認証サービスを使用すると、 Unified Manager へのアクセスを許可する前に、リモートユーザまたはリモートグループを認証サーバで認証できます。事前定義された認証サービス (Active Directory や OpenLDAP など) を使用するか、または独自の認証メカニズムを設定してユーザを認証できます。

- 必要なもの *
- リモート認証を有効にしておく必要があります。
- アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、 * 一般 * > * リモート認証 * をクリックします。
2. 次のいずれかの認証サービスを選択します。

を選択した場合は	操作
Active Directory	<p>a. 管理者の名前とパスワードを入力します。</p> <p>b. 認証サーバのベース識別名を指定します。</p> <p>たとえば、認証サーバのドメイン名が + ou@domain.com + である場合、ベース識別名は * cn=ou 、 dc=domain 、 dc=com * です。</p>
OpenLDAP	<p>a. バインド識別名とバインドパスワードを入力します。</p> <p>b. 認証サーバのベース識別名を指定します。</p> <p>たとえば、認証サーバのドメイン名が + ou@domain.com + である場合、ベース識別名は * cn=ou 、 dc=domain 、 dc=com * です。</p>

を選択した場合は	操作
その他	<p>a. バインド識別名とバインドパスワードを入力します。</p> <p>b. 認証サーバのベース識別名を指定します。</p> <p>たとえば、認証サーバのドメイン名が + ou@domain.com + である場合、ベース識別名は * cn=ou 、 dc=domain 、 dc=com * です。</p> <p>c. 認証サーバでサポートされている LDAP プロトコルのバージョンを指定します。</p> <p>d. ユーザ名、グループメンバーシップ、ユーザグループ、およびメンバーの属性を入力します。</p>



認証サービスを変更する場合は、既存の認証サーバを削除してから新しい認証サーバを追加する必要があります。

3. [保存 (Save)] をクリックします。

認証サーバを追加しています


認証サーバを追加して管理サーバでリモート認証を有効にすると、その認証サーバのリモートユーザが Unified Manager にアクセスできるようになります。

- 必要なもの *
- 次の情報が必要です。
 - 認証サーバのホスト名または IP アドレス
 - 認証サーバのポート番号
- 認証サーバのリモートユーザまたはリモートグループを管理サーバで認証できるように、リモート認証を有効にし、認証サービスを設定しておく必要があります。
- アプリケーション管理者のロールが必要です。

追加する認証サーバがハイアベイラビリティ (HA) ペアを構成している (同じデータベースを使用している) 場合は、パートナーの認証サーバも追加できます。これにより、いずれかの認証サーバにアクセスできない場合でも管理サーバはパートナーと通信できます。

手順

1. 左側のナビゲーションペインで、 * 一般 * > * リモート認証 * をクリックします。
2. [セキュアな接続を使用する *] オプションを有効または無効にします。

状況	操作
有効にします	<p>a. [セキュアな接続を使用（ Use Secure Connection * ）] オプションを選択します。</p> <p>b. [Authentication Servers] 領域で、 [Add] をクリックします。</p> <p>c. Add Authentication Server ダイアログボックスで、サーバの認証名または IP アドレス（ IPv4 または IPv6 ）を入力します。</p> <p>d. [ホストの認証] ダイアログボックスで、 [証明書の表示] をクリックします。</p> <p>e. [証明書の表示] ダイアログボックスで、証明書の情報を確認し、 [閉じる *] をクリックします。</p> <p>f. [ホストの許可] ダイアログボックスで、 [はい] をクリックします。</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Secure Connection authentication * オプションを有効にすると、 Unified Manager は認証サーバと通信して証明書を表示します。 Unified Manager では、セキュアな通信にはポート 636、セキュアでない通信にはポート 389 がデフォルトのポートとして使用されます。</p> </div>
無効にします	<p>a. [セキュアな接続を使用する *] オプションをオフにします。</p> <p>b. [Authentication Servers] 領域で、 [Add] をクリックします。</p> <p>c. [Add Authentication Server] ダイアログボックスで、サーバのホスト名または IP アドレス（ IPv4 または IPv6 ）、およびポートの詳細を指定します。</p> <p>d. [追加（ Add ）] をクリックします。</p>

追加した認証サーバが Servers 領域に表示されます。

3. 認証テストを実行し、追加した認証サーバでユーザを認証できることを確認します。

認証サーバの設定をテストする

認証サーバの設定を検証して、管理サーバが認証サーバと通信できるかどうかを確認できます。設定を検証するには、認証サーバからリモートユーザまたはリモートグループを検索し、設定済みの設定を使用して認証します。

- 必要なもの *
- リモートユーザまたはリモートグループを Unified Manager サーバで認証できるように、リモート認証を有効にし、認証サービスを設定しておく必要があります。
- 認証サーバからリモートユーザまたはリモートグループを管理サーバで検索して認証できるように、認証サーバを追加しておく必要があります。
- アプリケーション管理者のロールが必要です。

認証サービスが Active Directory に設定されている場合に、認証サーバのプライマリグループに属するリモートユーザの認証の検証では、認証結果にプライマリグループに関する情報は表示されません。

手順

1. 左側のナビゲーションペインで、* 一般 * > * リモート認証 * をクリックします。
2. [* 認証のテスト *] をクリックします。
3. Test User ダイアログボックスで、リモートユーザーのユーザー名とパスワード、またはリモートグループのユーザー名を指定し、* Test * をクリックします。

リモートグループを認証する場合、パスワードは入力しないでください。

アラートの追加

特定のイベントが生成されたときに通知するようにアラートを設定できます。アラートは、単一のリソース、リソースのグループ、または特定の重大度タイプのイベントについて設定することができます。通知を受け取る頻度を指定したり、アラートにスクリプトを関連付けたりできます。

- 必要なもの *
- イベント生成時に Active IQ Unified Manager サーバからユーザに通知を送信できるように、通知に使用するユーザの E メールアドレス、SMTP サーバ、SNMP トラップホストなどを設定しておく必要があります。
- アラートをトリガーするリソースとイベント、および通知するユーザのユーザ名または E メールアドレスを確認しておく必要があります。
- イベントに基づいてスクリプトを実行する場合は、Scripts ページを使用して Unified Manager にスクリプトを追加しておく必要があります。
- アプリケーション管理者またはストレージ管理者のロールが必要です。

アラートは、ここで説明するように、Alert Setup ページからアラートを作成するだけでなく、イベントを受信した後に Event Details ページから直接作成できます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Alert Setup * をクリックします。
2. [Alert Setup] ページで、[Add] をクリックします。
3. [アラートの追加] ダイアログボックスで、[* 名前 *] をクリックし、アラートの名前と概要を入力します。
4. [* リソース] をクリックし、アラートに含めるリソースまたはアラートから除外するリソースを選択します。

[* 次を含む名前 (* Name Contains)] フィールドでテキスト文字列を指定してフィルタを設定し、リソースのグループを選択できます。指定したテキスト文字列に基づいて、フィルタルールに一致するリソースのみが使用可能なリソースのリストに表示されます。指定するテキスト文字列では、大文字と小文字が区別されます。

あるリソースが対象に含めるルールと除外するルールの両方に該当する場合は、除外するルールが優先され、除外されたリソースに関連するイベントについてはアラートが生成されません。

5. [*Events] をクリックし、アラートをトリガーするイベント名またはイベントの重大度タイプに基づいてイベントを選択します。



複数のイベントを選択するには、Ctrl キーを押しながら選択します。

6. [*Actions] をクリックし、通知するユーザを選択し、通知頻度を選択し、SNMP トラップをトラップレシーバに送信するかどうかを選択し、アラートが生成されたときに実行するスクリプトを割り当てます。



ユーザに対して指定されている E メールアドレスを変更し、アラートを再び開いて編集しようとする、変更した E メールアドレスが以前に選択したユーザにマッピングされていないため、名前フィールドは空白になります。また、選択したユーザの E メールアドレスを Users ページで変更した場合、変更後の E メールアドレスは反映されません。

SNMP トラップを使用してユーザに通知することもできます。

7. [保存 (Save)] をクリックします。

アラートの追加例

この例は、次の要件を満たすアラートを作成する方法を示しています。

- アラート名： HealthTest
- リソース：名前に「 abc 」が含まれるすべてのボリュームを対象に含め、名前に「 xyz 」が含まれるすべてのボリュームを対象から除外する
- イベント：健全性に関するすべての重大なイベントを含みます
- アクション：「 + sample@domain.com + 」、「テスト」スクリプトを含み、15 分ごとにユーザーに通知する必要があります

[Add Alert] ダイアログボックスで、次の手順を実行します。

手順

1. [* 名前] をクリックし、[アラート名] フィールドに「 * **HealthTest** 」と入力します。
2. [* リソース] をクリックし、[含める] タブで、ドロップダウン・リストから [* ボリューム] を選択します。
 - a. 「 * Name Contains * 」フィールドに「 * abc 」と入力して、「 abc 」という名前のボリュームを表示します。
 - b. 「 * + 」を選択します [All Volumes whose name contains 'abc']+* を使用可能なリソース領域から選択したリソース領域に移動します。
 - c. [* 除外する *] をクリックし、[* 名前に * が含まれる *] フィールドに「 * xyz * 」と入力して、[* 追加] をクリックします。

3. [* イベント] をクリックし、[イベントの重要度] フィールドから [クリティカル *] を選択します。
4. [Matching Events] 領域から [* All Critical Events] を選択し、[Selected Events] 領域に移動します。
5. [* アクション *] をクリックし、[これらのユーザーに警告] フィールドに「 * sample@domain.com * 」と入力します。
6. 15 分ごとにユーザに通知するには、「 * 15 分ごとに通知する」を選択します。

指定した期間、受信者に繰り返し通知を送信するようにアラートを設定できます。アラートに対してイベント通知をアクティブにする時間を決める必要があります。

7. 実行するスクリプトの選択メニューで、 * テスト * スクリプトを選択します。
8. [保存 (Save)] をクリックします。

ローカルユーザのパスワードを変更しています

潜在的なセキュリティリスクを回避するために、ローカルユーザのログインパスワードを変更することができます。

- 必要なもの *

ローカルユーザとしてログインする必要があります。

リモートユーザとメンテナンスユーザのパスワードについては、この手順では変更できません。リモートユーザのパスワードを変更するには、パスワード管理者に問い合わせてください。メンテナンスユーザのパスワードを変更する手順については、を参照してください "[メンテナンスコンソールを使用する](#)"。

手順

1. Unified Manager にログインします。
2. トップ・メニュー・バーで、ユーザー・アイコンをクリックし、 * パスワードの変更 * をクリックします。

リモートユーザの場合、 * パスワードの変更 * オプションは表示されません。

3. Change Password ダイアログボックスで、現在のパスワードと新しいパスワードを入力します。
4. [保存 (Save)] をクリックします。

Unified Manager がハイアベイラビリティ構成の場合は、セットアップのもう一方のノードでパスワードを変更する必要があります。パスワードは両方のインスタンスで同じである必要があります。

セッションの非アクティブ時のタイムアウト設定

Unified Manager に非アクティブ時のタイムアウト値を指定して、一定の時間が経過したらセッションを自動的に終了するように設定できます。デフォルトでは、タイムアウトは 4、320 分（72 時間）に設定されています。

- 必要なもの *

アプリケーション管理者のロールが必要です。

この設定は、ログインしているすべてのユーザセッションに適用されます。



Security Assertion Markup Language (SAML) 認証を有効にしている場合は、このオプションを使用できません。

手順

1. 左側のナビゲーションペインで、* 一般 * > * 機能設定 * をクリックします。
2. [* 機能設定 *] ページで、次のいずれかのオプションを選択して非アクティブ時のタイムアウトを指定します。

状況	操作
セッションが自動的に閉じないようにタイムアウトを設定しない	[* アクティビティなしタイムアウト *] パネルで、スライダボタンを左（オフ）に移動し、[* 適用 *] をクリックします。
タイムアウト値として特定の時間（分）を設定します	[Inactivity Timeout] パネルで、スライダボタンを右（オン）に動かし、非アクティブ時のタイムアウト値を分単位で指定して、[Apply] をクリックします。

Unified Manager のホスト名を変更しています

必要に応じて、Unified Manager をインストールしたシステムのホスト名をあとから変更することができます。たとえば、タイプ、ワークグループ、監視対象のクラスタグループなどがわかるような名前に変更すると、Unified Manager サーバを識別しやすくなります。

ホスト名を変更する手順は、Unified Manager を VMware ESXi サーバ、Red Hat Linux サーバまたは CentOS Linux サーバ、Microsoft Windows サーバのいずれで実行しているかによって異なります。

Unified Manager 仮想アプライアンスのホスト名を変更する

ネットワークホストの名前は、Unified Manager 仮想アプライアンスの導入時に割り当てられます。このホスト名は導入後に変更することができます。ホスト名を変更する場合は、HTTPS 証明書も再生成する必要があります。

- 必要なもの *

このタスクを実行するには、Unified Manager にメンテナンスユーザとしてログインするか、アプリケーション管理者ロールが割り当てられている必要があります。

Unified Manager Web UI には、ホスト名（またはホストの IP アドレス）を使用してアクセスできます。導入時に静的 IP アドレスを使用してネットワークを設定した場合は、指定したネットワークホストの名前を使用します。DHCP を使用してネットワークを設定した場合は、DNS からホスト名を取得します。DHCP または DNS が適切に設定されていないと、ホスト名「Unified Manager」が自動的に割り当てられ、セキュリティ証明書に関連付けられます。

ホスト名を変更した場合、Unified Manager Web UI へのアクセスに新しいホスト名を使用するには、ホスト名の元の割り当て方法に関係なく、必ず新しいセキュリティ証明書を生成する必要があります。

ホスト名ではなくサーバの IP アドレスを使用して Web UI にアクセスする場合は、ホスト名を変更したときに新しい証明書を生成する必要はありません。ただし、証明書のホスト名が実際のホスト名と同じになるように証明書を更新することを推奨します。

Unified Manager でホスト名を変更した場合は、OnCommand Workflow Automation (WFA) でホスト名を手動で更新する必要があります。ホスト名は WFA では自動的に更新されません。

新しい証明書は、Unified Manager 仮想マシンを再起動するまで有効になりません。

手順

1. HTTPS セキュリティ証明書を生成する

新しいホスト名を使用して Unified Manager Web UI にアクセスする場合は、HTTPS 証明書を再生成して新しいホスト名に関連付ける必要があります。

2. Unified Manager 仮想マシンを再起動します

HTTPS 証明書を再生成したら、Unified Manager 仮想マシンを再起動する必要があります。

HTTPS セキュリティ証明書の生成

Active IQ Unified Manager を初めてインストールするときは、デフォルトの HTTPS 証明書がインストールされます。既存の証明書を置き換える新しい HTTPS セキュリティ証明書を生成することがあります。

- 必要なもの *

アプリケーション管理者のロールが必要です。

証明書を再生成する理由はいくつかあります。たとえば、識別名 (DN) の値を大きくする場合や、キーのサイズを大きくする場合や、有効期限を延長する場合、現在の証明書の有効期限が切れている場合などです。


Unified Manager Web UI にアクセスできない場合は、メンテナンスコンソールを使用して同じ値で HTTPS 証明書を再生成できます。証明書を再生成する際には、キーのサイズと有効期間を定義できます。を使用する場合 `Reset Server Certificate` メンテナンスコンソールからオプションを選択すると、397日間有効な新しいHTTPS証明書が作成されます。この証明書には、サイズが 2048 ビットの RSA キーがあります。

手順

1. 左側のナビゲーションペインで、* General * > * HTTPS Certificate * をクリックします。
2. [* HTTPS 証明書の再生成 *] をクリックします。

HTTPS 証明書の再生成ダイアログボックスが表示されます。

3. 証明書を生成する方法に応じて、次のいずれかのオプションを選択します。

状況	手順
現在の値で証明書を再生成します	[現在の証明書属性を使用して再生成 (Regenerate using current Certificate Attributes)] オプションをクリックし
別の値を使用して証明書を生成します	<p>[現在の証明書属性を更新する *] オプションをクリックします。</p> <p>新しい値を入力しない場合は、[共通名] フィールドと [代替名] フィールドに既存の証明書の値が使用されます。「共通名」は、ホストの FQDN に設定する必要があります。その他のフィールドには値は必要ありませんが、電子メール、会社、部署、証明書に値を入力する場合は、[市区町村]、[都道府県]、および [国] を選択します。使用可能なキー・サイズ (キー・アルゴリズムは「RSA」) と有効期間から選択することもできます。</p> <div>  <ul style="list-style-type: none"> • キーサイズに指定できる値は、です 2048、3072 および 4096。 • 有効期間は、1 日 ~ 最大 36500 日です。 <p>有効期間は 36500 日ですが、有効期間は 397 日以内または 13 か月以内にすることをお勧めします。397 日以上の有効期間を選択し、この証明書の CSR をエクスポートして既知の CA によって署名された証明書を取得する予定であるため、CA から返された署名済み証明書の有効性は 397 日に減少します。</p> <ul style="list-style-type: none"> • 証明書の代替名フィールドからローカル識別情報を削除する場合は、[ローカル識別情報を除外する (ローカルホストなど)] チェックボックスをオンにします。このチェックボックスをオンにすると、[代替名] フィールドに入力したフィールドのみが使用されます。空白のままにすると、結果の証明書に代替名フィールドがまったく表示されなくなります。 </div>

4. [はい] をクリックして証明書を再生成します。

5. 新しい証明書を有効にするために Unified Manager サーバを再起動します。
6. HTTPS 証明書を表示して新しい証明書の情報を確認します。

Unified Manager 仮想マシンを再起動しています

仮想マシンは、Unified Manager のメンテナンスコンソールから再起動できます。新しいセキュリティ証明書を生成した場合や仮想マシンで問題が発生した場合、仮想マシンの再起動が必要になります。

- 必要なもの *

仮想アプライアンスの電源をオンにします。

メンテナンスコンソールにメンテナンスユーザとしてログインします。

また、「ゲストを再起動」オプションを使用して、vSphere から仮想マシンを再起動することもできます。詳細については、VMware のドキュメントを参照してください。

手順

1. メンテナンスコンソールにアクセスします
2. システム構成 > 仮想マシンの再起動 * を選択します。

Linux システムで **Unified Manager** ホスト名を変更する

必要に応じて、Unified Manager をインストールした Red Hat Enterprise Linux または CentOS マシンのホスト名をあとから変更することができます。たとえば、タイプ、ワークグループ、監視対象のクラスターグループなどがわかるような名前に変更すると、Linux マシンのリストで Unified Manager サーバを識別しやすくなります。

- 必要なもの *

Unified Manager がインストールされている Linux システムへの root ユーザアクセスが必要です。

Unified Manager Web UI には、ホスト名（またはホストの IP アドレス）を使用してアクセスできます。導入時に静的 IP アドレスを使用してネットワークを設定した場合は、指定したネットワークホストの名前を使用します。DHCP を使用してネットワークを設定した場合は、DNS サーバからホスト名を取得します。

ホスト名を変更した場合、Unified Manager Web UI へのアクセスに新しいホスト名を使用するには、ホスト名の元の割り当て方法に関係なく、必ず新しいセキュリティ証明書を生成する必要があります。

ホスト名ではなくサーバの IP アドレスを使用して Web UI にアクセスする場合は、ホスト名を変更したときに新しい証明書を生成する必要はありません。ただし、証明書のホスト名が実際のホスト名と同じになるように証明書を更新することを推奨します。新しい証明書は、Linux マシンを再起動するまで有効になりません。

Unified Manager でホスト名を変更した場合は、OnCommand Workflow Automation（WFA）でホスト名を手動で更新する必要があります。ホスト名は WFA では自動的に更新されません。

手順

1. 変更する Unified Manager システムに root ユーザとしてログインします。

2. 次のコマンドを入力して、Unified Manager ソフトウェアと関連する MySQL ソフトウェアを停止します。

```
systemctl stop ocieau ocie mysqld
```

3. Linuxを使用してホスト名を変更します hostnamectl コマンドを実行します

```
hostnamectl set-hostname new_FQDN
```

```
hostnamectl set-hostname nuhost.corp.widget.com
```

4. サーバの HTTPS 証明書を再生成します。

```
/opt/netapp/essentials/bin/cert.sh create
```

5. ネットワークサービスを再起動します。

```
service network restart
```

6. サービスが再起動したら、新しいホスト名で ping を実行できるかどうかを確認します。

```
ping new_hostname
```

```
ping nuhost
```

元のホスト名に対して設定していたものと同じ IP アドレスが返されることを確認します。

7. ホスト名を変更して確認したら、次のコマンドを入力して Unified Manager を再起動します。

```
systemctl start mysqld ocie ocieau
```

ポリシーベースのストレージ管理を有効または無効にします

Unified Manager 9.7 以降では、ONTAP クラスタにストレージワークロード（ボリュームと LUN）をプロビジョニングし、割り当てられたパフォーマンスサービスレベルに基づいてワークロードを管理できます。この機能は ONTAP System Manager でワークロードを作成して QoS ポリシーを適用する処理に相当しますが、Unified Manager を使用して適用した場合は、Unified Manager インスタンスで監視しているすべてのクラスタのワークロードをプロビジョニングおよび管理できます。

アプリケーション管理者のロールが必要です。

このオプションはデフォルトで有効になっていますが、Unified Manager を使用してワークロードをプロビジョニングおよび管理しない場合は無効にできます。

このオプションを有効にすると、ユーザインターフェイスに新しい項目がいくつか追加されます。

新しいコンテンツ	場所
新しいワークロードのプロビジョニングページ	一般的なタスク * > * プロビジョニング * から使用できます
パフォーマンスサービスレベルポリシーの作成ページ	設定 * > * ポリシー * > * パフォーマンスサービスレベル * から選択できます
パフォーマンスストレージ効率化ポリシーの作成ページ	設定 * > * ポリシー * > * ストレージ効率化 * で確認できます
現在のワークロードパフォーマンスとワークロード IOPS を表示するパネル	ダッシュボードで確認できます

これらのページおよびこの機能の詳細については、製品のオンラインヘルプを参照してください。

手順

1. 左側のナビゲーションペインで、* 一般 * > * 機能設定 * をクリックします。
2. [機能の設定 *] ページで、次のいずれかのオプションを選択して、ポリシーベースのストレージ管理を無効または有効にします。

状況	操作
ポリシーベースのストレージ管理を無効にする	ポリシーベースのストレージ管理 * パネルで、スライダボタンを左に動かします。
ポリシーベースのストレージ管理を有効化	ポリシーベースのストレージ管理 * パネルで、スライダボタンを右に動かします。

Unified Manager のバックアップを設定しています

Unified Manager のバックアップ機能は、ホストシステムおよびメンテナンスコンソールから実行する一連の設定手順で設定できます。

設定手順の詳細については、を参照してください ["バックアップとリストアの処理の管理"](#)。

機能設定の管理

[機能設定] ページでは、Active IQ Unified Manager の特定の機能を有効または無効にできます。ポリシーに基づいたストレージオブジェクトの作成と管理、API ゲートウェイとログインバナーの有効化、アラート管理用スクリプトのアップロード、非アクティブ時間に基づく Web UI セッションのタイムアウト、Active IQ プラットフォームイベントの受信停止などが含まれます。



[機能の設定] ページは、アプリケーション管理者ロールを持つユーザーのみが使用できます。

スクリプトのアップロードについては、を参照してください ["スクリプトアップロードの有効化 / 無効化"](#)。

ポリシーベースのストレージ管理の有効化

ポリシーベースのストレージ管理 * オプションを使用すると、サービスレベル目標（SLO）に基づいてストレージを管理できます。このオプションはデフォルトで有効になっています。

この機能をアクティブ化すると、Active IQ Unified Manager インスタンスに追加された ONTAP クラスタのストレージワークロードをプロビジョニングし、割り当てられたパフォーマンスサービスレベルとストレージ効率化ポリシーに基づいてワークロードを管理できます。

この機能のアクティブ化または非アクティブ化は、* General * > * Feature Settings * > * Policy-Based Storage Management * から選択できます。この機能をアクティブ化すると、次のページで操作と監視を行うことができます。

- プロビジョニング（ストレージワークロードのプロビジョニング）
- * ポリシー * > * パフォーマンスサービスレベル *
- * ポリシー * > * ストレージ効率化 *
- クラスタセットアップページのパフォーマンスサービスレベルで管理されるワークロードの列
- ダッシュボード上のワークロードのパフォーマンスパネル *

画面を使用して、パフォーマンスサービスレベルとストレージ効率化ポリシーを作成したり、ストレージワークロードをプロビジョニングしたりできます。割り当てられたパフォーマンスサービスレベルに準拠したストレージワークロードと準拠しないストレージワークロードを監視することもできます。ワークロードのパフォーマンスとワークロードの IOPS パネルでは、データセンター内のクラスタの合計容量、使用可能容量、使用済み容量、およびパフォーマンス（IOPS）を、プロビジョニングされたストレージワークロードに基づいて評価することもできます。

この機能をアクティブ化したら、Unified Manager REST API を実行して、* メニューバー * > * ヘルプボタン * > * API ドキュメント * > * ストレージプロバイダ * カテゴリからこれらの機能の一部を実行できます。また、ホスト名または IP アドレスと URL を + <https://<hostname>/docs/api/> の形式で入力して REST API ページにアクセスすることもできます

APIの詳細については、を参照してください ["Active IQ Unified Manager REST APIの使用を開始する"](#)。

API ゲートウェイを有効にしてい

API ゲートウェイ機能を使用すると、ONTAP を個別にログインせずに、複数の Active IQ Unified Manager クラスタを一元的に管理できます。

この機能は、Unified Manager に最初にログインしたときに表示される設定ページから有効にできます。または、* 一般 * > * 機能設定 * > * API ゲートウェイ * からこの機能を有効または無効にすることもできます。

Unified Manager REST API と ONTAP REST API は別のものであり、Unified Manager REST API を使用して ONTAP REST API のすべての機能を利用できるわけではありません。ただし、Unified Manager では提供されていない特定の機能を管理するために ONTAP API にアクセスする必要がある場合は、API ゲートウェイ機

能を有効にして ONTAP API を実行できます。ゲートウェイは、ヘッダーと本文の形式を ONTAP API と同じにすることで、API 要求をトンネリングするプロキシとして機能します。Unified Manager のクレデンシャルを使用して特定の API を実行することで、個々のクラスタのクレデンシャルを渡すことなく ONTAP クラスタにアクセスして管理することができます。Unified Manager は単一の管理ポイントとして機能し、Unified Manager インスタンスで管理される ONTAP クラスタ全体で API を実行できます。API から返される応答は、対応する ONTAP REST API を ONTAP から直接実行した場合と同じです。

この機能を有効にしたあと、*メニューバー*>*ヘルプボタン*>*API ドキュメント*>*ゲートウェイ*カテゴリから Unified Manager REST API を実行できます。また、ホスト名または IP アドレスと URL をの形式で入力して REST API ページにアクセスすることもできます <https://<hostname>/docs/api/>

API の詳細については、を参照してください "[Active IQ Unified Manager REST API の使用を開始する](#)"。

非アクティブ時のタイムアウトの指定

Active IQ Unified Manager に非アクティブ時のタイムアウト値を指定できます。非アクティブな状態が指定した時間を経過すると、アプリケーションは自動的にログアウトされます。このオプションはデフォルトで有効になっています。

この機能を非アクティブにするか、*一般*>*機能設定*>*非アクティブタイムアウト*から時間を変更できます。この機能をアクティブにしたら、システムが自動的にログアウトするまでの時間制限（分単位）を *logout after* フィールドに指定する必要があります。デフォルト値は 4320 分（72 時間）です。



Security Assertion Markup Language（SAML）認証を有効にしている場合は、このオプションを使用できません。

Active IQ ポータルイベントの有効化

Active IQ ポータルイベントを有効にするか無効にするかを指定できます。この設定を有効にすると、Active IQ ポータルでシステム構成やケーブル配線などに関する追加のイベントが検出されて表示されます。このオプションはデフォルトで有効になっています。

Active IQ Unified Manager でこの機能を有効にすると、Active IQ ポータルで検出されたイベントが表示されます。イベントは、すべての監視対象ストレージシステムから生成された AutoSupport メッセージに対して一連のルールを実行することによって作成されます。これらのイベントは Unified Manager の他のイベントとは異なり、システム構成、ケーブル配線、ベストプラクティス、および可用性の問題に関連するインシデントやリスクを特定します。

この機能をアクティブ化または非アクティブ化するには、*一般*>*機能設定*>*Active IQ ポータルイベント*を選択します。外部ネットワークへのアクセスがないサイトでは、*Storage Management*>*Event Setup*>*Upload Rules*からルールを手動でアップロードする必要があります。

この機能はデフォルトで有効になっています。この機能を無効にすると、Active IQ イベントが Unified Manager で検出または表示されなくなります。無効にすると、この機能を有効にすると、クラスタタイムゾーンの事前定義された時刻（00：15）に Unified Manager がクラスタで Active IQ イベントを受信できるようになります。

準拠のためのセキュリティ設定の有効化と無効化

Features Settings ページの *Security Dashboard* パネルにある *Customize* ボタンを

使用して、Unified Manager でセキュリティパラメータを有効または無効にして、コンプライアンス監視を実行できます。

このページで有効または無効になる設定によって、Unified Manager でのクラスタと Storage VM の全体的な準拠ステータスが制御されます。選択内容に応じて、対応する列がクラスタインベントリページの「セキュリティ：すべてのクラスタ」の「* セキュリティ：すべての Storage VM *」ビューと「Storage VM インベントリ」ページの「* セキュリティ：すべての Storage VM *」ビューに表示されます。



これらの設定を編集できるのは、管理者ロールのユーザだけです。

ONTAP クラスタ、Storage VM、およびボリュームのセキュリティ条件は、で定義されている推奨事項に照らして評価されます ["Security Hardening Guide for NetApp ONTAP 9"](#)。ダッシュボードおよびセキュリティページのセキュリティパネルには、クラスタ、Storage VM、およびボリュームのデフォルトのセキュリティコンプライアンスステータスが表示されます。また、セキュリティイベントが生成され、セキュリティ違反があるクラスタと Storage VM に対して有効になる管理操作も実行されます。

セキュリティ設定のカスタマイズ

ONTAP 環境に応じて準拠監視の設定をカスタマイズするには、次の手順を実行します。

手順

1. [一般]、[機能設定]、[セキュリティダッシュボード]、[カスタマイズ*]の順にクリックします。セキュリティダッシュボード設定のカスタマイズ* ポップアップが表示されます。



有効または無効にしたセキュリティコンプライアンスパラメータは、クラスタおよび Storage VM 画面のデフォルトのセキュリティビュー、レポート、およびスケジュールされたレポートに直接影響します。セキュリティパラメータを変更する前に、これらの画面から Excel レポートをアップロードした場合、ダウンロードした Excel レポートに問題がある可能性があります。

2. ONTAP クラスタのカスタム設定を有効または無効にするには、「* Cluster *」で必要な一般設定を選択します。クラスタコンプライアンスをカスタマイズするためのオプションについては、を参照してください ["クラスタコンプライアンスのカテゴリ"](#)。
3. Storage VM のカスタム設定を有効または無効にするには、「Storage VM *」で必要な一般設定を選択します。Storage VM コンプライアンスをカスタマイズするためのオプションについては、を参照してください ["Storage VM コンプライアンスのカテゴリ"](#)。

AutoSupport および認証設定のカスタマイズ

AutoSupport 設定 * セクションでは、AutoSupport からの ONTAP メッセージの送信に HTTPS 転送を使用するかどうかを指定できます。

認証設定 * セクションでは、デフォルトの ONTAP 管理者ユーザに対して Unified Manager のアラートを生成するように設定できます。

スクリプトアップロードの有効化 / 無効化

スクリプトを Unified Manager にアップロードして実行する機能は、デフォルトで有効

になっています。セキュリティ上の理由からこのアクティビティを許可しない場合は、この機能を無効にできます。

- 必要なもの *

アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* 一般 * > * 機能設定 * をクリックします。
2. [* 機能の設定 *] ページで、次のいずれかのオプションを選択してスクリプトを無効または有効にします。

状況	操作
スクリプトを無効にします	• スクリプトアップロード * パネルで、スライダボタンを左に動かします。
スクリプトを有効にします	• スクリプトアップロード * パネルで、スライダボタンを右に動かします。

ログインバナーを追加しています

ログインバナーを追加すると、システムへのアクセスを許可されているユーザ、ログインおよびログアウト時の使用条件などの情報を組織で表示できます。

このログインバナーのポップアップは、ストレージオペレータや管理者など、ログイン、ログアウト、セッションタイムアウトの際に表示されます。

メンテナンスコンソールを使用する

メンテナンスコンソールでは、ネットワークの設定、Unified Manager がインストールされているシステムの設定と管理、潜在的な問題の防止とトラブルシューティングに役立つその他のメンテナンスタスクを実行することができます。

メンテナンスコンソールで提供される機能

Unified Manager のメンテナンスコンソールでは、Unified Manager システムの設定を管理し、問題の発生を防ぐために必要な変更を行うことができます。

メンテナンスコンソールでは、Unified Manager をインストールしたオペレーティングシステムに応じて次の機能が提供されます。

- 仮想アプライアンスの問題、特に Unified Manager の Web インターフェイスを使用できない場合はトラブルシューティングを行ってください
- Unified Manager を新しいバージョンにアップグレードします
- テクニカルサポートに送信するサポートバンドルを生成する

- ネットワークの設定を行います
- メンテナンスユーザのパスワードを変更します
- パフォーマンス統計を送信するには、外部データプロバイダに接続してください
- パフォーマンスデータ収集の内部を変更します
- 以前にバックアップしたバージョンからの Unified Manager データベースと設定のリストア

メンテナンスユーザの役割

Unified Manager を Red Hat Enterprise Linux または CentOS システムにインストールする場合、インストール時にメンテナンスユーザが作成されます。メンテナンスユーザの名前は「umadmin」です。メンテナンスユーザは、Web UI でアプリケーション管理者のロールが割り当てられ、他のユーザを作成してロールを割り当てることができます。

メンテナンスユーザまたは umadmin ユーザは、Unified Manager のメンテナンスコンソールにもアクセスできます。

診断ユーザの権限

診断アクセスの目的は、テクニカルサポートからトラブルシューティングのサポートを受けられるようにすることです。このため、テクニカルサポートから指示された場合のみ診断アクセスを使用する必要があります。

診断ユーザは、テクニカルサポートからの指示を受けて、トラブルシューティングの目的で OS レベルのコマンドを実行できます。

メンテナンスコンソールへのアクセス

Unified Manager ユーザインターフェイスが動作状態でない場合、またはこのユーザインターフェイスにない機能を実行する必要がある場合は、メンテナンスコンソールにアクセスして Unified Manager システムを管理できます。

- 必要なもの *

Unified Manager をインストールして設定しておく必要があります。

15 分間操作を行わないと、メンテナンスコンソールからログアウトされます。



VMware にインストールした場合、VMware コンソールからメンテナンスユーザとしてすでにログインしているときは、Secure Shell を使用して同時にログインできません。

ステップ

1. メンテナンスコンソールにアクセスするには、次の手順を実行します。

オペレーティングシステム	実行する手順
VMware	a. Secure Shell を使用して、Unified Manager 仮想アプライアンスの IP アドレスまたは完全修飾ドメイン名に接続します。 b. メンテナンスユーザの名前とパスワードを使用してメンテナンスコンソールにログインします。
Linux の場合	a. Secure Shell を使用して、Unified Manager システムの IP アドレスまたは完全修飾ドメイン名に接続します。 b. メンテナンスユーザ（umadmin）の名前とパスワードでシステムにログインします。 c. 入力するコマンド <code>maintenance_console</code> を押します。
Windows の場合	a. 管理者のクレデンシャルで Unified Manager システムにログインします。 b. Windows 管理者として PowerShell を起動します。 c. 入力するコマンド <code>maintenance_console</code> を押します。

Unified Manager メンテナンスコンソールメニューが表示されます。

vSphere VM コンソールを使用してメンテナンスコンソールにアクセスする

Unified Manager ユーザーインターフェイスが動作状態でない場合、またはこのユーザーインターフェイスにない機能を実行する必要がある場合は、メンテナンスコンソールにアクセスして仮想アプライアンスを再設定できます。

- 必要なもの *
- maintenance ユーザである必要があります。
- メンテナンスコンソールにアクセスするには、仮想アプライアンスの電源をオンにする必要があります。

手順

1. vSphere Client で、Unified Manager 仮想アプライアンスを探します。
2. [* コンソール *] タブをクリックします。
3. コンソールウィンドウ内をクリックしてログインします。
4. ユーザ名とパスワードを使用してメンテナンスコンソールにログインします。

15 分間操作を行わないと、メンテナンスコンソールからログアウトされます。

メンテナンスコンソールのメニュー

メンテナンスコンソールは各種のメニューで構成され、Unified Manager サーバの特別な機能や設定の保守と管理を行うことができます。

Unified Manager をインストールしたオペレーティングシステムに応じて、メンテナンスコンソールは次のメニューで構成されます。

- Upgrade Unified Manager （VMware のみ）
- Network Configuration （VMware のみ）
- System Configuration （VMware のみ）
 - a. サポート/診断
 - b. サーバ証明書をリセットします
 - c. 外部データプロバイダ
 - d. バックアップのリストア
 - e. パフォーマンスポーリング間隔の設定
 - f. SAML 認証を無効にする
 - g. アプリケーションポートを表示/変更します
 - h. デバッグログの構成
 - i. MySQLポート3306へのアクセスを制御します
 - j. 終了します

特定のメニューオプションにアクセスするための番号をリストから選択します。たとえば、バックアップとリストアの場合は、「4」を選択します。

Network Configuration （ネットワーク設定）メニュー

Network Configuration メニューでは、ネットワーク設定を管理できます。このメニューは、Unified Manager ユーザインターフェイスを使用できない場合に使用してください。



Unified Manager が Red Hat Enterprise Linux 、CentOS 、または Microsoft Windows にインストールされている場合は、このメニューを使用できません。

次のメニュー項目を選択できます。

- * IP アドレス設定 * を表示します

仮想アプライアンスの現在のネットワーク設定について、IP アドレス、ネットワーク、ブロードキャストアドレス、ネットマスク、ゲートウェイ、および DNS サーバです。

- * IP アドレス設定の変更 *

IP アドレス、ネットマスク、ゲートウェイ、DNS サーバなど、仮想アプライアンスのネットワーク設定を変更できます。メンテナンスコンソールでネットワーク設定を DHCP から静的ネットワークに切り替

えた場合は、ホスト名を編集できません。変更を実行するには、[* 変更をコミットする *]を選択する必要があります。

- * ドメイン名検索設定を表示 *

ホスト名の解決に使用されるドメイン名検索リストが表示されます。

- * ドメイン名検索設定の変更 *

ホスト名を解決する際に検索するドメイン名を変更できます。変更を実行するには、[* 変更をコミットする *]を選択する必要があります。

- * スタティックルートを表示 *

現在の静的ネットワークルートが表示されます。

- * スタティックルートの変更 *

静的ネットワークルートを追加または削除できます。変更を実行するには、[* 変更をコミットする *]を選択する必要があります。

- * ルートを追加 *

静的ルートを追加できます。

- * ルートの削除 *

静的ルートを削除できます。

- * 戻る *

メインメニュー * に戻ります。

- * 終了 *

メンテナンスコンソールを終了します。

- * ネットワークインターフェイスを無効にします。 *

使用可能なネットワークインターフェイスを無効にします。使用可能なネットワークインターフェイスが1つしかない場合は、それを無効にすることはできません。変更を実行するには、[* 変更をコミットする *]を選択する必要があります。

- * ネットワーク・インターフェイスを有効にする *

使用可能なネットワークインターフェイスを有効にします変更を実行するには、[* 変更をコミットする *]を選択する必要があります。

- * 変更を確定 *

仮想アプライアンスのネットワーク設定に加えた変更を適用します。変更を有効にするには、このオプションを選択する必要があります。そうしないと、変更は行われません。

- * ホストに Ping を実行します *

IP アドレスの変更や DNS 設定を確認するために、ターゲットホストに ping を実行します。

- * デフォルト設定に復元 *

すべての設定を工場出荷時のデフォルトにリセットします。変更を実行するには、[* 変更をコミットする*]を選択する必要があります。

- * 戻る *

メインメニュー * に戻ります。

- * 終了 *

メンテナンスコンソールを終了します。

System Configuration (システム設定) メニュー

System Configuration メニューでは、サーバのステータスの表示、仮想マシンのリブートとシャットダウンなど、さまざまなオプションを指定して仮想アプライアンスを管理できます。



Unified Manager を Linux または Microsoft Windows システムにインストールしている場合、このメニューには「Restore from a Unified Manager Backup」オプションのみが表示されます。

次のメニュー項目を選択できます。

- * サーバーステータスを表示 *

現在のサーバステータスを表示します。ステータスには「Running」と「Not Running」があります。

サーバが実行されていない場合は、テクニカルサポートに連絡する必要があります。

- * 仮想マシンの再起動 *

すべてのサービスを停止して仮想マシンをリブートします。リブート後、仮想マシンとサービスが再起動します。

- * 仮想マシンのシャットダウン *

すべてのサービスを停止して、仮想マシンをシャットダウンします。

このオプションは、仮想マシンコンソールからのみ選択できます。

- * < ログインユーザー > ユーザーパスワード * を変更します

現在ログインしているユーザのパスワードを変更します。変更できるのはメンテナンスユーザだけです。

- * データディスクのサイズを増やします。 *

仮想マシンのデータディスク（ディスク 3）のサイズを拡張します。

- * スワップ・ディスク・サイズの増加 *

仮想マシンのスワップディスク（ディスク 2）のサイズを拡張します。

- * タイムゾーンの変更 *

タイムゾーンを自分の場所に変更します。

- * NTP サーバーを変更 *

IP アドレスや Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）などの NTP サーバ設定を変更します。

- * NTP サービスの変更 *

を切り替えます ntp および systemd-timesyncd サービス：

- * Unified Manager バックアップからのリストア *

以前にバックアップしたバージョンから Unified Manager データベースと設定をリストアします。

- * サーバー証明書をリセット *

サーバセキュリティ証明書をリセットします。

- * ホスト名を変更 *

仮想アプライアンスがインストールされているホストの名前を変更します。

- * 戻る *

System Configuration（システム設定）メニューを終了し、Main Menu（メインメニュー）に戻ります。

- * 終了 *

メンテナンスコンソールメニューを終了します。

Support and Diagnostics（サポートと診断）メニュー

Support and Diagnostics メニューでは、トラブルシューティングのサポートを受けるためにテクニカルサポートに送信できるサポートバンドルを生成することができます。

次のメニューオプションを使用できます。

- * ライトサポートバンドル * を生成します

30 日間のログと構成データベースのレコードを含む軽量のサポートバンドルを作成できます。パフォーマンスデータ、取得記録ファイル、サーバヒープダンプは含まれません。

- * サポートバンドル * を生成します

診断ユーザのホームディレクトリに診断情報を含む完全なサポートバンドル（7-Zip ファイル）を作成できます。システムがインターネットに接続されている場合は、ネットアップにサポートバンドルをアップロードすることもできます。

このファイルには、AutoSupport メッセージで生成された情報、Unified Manager データベースの内容、Unified Manager サーバの内部に関する詳細なデータ、および通常は AutoSupport メッセージや軽量のサポートバンドルには含まれない詳細なログが収められます。

その他のメニューオプション

次に示すメニューオプションでは、Unified Manager サーバでさまざまな管理タスクを実行することができます。

次のメニュー項目を選択できます。

• * サーバ証明書をリセット *

HTTPS サーバ証明書を再生成します。

Unified Manager の GUI でサーバ証明書を再生成します。そのためには、* General * > * HTTPS Certificates * > * Regenerate HTTPS Certificate * をクリックします。

• * SAML 認証を無効にします *

SAML 認証を無効にし、Unified Manager の GUI にアクセスするユーザのアイデンティティプロバイダ（IdP）によるサインオン認証を中止します。このコンソールオプションは、一般に、IdP サーバまたは SAML の設定を使用する問題で Unified Manager の GUI へのアクセスがブロックされる場合に使用します。

• * 外部データプロバイダ *

Unified Manager を外部データプロバイダに接続するためのオプションを提供します。接続が確立されると、パフォーマンスデータが外部サーバに送信されて、ストレージパフォーマンスのエクスポートがサードパーティ製ソフトウェアを使用してパフォーマンス指標をグラフ化できるようになります。次のオプションが表示されます。

- *Display Server Configuration *-- 外部データプロバイダの現在の接続設定と構成設定を表示します
- * サーバ接続の追加 / 変更 *-- 外部データプロバイダの新しい接続設定を入力したり、既存の設定を変更したりすることができます。
- * Modify Server Configuration * — 外部データプロバイダの新しい設定を入力したり、既存の設定を変更したりすることができます。
- *Delete Server Connection *-- 外部データプロバイダへの接続を削除します

接続を削除すると、Unified Manager は外部サーバとの接続を失います。

• バックアップの復元

詳細については、のトピックを参照してください ["バックアップとリストアの処理の管理"](#)。

• * パフォーマンスポーリング間隔の設定 *

Unified Manager がクラスタからパフォーマンス統計データを収集する頻度を設定するためのオプションを提供します。デフォルトの収集間隔は 5 分です。

大規模なクラスタからの収集が時間内に完了しない場合は、この間隔を 10 分または 15 分に変更できます。

- * アプリケーションポートの表示 / 変更 *

Unified Manager がセキュリティ上の理由から、HTTP および HTTPS プロトコルに使用するデフォルトのポートを変更するオプションが用意されています。デフォルトのポートは、HTTP の場合は 80、HTTPS の場合は 443 です。

- * MySQLポート3306 *へのアクセスを制御します

ホストからデフォルトのMySQLポート3306へのアクセスを制御します。セキュリティ上の理由から、このポート経由のアクセスは、Linux、Windows、およびVMware vSphereシステムへのUnified Managerの新規インストール時にlocalhostにのみ制限されます。このオプションを使用すると、ローカルホストとリモートホストの間でこのポートの表示/非表示を切り替えることができます。つまり、環境内のlocalhostに対してのみポートが有効になっている場合は、このポートをリモートホストでも使用できるようにすることができます。または、すべてのホストに対して有効にすると、このポートのアクセスをlocalhostのみに制限できます。アクセスがリモートホストで有効になっていた場合は、アップグレードシナリオで設定が保持されます。

- * 終了 *

メンテナンスコンソールメニューを終了します。

Windows でメンテナンスユーザのパスワードを変更する

Unified Manager のメンテナンスユーザのパスワードを必要に応じて変更することができます。

手順

1. Unified Manager Web UI のログインページで、* パスワードを忘れた場合 * をクリックします。

パスワードをリセットするユーザの名前を入力するよう求めるページが表示されます。

2. ユーザー名を入力し、* Submit * をクリックします。

パスワードをリセットするためのリンクが記載された E メールが、そのユーザ名に定義された E メールアドレスに送信されます。

3. Eメールの * パスワードのリセットリンク * をクリックし、新しいパスワードを定義します。
4. Web UI に戻り、新しいパスワードを使用して Unified Manager にログインします。

Linux システムでの umadmin パスワードの変更

セキュリティ上の理由から、インストールプロセスの完了後すぐに Unified Manager の umadmin ユーザのデフォルトパスワードを変更する必要があります。パスワードは、必要に応じてあとからいつでも再変更できます。

- 必要なもの *
- Unified Manager が Red Hat Enterprise Linux システムまたは CentOS Linux システムにインストールされている必要があります。
- Unified Manager がインストールされている Linux システムの root ユーザのクレデンシャルが必要です。

手順

1. Unified Manager が実行されている Linux システムに root ユーザとしてログインします。
2. umadmin パスワードを変更します。

```
passwd umadmin
```

umadmin ユーザの新しいパスワードを入力するように求められます。

Unified Manager が HTTP および HTTPS プロトコルに使用するポートを変更する

Unified Manager が HTTP および HTTPS プロトコルに使用するデフォルトのポートは、セキュリティ上の理由からインストール後に変更することができます。デフォルトのポートは、HTTP の場合は 80、HTTPS の場合は 443 です。

- 必要なもの *

Unified Manager サーバのメンテナンスコンソールへのログインが許可されているユーザ ID とパスワードが必要です。



Mozilla Firefox または Google Chrome ブラウザでは、安全でないとみなされるポートがいくつかあります。HTTP トラフィックと HTTPS トラフィックに新しいポート番号を割り当てる前に、ブラウザで確認してください。安全でないポートを選択すると、システムにアクセスできなくなる可能性があります。その場合、カスタマーサポートに連絡して解決を依頼する必要があります。

ポートを変更すると Unified Manager のインスタンスが自動的に再起動されるため、システムを短時間停止しても問題のないタイミングであることを確認してください。

1. SSH を使用して、Unified Manager ホストにメンテナンスユーザとしてログインします。

Unified Manager メンテナンスコンソールのプロンプトが表示されます。

2. 「* アプリケーションポートの表示 / 変更 *」というラベルの付いたメニューオプションの番号を入力し、Enter キーを押します。
3. プロンプトが表示されたら、メンテナンスユーザのパスワードをもう一度入力します。
4. HTTP ポートと HTTPS ポートの新しいポート番号を入力し、Enter キーを押します。

ポート番号を空白のままにすると、プロトコルのデフォルトポートが割り当てられます。

ポートを変更して Unified Manager をすぐに再起動するかどうかを確認するメッセージが表示されます。

5. 「* y *」と入力してポートを変更し、Unified Manager を再起動します。

6. メンテナンスコンソールを終了します。

この変更が完了したら、ユーザは Unified Manager Web UI にアクセスするために、URL に新しいポート番号を追加する必要があります。たとえば、+ <https://host.company.com:1234>+ 、 + <https://12.13.14.15:1122>+ 、 + [https://\[2001:db8:0:1\]:2123](https://[2001:db8:0:1]:2123)+ のように指定します。

ネットワークインターフェイスの追加

ネットワークトラフィックを分離する必要がある場合は、新しいネットワークインターフェイスを追加できます。

- 必要なもの *

vSphere を使用して仮想アプライアンスにネットワークインターフェイスを追加しておく必要があります。

仮想アプライアンスの電源をオンにする必要があります。



Unified Manager が Red Hat Enterprise Linux または Microsoft Windows にインストールされている場合は、この処理を実行できません。

手順

1. vSphere コンソールのメインメニューで、 * System Configuration * > * Reboot Operating System * を選択します。

リブート後、新たに追加したネットワークインターフェイスはメンテナンスコンソールで検出できます。

2. メンテナンスコンソールにアクセスします
3. ネットワーク構成 > ***Enable Network Interface** を選択します。
4. 新しいネットワークインターフェイスを選択し、 * Enter * キーを押します。
 - eth1 * を選択し、 * Enter * を押します。
5. 「 * y * 」と入力してネットワーク・インターフェイスを有効にします。
6. ネットワーク設定を入力します。

静的インターフェイスを使用している場合、または DHCP が検出されない場合は、ネットワーク設定を入力するように求められます。

ネットワーク設定を入力すると、自動的に **Network Configuration** メニューに戻ります。

7. [変更のコミット *] を選択します。

ネットワークインターフェイスを追加するには、変更をコミットする必要があります。

Unified Manager データベースディレクトリにディスクスペースを追加しています

Unified Manager データベースディレクトリには、ONTAP システムから収集された健全性とパフォーマンスのデータがすべて含まれています。状況によっては、データベースディレクトリのサイズの拡張が必要になることがあります。

たとえば、Unified Manager で多数のクラスタからデータを収集している場合、各クラスタに多数のノードがあると、データベースディレクトリがいっぱいになることがあります。データベースディレクトリの使用率が 90% の場合は警告イベントが生成され、ディレクトリの使用率が 95% の場合は重大イベントが生成されます。



ディレクトリの使用率が 95% に達すると、クラスタから追加のデータが収集されなくなります。

データディレクトリの容量を追加する手順は、Unified Manager を VMware ESXi サーバ、Red Hat Linux サーバまたは CentOS Linux サーバ、Microsoft Windows サーバのいずれで実行しているかによって異なります。

Linux ホストのデータディレクトリにスペースを追加しています

に十分なディスクスペースを割り当てていない場合 /opt/netapp/data Unified Managerをサポートするディレクトリ：Linuxホストを最初にセットアップしたあとにUnified Managerをインストールしたときに、のディスクスペースを増やしてインストール後にディスクスペースを追加できます /opt/netapp/data ディレクトリ。

• 必要なもの *

Unified Manager がインストールされている Red Hat Enterprise Linux マシンまたは CentOS Linux マシンへの root ユーザアクセスが必要です。

データディレクトリのサイズを拡張する前に Unified Manager データベースをバックアップすることを推奨します。

手順

1. ディスクスペースを追加する Linux マシンに root ユーザとしてログインします。
2. Unified Manager サービスと関連する MySQL ソフトウェアを次の順序で停止します。

```
systemctl stop ocieau ocie mysqld
```

3. 一時バックアップフォルダを作成する（例： /backup-data）には、現在のデータを格納できるだけの十分なディスクスペースがあります /opt/netapp/data ディレクトリ。
4. 既存のの内容と権限の設定をコピーします /opt/netapp/data ディレクトリをバックアップデータディレクトリに移動します。

```
cp -arp /opt/netapp/data/* /backup-data
```

5. SE Linux が有効になっている場合：

a. 既存のフォルダのSE Linuxタイプを取得します /opt/netapp/data フォルダ：

```
se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1
```

次のような情報が返されます。

```
echo $se_type  
mysql_d_db_t
```

- a. `chcon` コマンドを実行して、バックアップディレクトリの SE Linux タイプを設定します。

```
chcon -R --type=mysql_d_db_t /backup-data
```

6. の内容を削除します `/opt/netapp/data` ディレクトリ：

- a. `cd /opt/netapp/data`
- b. `rm -rf *`

7. のサイズを展開します `/opt/netapp/data` LVMのコマンドを使用するかディスクを追加して、ディレクトリのサイズを150GB以上にします。



を作成した場合は `/opt/netapp/data` ディスクからはマウントしないでください
`/opt/netapp/data` NFS共有またはCIFS共有として設定する。このため、ディスクスペースを拡張しようとする、などの一部のLVMコマンドが実行されます `resize` および `extend` 期待どおりに動作しない可能性があります。

8. を確認します `/opt/netapp/data` ディレクトリの所有者 (`mysql`) とグループ (`root`) は変更されません。

```
ls -ltr /opt/netapp/ | grep data
```

次のような情報が返されます。

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. SE Linuxが有効になっている場合は、のコンテキストを確認します `/opt/netapp/data` ディレクトリが `mysql_d_db_t` に設定されたままである

- a. `touch /opt/netapp/data/abc`
- b. `ls -Z /opt/netapp/data/abc`

次のような情報が返されます。

```
-rw-r--r--. root root unconfined_u:object_r:mysql_d_db_t:s0  
/opt/netapp/data/abc
```

10. `abc` というファイルを削除して、この余分なファイルがデータベースエラーを原因しないようにします。

11. 拡張したバックアップデータの内容をコピーします `/opt/netapp/data` ディレクトリ：

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. SE Linux が有効になっている場合は、次のコマンドを実行します。

```
chcon -R --type=mysqlld_db_t /opt/netapp/data
```

13. MySQL サービスを開始します。

```
systemctl start mysqld
```

14. MySQL サービスが開始されたら、ocie サービスと ocieau サービスを次の順序で開始します。

```
systemctl start ocie ocieau
```

15. すべてのサービスが開始されたら、バックアップフォルダを削除します /backup-data :

```
rm -rf /backup-data
```

VMware 仮想マシンのデータディスクにスペースを追加しています

Unified Manager データベースのデータディスクのスペースを増やす必要がある場合は、インストール後に Unified Manager のメンテナンスコンソールを使用してディスクスペースを増やして容量を追加できます。

- 必要なもの *
- vSphere Client へのアクセス権が必要です。
- 仮想マシンにスナップショットがローカルに格納されていないことが必要です。
- メンテナンスユーザのクレデンシャルが必要です。

仮想ディスクのサイズを拡張する前に仮想マシンをバックアップすることをお勧めします。

手順

1. vSphere Clientで、Unified Manager仮想マシンを選択し、データにディスク容量を追加します disk 3。詳細については、VMware のドキュメントを参照してください。

Unified Manager の導入では、ごくまれに「Hard Disk 3」ではなく「Hard Disk 2」がデータディスクに使用されることがあります。これが導入環境で発生した場合は、ディスクのサイズを大きくします。データディスクには、常に他のディスクよりも多くの容量があります。

2. vSphere Client で、Unified Manager 仮想マシンを選択し、* Console * タブを選択します。
3. コンソールウィンドウ内をクリックし、ユーザ名とパスワードを使用してメンテナンスコンソールにログインします。
4. メインメニューで、**System Configuration** オプションの番号を入力します。
5. System Configuration Menu (システム構成メニュー) で、* データディスクサイズの増加 * オプションの数値を入力します。

Microsoft Windows サーバの論理ドライブにスペースを追加する

Unified Manager データベースのディスクスペースを増やす必要がある場合は、Unified Manager がインストールされている論理ドライブに容量を追加できます。

- 必要なもの *

Windows の管理者権限が必要です。

ディスクスペースを追加する前に Unified Manager データベースをバックアップすることを推奨します。

手順

1. ディスクスペースを追加する Windows サーバに管理者としてログインします。
2. スペースを追加する方法に応じて、該当する手順を実行します。

オプション	説明
物理サーバで、Unified Manager server がインストールされている論理ドライブに容量を追加する。	Microsoft の次のトピックの手順に従います。 "基本ボリュームを拡張します"
物理サーバで、ハードディスクドライブを追加します。	Microsoft の次のトピックの手順に従います。 "ハードディスクドライブの追加"
仮想マシンで、ディスクパーティションのサイズを拡張します。	VMware の次のトピックの手順に従います。 "ディスクパーティションのサイズを拡張する"

ユーザアクセスの管理

Active IQ Unified Manager へのユーザアクセスを制御するために、ロールを作成し、機能を割り当てることができます。Unified Managerで選択したオブジェクトにアクセスするために必要な権限を持つユーザを特定できます。これらのロールと機能を持つユーザのみがUnified Managerでオブジェクトを管理できます。

ユーザを追加する

ユーザページを使用して、ローカルユーザまたはデータベースユーザを追加できます。また、認証サーバに属するリモートユーザやリモートグループを追加することもできます。追加したユーザにロールを割り当てることで、ユーザはロールの権限に基づいて Unified Manager でストレージオブジェクトやデータを管理したり、データベースのデータを表示したりできます。

- 必要なもの *
- アプリケーション管理者のロールが必要です。
- リモートのユーザまたはグループを追加する場合は、リモート認証を有効にし、認証サーバを設定しておく必要があります。
- SAML 認証を設定して、グラフィカルインターフェイスにアクセスするユーザをアイデンティティプロバイダ（IdP）で認証する場合は、これらのユーザが「morte」ユーザとして定義されていることを確認

します。

SAML 認証が有効になっている場合、「ローカル」または「メンテナンス」タイプのユーザーに UI へのアクセスは許可されません。

Windows Active Directory からグループを追加した場合は、ネストされたサブグループが無効になっていないかぎり、すべての直接メンバーとネストされたサブグループは Unified Manager で認証できます。OpenLDAP またはその他の認証サービスからグループを追加した場合は、そのグループの直接のメンバーだけが Unified Manager で認証されます。

手順

1. 左側のナビゲーションペインで、* 一般 * > * ユーザー * をクリックします。
2. [ユーザー] ページで、[* 追加] をクリックします。
3. [ユーザーの追加] ダイアログボックスで、追加するユーザーのタイプを選択し、必要な情報を入力します。

必要なユーザ情報を入力するときは、そのユーザに固有の E メールアドレスを指定する必要があります。複数のユーザで共有している E メールアドレスは指定しないでください。

4. [追加 (Add)] をクリックします。

データベースユーザを作成しています

Workflow Automation と Unified Manager の間の接続をサポートする場合や、データベースビューにアクセスする場合は、まず Unified Manager Web UI で、Integration Schema ロールまたは Report Schema ロールを持つデータベースユーザを作成する必要があります。

- 必要なもの *

アプリケーション管理者のロールが必要です。

データベースユーザは、Workflow Automation との統合およびレポート固有のデータベースビューへのアクセスを行うことができます。データベースユーザは、Unified Manager Web UI やメンテナンスコンソールにはアクセスできず、API 呼び出しも実行できません。

手順

1. 左側のナビゲーションペインで、* 一般 * > * ユーザー * をクリックします。
2. ユーザーページで、* 追加 * をクリックします。
3. [ユーザーの追加] ダイアログボックスの [タイプ] ドロップダウンリストで [データベースユーザー *] を選択します。
4. データベースユーザの名前とパスワードを入力します。
5. [* 役割 *] ドロップダウンリストで、適切な役割を選択します。

実行する作業	このロールを選択します
Unified Manager を Workflow Automation に接続しています	統合スキーマ
レポートおよびその他のデータベースビューにアクセスする	レポートスキーマ

6. [追加 (Add)] をクリックします。

ユーザ設定の編集

各ユーザを指定する E メールアドレスやロールなどのユーザ設定を編集することができます。たとえば、ストレージオペレータのユーザのロールを変更して、そのユーザにストレージ管理者の権限を割り当てることができます。

- 必要なもの *

アプリケーション管理者のロールが必要です。

ユーザに割り当てられているロールを変更すると、次のいずれかのアクションが発生したときに変更が適用されます。

- ユーザが Unified Manager からログアウトして再度ログインしたとき
- セッションのタイムアウトが 24 時間に達しました。

手順

1. 左側のナビゲーションペインで、* 一般 * > * ユーザー * をクリックします。
2. ユーザーページで、設定を編集するユーザーを選択し、* 編集 * をクリックします。
3. [ユーザーの編集] ダイアログボックスで、ユーザーに指定されている適切な設定を編集します。
4. [保存 (Save)] をクリックします。

ユーザの表示

ユーザページを使用して、Unified Manager を使用してストレージオブジェクトとデータを管理するユーザのリストを表示できます。ユーザの詳細を表示できます。これには、ユーザ名、ユーザのタイプ、E メールアドレス、ユーザに割り当てられているロールなどの情報が含まれます。

- 必要なもの *

アプリケーション管理者のロールが必要です。

ステップ

1. 左側のナビゲーションペインで、* 一般 * > * ユーザー * をクリックします。

ユーザまたはグループを削除する

管理サーバデータベースから 1 人以上のユーザを削除して、特定のユーザが Unified Manager にアクセスできないようにすることができます。また、グループを削除して、グループ内のすべてのユーザが管理サーバにアクセスできないようにすることもできます。

- 必要なもの *
- リモートグループを削除するときは、リモートグループのユーザに割り当てられているイベントを再割り当てしておく必要があります。

ローカルユーザまたはリモートユーザを削除する場合は、それらのユーザに割り当てられていたイベントの割り当てが自動的に解除されます。

- アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* 一般 * > * ユーザー * をクリックします。
2. [ユーザー] ページで、削除するユーザーまたはグループを選択し、[削除 *] をクリックします。
3. [はい] をクリックして削除を確定します。

RBAC とは

RBAC（ロールベースアクセス制御）を使用すると、Active IQ Unified Manager サーバのさまざまな機能やリソースにアクセスできるユーザを制御できます。

ロールベースアクセス制御の機能

管理者は、ロールベースアクセス制御（RBAC）を使用してロールを定義することで、ユーザのグループを管理できます。特定の機能のアクセスを選択した管理者に制限する必要がある場合は、その管理者の管理者アカウントを設定する必要があります。管理者が表示できる情報と、管理者が実行できる処理を制限する場合は、作成した管理者アカウントにロールを適用する必要があります。

管理サーバでは、ユーザログインとロールの権限に対して RBAC を使用します。管理サーバで管理ユーザアクセスのデフォルト設定を変更していない場合は、ログインして設定を表示する必要はありません。

特定の権限を必要とする処理を開始すると、管理サーバによってログインを求められます。たとえば、管理者アカウントを作成するには、アプリケーション管理者アカウントのアクセス権でログインする必要があります。

ユーザタイプの定義

ユーザは、アカウントの種類に基づいて、リモートユーザ、リモートグループ、ローカルユーザ、データベースユーザ、およびメンテナンスユーザの各タイプに分類されます。それぞれのタイプには、管理者ロールを持つユーザによって独自のロールが割り当てられます。

Unified Manager には次のユーザタイプがあります。

- * メンテナンスユーザ *

Unified Manager の初期設定時に作成されます。メンテナンスユーザは、別のユーザを作成してロールを割り当てます。メンテナンスコンソールにアクセスできる唯一のユーザでもあります。Unified Manager を Red Hat Enterprise Linux または CentOS システムにインストールしている場合、メンテナンスユーザのユーザ名は「umadmin」です。

- * ローカルユーザ *

Unified Manager UI にアクセスし、メンテナンスユーザまたはアプリケーション管理者ロールを持つユーザから割り当てられたロールに基づいて操作を実行します。

- * リモートグループ *

認証サーバに保存されているクレデンシャルを使用して Unified Manager UI にアクセスするユーザのグループです。このアカウントの名前は、認証サーバに保存されているグループの名前と一致している必要があります。リモートグループのユーザは、各自のユーザクレデンシャルを使用して Unified Manager UI にアクセスできます。リモートグループに割り当てられたロールに基づいて操作を実行できます。

- * リモートユーザ *

認証サーバに保存されているクレデンシャルを使用して Unified Manager UI にアクセスします。リモートユーザは、メンテナンスユーザまたはアプリケーション管理者ロールを持つユーザから割り当てられたロールに基づいて操作を実行します。

- * データベースユーザ *

Unified Manager データベースのデータへの読み取り専用アクセスが許可されます。Unified Manager の Web インターフェイスやメンテナンスコンソールにはアクセスできず、API 呼び出しも実行できません。

ユーザロールの定義

メンテナンスユーザまたはアプリケーション管理者が、各ユーザにロールを割り当てます。各ロールには特定の権限が含まれています Unified Manager で実行できる操作の範囲は、割り当てられたロールとその権限で決まります。

Unified Manager には、事前定義された次のユーザロールが用意されて

- * 演算子 *

履歴や容量の傾向など、Unified Manager によって収集されたストレージシステムの情報やその他のデータを表示します。このロールを割り当てられたストレージオペレータは、イベントについて、表示、割り当て、応答、解決、メモの追加などの操作が可能です。

- * ストレージ管理者 *

Unified Manager でのストレージ管理処理の設定を行います。このロールを割り当てられたストレージ管理者は、しきい値の設定、およびアラートなどのストレージ管理用のオプションやポリシーの作成が可能です。

• * アプリケーション管理者 *

ストレージ管理以外の設定を行います。ユーザ、セキュリティ証明書、データベースアクセスのほか、認証などの管理オプションを使用できます。SMTP、ネットワーク、および AutoSupport。



Unified Manager を Linux システムにインストールした場合は、アプリケーション管理者ロールが割り当てられた最初のユーザに自動的に「umadmin」という名前が付けられます。

• * 統合スキーマ *

Unified Manager と OnCommand Workflow Automation（WFA）の統合用に Unified Manager のデータベースビューにアクセスするための読み取り専用アクセスが許可されます。

• * レポートスキーマ *

レポートおよびその他のデータベースビューに Unified Manager データベースから直接アクセスするための読み取り専用アクセスが許可されます。表示できるデータベースは次のとおりです。

- NetApp_model_view
- パフォーマンス
- ocum
- ocum_report
- ocum_report_BIRT
- OPM
- 頭皮管理者

Unified Manager のユーザロールと機能

Unified Manager で実行できる操作は、割り当てられているユーザロールに基づいて決まります。

次の表に、各ユーザロールで実行できる機能を示します。

機能	演算子	ストレージ管理者	アプリケーション管理者	統合スキーマ	レポートスキーマ
ストレージシステムの情報を表示する	•	•	•	•	•
履歴や容量のトレンドなど、その他のデータを確認できます	•	•	•	•	•

機能	演算子	ストレージ管理者	アプリケーション管理者	統合スキーマ	レポートスキーマ
イベントを表示、割り当て、解決します	•	•	•		
SVM の関連付けやリソースプールなどのストレージサービスオブジェクトを表示する	•	•	•		
しきい値ポリシーを表示します	•	•	•		
SVM の関連付けやリソースプールなどのストレージサービスオブジェクトを管理する		•	•		
アラートを定義		•	•		
ストレージ管理オプションの管理		•	•		
ストレージ管理ポリシーを管理する		•	•		
ユーザを管理します			•		
管理オプションの管理			•		
しきい値ポリシーを定義			•		
データベースアクセスの管理			•		

機能	演算子	ストレージ管理者	アプリケーション管理者	統合スキーマ	レポートスキーマ
WFA との統合の管理とデータベースビューへのアクセス				•	
レポートのスケジュール設定と保存		•	•		
管理アクションから「Fix it」オペレーションを実行します		•	•		
データベースビューへの読み取り専用アクセスを提供します					•

SAML 認証の設定を管理する

リモート認証の設定が完了したら、Security Assertion Markup Language（SAML）認証を有効にして、Unified Manager の Web UI にアクセスするリモートユーザをセキュアなアイデンティティプロバイダ（IdP）で認証するように設定できます。

SAML 認証を有効にしたあとで Unified Manager のグラフィカルユーザインターフェイスにアクセスできるのはリモートユーザのみです。ローカルユーザとメンテナンスユーザは UI にアクセスできません。この設定は、メンテナンスコンソールにアクセスするユーザには影響しません。

アイデンティティプロバイダの要件

すべてのリモートユーザについてアイデンティティプロバイダ（IdP）を使用して SAML 認証を実行するように Unified Manager で設定するときは、Unified Manager に正しく接続できるように、いくつかの必要な設定を確認しておく必要があります。

Unified Manager の URI とメタデータを IdP サーバに入力する必要があります。この情報は、Unified Manager の SAML 認証ページからコピーできます。Unified Manager は、Security Assertion Markup Language（SAML）標準のサービスプロバイダ（SP）とみなされます。

サポートされている暗号化標準

- Advanced Encryption Standard（AES）：AES-128 および AES-256
- Secure Hash Algorithm（SHA）：SHA-1 および SHA-256

検証済みのアイデンティティプロバイダ

- Shibboleth
- Active Directory フェデレーションサービス (ADFS)

ADFS の設定要件

- 3 つの要求ルールを次の順序で定義する必要があります。これらは、この証明書利用者信頼エントリに対する ADFS SAML 応答を Unified Manager で解析するために必要です。

要求規則	価値
Sam - アカウント名	名前 ID
Sam - アカウント名	urn : OID : 0.9.2342.19200300.100.1.1
トークングループ — 修飾されていない名前	urn : OID : 1.3.6.1.4.1.5923.1.5.1.1

- 認証方法を「フォーム認証」に設定する必要があります。設定しないと、Unified Manager からログアウトするときにユーザにエラーが表示されることがあります。次の手順を実行します。
 - a. ADFS 管理コンソールを開きます。
 - b. 左側のツリー・ビューで [Authentication Policies] フォルダをクリックします
 - c. 右の [アクション] で、[グローバルプライマリ認証ポリシーの編集] をクリックします。
 - d. イン트라ネット認証方式をデフォルトの「Windows 認証」ではなく「フォーム認証」に設定します。
- Unified Manager のセキュリティ証明書が CA 署名証明書の場合、IdP 経由でのログインが拒否されることがあります。この問題を解決する方法は 2 つあります。
 - 次のリンクの手順に従って、CA 証明書チェーンの関連する証明書利用者についての ADFS サーバでの失効チェックを無効にします。

["証明書利用者信頼ごとの失効チェックを無効にします"](#)

- ADFS サーバ内にある CA サーバで Unified Manager サーバ証明書要求に署名します。

その他の設定要件

- Unified Manager のクロックスキューは 5 分に設定されているため、IdP サーバと Unified Manager サーバの時間の差が 5 分を超えないようにします。時間の差が 5 分を超えると認証が失敗します。

SAML 認証の有効化

Security Assertion Markup Language (SAML) 認証を有効にして、Unified Manager の Web UI にアクセスするリモートユーザをセキュアなアイデンティティプロバイダ (IdP) で認証するように設定できます。

- 必要なもの *
- リモート認証を設定し、正常に実行されることを確認しておく必要があります。

- アプリケーション管理者ロールが割り当てられたリモートユーザまたはリモートグループを少なくとも 1 つ作成しておく必要があります。
- アイデンティティプロバイダ（IdP）が Unified Manager でサポートされ、設定が完了している必要があります。
- IdP の URL とメタデータが必要です。
- IdP サーバへのアクセスが必要です。

Unified Manager で SAML 認証を有効にしたあと、Unified Manager サーバのホスト情報を使用して IdP を設定するまでは、ユーザはグラフィカルユーザインターフェイスにアクセスできません。そのため、設定プロセスを開始する前に、両方の接続を完了できるように準備しておく必要があります。IdP の設定は、Unified Manager の設定前にも設定後にも実行できます。

SAML 認証を有効にしたあとで Unified Manager のグラフィカルユーザインターフェイスにアクセスできるのはリモートユーザのみです。ローカルユーザとメンテナンスユーザは UI にアクセスできません。この設定は、メンテナンスコンソール、Unified Manager コマンド、ZAPI にアクセスするユーザには影響しません。



このページで SAML の設定を完了すると、Unified Manager が自動的に再起動されます。

手順

1. 左側のナビゲーションペインで、* General * > * SAML Authentication * をクリックします。
2. Enable SAML authentication * チェックボックスをオンにします。

IdP の接続の設定に必要なフィールドが表示されます。

3. IdP の URI と Unified Manager サーバを IdP に接続するために必要な IdP メタデータを入力します。

IdP サーバに Unified Manager サーバから直接アクセスできる場合は、IdP の URI を入力したあとに「* IdP メタデータの取得」ボタンをクリックすると、IdP のメタデータフィールドに自動的に値が入力されます。

4. Unified Manager のホストメタデータ URI をコピーするか、メタデータを XML テキストファイルに保存します。

この情報を使用して IdP サーバを設定できます。

5. [保存（Save）] をクリックします。

設定を完了して Unified Manager を再起動するかどうかの確認を求めるメッセージボックスが表示されます。

6. [確認してログアウト *] をクリックすると、Unified Manager が再起動します。

許可されたリモートユーザが Unified Manager のグラフィカルインターフェイスにアクセスする際にクレデンシャルを入力するページが、次回から Unified Manager のログインページではなく IdP のログインページに変わります。

まだ完了していない場合は、IdP にアクセスし、Unified Manager サーバの URI とメタデータを入力して設定を完了します。



アイデンティティプロバイダに ADFS を使用している場合は、Unified Manager GUI で ADFS のタイムアウトが考慮されず、Unified Manager のセッションタイムアウトに達するまでセッションが継続されます。GUI セッションのタイムアウトを変更するには、* General * > * Feature Settings * > * Inactivity Timeout * をクリックします。

SAML 認証に使用するアイデンティティプロバイダを変更する

Unified Manager でリモートユーザの認証に使用するアイデンティティプロバイダ (IdP) を変更することができます。

- 必要なもの *
- IdP の URL とメタデータが必要です。
- IdP へのアクセスが必要です。

新しい IdP の設定は、Unified Manager の設定前にも設定後にも実行できます。

手順

1. 左側のナビゲーションペインで、* General * > * SAML Authentication * をクリックします。
2. 新しい IdP の URI と Unified Manager サーバを IdP に接続するために必要な IdP メタデータを入力します。

Unified Manager サーバから IdP に直接アクセスできる場合は、IdP の URL を入力したあとに「* IdP メタデータの取得」ボタンをクリックすると、IdP のメタデータフィールドに自動的に値が入力されます。

3. Unified Manager のメタデータ URI をコピーするか、メタデータを XML テキストファイルに保存します。
4. [構成の保存 *] をクリックします。

設定を変更するかどうかの確認を求めるメッセージボックスが表示されます。

5. [OK] をクリックします。

新しい IdP にアクセスし、Unified Manager サーバの URI とメタデータを入力して設定を完了します。

許可されたリモートユーザが Unified Manager のグラフィカルインターフェイスにアクセスする際にクレデンシャルを入力するページが、次回から古い IdP のログインページではなく新しい IdP のログインページに変わります。

Unified Manager セキュリティ証明書変更後に SAML 認証設定を更新しています

Unified Manager サーバにインストールされている HTTPS セキュリティ証明書が変更されたときは、SAML 認証の設定を更新する必要があります。証明書は、ホストシステムの名前を変更したり、ホストシステムに新しい IP アドレスを割り当てたり、システムのセキュリティ証明書を手動で変更したりすると更新されます。

セキュリティ証明書が変更されたあとに Unified Manager サーバが再起動されると、SAML 認証は機能せず、ユーザは Unified Manager のグラフィカルインターフェイスにアクセスできなくなります。ユーザインターフェイスに再びアクセスできるようにするには、IdP サーバと Unified Manager サーバの両方で SAML 認

証の設定を更新する必要があります。

手順

1. メンテナンスコンソールにログインします。
2. メインメニュー * で、 * SAML 認証を無効にする * オプションの番号を入力します。

SAML 認証を無効にして Unified Manager を再起動することの確認を求めるメッセージが表示されます。

3. 更新された FQDN または IP アドレスを使用して Unified Manager のユーザインターフェイスを起動し、更新されたサーバ証明書をブラウザで受け入れ、メンテナンスユーザのクレデンシャルを使用してログインします。
4. [* Setup/Authentication] ページで [* SAML Authentication*] タブを選択し、IdP 接続を設定します。
5. Unified Manager のホストメタデータ URI をコピーするか、メタデータを XML テキストファイルに保存します。
6. [保存 (Save)] をクリックします。

設定を完了して Unified Manager を再起動するかどうかの確認を求めるメッセージボックスが表示されます。

7. [確認してログアウト *] をクリックすると、Unified Manager が再起動します。
8. IdP サーバにアクセスし、Unified Manager サーバの URI とメタデータを入力して設定を完了します。

アイデンティティプロバイダ	設定手順
ADFS (ADFS)	<ol style="list-style-type: none">a. ADFS 管理 GUI で、既存の証明書利用者信頼エントリを削除します。b. を使用して、新しい証明書利用者信頼エントリを追加します saml_sp_metadata.xml 更新したUnified Managerサーバを使用します。c. Unified Manager がこの証明書利用者信頼エントリに対する ADFS SAML 応答を解析するために必要な 3 つの要求規則を定義します。d. ADFS Windows サービスを再開します。
Shibboleth	<ol style="list-style-type: none">a. Unified Managerサーバの新しいFQDNをで更新します attribute-filter.xml および relying-party.xml ファイル。b. Apache Tomcat Web サーバを再起動し、ポート 8005 がオンラインになるまで待ちます。

9. Unified Manager にログインし、IdP 経由で SAML 認証が想定どおりに機能することを確認します。

SAML 認証を無効にします

Unified Manager Web UI にログインするリモートユーザのセキュアなアイデンティティプロバイダ (IdP) による認証を中止する場合は、SAML 認証を無効にします。SAML

認証が無効な場合は、Active Directory や LDAP などの設定済みのディレクトリサービスプロバイダがサインオン認証を実行します。

SAML 認証を無効にすると、設定されているリモートユーザに加え、ローカルユーザとメンテナンスユーザもグラフィカルユーザインターフェイスにアクセスできるようになります。

SAML 認証は、グラフィカルユーザインターフェイスにアクセスできない場合は Unified Manager メンテナンスコンソールを使用して無効にすることもできます。



SAML 認証を無効にしたあと、Unified Manager が自動的に再起動されます。

手順

1. 左側のナビゲーションペインで、* General * > * SAML Authentication * をクリックします。
2. [SAML 認証を有効にする *] チェックボックスをオフにします。
3. [保存 (Save)] をクリックします。

設定を完了して Unified Manager を再起動するかどうかの確認を求めるメッセージボックスが表示されます。

4. [確認してログアウト *] をクリックすると、Unified Manager が再起動します。

リモートユーザが Unified Manager のグラフィカルインターフェイスにアクセスする際にクレデンシャルを入力するページが、次回から IdP のログインページではなく Unified Manager のログインページに変わります。

IdP にアクセスし、Unified Manager サーバの URI とメタデータを削除します。

メンテナンスコンソールから **SAML** 認証を無効にする

Unified Manager GUI にアクセスできない場合は、必要に応じてメンテナンスコンソールから SAML 認証を無効にすることができます。この状況は、設定に誤りがある場合や IdP にアクセスできない場合に発生します。

- 必要なもの *

メンテナンスコンソールにメンテナンスユーザとしてアクセスできる必要があります。

SAML 認証が無効な場合は、Active Directory や LDAP などの設定済みのディレクトリサービスプロバイダがサインオン認証を実行します。設定されているリモートユーザに加え、ローカルユーザとメンテナンスユーザもグラフィカルユーザインターフェイスにアクセスできるようになります。

SAML 認証は、UI のセットアップ / 認証のページから無効にすることもできます。



SAML 認証を無効にしたあと、Unified Manager が自動的に再起動されます。

手順

1. メンテナンスコンソールにログインします。
2. メインメニュー * で、* SAML 認証を無効にする * オプションの番号を入力します。

SAML 認証を無効にして Unified Manager を再起動することの確認を求めるメッセージが表示されます。

3. 「*y*」と入力して Enter キーを押すと、Unified Manager が再起動します。

リモートユーザが Unified Manager のグラフィカルインターフェイスにアクセスする際にクレデンシャルを入力するページが、次回から IdP のログインページではなく Unified Manager のログインページに変わります。

必要に応じて、IdP にアクセスして Unified Manager サーバの URL とメタデータを削除します。

SAML Authentication ページ

SAML 認証ページを使用して、Unified Manager の Web UI にログインするリモートユーザを SAML を使用してセキュアなアイデンティティプロバイダ（IdP）で認証するように Unified Manager を設定できます。

- SAML 設定を作成または変更するには、アプリケーション管理者ロールが必要です。
- リモート認証を設定しておく必要があります。
- リモートユーザまたはリモートグループを少なくとも 1 つ設定しておく必要があります。

リモート認証とリモートユーザの設定が完了したら、SAML 認証を有効にするチェックボックスをオンにして、セキュアなアイデンティティプロバイダを使用した認証を有効にすることができます。

- * IdP URI *

Unified Manager サーバから IdP にアクセスするための URI。URI の例を次に示します。

ADFS の URI の例：

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml
```

Shibboleth の URI の例：

```
https://centos7.ntap2016.local/idp/shibboleth
```

- * IdP メタデータ *

XML 形式の IdP メタデータ。

Unified Manager サーバから IdP の URL にアクセスできる場合は、「* IdP メタデータの取得方法 *」ボタンをクリックしてこのフィールドに値を入力できます。

- * ホストシステム（FQDN） *

インストール時に定義された Unified Manager ホストシステムの FQDN。この値は必要に応じて変更できます。

- * ホスト URI *

IdP から Unified Manager ホストシステムにアクセスするための URI。

- * ホストメタデータ *

XML 形式のホストシステムメタデータ

認証の管理

Unified Manager サーバで LDAP または Active Directory のいずれかを使用して認証を有効にし、サーバと連携してリモートユーザを認証するように設定することができます。

リモート認証の有効化、認証サービスのセットアップ、認証サーバの追加については、「Unified Manager でアラート通知を送信するための設定」の前のセクションを参照してください。

認証サーバを編集しています

Unified Manager サーバが認証サーバとの通信に使用するポートを変更することができます。

- 必要なもの *

アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* 一般 * > * リモート認証 * をクリックします。
2. [ネストされたグループの検索を無効にする *] ボックスをオンにします。
3. [* 認証サーバ *] 領域で、編集する認証サーバを選択し、[* 編集] をクリックします。
4. Edit Authentication Server* ダイアログボックスで、ポートの詳細を編集します。
5. [保存 (Save)] をクリックします。

認証サーバを削除しています

Unified Manager サーバが認証サーバと通信できないようにするには、認証サーバを削除します。たとえば、管理サーバが通信する認証サーバを変更する場合は、認証サーバを削除して新しい認証サーバを追加できます。

- 必要なもの *

アプリケーション管理者のロールが必要です。

認証サーバを削除すると、認証サーバのリモートユーザまたはリモートグループは Unified Manager にアクセスできなくなります。

手順

1. 左側のナビゲーションペインで、* 一般 * > * リモート認証 * をクリックします。
2. 削除する認証サーバーを 1 つ以上選択し、* 削除 * をクリックします。
3. [はい] をクリックして、削除要求を確定します。

[セキュアな接続を使用する *] オプションが有効になっている場合、認証サーバに関連付けられている証明書は認証サーバとともに削除されます。

Active Directory または OpenLDAP による認証

管理サーバでリモート認証を有効にし、管理サーバが認証サーバと通信するように設定すると、認証サーバ内のユーザが Unified Manager にアクセスできるようになります。

事前定義された次の認証サービスのいずれかを使用するか、独自の認証サービスを指定できます。

- Microsoft Active Directory の略



Microsoft のライトウェイトディレクトリサービスは使用できません。

- OpenLDAP

必要な認証サービスを選択し、適切な認証サーバを追加してその認証サーバのリモートユーザが Unified Manager にアクセスできるようにします。リモートのユーザまたはグループのクレデンシャルは、認証サーバで管理されます。管理サーバでは、設定された認証サーバ内のリモートユーザの認証に Lightweight Directory Access Protocol (LDAP) を使用します。

Unified Manager で作成されたローカルユーザについては、管理サーバのデータベースでユーザ名とパスワードが管理されます。管理サーバで認証が実行され、Active Directory 認証または OpenLDAP 認証が使用されることはありません。

監査ログ

監査ログを使用すると、監査ログが侵害されたかどうかを検出できます。ユーザが実行するすべてのアクティビティが監視され、監査ログに記録されます。監査は、Active IQ Unified Manager のすべてのユーザーインターフェイスと公開されている API の機能に対して実行されます。

Active IQ Unified Manager で使用可能なすべての監査ログファイルを表示してアクセスするには、*監査ログ：ファイルビュー*を使用します。監査ログ：ファイルビュー内のファイルは、作成日に基づいて一覧表示されます。このビューには、インストール時またはシステム内にアップグレードされたときにキャプチャされたすべての監査ログの情報が表示されます。Unified Manager で何らかの操作を実行すると、情報が更新され、ログに記録されます。各ログファイルのステータスは、ログファイルの改ざんや削除を検出するためにアクティブに監視される「File Integrity Status」属性を使用して取得されます。システムで監査ログが使用可能になると、監査ログの状態は次のいずれかになります。

状態	説明
アクティブ	ログが現在ログに記録されているファイル。
正常	非アクティブで圧縮され、システムに格納されているファイル。

状態	説明
改ざんされた	手動でファイルを編集したユーザーによって侵害されたファイル。
manual_delete_delete	許可されたユーザーによって削除されたファイル。
rollOver_delete	ローリング設定ポリシーに基づいて移動したために削除されたファイル。
予期しない削除です	不明な理由で削除されたファイル。

Audit Log ページには、次のコマンドボタンがあります。

- 設定
- 削除
- ダウンロード

delete ボタンを使用すると、Audit Logs ビューに表示されている監査ログを削除できます。監査ログを削除したり、ファイルを削除する理由を指定したりできます。これにより、あとで有効な削除を確認するのに役立ちます。理由列には、削除操作を実行したユーザの名前と理由が表示されます。



ログファイルを削除すると、原因によってシステムからファイルが削除されますが、DB テーブル内のエントリは削除されません。

監査ログは、監査ログセクションの * download * ボタンを使用して Active IQ Unified Manager からダウンロードし、監査ログファイルをエクスポートできます。「normal」または「Tampered」とマークされたファイルは、圧縮された形式でダウンロードされます .gzip の形式で入力し

監査ログファイルは定期的にアーカイブされ、参照用にデータベースに保存されます。アーカイブの前に、監査ログはセキュリティと整合性を維持するためにデジタル署名されます。

フルAutoSupport バンドルの生成時に、サポートバンドルにはアーカイブされた監査ログファイルとアクティブな監査ログファイルの両方が含まれます。ただし、簡易サポートバンドルが生成されると、アクティブな監査ログのみが含まれます。アーカイブされた監査ログは含まれません。

監査ログを設定しています

監査ログセクションの *Configure* ボタンを使用して、監査ログファイルのローリングポリシーを設定したり、監査ログのリモートロギングを有効にしたりできます。

システムに保存するデータの量と頻度に応じて、* 最大ファイルサイズ * と * 監査ログの保持日数 * の値を設定できます。フィールド * total audit log size * は、システムに存在する監査ログデータの合計サイズです。ロールオーバーポリシーは、「* 監査ログの保持日数 *」、「* 最大ファイルサイズ *」、および「* 監査ログの合計サイズ *」フィールドの値によって決まります。監査ログのバックアップのサイズが、監査ログの合計サイズ * で設定された値に達すると、最初にアーカイブされたファイルが削除されます。つまり、最も古いファイルが削除されます。しかし、ファイルエントリはデータベースで引き続き使用でき、「ロールオーバー削除」とマークされます。監査ログの保持日数 * は、監査ログファイルを保持する日数です。このフィールドに設定された値より古いファイルは、ロールオーバーされます。

手順

1. [*** 監査ログ >**] > [**構成 ***] をクリックします。
2. 最大ファイルサイズ *、監査ログの合計サイズ *、監査ログの保持日数 * の値を入力します。

リモート・ロギングを有効にする場合は、* リモート・ロギングを有効にする * を選択する必要があります。

監査ログのリモートロギングを有効にする

監査ログの設定ダイアログ・ボックスのリモート・ログを有効にするチェックボックスをオンにすると、リモート監査ログを有効にできます。この機能を使用すると、監査ログをリモートの syslog サーバに転送できます。これにより、スペースに制約がある場合でも監査ログを管理できます。

監査ログのリモートロギングは、Active IQ Unified Manager サーバ上の監査ログファイルが改ざんされた場合に備えて、改ざんを防止するためのバックアップ機能を提供します。

手順

1. [監査ログの設定 *] ダイアログボックスで、[リモートログを有効にする *] チェックボックスをオンにします。

リモートロギングを設定するための追加フィールドが表示されます。

2. 接続先のリモートサーバの * hostname * と * port * を入力します。
3. サーバー CA 証明書 * フィールドで、* 参照 * をクリックしてターゲットサーバのパブリック証明書を選択します。

証明書はにアップロードする必要があります。pem の形式で入力しこの証明書は、ターゲットの syslog サーバから取得し、有効期限が切れていないことを確認する必要があります。証明書には、の一部として選択した「ホスト名」が含まれている必要があります SubjectAltName (SAN) 属性。

4. 次のフィールドの値を入力します。* charset*、* connection timeout *、* reconnection delay *。

これらのフィールドの値はミリ秒単位で指定します。

5. [format] フィールドと [protocol] フィールドで、必要な syslog 形式と TLS プロトコルのバージョンを選択します。
6. ターゲット Syslog サーバで証明書ベースの認証が必要な場合は、* クライアント認証を有効にする * チェックボックスを選択します。

監査ログ設定を保存する前に、クライアント認証証明書をダウンロードして Syslog サーバにアップロードする必要があります。そうしないと、接続が失敗します。syslog サーバのタイプによっては、クライアント認証証明書のハッシュの作成が必要になる場合があります。

例：syslog-ngには、コマンドを使用して証明書の<hash>が作成されている必要があります `openssl x509 -noout -hash -in cert.pem` をクリックし、クライアント認証証明書を<hash>.0のあとのファイルにシンボリックリンクする必要があります。

7. サーバとの接続を設定し、リモートロギングを有効にするには、* Save * をクリックします。

[監査ログ] ページに移動します。

Remote Authentication ページの略

Remote Authentication ページでは、Unified Manager Web UI にログインするリモートユーザを認証できるように、Unified Manager と認証サーバの通信を設定することができます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

[リモート認証を有効にする] チェックボックスをオンにすると、認証サーバを使用してリモート認証を有効にできます。

- * 認証サービス *

Active Directory や OpenLDAP などのディレクトリサービスプロバイダでユーザを認証するように管理サーバを設定するか、または独自の認証メカニズムを指定できます。認証サービスは、リモート認証を有効にした場合にのみ指定できます。

- * Active Directory *

- 管理者の名前

認証サーバの管理者名を指定します。

- パスワード

認証サーバにアクセスするためのパスワードを指定します。

- ベース識別名

認証サーバでのリモートユーザの場所を指定します。たとえば、認証サーバのドメイン名が `+ou@domain.com +` である場合、ベース識別名は `* cn=ou、dc=domain、dc=com *` です。

- ネストされたグループの検索を無効化

ネストされたグループの検索を有効にするか無効にするかを指定します。デフォルトでは、このオプションは無効になっています。Active Directory を使用する場合は、ネストされたグループのサポートを無効にすることで認証を高速化できます。

- セキュアな接続を使用します

認証サーバとの通信に使用する認証サービスを指定します。

- * OpenLDAP *

- バインド識別名

認証サーバでリモートユーザを検出する際にベース識別名とともに使用されるバインド識別名を指定します。

- バインドパスワード

認証サーバにアクセスするためのパスワードを指定します。

- ベース識別名

認証サーバでのリモートユーザの場所を指定します。たとえば、認証サーバのドメイン名が + [ou@domain.com](#) + である場合、ベース識別名は * cn=ou 、 dc=domain 、 dc=com * です。

- セキュアな接続を使用します

LDAP認証サーバとの通信にSecure LDAPを使用することを指定します。

- * その他 *

- バインド識別名

設定した認証サーバでリモートユーザを検出する際にベース識別名とともに使用されるバインド識別名を指定します。

- バインドパスワード

認証サーバにアクセスするためのパスワードを指定します。

- ベース識別名

認証サーバでのリモートユーザの場所を指定します。たとえば、認証サーバのドメイン名が + [ou@domain.com](#) + である場合、ベース識別名は * cn=ou 、 dc=domain 、 dc=com * です。

- プロトコルバージョン

認証サーバでサポートされる Lightweight Directory Access Protocol (LDAP) のバージョンを指定します。プロトコルのバージョンを自動的に検出するか、バージョン 2 または 3 に設定するかを指定できます。

- ユーザー名属性

管理サーバによって認証されるユーザログイン名を含む認証サーバ内の属性の名前を指定します。

- グループメンバーシップ属性

ユーザの認証サーバで指定されている属性と値に基づいて管理サーバのグループメンバーシップをリモートユーザに割り当てる値を指定します。

- UGID

リモートユーザが GroupOfUniqueNames オブジェクトのメンバーとして認証サーバに含まれている場合は、このオプションを使用して、 GroupOfUniqueNames オブジェクトで指定されている属性を基に管理サーバのグループメンバーシップをリモートユーザに割り当てることができます。

- ネストされたグループの検索を無効化

ネストされたグループの検索を有効にするか無効にするかを指定します。デフォルトでは、このオプションは無効になっています。Active Directory を使用する場合は、ネストされたグループのサポートを無効にすることで認証を高速化できます。

- メンバー

認証サーバがグループの個々のメンバーに関する情報を格納するために使用する属性の名前を指定します。

- ユーザオブジェクトクラス

リモート認証サーバ内のユーザのオブジェクトクラスを指定します。

- グループオブジェクトクラス

リモート認証サーバ内のすべてのグループのオブジェクトクラスを指定します。



Member, User Object Class, _Group オブジェクト *Class_attributes* に入力する値は、Active Directory、OpenLDAP、およびLDAPの設定に追加する値と同じである必要があります。そうしないと、認証が失敗する可能性があります。

- セキュアな接続を使用します

認証サーバとの通信に使用する認証サービスを指定します。



認証サービスを変更する場合は、既存の認証サーバをすべて削除してから新しい認証サーバを追加してください。

Authentication Servers 領域

Authentication Servers 領域には、管理サーバがリモートユーザの検索および認証のために通信する認証サーバが表示されます。リモートのユーザまたはグループのクレデンシャルは、認証サーバで管理されます。

- * コマンドボタン *

認証サーバを追加、編集、または削除できます。

- 追加 (Add)

認証サーバを追加できます。

追加する認証サーバがハイアベイラビリティペアを構成している（同じデータベースを使用している）場合は、パートナーの認証サーバも追加できます。これにより、いずれかの認証サーバにアクセスできない場合でも管理サーバはパートナーと通信できます。

- 編集

選択した認証サーバの設定を編集できます。

- 削除

選択した認証サーバを削除します。

- * 名前または IP アドレス *

管理サーバでユーザの認証に使用される認証サーバのホスト名または IP アドレスが表示されます。

- * ポート *

認証サーバのポート番号が表示されます。

- * 認証のテスト *

このボタンでは、リモートのユーザまたはグループを認証することで認証サーバの設定を検証します。

テストの際にユーザ名のみを指定すると、管理サーバは認証サーバでリモートユーザを検索しますが、ユーザの認証は行いません。ユーザ名とパスワードを指定すると、管理サーバはリモートユーザの検索と認証を行います。

リモート認証が無効になっている場合は、認証をテストできません。

セキュリティ証明書の管理

Unified Manager サーバで HTTPS を設定することで、セキュアな接続を介してクラスタを監視および管理できるようになります。

HTTPS セキュリティ証明書の表示

HTTPS 証明書の詳細をブラウザで取得した証明書と比較して、Unified Manager に対するブラウザの暗号化された接続が妨害されていないことを確認できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

証明書を表示すると、再生成された証明書の内容を検証したり、Unified Manager へのアクセスに使用できる Subject Alternative Name (SAN) を表示したりできます。

ステップ

1. 左側のナビゲーションペインで、* General * > * HTTPS Certificate * をクリックします。

HTTPS 証明書がページの上部に表示されます

HTTPS 証明書ページに表示されるものよりも詳細なセキュリティ証明書情報を表示する必要がある場合は、ブラウザで接続証明書を表示できます。

HTTPS 証明書署名要求のダウンロード

認証局にファイルを送信して署名を求めるために、現在の HTTPS セキュリティ証明書の証明書署名要求をダウンロードできます。CA 署名証明書は、中間者攻撃を阻止するのに役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

- 必要なもの *

アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* General * > * HTTPS Certificate * をクリックします。
2. [* HTTPS 証明書署名要求のダウンロード *] をクリックします。
3. を保存します <hostname>.csr ファイル。

認証局にファイルを送信して署名を求め、署名済み証明書をインストールできます。

CA 署名済みで返された HTTPS 証明書をインストールする

認証局から署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。アップロードしてインストールするファイルは、既存の自己署名証明書の署名済みバージョンである必要があります。CA 署名証明書は、中間者攻撃を阻止するのに役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

- 必要なもの *

次の作業を完了しておきます。

- 証明書署名要求ファイルをダウンロードし、認証局によって署名されています
- 証明書チェーンを PEM 形式で保存します
- チェーンに含まれるすべての証明書について、Unified Manager サーバ証明書からルート署名証明書への中間証明書も含めます

アプリケーション管理者のロールが必要です。



CSR 作成の証明書の有効期間が 397 日を超える場合、証明書の署名と返却の前に CA によって有効期間が 397 日に短縮されます

手順

1. 左側のナビゲーションペインで、* General * > * HTTPS Certificate * をクリックします。
2. [* HTTPS 証明書のインストール *] をクリックします。
3. 表示されるダイアログボックスで、「* ファイルを選択 ... *」をクリックして、アップロードするファイルを探します。
4. ファイルを選択し、* Install * をクリックしてファイルをインストールします。

詳細については、を参照してください ["外部ツールを使用して生成された HTTPS 証明書のインストール"](#)。

証明書チェーンの例

証明書チェーンファイルの表示例を次に示します。

```

-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----

```

外部ツールを使用して生成された **HTTPS** 証明書のインストール

自己署名または CA 署名の証明書をインストールできます。証明書は、OpenSSL、BoringSSL、LetsEncrypt などの外部ツールを使用して生成されます。

秘密鍵と証明書チェーンをロードするのは、外部で生成された公開鍵と秘密鍵のペアであるためです。許可される鍵ペアアルゴリズムは「RSA」と「EC」です。[一般] セクションの [HTTPS 証明書] ページで、[* HTTPS 証明書のインストール] オプションを使用できます。アップロードするファイルは、次の入力形式である必要があります。

1. Active IQ Unified Manager ホストに属するサーバの秘密鍵
2. 秘密鍵と一致するサーバの証明書
3. ルートまでの CA の証明書（上記の証明書への署名に使用）

EC キーペアを含む証明書をロードするための形式

許可される曲線は "prime256v1" と "ecp384r1" です。外部で生成された EC ペアを含む証明書の例：

```

-----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----

```

```

-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----

```

RSA キーペアを含む証明書をロードするための形式

ホスト証明書に属する RSA キーペアで使用できるキーサイズは、2048、3072、および 4096 です。外部で生成された *RSA キーペア* の証明書：

```

-----BEGIN RSA PRIVATE KEY-----
<RSA private key of Server>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----

```

証明書をアップロードしたら、Active IQ Unified Manager インスタンスを再起動して変更を有効にする必要があります。

外部で生成された証明書をアップロードする際にチェック

システムは、外部ツールを使用して生成された証明書をアップロードする際にチェックを実行します。いずれかのチェックに失敗すると、証明書は拒否されます。また、製品内の CSR から生成された証明書、および外部ツールを使用して生成された証明書の検証も含まれます。

- 入力された秘密鍵が、入力されたホスト証明書に照らして検証されます。
- ホスト証明書の Common Name （CN；共通名）とホストの FQDN の照合が行われます。

- ホスト証明書の Common Name（CN；共通名）を空または空白にしたり、localhost に設定したりすることはできません。
- 有効開始日は将来の日付にすることはできません。また、証明書の有効期限は過去の日付にすることはできません。
- 中間 CA または CA が存在する場合、証明書の有効開始日を将来の日付にすることはできません。また、有効期限は過去の日付にすることはできません。



入力内の秘密鍵を暗号化しないでください。暗号化された秘密鍵がある場合、それらの秘密鍵はシステムで拒否されます。

例 1.

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

例 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

例 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

証明書管理のページの説明

HTTPS 証明書ページを使用して、現在のセキュリティ証明書を表示したり、新しい HTTPS 証明書を生成したりできます。

HTTPS 証明書ページ

HTTPS 証明書ページでは、現在のセキュリティ証明書の表示、証明書署名要求のダウンロード、新しい自己署名 HTTPS 証明書の生成、新しい HTTPS 証明書のインストールを行うことができます。

新しい自己署名 HTTPS 証明書を生成していない場合は、インストール時に生成された証明書がこのページに表示されます。

コマンドボタン

各コマンドボタンを使用して次の処理を実行できます。

- * HTTPS 証明書署名要求 * をダウンロードします

現在インストールされている HTTPS 証明書の証明書要求をダウンロードします。認証局にファイルを送信して署名を求めるプロンプトがブラウザに表示され、<hostname> .CSR ファイルを保存します。

- * HTTPS 証明書をインストール *

認証局から署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。新しい証明書は、管理サーバを再起動すると有効になります。

- * HTTPS 証明書の再生成 *

現在のセキュリティ証明書に代わる新しい自己署名HTTPS証明書を生成できます。新しい証明書は、Unified Manager を再起動すると有効になります。

HTTPS 証明書の再生成ダイアログボックス

HTTPS 証明書の再生成ダイアログボックスでは、セキュリティ情報をカスタマイズし、その情報を使用して新しい HTTPS 証明書を生成できます。

このページには現在の証明書の情報が表示されます。

[現在の証明書属性を使用して再生成] および [現在の証明書属性を更新] を選択すると ' 現在の情報で証明書を再生成するか ' 新しい情報で証明書を生成できます

- * 共通名 *

必須保護する対象の完全修飾ドメイン名（FQDN）。

Unified Manager のハイアベイラビリティ構成では、仮想 IP アドレスを使用します。

- * 電子メール *

任意。組織に問い合わせるための E メールアドレス。通常は、証明書管理者または IT 部門の E メールアドレスです。

- * 会社名 *

任意。通常は会社の法人名です。

- * 部門 *

任意。社内の部署の名前。

- * 都市 *

任意。会社の所在地の市区町村。

- * 状態 *

任意。会社の所在地の都道府県。

- * 国 *

任意。会社の所在地の国。通常は ISO の 2 文字の国コードです。

- * 別名 *

必須既存のローカルホストやその他のネットワークアドレスに加えて、このサーバへのアクセスに使用できるプライマリ以外のドメイン名が追加されました。代行名はそれぞれカンマで区切ります。

証明書の代替名フィールドからローカル識別情報を削除する場合は 'ローカル識別情報を除外 (localhost など) チェックボックスをオンにしますこのチェックボックスをオンにすると、[代替名] フィールドに入力したフィールドのみが使用されます。空白のままにすると、結果の証明書に代替名フィールドがまったく表示されなくなります。

- * キーサイズ (キーアルゴリズム: RSA) *

キーアルゴリズムは rsa に設定されています。キーサイズは 2048、3072、または 4096 のいずれかを選択できます。デフォルトのキー・サイズは 2048 ビットに設定されています。

- * 有効期間 *

デフォルトの有効期間は 397 日です。以前のバージョンからアップグレードした場合は、以前の証明書の有効性が変更されていない可能性があります。

詳細については、を参照してください "[HTTPS証明書の生成](#)"。

ストレージを監視および管理する

Active IQ Unified Manager の概要

Active IQ Unified Manager（旧 OnCommand Unified Manager）を使用すると、ONTAP ストレージシステムの健全性とパフォーマンスを 1 つのインターフェイスから監視および管理できます。

Unified Manager には次の機能があります。

- ONTAP ソフトウェアがインストールされたシステムの検出、監視、通知
- 容量、セキュリティ、パフォーマンスなど、環境の健全性をダッシュボードに表示します。
- アラート、イベント、およびしきい値インフラが強化されています。
- IOPS（処理数）、MBps（スループット）、レイテンシ（応答時間）、利用率など、ワークロードのアクティビティを時系列で示す詳細なグラフを表示します。パフォーマンス容量とキャッシュ比率：
- クラスタコンポーネントを過剰に消費しているワークロードと、アクティビティの増加によってパフォーマンスが影響を受けたワークロードを特定します。
- 特定のインシデントやイベントに対処するために実行できる推奨される対処方法を提供します。一部のイベントには「修正」ボタンが表示され、問題をただちに解決できます。
- OnCommand Workflow Automation との統合により、保護ワークフローが自動化されています。
- LUN やファイル共有などの新しいワークロードを Unified Manager から直接作成し、パフォーマンスサービスレベルを割り当てて、そのワークロードを使用してアプリケーションにアクセスするユーザに対してパフォーマンスとストレージの目標を定義することができます。

Active IQ Unified Manager の健全性監視の概要

Active IQ Unified Manager（旧 OnCommand Unified Manager）では、ONTAP ソフトウェアを実行する多数のシステムを一元化されたユーザインターフェイスで監視できます。Unified Manager サーバインフラは拡張性とサポート性に優れ、高度な監視機能と通知機能を備えています。

Unified Manager の主な機能には、クラスタの可用性と容量の監視 / 通知 / 管理、保護機能の管理、診断データの収集とテクニカルサポートへの送信などがあります。

Unified Manager を使用してクラスタを監視できます。クラスタで問題が発生すると、Unified Manager のイベントを通じて問題の詳細が通知されます。一部のイベントでは、問題を解決するための対応策も提示されます。問題が発生したときに E メールや SNMP トラップで通知されるように、イベントにアラートを設定することができます。

Unified Manager では、アノテーションを関連付けることで環境内のストレージオブジェクトを管理できます。カスタムアノテーションを作成し、ルールに基づいて動的にクラスタ、Storage Virtual Machine（SVM）、およびボリュームを関連付けることができます。

また、それぞれのクラスタオブジェクトについて、容量や健全性のグラフに表示される情報を使用してストレージ要件を計画することもできます。

物理容量と論理容量

Unified Manager は、ONTAP ストレージオブジェクトに使用される物理スペースと論理スペースの概念を利用します。

- 物理容量：物理スペースは、ボリュームで使用されているストレージの物理ブロックを表します。「物理使用容量」は、通常、ストレージ効率化機能（重複排除や圧縮など）からのデータ削減のため、使用済み論理容量よりも小さくなります。
- 論理容量：論理スペースは、ボリューム内の使用可能なスペース（論理ブロック）を表します。論理スペースとは、重複排除や圧縮の結果を考慮せずに、理論上のスペースをどのように使用できるかを指します。「Logical space used」は、使用済みの物理スペースに加えて、設定済みの Storage Efficiency 機能（重複排除や圧縮など）による削減量を示します。Snapshot コピー、クローン、その他のコンポーネントが含まれ、データ圧縮やその他の物理スペースの削減が反映されていないため、この測定値は、多くの場合、物理使用容量よりも大きく表示されます。したがって、合計論理容量は、プロビジョニング済みスペースよりも多くなる可能性があります。

容量の単位

Unified Manager は、1024（ 2^{10} ）バイトのバイナリ単位に基づいてストレージ容量を計算します。ONTAP 9.10.0 以前では、これらの単位は KB、MB、GB、TB、PB として表示されていました。ONTAP 9.10.1 以降、Unified Manager では KiB、MiB、GiB、TiB、および PiB として表示されます。



スループットに使用される単位は、すべてのリリースのONTAP について、1秒あたりのキロバイト数（Kbps）、1秒あたりのメガバイト数（Mbps）、1秒あたりのギガバイト数（Gbps）、1秒あたりのテラバイト数（Tbps）などとなります。

Unified Manager for ONTAP 9.10.0 以前の容量ユニットが表示 されます	Unified Manager for ONTAP 9.10.1 で表示される容量の単位	計算	バイト単位の値
KB	KiB	1024	1024 バイト
MB	MiB	1024 * 1024	1,048,576 バイト
GB	GiB	1024 * 1024 * 1024	1,073,741,824 バイト
容量	TiB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 バイト

Active IQ Unified Manager によるパフォーマンス監視の概要

Active IQ Unified Manager（旧 OnCommand Unified Manager）は、NetApp ONTAP ソフトウェアを実行するシステムを対象に、パフォーマンス監視機能とパフォーマンスイベントの根本原因分析機能を提供します。

Unified Manager では、クラスタコンポーネントを過剰に消費しているワークロードや、クラスタ上のその他のワークロードのパフォーマンスを低下させているワークロードを特定できます。パフォーマンスしきい値ポリシーを定義して特定のパフォーマンスカウンタの最大値を指定し、しきい値を超えたときにイベントが生成

されるようにすることもできます。Unified Manager は、管理者がイベントに対処してパフォーマンスを平常時のレベルに戻すことができるよう、このようなパフォーマンスイベントに関するアラートをユーザに通知します。Unified Manager の UI でイベントを表示および分析できます。

Unified Manager は、次の 2 種類のワークロードのパフォーマンスを監視します。

- ユーザ定義のワークロード

このワークロードは、クラスタに作成した FlexVol ボリュームと FlexGroup ボリュームで構成されます。

- システム定義のワークロード

このワークロードは、内部のシステムアクティビティで構成されます。

Unified Manager REST API の使用

Active IQ Unified Manager には、ストレージ環境の監視と管理に関する情報を表示するための REST API が用意されています。また、ポリシーに基づいてストレージオブジェクトをプロビジョニングおよび管理できる API もあります。

Unified Manager でサポートされている API ゲートウェイを使用して、ONTAP で管理されるすべてのクラスタに対して ONTAP API を実行することもできます。

Unified Manager REST API については、を参照してください ["Active IQ Unified Manager REST API の使用を開始する"](#)。

Unified Manager サーバの機能

Unified Manager サーバインフラは、データ収集ユニット、データベース、アプリケーションサーバで構成され、検出、監視、ロールベースアクセス制御（RBAC）、監査、ロギングなどのインフラサービスを提供します。

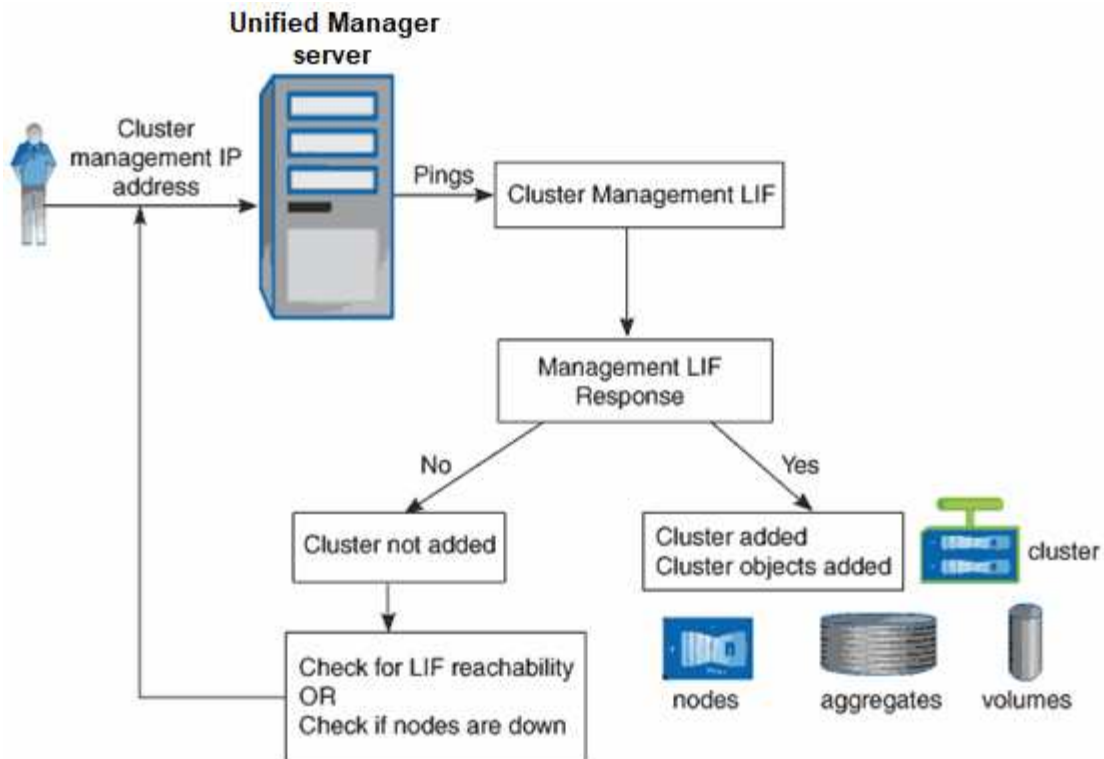
Unified Manager は、クラスタの情報を収集してデータベースにデータを格納し、そのデータを分析してクラスタに問題がないかどうかを確認します。

検出プロセスの仕組み

クラスタを Unified Manager に追加すると、サーバによってクラスタオブジェクトが検出され、サーバのデータベースに追加されます。検出プロセスの仕組みを理解しておくと、組織のクラスタとそのオブジェクトを管理する際に役立ちます。

デフォルトの監視間隔は 15 分です。Unified Manager サーバにクラスタを追加した場合、そのクラスタの詳細が Unified Manager の UI に表示されるまでに 15 分かかります。

次の図は、Active IQ Unified Manager での検出プロセスを示しています。



ユーザインターフェイスの概要

Unified Manager のユーザインターフェイスの主な構成要素は、監視対象のオブジェクトを一目で把握できるダッシュボードです。また、ユーザインターフェイスを使用して、すべてのクラスタオブジェクトを表示できます。

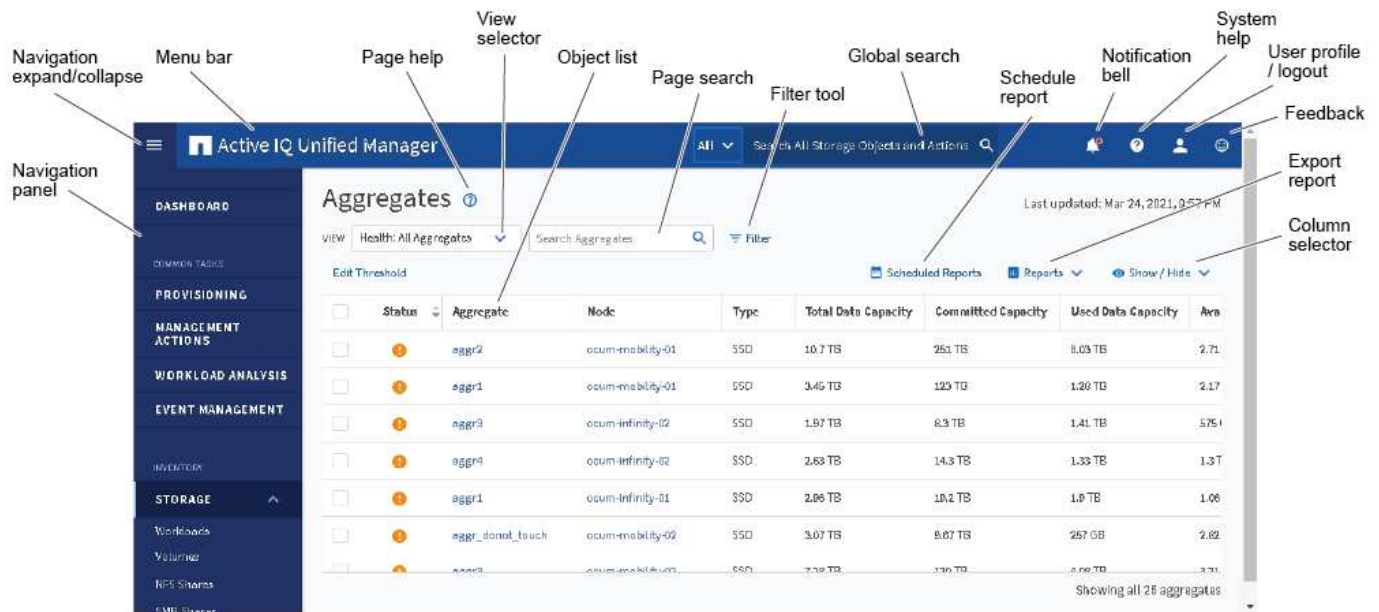
必要に応じて、優先するビューを選択したり、操作ボタンを使用したりできます。画面設定はワークスペースに保存されるため、必要なすべての機能が Unified Manager の起動時に表示されます。ただし、あるビューから別のビューに移動してから元のビューに戻ると、表示内容が異なる場合があります。

一般的なウィンドウレイアウト

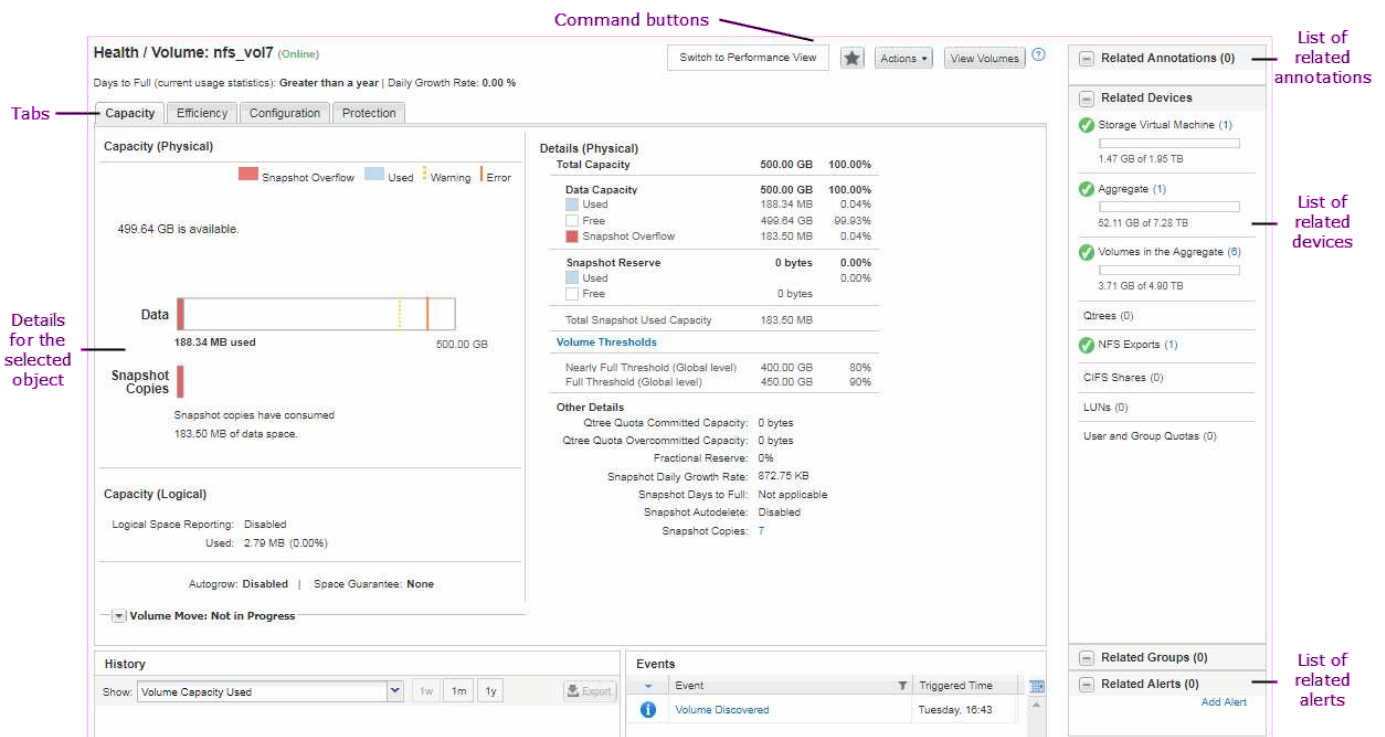
一般的なウィンドウレイアウトを理解しておく、Active IQ Unified Manager を効果的に操作して使用できるようになります。Unified Manager のほとんどのウィンドウは、オブジェクトリストまたは詳細の 2 つの一般的なレイアウトの 1 つに似ています。推奨される表示設定は 1280 × 1024 ピクセル以上です。

次の図のすべての要素がすべてのウィンドウに含まれているわけではありません。

オブジェクトリストウィンドウのレイアウト



オブジェクト詳細ウィンドウのレイアウト




ウィンドウレイアウトのカスタマイズ

Active IQ Unified Manager を使用して、ストレージオブジェクトとネットワークオブジェクトのページに表示される情報のレイアウトをカスタマイズできます。ウィンドウをカスタマイズすることによって、表示するデータやその表示方法を制御できます。

• * 並べ替え *

列エントリのソート順序を変更するには、列ヘッダーをクリックします。列見出しをクリックすると、ソート用矢印（▲ および ▼）が表示されます。

• * フィルタリング *

フィルタアイコン（) フィルタを適用して、指定した条件に一致するエントリだけが表示されるようにストレージオブジェクトとネットワークオブジェクトのページの情報の表示をカスタマイズします。フィルタは、[フィルタ (Filters)] パネルから適用します。

[フィルタ (Filters)] パネルでは、選択したオプションに基づいてほとんどの列をフィルタできます。たとえば、Health : All Volumes (正常性:すべてのボリューム) ビューで、State (状態) で適切なフィルタオプションを選択することにより、Filters (フィルタ) ペインを使用して、オフラインになっているすべてのボリュームを表示できます。

容量関連の列に表示される容量データは小数点以下 2 桁に四捨五入され、適切な単位で表示されます。これは、容量の列をフィルタする場合にも適用されます。たとえば、「Health : All aggregates」ビューの「Total Data Capacity」列でフィルタを使用すると、20.45GB を超えるデータをフィルタする場合、実際には 20.454GB のデータが 20.45GB と表示されます。同様に、20.45GB 未満のデータをフィルタすると、実際には 20.449GB のデータが 20.45GB と表示されます。

フィルタを「使用可能なデータ」の列で使用する場合、すべてのアグリゲートビューで 20.45% を超えるデータをフィルタすると、実際には 20.454% と表示されます。同様に、20.45% 未満のデータをフィルタすると、実際には 20.449% のデータが 20.45% と表示されます。

• * 列の表示 / 非表示 *

列表示アイコン (* 表示 / 非表示 *) をクリックして、表示する列を選択できます。適切な列を選択したら、マウスでドラッグして並べ替えることができます。

• * 検索中 *

検索ボックスを使用して特定のオブジェクト属性を検索し、インベントリページ内の項目のリストを絞り込むことができます。たとえば、「cloud」と入力してボリュームインベントリページ内のボリュームのリストを絞り込むと、「cloud」という単語が含まれているすべてのボリュームを表示できます。

• * データのエクスポート *



[Reports] ボタン (または[*Export] ボタン) をクリックすると、データをカンマ区切り値でエクスポートできます (.csv) ファイル、(.pdf) ドキュメント、またはMicrosoft Excel (.xlsx) レポートを作成するには、エクスポートしたデータをファイルして使用します。

Unified Manager ヘルプを使用する

このヘルプには、Active IQ Unified Manager に含まれているすべての機能に関する情報が含まれています。目次、索引、または検索ツールを使用して、機能に関する情報や機能の使用方法を検索できます。

Unified Manager のユーザインターフェイスの各タブおよびメニューバーからヘルプを表示できます。

ヘルプの検索ツールは部分的な単語に対しては機能しません。

- 特定のフィールドまたはパラメータの詳細を確認するには、をクリックします .
- すべてのヘルプコンテンツを表示するには、* をクリックします  メニューバーの > ヘルプ / ドキュメント

ナビゲーションペインで目次の一部を展開すると、より詳細な情報を確認できます。

- ヘルプの内容を検索するには、ナビゲーションペインの * 検索 * タブをクリックし、検索する単語または一連の単語を入力して、* 移動 * をクリックします
- ヘルプトピックを印刷するには、プリンタのアイコンをクリックします。

よく見るヘルプトピックのブックマーク登録

[ヘルプのお気に入り] タブでは、頻繁に使用するヘルプトピックをブックマークできます。ブックマークに登録すると、お気に入りのトピックにすばやくアクセスできます。

手順

1. お気に入りに追加するヘルプトピックに移動します。
2. [* お気に入り *] をクリックし、[* 追加 *] をクリックします。

ストレージオブジェクトを検索しています

特定のオブジェクトにすばやくアクセスするには、メニューバーの上部にある「すべてのストレージオブジェクトの検索」フィールドを使用します。すべてのオブジェクトをグローバルに検索する方法を使用すると、特定のオブジェクトをタイプ別にすばやく見つけることができます。検索結果はストレージオブジェクトのタイプ別に表示され、ドロップダウンメニューを使用してさらにオブジェクト別に絞り込むことができます。

- 必要なもの *
- このタスクを実行するには、オペレータ、アプリケーション管理者、またはストレージ管理者のいずれかのロールが割り当てられている必要があります。
- 検索キーワードは 3 文字以上にする必要があります。

ドロップダウンメニュー値「all」を使用すると、グローバル検索では、すべてのオブジェクトカテゴリで見つかった結果の合計数が表示されます。オブジェクトカテゴリごとに検索結果は最大 25 件まで表示されます。ドロップダウンメニューから特定のオブジェクトタイプを選択して、検索の対象を特定のオブジェクトタイプに絞り込むことができます。この場合、結果のリストに表示されるオブジェクトの数は上位 25 個に限定されません。

次のオブジェクトタイプを検索できます。

- クラスタ
- ノード
- Storage VMs
- アグリゲート
- 個のボリューム

- qtree
- SMB 共有
- NFS 共有
- ユーザクォータまたはグループクォータ
- LUN
- NVMe ネームスペース
- イニシエータグループ
- イニシエータ
- 整合グループ

ワークロード名を入力すると、該当するボリュームまたは LUN カテゴリのワークロードのリストが返されます。

検索結果内の任意のオブジェクトをクリックすると、そのオブジェクトの健全性の詳細ページが表示されます。オブジェクトに直接健全性ページがない場合は、親オブジェクトの健全性ページが表示されます。たとえば、特定の LUN を検索する場合は、その LUN が配置されている SVM の詳細ページが表示されます。

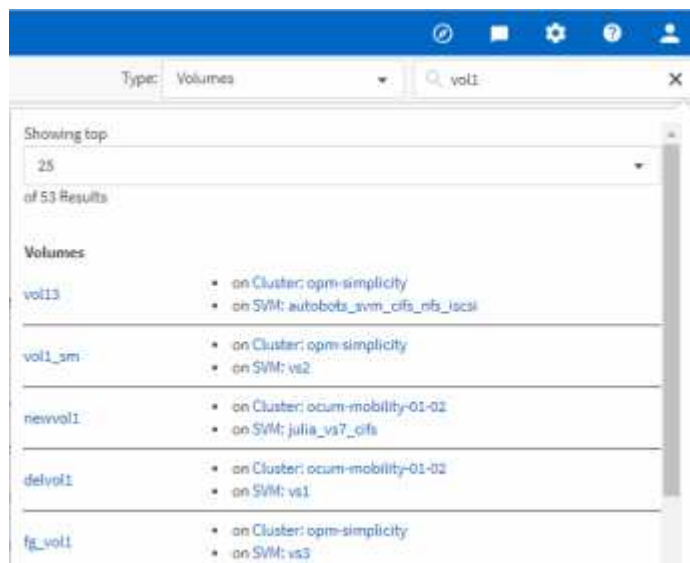


ポートと LIF はグローバル検索バーでは検索できません。

手順

1. メニューからオブジェクトタイプを選択すると、検索結果が 1 つのオブジェクトタイプに絞り込みます。
2. [すべてのストレージオブジェクトの検索] フィールドに、オブジェクト名の 3 文字以上を入力します。

この例では、ドロップダウンボックスで Volumes オブジェクトタイプが選択されています。「* Search All Storage Objects *」フィールドに「vol1」と入力すると、名前にこれらの文字が含まれているすべてのボリュームのリストが表示されます。



ストレージデータをレポートとしてエクスポートする

ストレージデータをさまざまな出力形式でエクスポートし、エクスポートしたデータを

使用してレポートを作成できます。たとえば、未解決の重大イベントが 10 件ある場合、イベント管理のインベントリページからデータをエクスポートしてレポートを作成し、問題を解決できる管理者にレポートを送信できます。

にデータをエクスポートできます .csv ファイル、.xlsx ファイル、または .pdf ストレージおよび*ネットワーク*インベントリページから文書化し、エクスポートしたデータを使用してレポートを作成します。製品には、他の場所のみがあります .csv または .pdf ファイルを生成できます。

手順

- 1. 次のいずれかを実行します。

エクスポートする項目	手順
ストレージオブジェクトのインベントリの詳細	左側のナビゲーションメニューから * Storage * または * Network * をクリックし、ストレージオブジェクトを選択します。システムで提供されているビューのいずれか、または作成したカスタムビューを選択します。
QoS ポリシーグループの詳細	左側のナビゲーションメニューから、 * Storage * > * QoS Policy Groups * をクリックします。
ストレージ容量と保護の履歴の詳細	ストレージ * > * アグリゲート * または * ストレージ * > * ボリューム * をクリックして、1 つまたは複数のアグリゲートまたはボリュームを選択します。
イベントの詳細	左側のナビゲーションメニューから、 * イベント管理 * をクリックします。
上位 10 個のストレージオブジェクトのパフォーマンスの詳細	[* ストレージ * > * クラスタ * > * パフォーマンス : すべてのクラスタ *] をクリックし、クラスタを選択して [* パフォーマンスストップ *] タブを選択します。次に、ストレージオブジェクトとパフォーマンスカウンタを選択します。

- 2. [Reports] ボタン（または一部の UI ページの [*Export] ボタン）をクリックします。
- 3. 「 * CSV のダウンロード * 」、「PDF のダウンロード * 」、または「 * Excel のダウンロード * 」をクリックして、エクスポート要求を確認します。

Top Performers タブでは、表示している単一のクラスタまたはデータセンター内のすべてのクラスタの統計のレポートをダウンロードできます。

ファイルがダウンロードされます。

- 4. 該当するアプリケーションでファイルを開きます。
 - 関連情報 *

"[ケンセンセイ / クラスタインベントリヘエシ](#)"

インベントリページの内容のフィルタリング

Unified Manager でインベントリページのデータをフィルタリングして、特定の条件に基づいてデータをすばやく特定できます。フィルタリングを使用すると、Unified Manager のページの内容を絞り込んで、関心のある結果だけを表示できます。そのため、関心のあるデータだけを効率的に表示できます。

環境設定に基づいてグリッド表示をカスタマイズするには、* フィルタリング * を使用します。使用可能なフィルタオプションは、グリッドで表示しているオブジェクトタイプによって異なります。フィルタが現在適用されている場合は、[フィルタ (Filter)] ボタンの右側に適用されたフィルタの数が表示されます。

3 種類のフィルタパラメータがサポートされています。

パラメータ	検証
文字列 (テキスト)	演算子は、* contains *、* starts with *、* ends with *、および * does not contain * です。
番号	演算子は、* より大きい *、* より小さい *、* の最後の *、および * の間です。
列挙 (テキスト)	演算子は * は * で、* は * ではありません。

各フィルタには、列、演算子、および値のフィールドが必要です。使用可能なフィルタは、現在のページのフィルタ可能な列に基づいています。適用できるフィルタは 4 つまでです。フィルタパラメータの組み合わせに基づいてフィルタされた結果が表示されます。フィルタされた結果は、現在表示されているページだけでなく、フィルタ処理された検索のすべてのページに適用されます。

フィルタパネルを使用してフィルタを追加できます。

1. ページの上部にある * Filter * ボタンをクリックします。フィルタリングパネルが表示されます。
2. 左側のドロップダウンリストをクリックし、*Cluster*、パフォーマンスカウンタなどのオブジェクトを選択します。
3. 中央のドロップダウンリストをクリックし、使用する演算子を選択します。
4. 最後のリストで値を選択または入力して、そのオブジェクトのフィルタを完成させます。
5. 別のフィルタを追加するには、[* + フィルタの追加 *] をクリックします。追加のフィルタフィールドが表示されます。前述の手順に従って、このフィルタを設定します。4 番目のフィルタを追加すると、[* + フィルタを追加 *] ボタンは表示されなくなります。
6. [フィルタを適用 (Apply Filter)] をクリックする。フィルタオプションがグリッドに適用され、フィルタボタンの右側にフィルタの数が表示されます。
7. フィルタパネルを使用して、削除するフィルタの右側にあるゴミ箱アイコンをクリックして、個々のフィルタを削除します。
8. すべてのフィルターを削除するには、フィルターパネルの下部にある * リセット * をクリックします。

フィルタリングの例

次の図は、フィルタパネルと 3 つのフィルタを示しています。フィルタを最大 4 つまでしか使用できない場合は、「* + フィルタを追加 *」ボタンが表示されます。

MBps	greater than	5	MBps	🗑️
Node	name starts with	test		🗑️
Type	is	FCP Port		🗑️

+ Add Filter

Cancel Apply Filter

[フィルタの適用 (Apply Filter)] をクリックすると、[フィルタ (Filtering)] パネルが閉じ、フィルタが適用され、適用されているフィルタの数が表示されます (3)。

通知ベルからのアクティブイベントの表示

通知ベル () をクリックすると、Unified Manager が追跡している最も重要なアクティブイベントを簡単に確認できます。

アクティブイベントのリストでは、すべてのクラスタの重大イベント、エラーイベント、警告イベント、アップグレードイベントの総数を確認できます。このリストには過去 7 日間のイベントが含まれ、情報イベントは含まれません。リンクをクリックすると、関心のあるイベントのリストを表示できます。

クラスタが到達不能な場合は、Unified Manager がその情報をこのページに表示します。到達不能なクラスタに関する詳細情報を表示するには、* Details * ボタンをクリックします。この操作により、[イベントの詳細] ページが開きます。このページには、管理ステーションの容量不足や RAM などのスケール監視の問題も表示されます。

手順

1. メニューバーでをクリックします .
2. アクティブなイベントの詳細を表示するには、「2 Capacity」や「4 Performance」などのイベントテキストのリンクをクリックします。

ダッシュボードからクラスタを監視および管理する

ダッシュボードには、監視対象の ONTAP システムの現在までの健全性に関する履歴情報がわかりやすく表示されます。ダッシュボードには「パネル」が表示され、監視しているクラスタの全体的な容量、パフォーマンス、およびセキュリティの健全性を評価できます。

また、ONTAP の一部の問題については、ONTAP System Manager や ONTAP CLI を使用しなくても、Unified Manager ユーザインターフェイスから直接修正することができます。

ダッシュボードの上部で、すべての監視対象クラスタの情報を表示するか、特定のクラスタの情報を表示する

かを選択できます。最初にすべてのクラスタのステータスを表示してから、詳細情報を確認する場合は個々のクラスタにドリルダウンできます。



以下のパネルの一部は、構成に応じてページに表示されない場合があります。

パネル	説明
管理操作	Unified Manager で問題の解決策を診断して特定できる場合、その解決策は「 * Fix it * 」ボタンでこのパネルに表示されます。
容量	ローカル階層とクラウド階層の合計容量と使用済み容量、およびローカル容量が上限に達するまでの日数が表示されます。
パフォーマンス容量	各クラスタのパフォーマンス容量とパフォーマンス容量が上限に達するまでの日数が表示されます。
ワークロード IOPS	特定の IOPS 範囲で現在実行されているワークロードの総数が表示されます。
ワークロードのパフォーマンス	定義された各パフォーマンスサービスレベルに割り当てられている準拠ワークロードと非準拠ワークロードの総数が表示されます。
セキュリティ	準拠または非準拠のクラスタ数、準拠または非準拠の SVM 数、暗号化されたボリュームまたはされていないボリュームの数が表示されます。
保護	SVM-DR関係で保護されている Storage VM の数、SnapMirror関係で保護されているボリューム、Snapshotで保護されているボリューム、およびMetroCluster で保護されているクラスタが表示されます。
使用状況の概要	IOPS、スループット（MBps）、または使用済み物理容量が大きい順にクラスタが表示されます。

ダッシュボードページ

ダッシュボードページには、監視しているクラスタの容量、パフォーマンス、セキュリティの健全性の概要がパネルに表示されます。このページの管理操作パネルには、Unified Manager が特定のイベントを解決するために実行できる修正が表示されます。

ほとんどのパネルには、そのカテゴリのアクティブイベントの数および過去 24 時間に追加された新しいイベントの数も表示されます。この情報から、イベントを解決するために詳細な分析が必要なクラスタを決定できます。イベントをクリックすると、上位のイベントが表示され、そのカテゴリのアクティブなイベントをフィルタリングして表示する Event Management インベントリページへのリンクが表示されます。

ダッシュボードの上部で、すべての監視対象クラスタ（「すべてのクラスタ」）の情報を表示するか、特定のクラスタの情報を表示するかを選択できます。最初にすべてのクラスタのステータスを表示してから、詳細情報を確認する場合は個々のクラスタにドリルダウンできます。



構成に応じて、次のパネルの一部がダッシュボードに表示されます。

【管理操作】パネル

問題によっては、Unified Manager の詳細な診断によって 1 つの解決策が提供されることがあります。解決策がある場合は、このパネルに * Fix it * または * Fix All * ボタンで表示されます。このような問題は Unified Manager から直接解決できます。ONTAP System Manager や ONTAP CLI を使用する必要はありません。すべての問題を表示するには、「参照」をクリックします ["ONTAP の問題を Unified Manager から直接修正"](#) を参照してください。

容量パネル

すべてのクラスタを表示している場合、このパネルには、各クラスタの使用済み物理容量（Storage Efficiency 削減を適用したあと）と使用可能な物理容量（Storage Efficiency による削減量の削減量を含まない）、およびディスクがフルになるまでの予測日数が表示されます。および ONTAP の Storage Efficiency 設定に基づくデータ削減率の割合を表示します。また、設定されているクラウド階層の使用済み容量も表示されます。棒グラフをクリックすると、そのクラスタのアグリゲートのインベントリページが表示されます。「フルまでの日数」というテキストをクリックすると容量の残り日数が最も少ないアグリゲートを示すメッセージが表示され、そのアグリゲート名をクリックすると詳細が表示されます。

単一のクラスタを表示している場合、このパネルには、データアグリゲートの物理使用容量と使用可能な物理容量がローカル階層とクラウド階層のそれぞれのディスクタイプでソートされて表示されます。ディスクタイプの棒グラフをクリックすると、そのディスクタイプを使用しているボリュームのボリュームインベントリページが表示されます。

Performance Capacity（パフォーマンス容量）パネル

すべてのクラスタを表示している場合、このパネルには、各クラスタのパフォーマンス容量（過去 1 時間の平均）とパフォーマンス容量が上限に達するまでの日数（日次増加率に基づく）が表示されます。棒グラフをクリックすると、そのクラスタのノードインベントリページが表示されます。ノードインベントリページには、過去 72 時間のパフォーマンス容量の平均が表示されます。フルまでの日数というテキストをクリックするとパフォーマンス容量の残り日数が最も少ないノードを示すメッセージが表示され、そのノード名をクリックすると詳細が表示されます。

単一のクラスタを表示している場合、このパネルには、そのクラスタの使用済みパフォーマンス容量の割合、合計 IOPS、合計スループット（MBps）、およびこれらの 3 つの指標が上限に達するまでの想定日数が表示されます。

ワークロードの IOPS パネル

単一のクラスタを表示している場合、このパネルには、特定の範囲の IOPS で現在実行されているワークロードの総数、およびグラフにカーソルを合わせると各ディスクタイプの数が表示されます。

ワークロードのパフォーマンスパネル

このパネルには、各パフォーマンスサービスレベル（PSL）ポリシーに割り当てられている準拠ワークロードと非準拠ワークロードの総数が表示されます。また、PSL が割り当てられていないアグリゲートの数も表示されます。棒グラフをクリックすると、そのポリシーに割り当てられている準拠ワークロードがワークロー

ドページに表示されます。棒グラフの横に表示された数字をクリックすると、そのポリシーに割り当てられている準拠ワークロードと非準拠ワークロードが表示されます。

セキュリティパネル

Securityパネルには、現在のビューに応じて、すべてのクラスタまたは単一のクラスタのセキュリティステータスの概要が表示されます。このパネルには次の情報が表示

- 過去24時間に受信したセキュリティイベントのリスト。イベントをクリックすると、そのイベントの詳細がイベントの詳細ページに表示されます
- クラスタのセキュリティステータス（準拠クラスタと非準拠クラスタの数）
- Storage VMのセキュリティステータス（準拠Storage VMと非準拠Storage VMの数）
- ボリューム暗号化ステータス（暗号化されているボリュームまたは暗号化されていないボリュームの数）
- ボリュームのランサムウェア対策のステータス（ランサムウェア対策が有効または無効になっているボリュームの数）

準拠クラスタと非準拠クラスタ、Storage VM、暗号化ボリュームと非暗号化ボリューム、およびボリュームのランサムウェア対策ステータスの棒グラフをクリックすると、該当するページに移動し、フィルタリングされたクラスタ、Storage VM、およびボリュームのセキュリティの詳細を表示できます。

コンプライアンスは、に基づいています ["ONTAP 9 セキュリティ設定ガイド"](#)。パネル上部の右矢印をクリックして、Securityページですべてのクラスタのセキュリティの詳細を表示します。詳細については、を参照してください ["クラスタと Storage VM の詳細なセキュリティステータスの表示"](#)。

データ保護パネル

このパネルには、データセンター内の 1 つまたはすべてのクラスタのデータ保護の概要が表示されます。ONTAP の過去24時間に生成されたデータ保護イベント、MetroCluster イベント、およびアクティブイベントの総数が表示されます。これらの各イベントのリンクをクリックすると、[イベントの詳細] ページが表示されます。[すべて表示 *] リンクをクリックすると、[イベント管理] イベントリページですべてのアクティブな保護イベントを表示できます。パネルに次の情報が表示され

- クラスタ内のボリューム、またはSnapshotコピーで保護されているデータセンター内のすべてのクラスタのボリューム数。
- クラスタ内のボリューム、またはSnapMirror関係で保護されているデータセンター内のすべてのクラスタのボリューム数。SnapMirror関係では、ソースクラスタのボリューム数が考慮されます。
- IPまたはFC経由でMetroCluster 構成で保護されているデータセンター内のクラスタまたはすべてのクラスタの数。
- 遅延ステータスに基づいて、SnapMirrorのRecovery Point Objective（RPO；目標復旧時点）遅延が設定されたボリューム関係の数。

マウスのカーソルを合わせると、それぞれのカウントと凡例を表示できます。パネル上部の右矢印をクリックすると、データ保護ページで1つまたはすべてのクラスタの詳細を確認できます。また、以下をクリックすることもできます。

- 保護されていないボリュームとSnapshotコピーで保護されているボリュームの棒グラフ。ボリュームのページに移動して詳細を確認できます。
- 保護されているクラスタ、またはMetroCluster 構成で保護されていないクラスタの棒グラフ。クラスタページに移動して詳細を確認できます。

- すべての関係の棒グラフが関係ページに表示され、詳細はソースクラスタに基づいてフィルタされます。

詳細については、を参照してください ["ボリュームの保護ステータスを表示しています"](#)。

使用状況の概要パネル

すべてのクラスタを表示している場合、IOPS、スループット（MBps）、または使用済み物理容量が大きい順にクラスタを表示できます。

単一のクラスタを表示している場合は、IOPS、スループット（MBps）、または使用済み論理容量が大きい順にワークロードを表示できます。

- 関連情報 *

["Unified Manager の自動修正措置を使用した問題の修正"](#)

["パフォーマンスイベントに関する情報を表示する"](#)

["パフォーマンス容量と使用可能な IOPS の情報を使用してパフォーマンスを管理する"](#)

["ボリューム / 健全性の詳細ページ"](#)

["パフォーマンスイベントの分析と通知"](#)

["概要のイベントの重大度タイプ"](#)

["パフォーマンスイベントのソース"](#)

["クラスタのセキュリティ目標の管理"](#)

["パフォーマンスクラスタランディングページからのクラスタパフォーマンスの監視"](#)

["パフォーマンスインベントリページを使用したパフォーマンスの監視"](#)

ONTAP の問題または機能を Unified Manager から直接管理する

ONTAP の一部の問題を修正したり、ONTAP の特定の機能を Unified Manager ユーザーインターフェイスから直接管理したりできます。ONTAP System Manager や ONTAP CLI を使用する必要はありません。「管理操作」オプションは、Unified Manager イベントをトリガーした ONTAP のさまざまな問題に対する修正を提供します。

左側のナビゲーションペインで * 管理操作 * オプションを選択すると、管理操作ページから直接問題を修正できます。管理操作は、ダッシュボードの管理操作パネル、イベントの詳細ページ、および左側のナビゲーションメニューのワークロード分析からも実行できます。

問題によっては、Unified Manager の詳細な診断によって 1 つの解決策が提供されることがあります。ランサムウェア対策の監視など、ONTAP の一部の機能については、Unified Manager で内部チェックが実行され、特定の対処が推奨されます。解決策がある場合は、[管理アクション] の [* 修正] ボタンで表示されます。[* Fix it*（修正）] ボタンをクリックして、問題を修正します。アプリケーション管理者またはストレージ管理者のロールが必要です。

Unified Manager からクラスタに ONTAP コマンドが送信され、要求された修正が実行されます。修正が完了

すると、イベントは廃止状態になります。

一部の管理操作では、* すべて修正 * ボタンを使用して、複数のストレージオブジェクトで同じ問題を修正できます。たとえば、「ボリュームスペースがフル」イベントが発生しているボリュームが 5 つある場合に、「ボリュームの自動拡張を有効にする」の「すべてを修正」管理操作をクリックすると解決できます。ワンクリックで、この問題を 5 つのボリュームで修正できます。

自動修正を使用して管理できる ONTAP の問題と機能については、を参照してください ["Unified Manager で解決可能な問題"](#)。

【修正】または【すべて修正】ボタンが表示されたら、どのようなオプションがありますか

Management Actions ページには、Unified Manager にイベントを通じて通知された問題を修正するための * Fix it * または * Fix All * ボタンが表示されます。

必要に応じて、ボタンをクリックして問題を修正することをお勧めします。ただし、Unified Manager の推奨事項に従って問題を解決するかどうかは不明な場合は、次の操作を実行できます。

何をしますか？	* アクション *
特定されたすべてのオブジェクトの問題を Unified Manager で修正する。	「* すべて修正 *」ボタンをクリックします。
この時点で特定されたオブジェクトの問題を修正しないでください。また、イベントが再び発生するまでこの管理操作は表示されません。	下矢印をクリックし、* すべてを却下 * をクリックします。
特定された一部のオブジェクトでのみ問題を修正します。	管理操作の名前をクリックしてリストを展開し、* 修正 * アクションをすべて表示します。次に、個々の管理操作を修正または削除する手順を実行します。

何をしますか？	アクション
Unified Manager で問題を修正する。	[* Fix it* （修正）] ボタンをクリックします。
この時点では問題を修正しないでください。イベントが再び発生するまでこの管理操作は表示されません。	下矢印をクリックし、* Dismiss * （キャンセル）をクリックします。
問題について理解しやすくするために、このイベントの詳細を表示する	<ul style="list-style-type: none">• [修正（Fix it）] ボタンをクリックして、結果のダイアログボックスに適用される修正を確認します。• 下矢印をクリックし、* イベントの詳細を表示 * をクリックしてイベントの詳細ページを表示します。 <p>問題を修正する場合は、これらのいずれかの結果ページで [* Fix it* （修正）] をクリックします。</p>

何をしますか？	アクション
問題について理解しやすくするために、このストレージオブジェクトの詳細を表示する	ストレージオブジェクトの名前をクリックすると、パフォーマンスエクスプローラまたは健全性の詳細ページに詳細が表示されます。

修正は、次の 15 分間に実施される構成ポーリングで反映される場合もあります。構成の変更が検証されてイベントが廃止状態になるまでに最大数時間かかることもあります。

完了または進行中の管理アクションのリストを表示するには、フィルタアイコンをクリックし、* 完了 * または * 進行中 * を選択します。

すべてのオペレーションがシリアルに実行されるように修正します。このため、[進行中] パネルを表示すると、[ステータス *- 進行中] が表示されるオブジェクトと、[ステータス *Scheduled (ステータス * スケジュール済み)] が表示されるオブジェクトがあります。これは、実装を待機していることを意味します。


修正するように選択した管理アクションのステータスの表示

修正対象として選択したすべての管理アクションのステータスは、管理アクションページで確認できます。ほとんどの操作は、Unified Manager からクラスタに ONTAP コマンドが送信されたあと、ほぼ完了 * と表示されます。ただし、ボリュームの移動などの一部の処理には時間がかかることがあります。

管理操作ページでは、次の 3 つのフィルタを使用できます。

- * Completed * には、正常に完了した管理操作と失敗した管理操作の両方が表示されます。* 失敗した * アクションは、問題を手動で指定できるように、失敗の理由を提供します。
- * 実行中 * 実行中の管理操作と実行予定の管理操作の両方が表示されます。
- * 推奨 * : すべての監視対象クラスタで現在アクティブなすべての管理操作が表示されます。

手順

1. 左側のナビゲーションペインで、* 管理操作 * をクリックします。または、 **ダッシュボード** * の * 管理操作 * パネルの上部で、表示するビューを選択します。

[Management Actions] ページが表示されます。

2. 「* 概要 *」フィールドの管理操作の横にあるチャレットアイコンをクリックすると、問題の修正に使用される問題とコマンドの詳細を確認できます。
3. 失敗したアクション * を表示するには、* 完了 * 表示の * ステータス * 列でソートします。同じ目的で * フィルタ * ツールを使用できます。
4. 失敗した管理アクションの詳細を表示する場合や、推奨される管理アクションを修正する場合は、拡張領域で管理アクションの横にあるチャレットアイコンをクリックしたあとに、「* イベントの詳細を表示」をクリックします。このページから * Fix it * ボタンを使用できます。

Unified Manager で解決可能な問題

Active IQ Unified Manager の自動修復機能を使用すると、ONTAP の特定の問題を解決したり、ランサムウェア対策の監視などの ONTAP の一部の機能を Unified Manager で

効果的に管理したりできます。

この表では、Unified Manager Web UI の * Fix it * または * Fix All * ボタンを使用して直接管理できる ONTAP の問題と機能について説明します。

イベント名と概要	管理操作	「修正」処理
ボリュームスペースがフルです ボリュームにスペースがほとんど残っておらず、容量の「フル」しきい値を超えています。このしきい値は、デフォルトではボリュームサイズの 90% に設定されています。	ボリュームの自動拡張を有効にする	Unified Manager はこのボリュームにボリュームの自動拡張が設定されていないことを特定し、必要に応じてボリュームの容量が拡張されるようにこの機能を有効にします。
inode がフルです このボリュームの inode が不足しており、新しいファイルを受け入れることはできません。	ボリュームの inode の数を増やします	ボリュームの inode の数を 2% 増やします。
ストレージ階層ポリシーの不一致が検出されました ボリュームにアクセス頻度の低いデータが大量にあり、現在の階層化ポリシーが「snapshot-only」または「none」に設定されている。	クラウドの自動階層化を有効化	ボリュームはすでに FabricPool に存在するため、階層化ポリシーが「auto」に変更され、アクセス頻度の低いデータが低コストのクラウド階層に移動されます。
ストレージ階層の不一致が検出されました アクセス頻度の低いデータがボリュームに大量にありますが、クラウド対応のストレージ階層（FabricPool）に配置されていません。	ボリュームのストレージ階層を変更します	アクセス頻度の低いデータをクラウド階層に移動するには、ボリュームをクラウド対応ストレージ階層に移動し、階層化ポリシーを「自動」に設定します。
監査ログが無効です Storage VM の監査ログが有効になっていません	Storage VM の監査ログを有効にしてください	Storage VM の監査ログを有効にします。 Storage VM にローカルまたはリモートの監査ログの場所が設定されている必要があります。

イベント名と概要	管理操作	「修正」処理
<p>ログインバナーが無効です</p> <p>アクセス制限をクリアしてセキュリティを強化するには、クラスタのログインバナーを有効にする必要があります。</p>	<p>クラスタのログインバナーを設定します</p>	<p>クラスタ・ログイン・バナーを「許可されたユーザーにアクセス制限」に設定します。</p>
<p>ログインバナーが無効です</p> <p>アクセス制限を明確にしてセキュリティを強化するには、Storage VM のログインバナーを有効にする必要があります。</p>	<p>Storage VM のログインバナーを設定します</p>	<p>Storage VM のログインバナーを「許可されたユーザだけにアクセス」に設定します。</p>
<p>SSH でセキュアでない暗号が使用されています</p> <p>サフィックスが「-cbc」の暗号は安全でないとみなされます。</p>	<p>セキュアでない暗号をクラスタから削除してください</p>	<p>安全でない暗号（aes192-cbc や aes128-cbc など）をクラスタから削除します。</p>
<p>SSH でセキュアでない暗号が使用されています</p> <p>サフィックスが「-cbc」の暗号は安全でないとみなされます。</p>	<p>セキュアでない暗号を Storage VM から削除してください</p>	<p>安全でない暗号（aes192-cbc や aes128-cbc など）をストレージ VM から削除します。</p>
<p>AutoSupport HTTPS 転送が無効です</p> <p>AutoSupport メッセージのテクニカルサポートへの送信に使用される転送プロトコルを暗号化する必要があります。</p>	<p>AutoSupport メッセージの転送プロトコルとして HTTPS を設定します</p>	<p>クラスタ上の AutoSupport メッセージの転送プロトコルとして HTTPS を設定します。</p>
<p>クラスタ負荷の不均衡しきい値を超過</p> <p>クラスタ内のノード間で負荷が不均衡になっています。このイベントは、ノード間の使用済みパフォーマンス容量の差が 30% を超えた場合に生成されます。</p>	<p>クラスタワークロードを分散します</p>	<p>Unified Manager は別のノードに移動することで不均衡が最も解消されるボリュームを特定し、そのボリュームを移動します。</p>

イベント名と概要	管理操作	「修正」処理
<p>クラスタ容量の不均衡しきい値を超過</p> <p>クラスタ内のアグリゲート間で容量が不均衡になっています。このイベントは、アグリゲート間の使用済み容量の差が 70% を超えた場合に生成されます。</p>	クラスタ容量を分散します	Unified Manager は別のアグリゲートに移動することで不均衡が最も解消されるボリュームを特定し、そのボリュームを移動します。
<p>使用済みパフォーマンス容量のしきい値を超過</p> <p>1 つ以上のアクティブなワークロードによる利用率を下げないと、ノードの負荷が過剰になる可能性があります。このイベントは、ノードの使用済みパフォーマンス容量の値が 12 時間以上 100% を超えた場合に生成されます。</p>	ノードの高負荷を制限します	Unified Manager は IOPS が高いボリュームを特定し、想定およびピークの過去の IOPS レベルを使用して QoS ポリシーを適用して、ノードの負荷を軽減します。
<p>動的イベントの警告しきい値を超過</p> <p>一部のワークロードの負荷が異常に高いためにノードがすでに過負荷状態です。</p>	ノードの過負荷を軽減します	Unified Manager は IOPS が高いボリュームを特定し、想定およびピークの過去の IOPS レベルを使用して QoS ポリシーを適用して、ノードの負荷を軽減します。
<p>テイクオーバーを実行できません</p> <p>フェイルオーバーが無効になっているため、停止中またはリブート中のノードが使用可能な状態に戻るまではノードのリソースへのアクセスが失われます。</p>	ノードフェイルオーバーを有効にします	Unified Manager が該当するコマンドを送信し、クラスタ内のすべてのノードのフェイルオーバーを有効にします。
<p>オプション cf.takeover.on_panic の設定が OFF になっています</p> <p>ノードシェルトオプション「cf.takeover.on_panic」が * off * に設定されており、HA 構成のシステムで問題を原因できます。</p>	パニック時のテイクオーバーを有効にする	Unified Manager が該当するコマンドを送信し、この設定を * on * に変更します。

イベント名と概要	管理操作	「修正」処理
<p>ノードシェルオプション snapmirror.enable を無効化</p> <p>古いノードシェルオプション「 snapmirror.enable」は * on * に設定されており、ONTAP 9.3 以降へのアップグレード後のブート時に問題を原因することができます。</p>	<p>snapmirror.enable オプションを off に設定します</p>	<p>Unified Manager が該当するコマンドを送信し、この設定を * off * に変更します。</p>
<p>Telnet が有効です</p> <p>Telnet は安全性が高くなく、暗号化されていない方法でデータが渡されるため、潜在的なセキュリティ問題を示します。</p>	<p>Telnet を無効にします</p>	<p>Unified Manager が適切なコマンドをクラスタに送信し、Telnet を無効にします。</p>
<p>Storage VM にランサムウェア対策学習を設定する</p> <p>ライセンスのあるクラスタでランサムウェア対策の監視を定期的にチェックします。Storage VM がこのようなクラスタ内の NFS ボリュームまたは SMB ボリュームのみをサポートするかどうかを検証します。</p>	<p>Storage VMをに配置します learning ランサムウェア対策モニタリングのモード</p>	<p>Unified Managerはランサムウェア対策の監視をに設定します learning クラスタ管理コンソールを通じてStorage VMの状態を表示します。Storage VM に作成されたすべての新しいボリュームでランサムウェア対策モニタリングが自動的に学習モードに移行されます。ONTAP は、この有効化を通じてボリュームのアクティビティのパターンを学習し、潜在的な悪意のある攻撃による異常を検出します。</p>
<p>ボリュームのランサムウェア対策学習を設定する</p> <p>ライセンスのあるクラスタでランサムウェア対策の監視を定期的にチェックします。ボリュームがこのようなクラスタで NFS サービスまたは SMB サービスのみをサポートするかどうかを検証します。</p>	<p>ボリュームをに配置します learning ランサムウェア対策モニタリングのモード</p>	<p>Unified Managerはランサムウェア対策の監視をに設定します learning クラスタ管理コンソールからボリュームの状態を確認します。ONTAP は、この有効化を通じてボリュームのアクティビティのパターンを学習し、潜在的な悪意のある攻撃による異常を検出します。</p>

イベント名と概要	管理操作	「修正」処理
<p>ボリュームのアンチランサムウェアを有効化</p> <p>ライセンスのあるクラスタでランサムウェア対策の監視を定期的にチェックします。ボリュームがあるかどうかを検出します</p> <p>learning ランサムウェア対策モニタリングのモードが45日以上継続しており、アクティブモードに移行する見込みがあると判断されます。</p>	<p>ボリュームをに配置します</p> <p>active ランサムウェア対策モニタリングのモード</p>	<p>Unified Managerはランサムウェア対策の監視をに設定します</p> <p>active クラスタ管理コンソールを介してボリュームにインストールします。ONTAP は、この有効化を通じて、ボリュームのアクティビティのパターンを学習し、潜在的な悪意のある攻撃による異常を検出して、データ保護アクションに対するアラートを作成できます。</p>
<p>ボリュームのアンチランサムウェアを無効にする</p> <p>ライセンスのあるクラスタでランサムウェア対策の監視を定期的にチェックします。ボリュームに対するアクティブなアンチランサムウェアの監視中に繰り返し発生する通知を検出します（たとえば、ランサムウェアによる攻撃が発生する可能性があるという複数の警告が 30 日以上返されます）。</p>	<p>ボリュームでランサムウェア対策の監視を無効にする</p>	<p>Unified Manager では、クラスタ管理コンソールを使用したボリュームでのランサムウェア対策監視が無効になります。</p>

スクリプトによる管理操作の上書き

カスタムスクリプトを作成してアラートに関連付けることで、特定のイベントに対して特定の処理を実行できます。この処理に使用できるデフォルトの管理操作は、管理操作ページや Unified Manager のダッシュボードでは選択できません。

あるイベントタイプに対して特定の操作を実行し、Unified Manager の管理操作機能の一部として修正しないように選択するには、特定の操作用のカスタムスクリプトを設定します。その後、スクリプトをそのイベントタイプのアラートに関連付けることで、このようなイベントを個別に管理できます。この場合、その特定のイベントタイプに対する管理操作は生成されません。このイベントタイプについては、管理操作ページまたは Unified Manager のダッシュボードでは生成されません。

クラスタの管理

Unified Manager を使用してクラスタを監視、追加、編集、削除することで、ONTAP クラスタを管理できます。

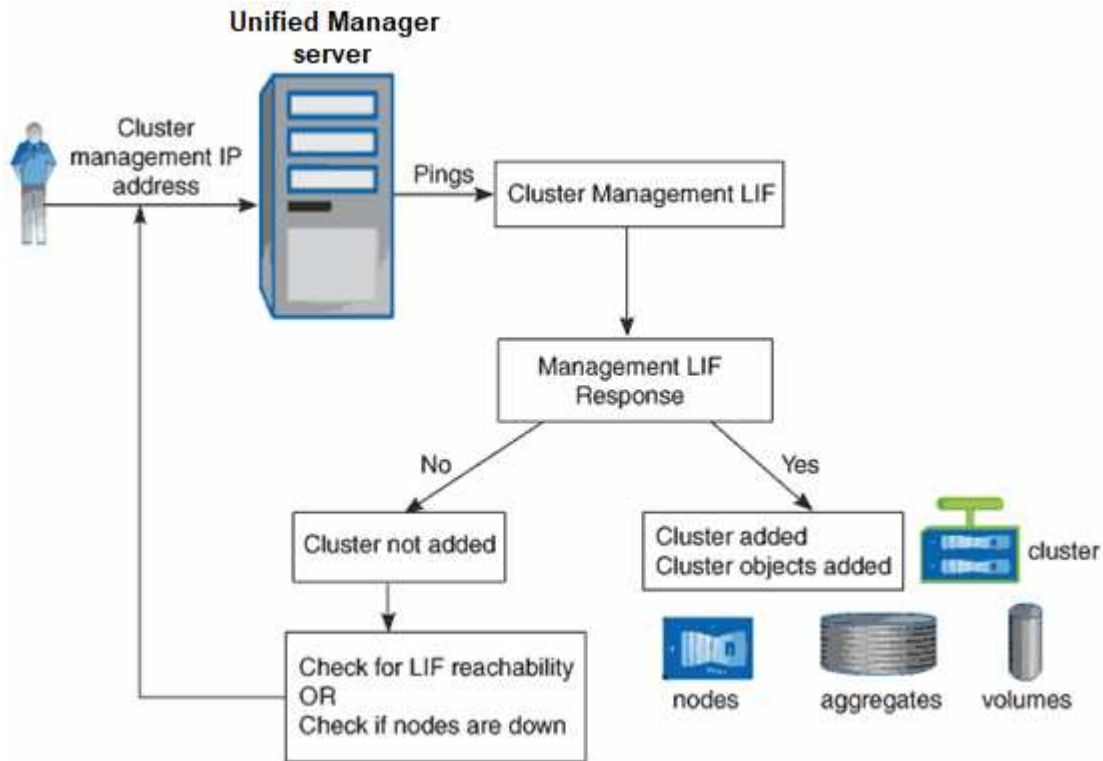
クラスタ検出プロセスの仕組み

Unified Manager にクラスタを追加すると、サーバによってクラスタオブジェクトが検出され、サーバのデータベースに追加されます。検出プロセスの仕組みを理解しておく

と、組織のクラスタとそのオブジェクトを管理する際に役立ちます。

クラスタ構成情報を収集する監視間隔は 15 分です。たとえば、クラスタを追加したあとに、クラスタオブジェクトが Unified Manager の UI に表示されるまでに 15 分かかります。この時間は、クラスタに変更を加えた場合にも当てはまります。たとえば、クラスタ内の SVM に 2 つの新しいボリュームを追加した場合、それらの新しいオブジェクトが UI に表示されるのは次のポーリング間隔のあとであるため、最大で 15 分後になります。

次の図は検出プロセスを示しています。



新しいクラスタのオブジェクトがすべて検出されると、Unified Manager が過去 15 日間の履歴パフォーマンスデータの収集を開始します。これらの統計は、データの継続性収集機能を使用して収集されます。この機能では、クラスタが追加された直後から 2 週間分のクラスタのパフォーマンス情報を入手できます。データの継続性収集サイクルの完了後、デフォルトではクラスタのリアルタイムのパフォーマンスデータが 5 分ごとに収集されます。



15 日分のパフォーマンスデータを収集すると CPU に負荷がかかるため、新しいクラスタを複数追加する場合は、データの継続性収集のポーリングが同時に多数のクラスタで実行されないように、時間差をつけて追加するようにしてください。

監視対象クラスタのリストの表示

クラスタセットアップページを使用して、クラスタのインベントリを表示できます。名前や IP アドレス、通信ステータスなど、クラスタに関する詳細を確認できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ステップ

1. 左側のナビゲーションペインで、* Storage Management * > * Cluster Setup * をクリックします。+ Unified Managerで管理しているストレージ環境内のすべてのクラスタが表示されます。クラスタのリストは、収集状態の重大度レベル列でソートされます。列ヘッダーをクリックすると、別の列でクラスタをソートできます。

クラスタを追加する

Active IQ Unified Manager にクラスタを追加して監視することができます。たとえば、クラスタの健全性、容量、パフォーマンス、構成などの情報を取得して、発生する可能性がある問題を特定して解決できるようにすることができます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- クラスタのホスト名またはクラスタ管理 IP アドレス（IPv4 または IPv6）が必要です。

ホスト名を使用する場合は、クラスタ管理 LIF のクラスタ管理 IP アドレスに解決される必要があります。ノード管理 LIF を使用すると処理に失敗します。

- クラスタにアクセスするためのユーザ名とパスワードが必要です。

このアカウントには、アプリケーションアクセスが `_ontapi`、`console`、および `_http_` に設定された `_admin_role` が必要です。

- HTTPS プロトコルを使用してクラスタに接続するためのポート番号を確認しておく必要があります（通常はポート 443）。
- クラスタで ONTAP バージョン 9.1 以降が実行されている必要があります。
- Unified Manager サーバに十分なスペースが必要です。スペースの使用率が 90% を超えている場合、サーバにクラスタを追加することはできません。
- 必要な証明書を用意しておきます。Unified Managerでクラスタの追加時にセキュリティ証明書がインストールされます。

サーバ証明書：この証明書はUnified Managerが所有しています。デフォルトの自己署名SSL（HTTPS）証明書が生成され、Unified Managerの新規インストールが実行されます。セキュリティを強化するために、CA署名証明書にアップグレードすることを推奨します。サーバ証明書の有効期限が切れた場合は、再生成してUnified Managerを再起動し、サービスに新しい証明書を組み込む必要があります。SSL証明書の再生成の詳細については、を参照してください "[HTTPS セキュリティ証明書の生成](#)"。

相互TLS通信証明書：Unified ManagerとONTAP 間の相互TLS通信で使用されます。証明書ベースの認証は、ONTAP のバージョンに基づいてクラスタで有効になります。ONTAP バージョン9.5よりも前のバージョンを実行しているクラスタでは、証明書ベースの認証が有効になっていません。

古いバージョンのUnified ManagerをUnified Manager 9.12に更新する場合、クラスタの証明書ベースの認証は自動的に有効になりません。ただし、クラスタの詳細を変更して保存することで有効にできます。証明書の有効期限が切れた場合は、再生成して新しい証明書を組み込む必要があります。証明書の表示と再生成の詳細については、を参照してください "[クラスタを編集します](#)"。



- 証明書ベースの認証は、Web UIからクラスタを追加した場合に自動的に有効になります。メンテナンスコンソールからクラスタを追加した場合、証明書ベースの認証は有効になりません。
- クラスタで証明書ベースの認証が有効になっている場合に、Unified Managerのバックアップをサーバから作成し、ホスト名またはIPアドレスが変更された別のUnified Managerサーバにリストアすると、クラスタの監視が失敗することがあります。エラーを回避するには、クラスタの詳細を編集して保存します。クラスタの詳細の編集の詳細については、[を参照してください "クラスタを編集します"](#)。

クライアント証明書：ONTAP から受信したEMSメッセージの認証時に使用されます。この証明書はONTAP が所有しており、ONTAP クラスタをUnified Managerに追加する場合に必要です。有効期限が切れた証明書で Unified Manager にクラスタを追加することはできません。クライアント証明書の期限が切れている場合は、クラスタを追加する前に再生成する必要があります。ただし、追加済みのクラスタの証明書の有効期限が切れて Unified Manager で使用されている場合は、EMS メッセージが期限切れの証明書を使用して引き続き機能します。証明書の生成については、ナレッジベース（KB）の記事を参照してください ["System ManagerユーザインターフェイスでONTAP の自己署名証明書を更新する方法"](#)。

- 1 つの Unified Manager インスタンスでサポートできるノードの数には上限があります。ノードの数がサポートされる最大数を超える環境を監視する必要がある場合は、Unified Manager インスタンスを追加でインストールし、一部のクラスタを監視する必要があります。サポートされるノード数の一覧については、[を参照してください "Unified Manager ベストプラクティスガイド"](#)。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Cluster Setup * をクリックします。
2. クラスタセットアップページで、* 追加 * をクリックします。
3. [Add Cluster] ダイアログボックスで、必要に応じて値を指定し、[Submit] をクリックします。
4. [ホストの許可] ダイアログボックスで、[証明書の表示 *] をクリックして、クラスタに関する証明書情報を表示します。
5. 「* はい *」をクリックします。

Unified Manager 9.12では、クラスタの詳細を保存したあと、クラスタの双方向TLS通信の証明書を確認できます。

証明書ベースの認証が有効になっていない場合、Unified Managerはクラスタが最初に追加されたときのみ証明書をチェックします。Unified Manager では、ONTAP に対する API 呼び出しごとには証明書がチェックされません。

新しいクラスタのオブジェクトがすべて検出されると、Unified Manager が過去 15 日間の履歴パフォーマンスデータの収集を開始します。これらの統計は、データの継続性収集機能を使用して収集されます。この機能では、クラスタが追加された直後から 2 週間分のクラスタのパフォーマンス情報を入手できます。データの継続性収集サイクルの完了後、デフォルトではクラスタのリアルタイムのパフォーマンスデータが 5 分ごとに収集されます。



15 日分のパフォーマンスデータを収集すると CPU に負荷がかかるため、新しいクラスタを複数追加する場合は、データの継続性収集のポーリングが同時に多数のクラスタで実行されないように、時間差をつけて追加するようにしてください。また、データの継続性収集期間に Unified Manager を再起動すると、収集が停止し、その間のデータがパフォーマンスチャートに表示されません。

エラーメッセージが表示されてクラスタを追加できない場合は、次の問題がないかどうかを確認してください。



- 2つのシステムのクロックが同期されておらず、Unified Manager の HTTPS 証明書の開始日がクラスタの日付よりもあとの日付になっている。NTP などのサービスを使用してクロックを同期する必要があります。
- クラスタの EMS 通知の送信先が最大数に達しており、Unified Manager のアドレスを追加できない。デフォルトでは、クラスタで定義できる EMS 通知の送信先は 20 個までです。

• 関連情報 *

["ユーザを追加する"](#)

["クラスタリストおよび詳細の表示"](#)

["CA 署名済みで返された HTTPS 証明書をインストールする"](#)

クラスタを編集します

クラスタの編集ダイアログボックスを使用して、ホスト名または IP アドレス、ユーザ名、パスワード、ポートなど、既存のクラスタの設定を変更できます。

• 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。



Unified Manager 9.7 以降では、クラスタを追加する際に HTTPS のみを使用できます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Cluster Setup * をクリックします。
2. [* クラスタセットアップ *] ページで、編集するクラスタを選択し、[* 編集] をクリックします。
3. [クラスタの編集 (Edit Cluster)] ダイアログボックスで、必要に応じて値を変更します。+ Unified Manager 9.12に追加されたクラスタの詳細を変更した場合は、ONTAP のバージョンに基づいて、相互TLS通信の証明書の詳細を表示できます。ONTAP バージョンの詳細については、[を参照してください "相互TLS通信用の証明書"](#)。+[証明書の詳細]をクリックすると、証明書の詳細を表示できます。証明書の有効期限が切れている場合は、* Regenerate*ボタンをクリックして新しい証明書を組み込みます。
4. [Submit (送信)] をクリックします。
5. [ホストの許可] ダイアログボックスで、[証明書の表示 *] をクリックして、クラスタに関する証明書情報を表示します。
6. 「* はい *」 をクリックします。

◦ 関連情報 *

["ユーザを追加する"](#)

["クラスタリストおよび詳細の表示"](#)

クラスタの削除

Unified Manager からクラスタを削除するには、クラスタセットアップページを使用します。たとえば、クラスタの検出に失敗した場合やストレージシステムを運用停止する場合に、クラスタを削除できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

このタスクでは、選択したクラスタを Unified Manager から削除します。削除したクラスタは監視されなくなります。削除したクラスタに登録されていた Unified Manager のインスタンスは、クラスタから登録解除されます。

クラスタを削除すると、そのストレージオブジェクト、履歴データ、ストレージサービス、関連するイベントもすべて Unified Manager から削除されます。この変更は、次のデータ収集サイクルのあとでインベントリページと詳細ページに反映されます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Cluster Setup * をクリックします。
2. クラスタセットアップページで、削除するクラスタを選択し、* 削除 * をクリックします。
3. [* データソースの削除 *] メッセージダイアログで、[* 削除 *] をクリックして削除要求を確定します。
 - 関連情報 *

["ユーザを追加する"](#)

["クラスタリストおよび詳細の表示"](#)

クラスタの再検出

クラスタを手動で再検出することで、クラスタの健全性、監視ステータス、およびパフォーマンスステータスに関する最新情報を取得できます。

クラスタを更新する場合は、スペースが不足しているときにアグリゲートのサイズを拡張するなど、クラスタを手動で再検出できます。変更を検出するには、Unified Manager で検出します。

Unified Manager と OnCommand Workflow Automation (WFA) を連携させている場合は、WFA でキャッシュされたデータの再取得がトリガーされます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Cluster Setup * をクリックします。
2. [* Cluster Setup*] ページで、[* Rediscover*] をクリックします。

選択したクラスタが Unified Manager で再検出され、最新の健全性とパフォーマンスステータスが表示されます。

- 関連情報 *

["クラスタリストおよび詳細の表示"](#)

VMware 仮想インフラを監視する

Active IQ Unified Manager では、仮想インフラ内の仮想マシン（VM）を可視化し、仮想環境内のストレージやパフォーマンスの問題を監視してトラブルシューティングできます。この機能を使用すると、ストレージ環境におけるレイテンシの問題や、vCenter Server でパフォーマンスイベントが報告されたタイミングを特定できます。

ONTAP の一般的な仮想インフラ環境には、さまざまなコンポーネントがコンピューティングレイヤ、ネットワークレイヤ、ストレージレイヤに分散して配置されています。VM アプリケーションのパフォーマンス低下は、各レイヤのさまざまなコンポーネントでレイテンシが生じていることが原因である可能性があります。この機能は、ストレージまたは vCenter Server の管理者および IT ゼネラリストが、仮想環境でパフォーマンス問題を分析したり、問題がどのコンポーネントで発生したかを把握したりするのに役立ちます。

これで、VMware セクションの vCenter のメニューから vCenter Server にアクセスできるようになりました。表示されている各仮想マシンのプレビューには、新しいブラウザで vCenter Server を起動する [vCenter server] リンクがトポロジビューにあります。また、* トポロジの展開 * ボタンを使用して vCenter Server を起動し、* vCenter で表示 * ボタンをクリックして vCenter Server のデータストアを表示することもできます。

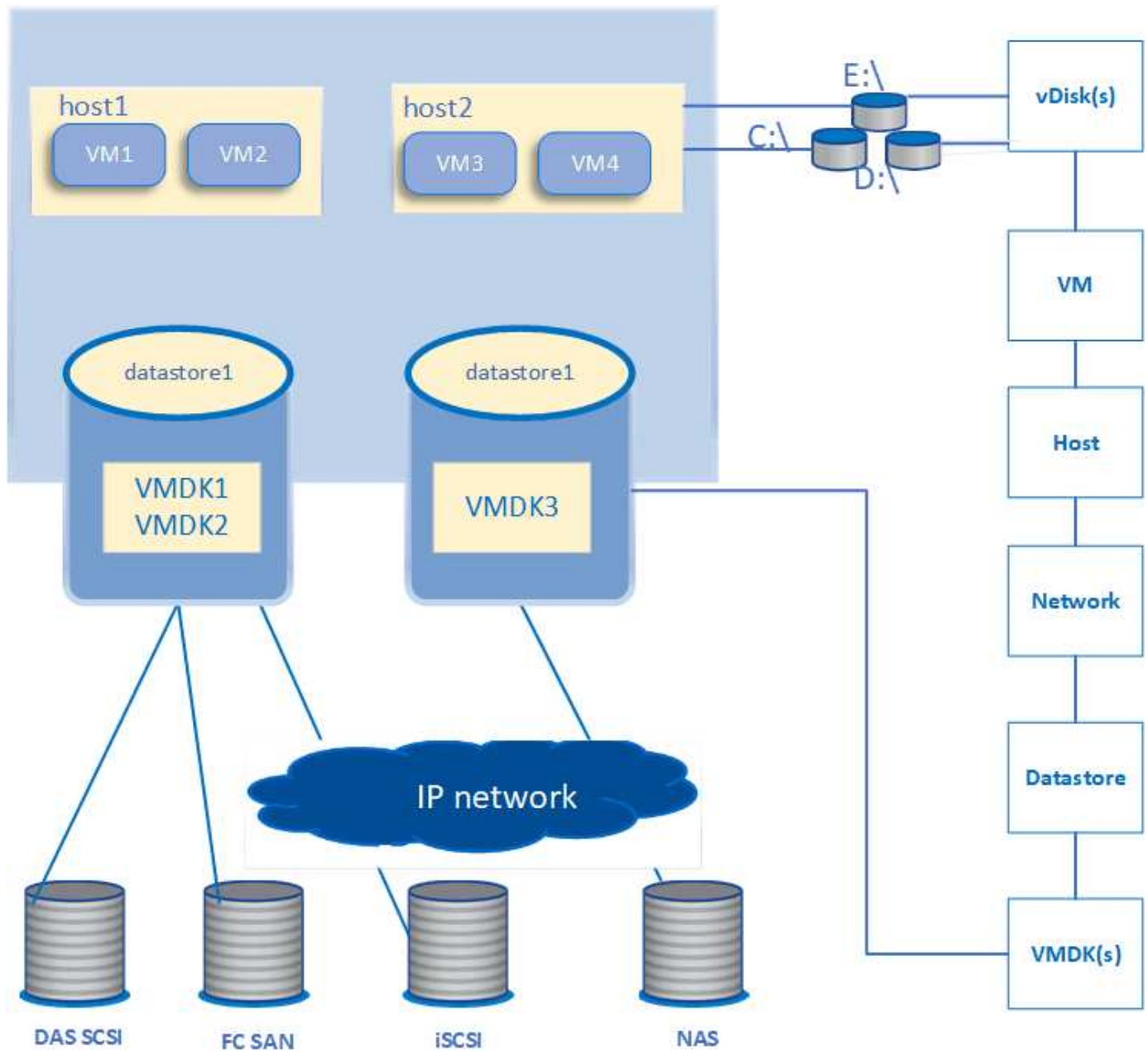
Unified Manager のトポロジビューには、仮想環境の基盤となるサブシステムが表示され、コンピューティングノード、ネットワーク、またはストレージでレイテンシ問題が発生したかどうかを確認されます。また、修復手順を実行して基盤となる問題に対応するために、パフォーマンス低下の原因となっているオブジェクトが強調表示されます。

ONTAP ストレージ上に導入される仮想インフラには、次のオブジェクトが含まれます。

- vCenter Server：仮想環境の VMware VM、ESXi ホスト、およびすべての関連コンポーネントを管理する一元化されたコントロールプレーンです。vCenter Server の詳細については、VMware のドキュメントを参照してください。
- ホスト：VMware の仮想化ソフトウェアである ESXi を実行し、VM をホストする物理システムまたは仮想システムです。
- データストア：データストアは、ESXi ホストに接続される仮想ストレージオブジェクトです。LUN やボリュームなどの ONTAP の管理可能なストレージエンティティであり、ログファイル、スクリプト、構成ファイル、仮想ディスクなどの VM ファイルのリポジトリとして使用され、SAN または IP ネットワーク接続を介して環境内のホストに接続されます。vCenter Server にマッピングされている ONTAP 外部のデータストアは、Unified Manager ではサポートされず、表示もされません。
- VM：VMware 仮想マシン。
- 仮想ディスク：拡張子が VMDK である VM に属するデータストア上の仮想ディスク。仮想ディスクのデータは対応する VMDK に格納されます。
- VMDK：仮想ディスク用のストレージスペースを提供するデータストア上の仮想マシンディスクです。仮想ディスクごとに対応する VMDK があります。

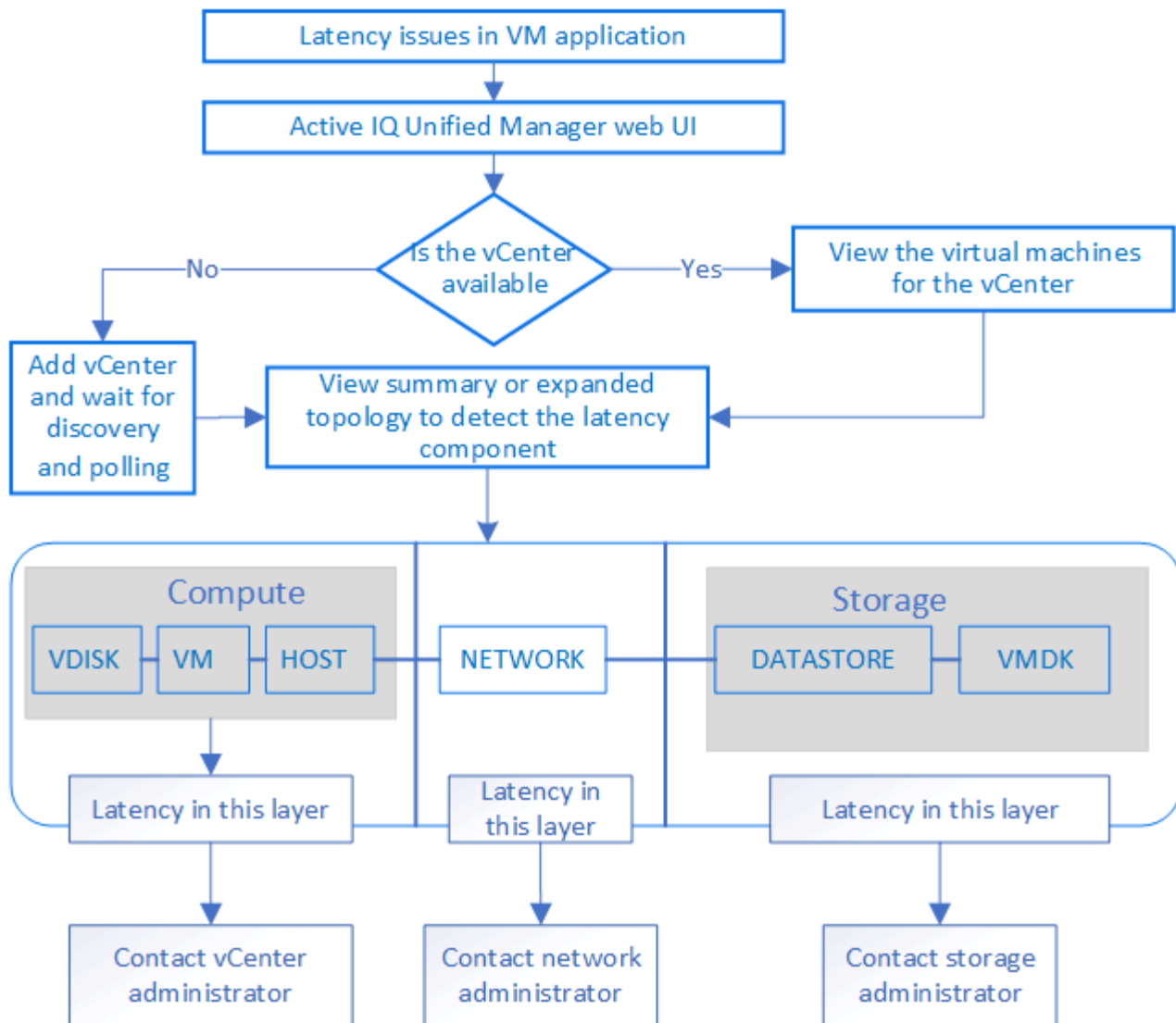
これらのオブジェクトは VM トポロジビューに表示されます。

- ONTAP での VMware 仮想化 *



• ユーザーワークフロー *

次の図は、VM トポロジビューを使用する一般的なユースケースを示しています。



サポートされない機能：

- vCenter Server インスタンスにマッピングされている ONTAP 外部のデータストアは、Unified Manager ではサポートされません。これらのデータストアに仮想ディスクがある VM もサポートされません。
- 複数の LUN にまたがるデータストアはサポートされません。
- ネットワークアドレス変換（NAT）を使用してデータ LIF（アクセスエンドポイント）をマッピングするデータストアはサポートされません。
- 複数LIF構成で同じIPアドレスを使用する異なるクラスタ上のデータストアとしてボリュームまたはLUNをエクスポートすることはできません。Unified Managerでは、どのデータストアがどのクラスタに属しているかを特定できません。

例：クラスタ A にデータストア A があるとしますデータストア A は、同じ IP アドレス x.x.x.x のデータ LIF を介してエクスポートされ、このデータストアに VMA が作成されます。同様に、クラスタ B にはデータストア B がありますデータストア B は、同じ IP アドレス x.x.x.x のデータ LIF を介してエクスポートされます。VM B はデータストア B に作成されますUM では、VMA のトポロジ用のデータストア A を対応する ONTAP ボリューム / LUN にマッピングしたり、VM B をマッピングしたりすることはできません

- データストアとしてサポートされるのは NAS ボリュームと SAN ボリューム（VMFS の場合は iSCSI と FCP）のみです。仮想ボリューム（VVol）はサポートされません。

- iSCSI 仮想ディスクのみがサポートされます。NVMe タイプと SATA タイプの仮想ディスクはサポートされません。
- これらのビューでは、さまざまなコンポーネントのパフォーマンスを分析するためのレポートを生成することはできません。
- Unified Manager の仮想インフラのみでサポートされる Storage Virtual Machine （ Storage VM ） ディザスタリカバリ （ DR ） セットアップの場合は、スイッチオーバーおよびスイッチバックのシナリオでアクティブな LUN を参照するように vCenter Server で設定を手動で変更する必要があります。手動操作なしでは、データストアにアクセスできなくなります。

vCenter Server を表示および追加する

仮想マシン（VM）のパフォーマンスの表示とトラブルシューティングを行うには、関連する vCenter Server を Active IQ Unified Manager インスタンスに追加する必要があります。

- 必要なもの *

vCenter Server を追加または表示する前に、次の点を確認してください。

- vCenter Server の名前を確認しておきます。
- vCenter Server の IP アドレスと必要なクレデンシャルを確認しておきます。vCenter Server 管理者または vCenter Server への読み取り専用アクセス権を持つ root ユーザのクレデンシャルが必要です。
- 追加する vCenter Server で vSphere 6.5 以降が実行されている必要があります。
- vCenter Server でのデータ収集設定は、の統計レベルに設定されます *Level 3* をクリックし、監視対象のすべてのオブジェクトについて必要な指標収集レベルを確認します。間隔はに必要があります *5 minutes* を選択し、保存期間をに設定します *1 day*。

詳細については、VMware のマニュアルの「vSphere Monitoring and Performance Guide」の「DATA Collection Levels」を参照してください。

- レイテンシ値を正しく計算するために、vCenter Server のレイテンシ値はマイクロ秒単位ではなくミリ秒単位で設定されている
- vCenter Server にデータストアを追加する際には、ホストの IP アドレスまたは完全修飾ドメイン名（FQDN）を使用できます。FQDN を追加する場合は、Unified Manager サーバがドメイン名を解決できることを確認してください。たとえば、Linux のインストールの場合は、ドメイン名がに追加されていることを確認します */etc/resolv.conf* ファイル。
- vCenter Server の現在の時刻が vCenter Server のタイムゾーンと同期されている。
- 検出が成功した場合は、vCenter Server に到達できます。
- vCenter Server を Unified Manager に追加する際に、VMware SDK への読み取りアクセスを可能にしておきます。これは、設定のポーリングに必要です。

Unified Manager は、追加されて検出されたすべての vCenter Server について、vCenter Server と ESXi サーバの詳細、ONTAP マッピング、データストアの詳細、ホストされている VM の数などの構成データを収集します。さらに、コンポーネントのパフォーマンス指標も収集されます。

手順

1. 「* vmware * > * vcenter *」に移動して、vCenter Server がリストに表示されているかどうかを確認し

ます。



vCenter Server を使用できない場合は、vCenter Server を追加する必要があります。

- a. [追加 (Add)] をクリックします。
- b. vCenter Server の正しい IP アドレスを追加し、デバイスに到達できることを確認してください。
- c. 管理者または vCenter Server への読み取り専用アクセス権を持つ root ユーザのユーザ名とパスワードを追加します。
- d. デフォルトの 443 以外のポートを使用している場合は、カスタムポート番号を追加します。
- e. [保存 (Save)] をクリックします。

検出に成功すると、表示されたサーバ証明書を承認します。

証明書を承認すると、使用可能な vCenter Server のリストに vCenter Server が追加されます。デバイスを追加しても、関連付けられている VM のデータ収集は開始されず、スケジュールされた間隔で収集されます。

2. vCenter Server が *vCenters* ページに表示されている場合は、* Status * フィールドにカーソルを合わせてステータスを確認し、vCenter Server が正常に動作しているか、警告またはエラーが発生しているかを確認します。



vCenter Server を追加すると、次のステータスが表示されます。ただし、vCenter Server を追加して正確に反映されるまでに、対応する VM のパフォーマンスデータとレイテンシデータが最大 1 時間かかることがあります。

- 緑：「正常」。vCenter Server が検出され、パフォーマンス指標が収集されたことを示します
 - 黄：「警告」（各オブジェクトの統計を取得するための vCenter Server の統計レベルが 3 以上に設定されていない場合など）
 - オレンジ：「Error」（例外、構成データ収集の失敗、vCenter Server に到達できないなどの内部エラーを示します）列の表示アイコン（* Show/Hide *）をクリックすると、vCenter Server のステータスメッセージを表示し、問題のトラブルシューティングを行うことができます。
3. vCenter Server に到達できない場合やクレデンシャルが変更されている場合は、* vCenter* > * Edit * を選択して vCenter Server の詳細を編集します。
 4. VMware vCenter Server の編集 * ページで必要な変更を行います。
 5. [保存 (Save)] をクリックします。
 - vCenter Server のデータ収集を開始します

vCenter Server は、リアルタイムのパフォーマンスデータのサンプルを 20 秒収集して 5 分ごとのサンプルに集計します。Unified Manager のパフォーマンスデータの収集スケジュールは、vCenter Server のデフォルトの設定に基づきます。Unified Manager は、vCenter Server から取得した 5 分ごとのサンプルを処理し、仮想ディスク、VM、およびホストの IOPS とレイテンシの 1 時間の平均を計算します。データストアの場合、Unified Manager は ONTAP から取得したサンプルに基づいて IOPS とレイテンシの 1 時間の平均を計算します。これらの値は毎時 00 分に更新されます。パフォーマンス指標は vCenter Server を追加した直後には収集されず、次の 1 時間の開始時にのみ収集されます。パフォーマンスデータのポーリングは、設定データ収集のサイクルが完了すると開始されます。

Unified Manager は、クラスタの構成データの収集と同じスケジュールで vCenter Server の構成データをポー

リングします。vCenter Server の構成とパフォーマンスのデータ収集スケジュールについては、「クラスタの構成とパフォーマンスのデータ収集アクティビティ」を参照してください。

- 関連情報 *

"クラスタの構成とパフォーマンスのデータの収集アクティビティ"

仮想マシンの監視

仮想マシン（VM）のアプリケーションでレイテンシ問題が発生した場合、原因の分析とトラブルシューティングのために VM の監視が必要になることがあります。VM を使用できるのは、vCenter Server と、VM ストレージをホストする ONTAP クラスタを Unified Manager に追加したときです。

VM の詳細は、* vmware * >> * Virtual Machines * ページに表示されます。可用性、ステータス、使用済み容量と割り当て済み容量、ネットワークレイテンシ、VM、データストア、ホストの IOPS とレイテンシなどの情報が表示されます。複数のデータストアをサポートしている VM の場合は、最もレイテンシが高いデータストアの指標がグリッドに表示され、追加のデータストアを示すアスタリスクアイコン（*）が付きます。アイコンをクリックすると、追加データストアの指標が表示されます。これらの列の一部は、ソートやフィルタに使用できません。



VM とその詳細を表示するには、ONTAP クラスタの検出（ポーリングまたは指標の収集）が完了している必要があります。クラスタが Unified Manager から削除されると、次の検出サイクルのあとで VM を使用できなくなります。

このページから、VM の詳細なトポロジを確認し、ホスト、仮想ディスク、データストアなど、VM が関連するコンポーネントを表示することもできます。トポロジビューには、基になるコンポーネントが各レイヤの次の順序で表示されます。* Virtual Disk * > * VM * > * Host * > * Network * > * Datastore * > * VMDK *。

I/O パスとコンポーネントレベルのレイテンシをトポロジの観点から確認し、パフォーマンス問題の原因かどうかを判断できます。トポロジのサマリビューには I/O パスが表示され、解決手順を特定できるように IOPS やレイテンシの問題があるコンポーネントが強調表示されます。また、トポロジの展開ビューで、各コンポーネントとそのコンポーネントのレイテンシを個別に確認することもできます。コンポーネントを選択すると、レイヤ内で強調表示されている I/O パスを確認できます。

トポロジのサマリビューの表示

トポロジのサマリビューで VM を表示してパフォーマンスの問題を特定するには、次の手順を実行します。

1. 「* vmware * > * Virtual Machines *」に移動します。
2. 検索ボックスに名前を入力して VM を検索します。また、* フィルター * ボタンをクリックして、特定の条件に基づいて検索結果をフィルターすることもできます。ただし、VM が見つからない場合は、対応する vCenter Server が追加されて検出されていることを確認してください。



vCenter Server で使用できる特殊文字（%、&、*、\$、#、@、!、\、/、:、*、?、"、<、>、|、;、'）を使用して、VM、クラスタ、データストア、フォルダ、または file です。VMware vCenter Server および ESX/ESXi Server では、表示名に使用される特殊文字はエスケープされません。ただし、Unified Manager で処理される名前は異なって表示されます。たとえば、という名前のVMがあります
%\$VC_AIQUM_clone_191124% vCenter Serverではと表示されます
%25\$VC_AIQUM_clone_191124%25 Unified Managerのを参照してください。名前に特殊文字が含まれる VM を照会する場合は、この問題をメモしておく必要があります。

3. VM のステータスを確認します。VM のステータスは vCenter Server から取得されます。ステータスは次のいずれかです。これらのステータスの詳細については、VMware のドキュメントを参照してください。
 - 正常
 - 警告
 - アラート
 - 監視対象外
 - 不明です
4. VM の横にある下矢印をクリックすると、コンピューティング、ネットワーク、ストレージの各レイヤにあるコンポーネントのトポロジのサマリビューが表示されます。レイテンシの問題があるノードは強調表示されます。サマリビューには、コンポーネントのワーストレイテンシが表示されます。たとえば、VM に複数の仮想ディスクがある場合、すべての仮想ディスクの中で最もレイテンシが高い仮想ディスクが表示されます。
5. 一定期間にわたるデータストアのレイテンシとスループットを分析するには、データストアオブジェクトアイコンの上にある * Workload Analyzer * ボタンをクリックします。ワークロード分析ページに移動して、期間を選択し、データストアのパフォーマンスチャートを表示できます。Workload Analyzer の詳細については、Workload Analyzer を使用したワークロードのトラブルシューティング _ を参照してください。

トポロジの展開ビューの表示

VM のトポロジの展開ビューでは、各コンポーネントにドリルダウンして個別に確認することができます。

手順

1. トポロジのサマリビューで、[* トポロジの展開 *] をクリックします。各コンポーネントの詳細なトポロジが個別に表示され、各オブジェクトのレイテンシを確認できます。データストアまたは VMDK に複数のノードが含まれているカテゴリでは、レイテンシが最も低いノードが赤で強調表示されます。
2. 特定のオブジェクトの IO パスを確認するには、そのオブジェクトをクリックして IO パスと対応するマッピングを確認します。たとえば、仮想ディスクのマッピングを表示するには、仮想ディスクをクリックして、対応する VMDK への強調表示されたマッピングを表示します。これらのコンポーネントのパフォーマンスが低下した場合は、ONTAP からさらに多くのデータを収集し、問題のトラブルシューティングを行うことができます。



VMDK については指標は報告されません。トポロジでは、VMDK 名のみ表示され、指標は表示されません。

- 関連情報 *

["Workload Analyzer を使用したワークロードのトラブルシューティング"](#)

ディザスタリカバリの設定における仮想インフラの表示

MetroCluster 構成または Storage Virtual Machine（Storage VM）ディザスタリカバリ（SVM DR）セットアップでホストされているデータストアの設定とパフォーマンスの指標を表示できます。

Unified Manager では、vCenter Server でデータストアとして接続された MetroCluster 構成の NAS ボリュームまたは LUN を表示できます。MetroCluster 構成でホストされるデータストアは、標準環境のデータストアと同じトポロジビューで表示されます。

vCenter Server のデータストアにマッピングされている Storage VM ディザスタリカバリ構成内の NAS ボリュームまたは LUN を表示することもできます。

MetroCluster 構成のデータストアの表示

MetroCluster 構成でデータストアを表示する前に、次の前提条件に注意してください。

- スイッチオーバーとスイッチバックが発生した場合は、HA ペアのプライマリクラスタとセカンダリクラスタ、および vCenter Server の検出が完了している必要があります。
- HA ペアのプライマリクラスタとセカンダリクラスタ、および vCenter Server を Unified Manager で管理する必要があります。
- ONTAP および vCenter Server で必要なセットアップを完了しておく必要があります。詳細については、ONTAP および vCenter のドキュメントを参照してください。

"ONTAP 9 ドキュメンテーション・センター"

データストアを表示する手順は次のとおりです。

1. [* vmware*>* Virtual Machines *] ページで、データストアをホストする VM をクリックします。Workload Analyzer * または datastore オブジェクトのリンクをクリックします。ボリュームまたは LUN をホストしているプライマリサイトが想定どおりに機能している場合の標準的なシナリオでは、プライマリサイトの vServer クラスタの詳細を確認できます。
2. 災害が発生し、セカンダリサイトに連続的にスイッチオーバーすると、データストアのリンクからセカンダリクラスタ内のボリュームまたは LUN のパフォーマンス指標が示されます。これは、クラスタの次のサイクルと、vServer の検出（取得）が完了したあとに反映されます。
3. スイッチバックが成功すると、データストアのリンクにプライマリクラスタ内のボリュームまたは LUN のパフォーマンス指標が再び反映されます。これは、クラスタと vServer の次の検出が完了したあとに反映されます。

Storage VM ディザスタリカバリ設定のデータストアの表示

Storage VM ディザスタリカバリ構成でデータストアを表示する前に、次の前提条件に注意してください。

- スイッチオーバーとスイッチバックが発生した場合は、HA ペアのプライマリクラスタとセカンダリクラスタ、および vCenter Server の検出が完了している必要があります。
- ソースクラスタとデスティネーションクラスタ、および Storage VM ピアの両方を Unified Manager で管理する必要があります。
- ONTAP および vCenter Server で必要なセットアップを完了しておく必要があります。

- NAS（NFS および VMFS）データストアの場合は、災害発生時にセカンダリ Storage VM の起動、データ LIF とルートの確認、vCenter Server での切断された接続の確立、VM の起動などの手順を実行します。

プライマリサイトへのスイッチバックの場合は、プライマリサイトがデータの提供を開始する前にボリューム間のデータを同期する必要があります。

- SAN（iSCSI および FC for VMFS）データストアの場合、vCenter Server はマウントされた LUN を VMFS 形式でフォーマットします。災害が発生した場合は、セカンダリ Storage VM を起動し、データ LIF とルートを確認する手順が含まれます。iSCSI ターゲットの IP がプライマリ LIF と異なる場合は、手動で追加する必要があります。新しい LUN は、ホストのストレージアダプタの iSCSI アダプタでデバイスとして使用できる必要があります。以降は、新しい LUN を含む新しい VMFS データストアを作成し、古い VM を新しい名前で登録する必要があります。VM が起動して実行されている必要があります。

リカバリの場合は、ボリューム間のデータを同期する必要があります。LUN を使用して新しい VMFS データストアを再度作成し、古い VM を新しい名前で登録する必要があります。

セットアップの詳細については、ONTAP および vCenter Server のドキュメントを参照してください。

"ONTAP 9 ドキュメンテーション・センター"

データストアを表示する手順は次のとおりです。

1. [* vmware*>* Virtual Machines *] ページで、データストアをホストする VM インベントリをクリックします。データストアオブジェクトのリンクをクリックします。標準的なシナリオでは、プライマリ Storage VM 内のボリュームと LUN のパフォーマンスデータを表示できます。
2. 災害が発生し、セカンダリ Storage VM に連続してスイッチオーバーされた場合、データストアのリンクからセカンダリ Storage VM 内のボリュームまたは LUN のパフォーマンス指標が参照されます。これは、クラスタの次のサイクルと、vServer の検出（取得）が完了したあとに反映されます。
3. スwitchバックが成功すると、データストアのリンクにプライマリ Storage VM のボリュームまたは LUN のパフォーマンス指標が再び反映されます。これは、クラスタと vServer の次の検出が完了したあとに反映されます。

サポート対象外のシナリオです

- MetroCluster 構成では、次の制限事項に注意してください。
 - のクラスタのみ NORMAL および SWITCHOVER 状態が取得されます。などのその他の状態 PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK`および `NOT_REACHABLE はサポートされていません。
 - 自動スイッチオーバー（ASO）が有効になっていない限り、プライマリクラスタがダウンした場合、セカンダリクラスタは検出できず、トポロジはプライマリクラスタ内のボリュームまたは LUN を引き続き参照します。
- Storage VM ディザスタリカバリ構成では、次の制限に注意してください。
 - Site Recovery Manager（SRM）または Storage Replication Adapter（SRA）が SAN ストレージ環境で有効になっている構成はサポートされません。

ワークロードのプロビジョニングと管理

Active IQ Unified Manager のアクティブ管理機能を使用すると、パフォーマンスサービスレベル、ストレージ効率化ポリシー、およびデータセンターのストレージワークロードをプロビジョニング、監視、管理するためのストレージプロバイダ API を利用できます。



この機能は Unified Manager にデフォルトで搭載されています。この機能を使用しない場合は、* Storage Management * > * Feature Settings * で無効にできます。

有効にした場合、Unified Manager のインスタンスで管理される ONTAP クラスタのワークロードをプロビジョニングできます。また、ワークロードにパフォーマンスサービスレベルやストレージ効率化ポリシーなどのポリシーを割り当て、それらのポリシーに基づいてストレージ環境を管理することもできます。

この機能を使用すると、次の機能を実行できます。

- 追加したクラスタでストレージワークロードを自動検出して、ストレージワークロードを簡単に評価して導入できるようにします
- NFS プロトコルと CIFS プロトコルをサポートする NAS ワークロードをプロビジョニングする
- iSCSI および FCP プロトコルをサポートする SAN ワークロードをプロビジョニングする
- 同じファイル共有で NFS プロトコルと CIFS プロトコルの両方がサポートされます
- パフォーマンスサービスレベルとストレージ効率化ポリシーを管理する
- ストレージワークロードにパフォーマンスサービスレベルとストレージ効率化ポリシーを割り当てています

UI の左側のペインで、* Provisioning *、* Storage * > * Workloads *、* Policies * の各オプションを使用して、さまざまな設定を変更できます。

これらのオプションを使用して、次の機能を実行できます。

- ストレージワークロードを * Storage * > * Workloads * ページで表示できます
- プロビジョニングワークロードのページからストレージワークロードを作成します
- パフォーマンスサービスレベルの作成と管理はポリシーから行います
- ポリシーからストレージ効率化ポリシーを作成および管理します
- ワークロードページからストレージワークロードにポリシーを割り当てます
- 関連情報 *

"ポリシーベースのストレージ管理"

ワークロードの概要

ワークロードとは、ボリュームや LUN などのストレージオブジェクトの入出力（I/O）処理のことです。ストレージのプロビジョニング方法は、想定されるワークロード要件に基づいています。Active IQ Unified Manager は、ストレージオブジェクトとの間にトラフィックが発生した時点でワークロードの統計情報の追跡を開始します。たとえば、

ユーザがデータベースまたは E メールアプリケーションの使用を開始した時点で、ワークロードの IOPS とレイテンシを取得できるようになります。

ワークロードページには、Unified Manager で管理されている ONTAP クラスタのストレージワークロードの概要が表示されます。このページには、パフォーマンスサービスレベルに準拠したストレージワークロードと準拠していないストレージワークロードに関する履歴情報が一目でわかるように表示されます。また、データセンター内のクラスタの合計容量、使用可能容量、使用済み容量、およびパフォーマンス（IOPS）を評価することもできます。



非準拠、利用不可、またはいずれのパフォーマンスサービスレベルでも管理されていないストレージワークロードの数を評価し、それらが準拠条件を満たし、使用容量、IOPS が確保されるために必要な措置を講じることを推奨します。

ワークロードページには次の 2 つのセクションがあります。

- ワークロードの概要： Unified Manager で管理されている ONTAP クラスタ上のストレージワークロード数を表示します。
- データセンターの概要：データセンター内のストレージワークロードの容量と IOPS を表示します。関連するデータは、データセンターレベルおよび個別に表示されます。

ワークロードの概要セクション

ワークロードの概要セクションには、ストレージワークロードについての累積情報がわかりやすく表示されます。ストレージワークロードのステータスは、割り当てられているパフォーマンスサービスレベルと割り当てられていないパフォーマンスサービスレベルに基づいて表示されます。

- *** Assigned ***：パフォーマンスサービスレベルが割り当てられているストレージワークロードについては、次のステータスが報告されます。
 - *** 準拠 ***：ストレージワークロードのパフォーマンスは、割り当てられているパフォーマンスサービスレベルに基づきます。ストレージワークロードが、関連付けられているパフォーマンスサービスレベルで定義されたしきい値レイテンシの範囲内にある場合、「準拠」とマークされます。準拠しているワークロードは青で表示されます。
 - *** 非準拠 ***：ストレージワークロードのレイテンシが、関連付けられたパフォーマンスサービスレベルで定義されたしきい値遅延を超えた場合、パフォーマンス監視中にストレージワークロードは「不適合」とマークされます。非準拠のワークロードはオレンジで表示されます。
 - *** 利用不可 ***：ストレージワークロードがオフラインの場合、または対応するクラスタに到達できない場合、ストレージワークロードは「利用不可」とマークされます。利用できないワークロードは赤で表示されます。
- *** 未割り当て ***：パフォーマンスサービスレベルが割り当てられていないストレージワークロードは「未割り当て」と報告されます。情報アイコンにその数が表示されます。

合計ワークロード数は、割り当て済みのワークロードと割り当てなしのワークロードの合計です。

このセクションに表示されるワークロードの総数をクリックすると、ワークロードのページに表示できます。

「Conformance by Performance Service Levels」サブセクションには、使用可能なストレージワークロードの総数が表示されます。

- 各タイプのパフォーマンスサービスレベルに準拠しています

- 割り当てられているパフォーマンスサービスレベルと推奨されるパフォーマンスサービスレベルが一致していません

データセンターの概要セクション

データセンターの概要セクションに、データセンター内のすべてのクラスタの使用可能容量と使用済み容量、および IOPS が図で表示されます。このデータを使用して、ストレージワークロードの容量と IOPS を管理します。このセクションには、すべてのクラスタのストレージワークロードに関する次の情報も表示されます。

- データセンター内のすべてのクラスタの合計容量、使用可能容量、使用済み容量
- データセンター内のすべてのクラスタの合計 IOPS、使用可能 IOPS、使用済み IOPS
- 各パフォーマンスサービスレベルに基づく使用可能容量と使用済み容量
- 各パフォーマンスサービスレベルに基づく使用可能 IOPS と使用済み IOPS
- パフォーマンスサービスレベルが割り当てられていないワークロードで使用されている合計スペースと IOPS
- パフォーマンスサービスレベル * に基づいて、データセンターの容量とパフォーマンスを計算する方法

使用済み容量と使用済み IOPS は、クラスタ内のすべてのストレージワークロードの合計使用済み容量とパフォーマンスに関して取得されます。

使用可能 IOPS は、ノードの想定レイテンシと推奨されるパフォーマンスサービスレベルに基づいて計算されます。これには、想定レイテンシがノード独自の想定レイテンシ以下であるすべてのパフォーマンスサービスレベルの使用可能 IOPS が含まれます。

使用可能容量は、アグリゲートの想定レイテンシと推奨されるパフォーマンスサービスレベルに基づいて計算されます。これには、想定レイテンシがアグリゲート独自の想定レイテンシ以下であるすべてのパフォーマンスサービスレベルの使用可能容量が含まれます。

ワークロードの表示

Unified Managerにクラスタを追加すると、各クラスタのストレージワークロードが自動的に検出されてワークロードページに表示されます。

Unified Manager は、ストレージワークロードで I/O 処理が開始された時点で、推奨される（推奨される PSL）に対するワークロードの分析を開始します。

FlexGroup ボリュームとそのコンスティチュエントは除外されます。

ワークロードの概要

ワークロードの概要ページには、データセンター内のワークロードの概要と、データセンターのスペースとパフォーマンスの概要が表示されます。

- ワークロードの概要*パネル：ワークロードの総数、および**PSL**が割り当てられている/割り当てられていないワークロードの数が表示されます。また、各**PSL**のワークロード数の内訳も表示されます。数をクリックすると、「すべてのワークロード」が表示され、フィルタリングされたワークロードが表示されます。また、システム推奨事項に一致しないワークロードの数を表示し、システム推奨の**PSL**を割り当てても、Assign System-Recommended PSL *ボタンをクリックすることで、該当するワークロードにPSLを割り当てることができます。

- *データセンターの概要*パネル：データセンターの使用可能スペースと使用済みスペース（TiB）とパフォーマンス（IOPS）が表示されます。各PSLの下にあるすべてのワークロードの使用可能スペースと使用済みスペース（TiB）とパフォーマンス（IOPS）も表示されます。

すべてのワークロードを表示します

ストレージ>ワークロード>すべてのワークロード*ページには、Unified Managerで管理されているONTAP クラスタに関連付けられているストレージワークロードが表示されます。

新たに検出されたストレージワークロードで I/O 処理が行われていない場合、ステータスは「I/O を待機中」になります。ストレージワークロードで I/O 処理が開始されると、Unified Manager が分析を開始し、ワークロードのステータスが「学習中 ...」に変わります。分析が完了すると（I/O 処理の開始から 24 時間以内）、ストレージワークロードに推奨される PSL が表示されます。

また、ストレージワークロードにストレージ効率化ポリシー（SEP）とパフォーマンスサービスレベル（PSL）を割り当てることもできます。複数のタスクを実行できます。

- ストレージワークロードを追加またはプロビジョニングする
- ワークロードのリストを表示してフィルタリングします
- PSL をストレージワークロードに割り当てます
- システム推奨の PSL を評価してワークロードに割り当てます
- ストレージワークロードに SEP を割り当てます

ストレージワークロードを追加またはプロビジョニングする

サポートされる LUN（iSCSI と FCP の両プロトコルをサポート）、NFS ファイル共有、SMB 共有にストレージワークロードを追加またはプロビジョニングできます。

手順

1. ストレージ>ワークロード>すべてのワークロード>作成*をクリックします。
2. ワークロードの作成詳細については、を参照してください ["ワークロードのプロビジョニングと管理"](#)。

ワークロードの表示とフィルタリング

All workloads（すべてのワークロード）画面では、データセンター内のすべてのワークロードを表示したり、PSL または名前に基づいて特定のストレージワークロードを検索したりできます。フィルタアイコンを使用して、検索条件を入力できます。ホストクラスタや Storage VM など、さまざまなフィルタ条件で検索できます。容量の合計 * オプションを使用すると、ワークロードの合計容量（MB）でフィルタリングできます。ただしこの場合は、合計容量がバイトレベルで比較されるため、返されるワークロードの数が変わる可能性があります。

各ワークロードについて、ホストクラスタと Storage VM などの情報、および割り当てられている PSL と SEP が表示されます。

また、このページではワークロードのパフォーマンスの詳細を確認することもできます。ワークロードの IOPS、容量、レイテンシに関する詳細情報を表示するには、「* 列の選択 / 順序」ボタンをクリックし、表示する列を選択します。パフォーマンスビューの列にはワークロードの平均 IOPS とピーク IOPS が表示され、ワークロードアナライザのアイコンをクリックすると詳細な IOPS 分析を確認できます。

ワークロードのパフォーマンスと容量の条件を分析します

IOPS分析*ポップアップの*ワークロードの分析*ボタンをクリックすると、ワークロード分析ページが開き、期間を選択して、選択したワークロードのレイテンシ、スループット、容量のトレンドを確認できます。Workload Analyzerの詳細については、を参照してください ["Workload Analyzer を使用したワークロードのトラブルシューティング"](#)。

パフォーマンスビュー * 列の棒グラフアイコンをクリックすると、ワークロードに関するパフォーマンス情報を表示してトラブルシューティングに役立てることができます。ワークロードの分析ページにパフォーマンスと容量のグラフを表示してオブジェクトを分析するには、*ワークロードの分析*ボタンをクリックします。

詳細については、を参照してください ["Workload Analyzer で表示されるデータは何ですか"](#)。

ワークロードにポリシーを割り当てます

各種のナビゲーションオプションを使用して、ストレージ効率化ポリシー（SEP）とパフォーマンスサービスレベル（PSL）をすべてのワークロードページからストレージワークロードに割り当てることができます。

単一のワークロードにポリシーを割り当てる

1 つのワークロードに PSL または SEP、またはその両方を割り当てることができます。次の手順を実行します。

1. ワークロードを選択します。
2. 行の横にある編集アイコンをクリックし、*編集*をクリックします。

[割り当てられているパフォーマンスサービスレベル*] フィールドと [ストレージ効率化ポリシー*] フィールドが有効になります。

3. 必要な PSL または SEP、またはその両方を選択します。
4. チェックマークアイコンをクリックして変更を適用します。



また、ワークロードを選択し、*その他の操作*をクリックしてポリシーを割り当てることもできます。

複数のストレージワークロードにポリシーを割り当てる

複数のストレージワークロードに PSL または SEP を一緒に割り当てることができます。次の手順を実行します。

1. ポリシーを割り当てるワークロードのチェックボックスを選択するか、データセンター内のすべてのワークロードを選択します。
2. [*その他のアクション*] をクリックします。
3. PSL を割り当てるには、「*パフォーマンスサービスレベルの割り当て」を選択してください。SEP を割り当てる場合は、*ストレージ効率化ポリシーの割り当て*を選択します。ポリシーを選択するためのポップアップが表示されます。
4. 適切なポリシーを選択し、*適用*をクリックします。ポリシーが割り当てられているワークロードの数が表示されます。ポリシーが割り当てられていないワークロードも、原因とともに表示されます。



選択したワークロードの数によっては、複数のワークロードにポリシーを適用する場合にしばらく時間がかかることがあります。[* バックグラウンドで実行 *] ボタンをクリックすると、バックグラウンドで処理を実行しながら他のタスクを続行できます。一括割り当てが完了したら、完了ステータスを確認できます。複数のワークロードに PSL を適用する場合、前のジョブの一括割り当ての実行中に別の要求をトリガーすることはできません。

システム推奨の PSL をワークロードに割り当て中です

PSL が割り当てられていないデータセンター内のストレージワークロードに、システム推奨の PSL を割り当てることができます。または、割り当てられた PSL がシステム推奨の対象と一致しません。この機能を使用するには、* Assign System Recommended PSL * ボタンをクリックします。特定のワークロードを選択する必要はありません。

推奨構成はシステム分析によって内部的に決定され、IOPS などのパラメータが使用可能な PSL の定義と一致しないワークロードに対してはスキップされます。ストレージワークロードに Waiting for I/O また、学習ステータスも除外されます。



Unified Manager がワークロード名で検索する特殊なキーワードを使用してシステム分析を上書きし、ワークロードに別の PSL を推奨します。ワークロードの名前に「ora」という文字が含まれている場合は、**Extreme Performance** PSL が推奨されます。ワークロードの名前に「VM」という文字が含まれている場合は、**Performance** PSL を使用することをお勧めします。

ナレッジベース (KB) の記事も参照してください "[Active IQ Unified Manager の「システム推奨のパフォーマンスサービスレベルの割り当て」](#) が変数の大きいワークロードに適応していません"

ファイル共有ボリュームのプロビジョニング

CIFS / SMB プロトコルと NFS プロトコルをサポートするファイル共有ボリュームは、既存のクラスタと Storage Virtual Machine (Storage VM) のプロビジョニングワークロードページから作成できます。

- 必要なもの *
- Storage VM にファイル共有ボリュームをプロビジョニングするためのスペースが必要です。
- Storage VM で SMB サービスと NFS サービスのいずれか、または両方を有効にする必要があります。
- ワークロードにパフォーマンスサービスレベル (PSL) とストレージ効率化ポリシー (SEP) を選択して割り当てる場合は、ワークロードの作成を開始する前にポリシーを作成しておく必要があります。

手順

1. [* Provision Workload*] ページで、作成するワークロードの名前を追加し、使用可能なリストからクラスタを選択します。
2. 選択したクラスタに基づいて、Storage VM * フィールドで、そのクラスタで使用可能な Storage VM がフィルタリングされます。リストから必要な Storage VM を選択します。

Storage VM でサポートされている SMB サービスと NFS サービスに基づいて、Host Information セクションで NAS オプションが有効になっています。

3. ストレージと最適化のセクションで、ストレージ容量と PSL を割り当てます。必要に応じて、ワークロードの SEP を割り当てます。

SEP の仕様が LUN に割り当てられ、PSL の定義が作成時にワークロードに適用されます。

4. ワークロードに割り当てた PSL を適用する場合は、「* パフォーマンス制限を適用する *」チェックボックスを選択します。

ワークロードに PSL を割り当てると、ワークロードが作成されるアグリゲートで、そのポリシーに定義されているパフォーマンスと容量の目標をサポートできることが保証されます。たとえば、ワークロードの PSL に「最高レベルのパフォーマンス」が割り当てられている場合、ワークロードをプロビジョニングするアグリゲートには、SSD ストレージなど、「最高レベルのパフォーマンス」ポリシーに指定されたパフォーマンスと容量が求められます。



このチェックボックスをオンにしないと、PSL はワークロードに適用されず、ダッシュボードのワークロードのステータスは「未割り当て」と表示されます。

5. 「* NAS *」オプションを選択します。

「* NAS *」オプションが有効になっていない場合は、選択した Storage VM が SMB 、 NFS 、またはその両方をサポートしているかどうかを確認してください。



SMB サービスと NFS サービスの両方に対して Storage VM が有効になっている場合は、「NFS で共有」チェックボックスと「SMB で共有」チェックボックスを選択し、NFS プロトコルと SMB プロトコルの両方をサポートするファイル共有を作成できます。SMB 共有と CIFS 共有のどちらかを作成する場合は、該当するチェックボックスのみを選択します。

6. NFS ファイル共有ボリュームの場合は、ファイル共有ボリュームにアクセスするホストまたはネットワークの IP アドレスを指定します。複数のホストの値をカンマで区切って入力できます。

ホストの IP アドレスを追加すると、ホストの詳細が Storage VM と一致しているかどうかチェックされ、指定したホストのエクスポートポリシーが作成されるか、または既存のポリシーがある場合はそのポリシーが使用されます。同じホストに対して複数の NFS 共有を作成した場合は、そのホストで使用可能な一致するルールを含むエクスポートポリシーがすべてのファイル共有で再利用されます。API を使用して NFS 共有をプロビジョニングする場合は、個々のポリシーのルールを指定したり、特定のポリシーキーを指定してポリシーを再利用したりすることができます。

7. SMB 共有の場合は、アクセスを許可するユーザまたはユーザグループを指定し、必要な権限を割り当てます。ユーザグループごとに、新しい Access Control List （ACL ; アクセス制御リスト）がファイル共有の作成時に生成されます。

8. [保存 （ Save ）] をクリックします。

ワークロードがストレージワークロードのリストに追加されます。

LUN のプロビジョニング

CIFS / SMB プロトコルと NFS プロトコルをサポートする LUN は、既存のクラスタおよび Storage Virtual Machine （ Storage VM ） 上のプロビジョニングワークロードのページで作成できます。

- 必要なもの *
- Storage VM に LUN をプロビジョニングするためのスペースが必要です。

- LUN を作成する Storage VM で iSCSI と FCP の両方が有効になっている必要があります。
- ワークロードにパフォーマンスサービスレベル（PSL）とストレージ効率化ポリシー（SEP）を選択して割り当てる場合は、ワークロードの作成を開始する前にポリシーを作成しておく必要があります。

手順

1. [* Provision Workload *] ページで、作成するワークロードの名前を追加し、使用可能なリストからクラスタを選択します。

選択したクラスタに基づいて、Storage VM * フィールドで、そのクラスタで使用可能な Storage VM がフィルタリングされます。

2. iSCSI サービスと FCP サービスをサポートする Storage VM をリストから選択します。

選択に基づいて、ホスト情報セクションで SAN オプションが有効になります。

3. 「ストレージと最適化 *」セクションで、ストレージ容量と PSL を割り当てます。必要に応じて、ワークロードの SEP を割り当てます。

SEP の仕様が LUN に割り当てられ、PSL の定義が作成時にワークロードに適用されます。

4. 割り当てられている PSL をワークロードに適用する場合は、「 * パフォーマンス制限を適用する *」チェックボックスを選択します。

ワークロードに PSL を割り当てると、ワークロードが作成されるアグリゲートで、そのポリシーに定義されているパフォーマンスと容量の目標をサポートできることが保証されます。たとえば、ワークロードに「最高レベルのパフォーマンス」PSL が割り当てられている場合、ワークロードをプロビジョニングするアグリゲートには、SSD ストレージなど、「最高レベルのパフォーマンス」ポリシーに指定されたパフォーマンスと容量が求められます。



このチェックボックスをオンにしない場合、PSL はワークロードに適用されず、ダッシュボードにワークロードのステータスはと表示されます `unassigned`。

5. [SAN] オプションを選択します。「 * san *」オプションが有効になっていない場合は、選択した Storage VM で iSCSI と FCP がサポートされているかどうかを確認してください。
6. ホスト OS を選択します。
7. LUN へのイニシエータのアクセスを制御するホストマッピングを指定します。既存のイニシエータグループ（igroup）を割り当てるか、新しい igroup を定義してマッピングできます。



LUN のプロビジョニング時に新しい igroup を作成した場合は、次の検出サイクル（最大 15 分）でその igroup が使用されるまで待つ必要があります。したがって、使用可能な igroup のリストから既存の igroup を使用することを推奨します。

新しい igroup を作成する場合は、「 * 新しいイニシエータグループを作成する *」ボタンを選択し、igroup の情報を入力します。

8. [保存（Save）] をクリックします。

LUN がストレージワークロードのリストに追加されます。

パフォーマンスサービスレベル

パフォーマンスサービスレベル (PSL) を使用すると、ワークロードに対してパフォーマンスとストレージの目標を定義できます。ワークロードの最初の作成時や編集時に、PSLをワークロードに割り当てることができます。

ストレージリソースは、サービスレベル目標 (SLO) に基づいて管理および監視されます。SLO は、必要なパフォーマンスと容量に基づくサービスレベルアグリーメントによって定義されます。Unified Manager では、SLO と言った場合、ネットアップストレージで実行されているアプリケーションの PSL の定義を表します。ストレージサービスの内容は、基盤となるリソースのパフォーマンスと利用率に基づいて決定されます。PSL はストレージサービス目標の概要です。ストレージプロバイダは、PSL を使用してワークロードに目標とするパフォーマンスと容量を指定できます。ワークロードに PSL を割り当てると、ONTAP 上の対応するワークロードがパフォーマンスと容量の目標で管理されます。各 PSL には、ピーク IOPS、想定 IOPS、絶対最小 IOPS、および想定レイテンシが適用されます。

Unified Manager には、次のタイプの PSL があります。

- システム定義：Unified Manager には、変更できない組み込みのポリシーがいくつか用意されています。事前定義された PSL は次のとおりです
 - 卓越したパフォーマンス
 - パフォーマンス
 - 価値

Extreme Performance、Performance、および Value PSL は、データセンターの一般的なストレージワークロードのほとんどに該当します。

Unified Manager には、データベースアプリケーションのパフォーマンスサービスレベルも3つあります。これらは、バースト IOPS をサポートする非常にハイパフォーマンスな PSL であり、スループットの要求が最も高いデータベースアプリケーションに適しています。

- データベースログの「最高レベル」
- データベース共有データ用の Extreme
- データベースデータ用の Extreme
- ユーザ定義：事前定義されたパフォーマンスサービスレベルが要件に合わない場合は、PSL を新たに作成してニーズに対応できます。詳細については、[を参照してください "パフォーマンスサービスレベルの作成と編集"](#)。
- * Extreme を超える場合*：PSL が最高レベルを超えると、PSL がシステム推奨となります。PSL を超えるワークロードには、Extreme よりも高い IOPS が必要です。ワークロードの内部分析は IOPS、容量、レイテンシに基づいて行われ、ストレージ>ワークロード>すべてのワークロード*画面で、これらのワークロードそれぞれについて PSL を超えることが推奨されます。PSL をワークロードに適用することで最適なパフォーマンスを確保できます。


ワークロードの IOPS パラメータは、ワークロードの動作に応じて動的に生成され、「最高レベル」を超える PSL の名前に追加されます Beyond Extreme <number-(peak IOPS/TB)> <number (expected IOPS/TB)>。たとえば、ピーク IOPS と想定 IOPS が設定されたワークロードがあるとシステムで判断された場合などです 106345 および 37929 ワークロードに対して生成される「Beyond Extreme PSL」は、それぞれにです Beyond Extreme 106345 37929。システムでこれらの PSL が推奨されますが、PSL をワークロードに割り当てると、該当する PSL にはとラベルが付けられます User-defined タイプ：

PSLを割り当ててワークロードを管理しています

PSLには、「* Policies > Performance Service Levels *」ページからアクセスできます。また、ストレージプロバイダAPIを使用してアクセスできます。PSL を割り当ててストレージワークロードを管理すると、ストレージワークロードを個別に管理する必要がなくなるため便利です。変更については、個別に管理するのではなく、別の PSL を再割り当てして管理することもできます。Unified Managerでは、内部の評価と推奨事項に基づいてワークロードにPSLを割り当てることができます。

システム推奨のPSLをワークロードに割り当て方法については、を参照してください ["システム推奨の PSL をワークロードに割り当て中です"](#)

パフォーマンスサービスレベルページには、使用可能な PSL ポリシーが表示されます。このページで、ポリシーを追加、編集、削除することができます。



システム定義の PSL またはワークロードに現在割り当てられている PSL は変更できません。ワークロードに割り当てられている PSL、または他に使用可能な PSL がない PSL は削除できません。

このページには、次の情報が表示されます。

フィールド	説明
名前	PSLの名前。
を入力します	システム定義のポリシーかユーザ定義のポリシーか。
想定 IOPS/TB	LUN またはファイル共有でアプリケーションが実行すると想定される最小 IOPS。想定 IOPS は、ストレージオブジェクトの割り当てサイズに基づいて、割り当てられる最小想定 IOPS を指定します。
最大 IOPS/TB	<p>LUN またはファイル共有でアプリケーションが実行できる最大 IOPS。ピーク IOPS は、ストレージオブジェクトの割り当てサイズまたは使用済みサイズに基づいて、割り当て可能な最大 IOPS を指定します。</p> <p>ピーク IOPS は割り当てポリシーを基準にして算出されます。割り当てポリシーは、 allocated-space または used-space のいずれかです。割り当てポリシーが allocated-space の場合は、ストレージオブジェクトのサイズに基づいてピーク IOPS が計算されます。割り当てポリシーが used-space の場合は、 Storage Efficiency 機能の効果を考慮し、ストレージオブジェクトに格納されているデータの量に基づいてピーク IOPS が計算されます。デフォルトでは、割り当てポリシーは used-space に設定されています。</p>

フィールド	説明
絶対最小 IOPS	<p>絶対最小 IOPS は、想定 IOPS がこの値より低い場合に使用されます。システム定義の PSL のデフォルト値は次のとおりです。</p> <ul style="list-style-type: none"> • 最高レベルのパフォーマンス：想定 IOPS \geq 6144/TB の場合、絶対最小 IOPS=1000 • パフォーマンス：6144/TB > 想定 IOPS \geq 2048/TB の場合、絶対最小 IOPS=500 • バリュース：2048/TB > 想定 IOPS \geq 128/TB の場合、絶対最小 IOPS=75 <p>システム定義のデータベース PSL のデフォルト値は次のとおりです。</p> <ul style="list-style-type: none"> • データベースログの最高レベル：想定 IOPS \geq 22528 の場合、絶対最小 IOPS =4000 • データベース共有データの最大 IOPS：想定 IOPS \geq 16384 の場合、絶対最小 IOPS=2000 • データベースデータの最高レベル：想定 IOPS \geq 12288 の場合、絶対最小 IOPS=2000 <p>カスタム PSL の絶対最小 IOPS の値の大きい方には、最大 75000 を指定できます。下の値は、次のように計算されます。</p> <p>1000/ 想定レイテンシ</p>
想定レイテンシ	処理あたりのミリ秒（ms/op）で表したストレージ IOPS の想定レイテンシ。
容量	クラスタ内の使用可能容量と使用済み容量の合計。
ワークロード	PSL が割り当てられているストレージワークロードの数。

ピーク IOPS と想定 IOPS が、ONTAP クラスタで一貫した差別化されたパフォーマンスを実現するのにどのように役立つかについては、次の技術情報アーティクルを参照してください。https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F["パフォーマンスの予算編成とは"]

PSLによって定義されるしきい値を超えているワークロードに対して生成されるイベント

ワークロードが過去1時間の想定レイテンシの値を30%超えた場合、Unified Managerは次のいずれかのイベントを生成して、潜在的なパフォーマンス問題をユーザに通知します。

- パフォーマンスサービスレベルポリシーに定義されたワークロードのボリュームレイテンシしきい値を超過

- ・ パフォーマンスサービスレベルポリシーに定義されたワークロードのLUNレイテンシしきい値を超過。

ワークロードを分析して、レイテンシの値が高くなる原因を確認することができます。

詳細については、次のリンクを参照してください。

- ・ ["ボリュームイベント"](#)
- ・ ["パフォーマンスしきい値ポリシーを超えた場合の動作"](#)
- ・ ["Unified Manager がワークロードのレイテンシを使用してパフォーマンスの問題を特定する仕組み"](#)
- ・ ["パフォーマンスイベントとは"](#)

システム定義のPSL

次の表に、システム定義の PSL に関する情報を示します。

パフォーマンスサービスレベル	概要とユースケース	想定レイテンシ (ミリ秒 / 処理)	最大 IOPS	想定 IOPS	絶対最小 IOPS
卓越したパフォーマンス	非常に高いスループットを非常に低いレイテンシで実現します レイテンシの影響を受けやすいアプリケーションに最適です	1.	12288	6144	1000
パフォーマンス	高いスループットを低いレイテンシで実現 データベースや仮想アプリケーションに最適です	2.	4096	2048	500

パフォーマンス サービスレベル	概要とユースケ ース	想定レイテンシ (ミリ秒 / 処理)	最大 IOPS	想定 IOPS	絶対最小 IOPS
価値	<p>高いストレージ容量を適度なレイテンシで実現します</p> <p>E メール、Web コンテンツ、ファイル共有、バックアップターゲットなどの大容量アプリケーションに最適です</p>	17	512	128	75
データベースログの「最高レベル」	<p>最小のレイテンシで最大スループットを実現</p> <p>データベースログをサポートするデータベースアプリケーションに最適です。データベースログは非常にバースト性が高く、常にロギングが必要であるため、この PSL は最高のスループットを提供します。</p>	1.	45056	22528	4、000
データベース共有データ用の Extreme	<p>非常に高いスループットを最小のレイテンシで実現</p> <p>共通のデータストアに格納されていて、データベース間で共有されているデータベースアプリケーションデータに最適です。</p>	1.	32768	16384	2000 年

パフォーマンスサービスレベル	概要とユースケース	想定レイテンシ (ミリ秒 / 処理)	最大 IOPS	想定 IOPS	絶対最小 IOPS
データベースデータ用の Extreme	<p>高いスループットを最小のレイテンシで実現</p> <p>データベーステーブル情報やメタデータなどのデータベースアプリケーションデータに最適です。</p>	1.	24576	12288	2000 年

パフォーマンスサービスレベルの作成と編集

システム定義のパフォーマンスサービスレベルがワークロードの要件に合わない場合は、ワークロードに最適化された独自のパフォーマンスサービスレベルを作成できます。

- 必要なもの *
- アプリケーション管理者のロールが必要です。
- パフォーマンスサービスレベル名は一意である必要があります。また、次のリザーブキーワードは使用できません。

Prime、Extreme、Performance、Value、Unassigned、Learning、Idle、Default、および None。

カスタムのパフォーマンスサービスレベルを作成および編集するには、パフォーマンスサービスレベルページで、ストレージにアクセスするアプリケーションに必要なサービスレベル目標を定義します。



ワークロードに現在割り当てられているパフォーマンスサービスレベルは変更できません。

手順

1. 左側のナビゲーションペインの * Settings * で、 * Policies * > * Performance Service Levels * を選択します。
2. パフォーマンスサービスレベル * ページで、新しいパフォーマンスサービスレベルを作成するか既存のパフォーマンスサービスレベルを編集するかに応じて、該当するボタンをクリックします。

目的	実行する手順
新しいパフォーマンスサービスレベルを作成します	[追加 (Add)] をクリックします。
既存のパフォーマンスサービスレベルを編集します	既存のパフォーマンスサービスレベルを選択し、 * 編集 * をクリックします。

パフォーマンスサービスレベルを追加または編集するためのページが表示されます。

3. パフォーマンスの目標を指定してパフォーマンスサービスレベルをカスタマイズし、* Submit * をクリックしてパフォーマンスサービスレベルを保存します。

新規または変更したパフォーマンスサービスレベルをワークロード（LUN、NFS ファイル共有、CIFS 共有）に適用できるのは、ワークロードページから、または新しいワークロードをプロビジョニングするときです。

ストレージ効率化ポリシーの管理

Storage Efficiency ポリシー（SEP）を使用して、ワークロードのストレージ効率化特性を定義することができます。ワークロードを最初に作成するとき、またはワークロードを編集して、ワークロードに SEP を割り当てることができます。

Storage Efficiency では、ストレージ利用率を高めてストレージコストを削減するシンプロビジョニング、重複排除、データ圧縮などのテクノロジーを使用します。スペース削減テクノロジーを個別に、または組み合わせて使用することで、ストレージ効率を最大限に高めることができます。ポリシーをストレージワークロードに関連付けると、指定されたポリシー設定がストレージワークロードに割り当てられます。Unified Manager では、システム定義とユーザ定義の SEP を割り当てて、データセンターのストレージリソースを最適化することができます。

Unified Manager には、システム定義の 2 つの SEP が「高」と「低」の 2 つあります。これらの SEP はデータセンターのほとんどのストレージワークロードに当てはまりますが、システム定義の SEP が要件に合わない場合は独自のポリシーを作成できます。

システム定義の SEP、またはワークロードに現在割り当てられている SEP は変更できません。ワークロードに割り当てられている SEP、または使用可能な SEP のみを削除することはできません。

Storage Efficiency Policies ページには、使用可能な SEP が表示され、カスタマイズした SEP の追加、編集、および削除が可能です。このページには、次の情報が表示されます。

フィールド	説明
名前	SEP の名前。
を入力します	システム定義のポリシーかユーザ定義のポリシーか。
スペースリザーベーション	ボリュームがシンプロビジョニングされているか、シックプロビジョニングされているか。

フィールド	説明
重複排除	<p>ワークロードで重複排除が有効になっているかどうか。</p> <ul style="list-style-type: none"> • インライン：ワークロードへの書き込み中に重複排除が実行されます • バックグラウンド：ワークロードで重複排除が実行されます • Disable：ワークロードで重複排除が無効になります
圧縮	<p>ワークロードでデータ圧縮を有効にするかどうか。</p> <ul style="list-style-type: none"> • Inline：ワークロードへの書き込み中にデータ圧縮が実行されます • バックグラウンド：ワークロードでデータ圧縮が実行されます • disable：ワークロードでデータ圧縮が無効になります
ワークロード	SEP が割り当てられているストレージワークロードの数

カスタムのストレージ効率化ポリシーを作成する場合のガイドラインを次に示します

既存の SEP がストレージワークロードのポリシー要件を満たしていない場合は、カスタム SEP を作成できます。ただし、ストレージワークロードにはシステム定義の SEP を使用して、必要な場合はカスタムの SEP のみを作成することを推奨します。

ワークロードに割り当てられている SEP は、すべてのワークロードページおよびボリューム / 健全性の詳細ページで確認できます。ダッシュボードの容量パネルおよび容量：すべてのクラスタビューで、これらの Storage Efficiency 機能に基づいてクラスタレベルのデータ削減率を表示できます。

ストレージ効率化ポリシーの作成と編集

システム定義のストレージ効率化ポリシーがワークロードの要件に合わない場合は、ワークロードに合わせて最適化された独自のストレージ効率化ポリシーを作成できます。

- 必要なもの *
- アプリケーション管理者のロールが必要です。
- ストレージ効率化ポリシーの名前は一意である必要があります。また、次のリザーブされているキーワードは使用できません。

High、Low、Unassigned、Learning、Idle、Default`および `None。

カスタムのストレージ効率化ポリシーを作成および編集するには、ストレージにアクセスするアプリケーション

ンに必要なストレージ効率化特性を定義します。



ワークロードに現在割り当てられているストレージ効率化ポリシーは変更できません。

手順

1. 左側のナビゲーションペインの * Settings * で、 * Policies * > * Storage Efficiency * を選択します。
2. ストレージ効率化ポリシー * ページで、新しいストレージ効率化ポリシーを作成するか既存のストレージ効率化ポリシーを編集するかに応じて、該当するボタンをクリックします。

目的	実行する手順
新しいストレージ効率化ポリシーを作成します	[追加 (Add)] をクリックします。
既存のストレージ効率化ポリシーを編集します	既存のストレージ効率化ポリシーを選択し、 * 編集 * をクリックします

ストレージ効率化ポリシーを追加または編集するためのページが表示されます。

3. ストレージ効率化の特性を指定してストレージ効率化ポリシーをカスタマイズし、 * Submit * をクリックしてストレージ効率化ポリシーを保存します。

新規または変更したストレージ効率化ポリシーをワークロード（LUN、NFS ファイル共有、CIFS 共有）にワークロードページから適用するか、または新しいワークロードをプロビジョニングする際に適用できます。

MetroCluster 構成を管理および監視する

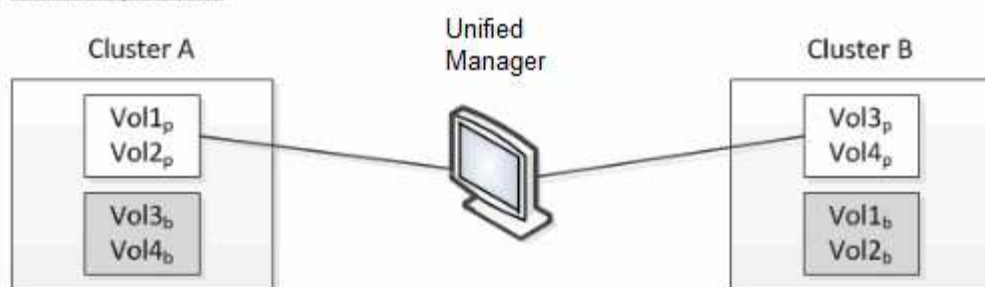
Unified Manager Web UIでは、MetroCluster 構成を監視することで、MetroCluster over FCおよびIP構成の接続に問題がないかを確認できます。接続問題を早期に検出することで、MetroCluster 構成を効果的に管理できます。

スイッチオーバーおよびスイッチバックの発生時のボリュームの動作

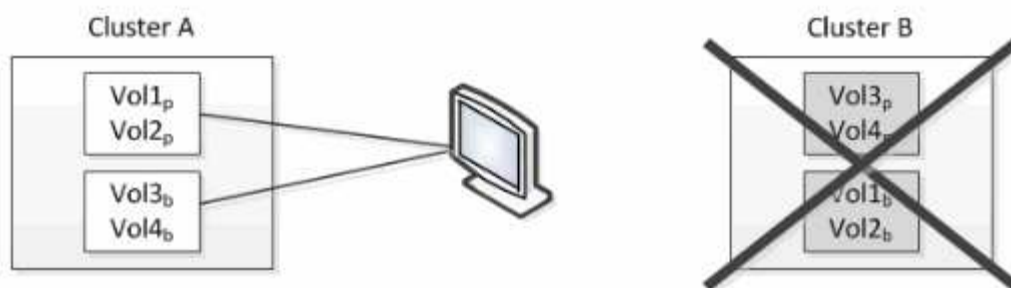
スイッチオーバーまたはスイッチバックをトリガーするイベント。原因アクティブボリュームをディザスタリカバリグループ内の一方のクラスタからもう一方のクラスタに移動します。クライアントにデータを提供していたアクティブなクラスタのボリュームは停止され、もう一方のクラスタのボリュームがアクティブ化されてデータの提供が開始されます。Unified Manager では、実行中のアクティブなボリュームのみが監視されます。

ボリュームが一方のクラスタからもう一方のクラスタに移動されるため、両方のクラスタを監視することを推奨します。Unified Manager では単 MetroCluster 一のインスタンスで両方のクラスタを監視できますが、監視する 2 つのクラスタ間の距離によっては、両方のクラスタを監視するために Unified Manager インスタンスが 2 つ必要になる場合があります。次の図は、Unified Manager の単一のインスタンスを示しています。

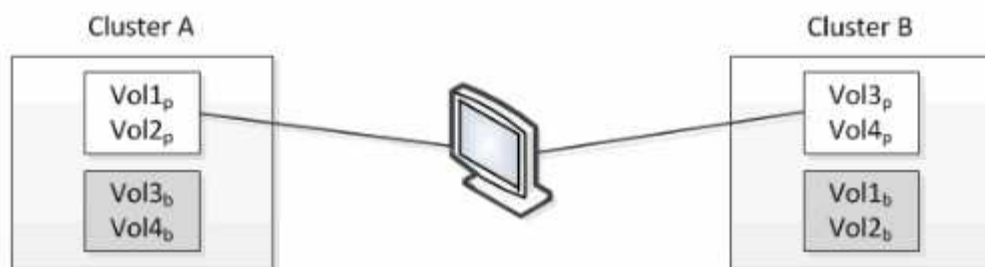
Normal operation



Cluster B fails --- switchover to Cluster A



Cluster B is repaired --- switchback to Cluster B



□ = active and monitored

■ = inactive and not monitored

名前に「p」が付いているボリュームはプライマリボリュームで、「b」が付いているボリュームは SnapMirror で作成されたミラーバックアップボリュームです。

通常運用時：

- クラスタ A には、Vol1p と Vol2p の 2 つのアクティブボリュームがあります。
- クラスタ B には、Vol3p と Vol4p の 2 つのアクティブボリュームがあります。
- クラスタ A の 2 つのボリュームが非アクティブ：Vol3b と Vol4b
- クラスタ B の 2 つのボリュームが非アクティブ：Vol1b および Vol2b

Unified Manager によって、アクティブなボリュームのそれぞれに関する情報（統計やイベントなど）が収集されます。Vol1p および Vol2p の統計情報はクラスタ A によって収集され、Vol3p および Vol4p の統計情報はクラスタ B によって収集されます。

重大な障害が発生してアクティブなボリュームがクラスタ B からクラスタ A にスイッチオーバーされると次のようになります。

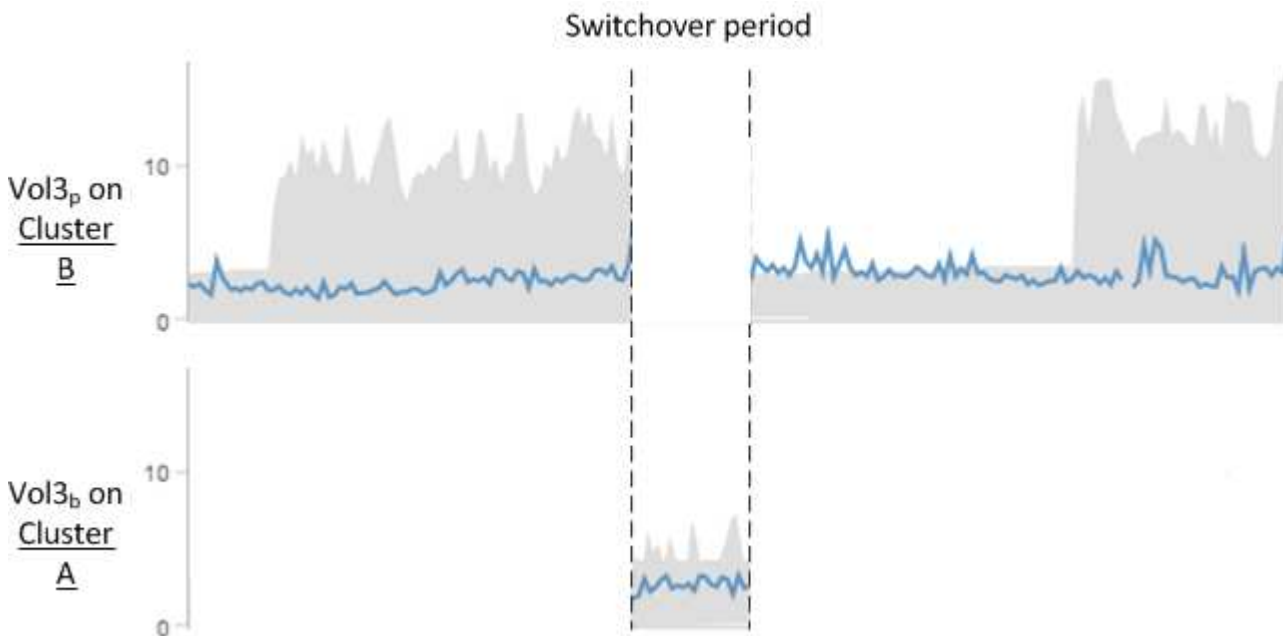
- クラスタ A には、Vol1p、Vol2p、Vol3b、Vol4b の 4 つのアクティブボリュームがあります。
- クラスタ B の 4 つのボリュームが非アクティブ：Vol3p、Vol4p、Vol1b、Vol2b。

通常運用時と同様に、Unified Manager でアクティブなボリュームのそれぞれに関する情報が収集されます。ただし、この場合は、クラスタ A によって Vol1p および Vol2p の統計情報が収集され、クラスタ A でも Vol3b および Vol4b の統計情報が収集されます

Vol3p と Vol3b は異なるクラスタにあるため、同じボリュームではないことに注意してください。Unified Manager の Vol3p に関する情報は Vol3b とは異なります。

- クラスタ A にスイッチオーバーしている間は、Vol3p の統計とイベントは表示されません。
- 最初のスイッチオーバーでは、Vol3b は履歴情報のない新しいボリュームのように見えます。

クラスタ B が復旧してスイッチバックが実行されると、クラスタ B の Vol3p が再びアクティブになり、スイッチオーバー中に過去の統計と統計のギャップが生じます。別のスイッチオーバーが発生するまで、Vol3b をクラスタ A で表示することはできません。



- スwitchバック後にクラスタ A の Vol3b など、非アクティブな MetroCluster ボリュームは「This volume was deleted」というメッセージで示されます。このボリュームは、実際には削除されていませんが、アクティブなボリュームでないため Unified Manager で現在監視されていません。
- 単一の Unified Manager で MetroCluster 構成の両方のクラスタを監視している場合にボリュームを検索すると、その時点でアクティブなボリュームの情報が返されます。たとえば、スイッチオーバーが発生してクラスタ A で Vol3 がアクティブになっている場合、「vol3」を検索すると、クラスタ A の Vol3b の統計とイベントが返されます

MetroCluster over FC構成のクラスタ接続ステータスの定義


MetroCluster over FC構成のクラスタ間の接続のステータスは、「Optimal」、「Impacted」「Down」のいずれかになります。接続ステータスを理解しておく



と、MetroCluster 構成を効果的に管理できるようになります。

接続ステータス	説明	アイコンが表示されます
最適	MetroCluster 構成のクラスタ間の接続は正常な状態です。	
影響を受ける	1 つ以上のエラーによってフェイルオーバー可用性のステータスが損なわれていますが、MetroCluster 構成の両方のクラスタは稼働しています。たとえば、ISL リンクが停止している、クラスタ間 IP リンクが停止している、パートナークラスタにアクセスできないなどの場合です。	
下へ	一方または両方のクラスタが停止しているか、クラスタがフェイルオーバーモードになっているため、MetroCluster 構成のクラスタ間の接続が停止しています。たとえば、災害によってパートナークラスタが停止している場合や、テスト目的で計画的スイッチオーバーを実行している場合などです。	<p>スイッチオーバーでエラー：</p>  <p>スイッチオーバー成功：</p> 

MetroCluster over FCのデータミラーリングのステータス定義

MetroCluster over FC構成では、データのミラーリングが可能で、サイト全体が利用できなくなった場合にフェイルオーバーを開始する機能も利用できます。MetroCluster over FC構成のクラスタ間のデータミラーリングのステータスは、「Normal」または「Mirroring Unavailable」のいずれかになります。これらのステータスを理解しておくと、MetroCluster 構成を効果的に管理できます。

データミラーリングのステータス	説明	アイコンが表示されます
正常	MetroCluster 構成のクラスタ間のデータミラーリングが正常な状態です。	

データミラーリングのステータス	説明	アイコンが表示されます
ミラーリングを使用できません	スイッチオーバーが原因で、MetroCluster 構成のクラスタ間のデータミラーリングが利用できない状態になっています。たとえば、災害によってパートナークラスタが停止している場合や、テスト目的で計画的スイッチオーバーを実行している場合などです。	<p>スイッチオーバーでエラー：</p>  <p>スイッチオーバー成功：</p> 

MetroCluster 構成を監視しています

MetroCluster 構成の接続の問題を監視することができます。クラスタ内のコンポーネントおよび接続のステータス、および MetroCluster 構成のクラスタ間の接続ステータスなどの詳細情報を確認できます。ここでは、MetroCluster over FCおよびMetroCluster over IP構成で保護されたクラスタの接続の問題を監視する方法について説明します。

MetroCluster 構成は、Active IQ Unified Manager の左ナビゲーションペインの次のビューで監視できます。

- ストレージ>*クラスタ*>*保護：MetroCluster *ビュー
- 保護>*関係*>*関係：MetroCluster *ビュー

Unified Managerでは、システムヘルスアラートを使用して、MetroCluster 構成のコンポーネントおよび接続のステータスを示します。

- 必要なもの *
- MetroCluster 構成のローカルクラスタとリモートクラスタの両方をActive IQ Unified Manager に追加する必要があります。
- MetroCluster over IP構成でメディエーターがサポートされる場合は、対応するAPIでメディエーターを設定してクラスタに追加する必要があります。
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

MetroCluster over FC構成の接続の問題を監視する

MetroCluster over FC構成のクラスタの場合は、接続グラフが* Cluster/Health * detailsページに表示されます。次の手順を実行します。

手順

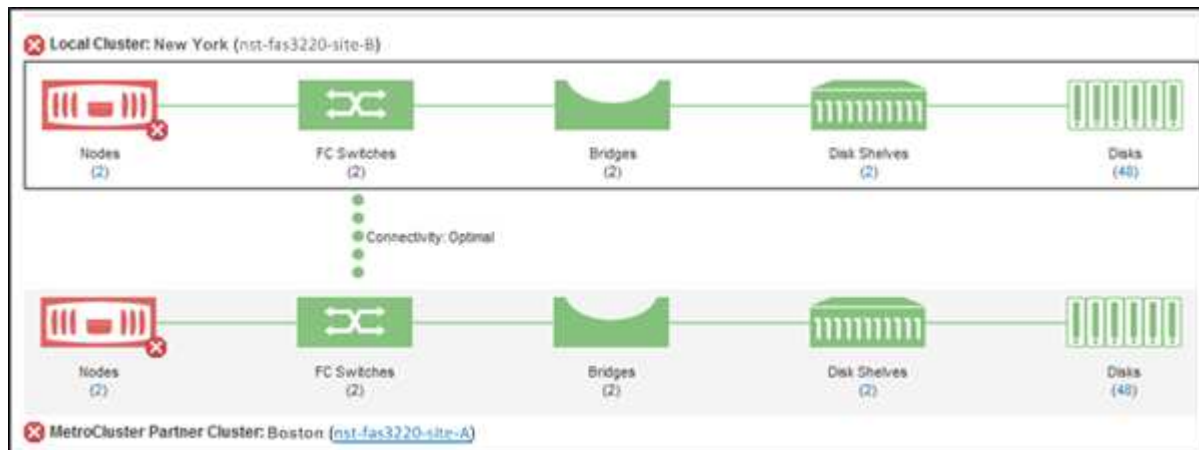
1. 左側のナビゲーションペインで、* Storage * > * Clusters * をクリックします。

監視対象であるすべてのクラスタのリストが表示されます。

2. Protection：MetroCluster *ビューで、MetroCluster over FC構成の詳細を表示するクラスタの名前をクリ

ックします。または、MetroCluster 構成のクラスタでフィルタすることもできます。

3. [* クラスタ / ヘルス * の詳細] ページで、[* MetroCluster 接続性 *] タブをクリックします。MetroCluster 接続*タブは、MetroCluster over FC構成でのみ使用できます。



対応するクラスタオブジェクト領域に、MetroCluster 構成のトポロジが表示されます。クラスタ / 健全性の詳細ページに表示される情報を基に、接続の問題を修正できます。たとえば、クラスタ内のノードとスイッチの間の接続が停止している場合は、次のアイコンが表示されます。



アイコンにカーソルを合わせると、生成されたイベントに関する詳細情報が表示されます。

MetroCluster 構成で接続の問題が見つかった場合は、System Manager にログインするか ONTAP CLI にアクセスして問題を解決する必要があります。

クラスタの健全性の判定の詳細については、を参照してください ["MetroCluster over FC構成でのクラスタの健全性を確認しています"](#)。

MetroCluster over IP構成で接続の問題を監視します

MetroCluster over IP構成のクラスタの場合は、接続グラフが*クラスタ*ページに表示されます。次の手順を実行します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Clusters * をクリックします。

監視対象であるすべてのクラスタのリストが表示されます。

2. Protection : MetroClusters *ビューで、MetroCluster over IP構成の詳細を表示するクラスタの名前をクリックします。または、MetroCluster 構成のクラスタでフィルタすることもできます。
3. キャレットをクリックして行を展開します v をクリックします。MetroCluster over IP構成で保護されているクラスタにのみ、キャレットアイコンが表示されます。

ソースサイトとミラーサイトのトポロジ、および接続に使用されているメディアエーターを表示することができます。次の情報を表示できます。

- サイト間の接続

- 両方のサイトに健全性と可用性の問題がある場合は、それらに問題があります
- メディエーター関連の問題
- レプリケーションに関連する問題。



ステータスは、Critical (❌)、エラー (⚠️)、または標準 (✅)。同じトポロジ内のプライマリデータとミラーデータのアグリゲートデータレプリケーションステータスも確認できます。

次の図では、ソースクラスタとデスティネーションクラスタ間のサイト間接続が利用できず、クラスタ間のメディエーターが設定されていないことを確認できます。



- ステータスアイコンをクリックします。エラー定義を含むメッセージが表示されます。MetroCluster over IP構成で問題のイベントが発生した場合は、メッセージの*イベントの表示*ボタンをクリックしてイベントの詳細を確認できます。問題とイベントを解決すると、このトポロジのステータスアイコンは正常な状態に変わります (✅)。
- さらに詳しい設定情報は、クラスタ/ヘルス*の詳細ページの*構成*タブにある* MetroCluster の概要*および*保護*のセクションで確認できます。



MetroCluster over IP構成の場合にのみ、クラスタトポロジを*クラスタ*ページで表示できます。MetroCluster over FC構成のクラスタの場合、クラスタ/健全性*の詳細ページの* MetroCluster Connectivity *タブにトポロジが表示されます。

- 関連情報 *
- ["クラスタ / 健全性の詳細ページ"](#)
- Relationship : metrocluster *ビューの詳細については、を参照してください ["MetroCluster 構成を監視しています"](#)。
- 「* Relationship : Last 1 Month Transfer Status *」 ビューの詳細については、を参照してください ["関係 : 過去 1 カ月の転送ステータス画面"](#)。
- 「* Relationship : Last 1 Month Transfer Rate *」 ビューの詳細については、を参照してください ["関係 : 過去 1 カ月の転送速度ビュー"](#)。

- 「* Relationship : All Relationships *」ビューの詳細については、を参照してください ["関係：すべての関係ビュー"](#)。

MetroCluster レプリケーションを監視しています

データのミラーリング中に論理接続の全体的な健全性を監視して診断することができます。アグリゲート、ノード、Storage Virtual Machine などのクラスタコンポーネントのミラーリングを中断する問題やリスクを特定することができます。

Unified Manager では、システムヘルスアラートを使用して、MetroCluster 構成のコンポーネントおよび接続のステータスを監視します。

- 必要なもの *

MetroCluster 構成のローカルクラスタとリモートクラスタの両方を、Unified Manager に追加する必要があります

MetroCluster over IP構成のレプリケーションの表示

MetroCluster over IP構成の場合は、左側のナビゲーションペインの次のビューから、MetroCluster over IPで保護されたクラスタのトポロジレビュービューにデータレプリケーションステータスが表示されます。

- ストレージ>*クラスタ*>*保護：MetroCluster *ビュー
- 保護>*関係*>*関係：MetroCluster *ビュー

詳細については、を参照してください ["MetroCluster over IPで接続の問題を監視します"](#)。

MetroCluster over FC構成のレプリケーションの表示

以下の手順に従って、MetroCluster over FC構成のデータレプリケーションの問題を特定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Clusters * をクリックします。

監視対象のクラスタのリストが表示されます。

2. [* Health: All Clusters]ビューで、MetroCluster レプリケーションの詳細を表示するクラスタの名前をクリックします。[クラスタ/ヘルスの詳細]ページで、[* MetroCluster レプリケーション*]タブをクリックします。

対応するクラスタオブジェクト領域のローカルサイトに、レプリケートされる MetroCluster 設定のトポロジが、データのミラー先であるリモートサイトの情報とともに表示されます。アイコンにカーソルを合わせると、生成されたイベントに関する詳細情報が表示されます。

レプリケーションの問題を修正するには、クラスタ / 健全性の詳細ページに表示される情報を使用します。MetroCluster 構成でミラーリングの問題が見つかった場合は、System Manager にログインするか ONTAP CLI にアクセスして問題を解決する必要があります。

- 関連情報 *

["クラスタ / 健全性の詳細ページ"](#)

クォータの管理

ユーザクォータとグループクォータを使用して、ユーザまたはユーザグループが使用できるディスクスペースの量やファイルの数を制限できます。ディスクやファイルの使用量、ディスクに設定されている各種の制限など、ユーザクォータとユーザグループクォータの情報を表示できます。

クォータ制限とは

ユーザクォータ制限とは、ユーザのスペース使用量がそのユーザのクォータで設定されている制限値に近づいているかどうか、または到達したかどうかを評価するために Unified Manager サーバで使用される値です。ソフトリミットを超えた場合や、ハードリミットに達した場合は、Unified Manager サーバでユーザクォータイベントが生成されます。

デフォルトでは、Unified Manager サーバは、クォータのソフトリミットを超えたユーザまたはクォータのハードリミットに達したユーザ、およびユーザクォータイベントが設定されているユーザに通知 E メールを送信します。アプリケーション管理者ロールのユーザは、指定した受信者にユーザクォータイベントまたはユーザグループクォータイベントを通知するアラートを設定できます。

ONTAP System Manager または ONTAP CLI を使用してクォータ制限を指定できます。

ユーザクォータとユーザグループクォータの表示

Storage VM / Health の詳細ページには、SVM で設定されているユーザクォータとユーザグループクォータに関する情報が表示されます。ユーザまたはユーザグループの名前、ディスクとファイルに設定されている制限、ディスクとファイルの使用済みスペース、および通知用の E メールアドレスを確認できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* Storage * > * Storage VM* をクリックします。
2. [* 健全性：すべての Storage VM] ビューで、Storage VM を選択し、[* ユーザクォータとグループクォータ *] タブをクリックします。

- 関連情報 *

["ユーザを追加する"](#)

E メールアドレスを生成するルールを作成しています

クラスタ、Storage Virtual Machine (SVM)、ボリューム、qtree、ユーザ、またはユーザグループに関連付けられたユーザクォータに基づいて、E メールアドレスを指定するルールを作成できます。クォータに違反が発生すると、指定した E メールアドレス

に通知が送信されます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- [Rules to Generate User and Group Quota Email Address] ページのガイドラインを確認しておく必要があります。

クォータの E メールアドレスのルールを定義して、実行順にそれらを入力する必要があります。たとえば、qtree1 でのクォータ違反に関する通知を E メールアドレス「qtree1@xyz.com」で受信し、それ以外の qtree については E メールアドレス「admin@xyz.com」を使用する場合は、次の順序でルールを指定する必要があります。

- if (\$qtree='qtree1') then qtree1@xyz.com
- if (\$qtree== *) then admin@xyz.com

指定したルールの条件がどれも満たされていない場合は、デフォルトのルールが使用されます。

```
if ( $user_or_group=* ) then $user_or_group@$domain
```

手順

1. 左側のナビゲーションペインで、 * General * > * Quota Email Rules * をクリックします。
2. 条件に基づいてルールを入力します。
3. [*Validate] をクリックして、ルールの構文を検証します。

ルールの構文が正しくない場合は、エラーメッセージが表示されます。構文を修正して、もう一度 * 検証 * をクリックする必要があります。

4. [保存 (Save)] をクリックします。
5. 作成した E メールアドレスが Storage * VM / Health * details ページの * User and Group Quotas * タブに表示されていることを確認します。

ユーザクォータとユーザグループクォータの E メール通知形式の作成

クォータ関連の問題がある場合（ソフトリミットを超えた場合、またはハードリミットに達した場合）にユーザまたはユーザグループに送信する E メール通知の形式を作成できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、 * General * > * Quota Email Format * をクリックします。
2. [* 差出人 *]、[* 件名 *]、および [* 電子メールの詳細 *] フィールドに詳細を入力または変更します。
3. 電子メール通知をプレビューするには、[* プレビュー] をクリックします。
4. [閉じる (Close)] をクリックしてプレビューウィンドウを閉じます。

5. 必要に応じて、E メール通知の内容を変更します。

6. [保存 (Save)] をクリックします。

ユーザクォータおよびグループクォータの E メールアドレスの編集

クラスタ、Storage Virtual Machine (SVM)、ボリューム、qtree、ユーザ、またはユーザグループに関連付けられたユーザクォータに基づいて、E メールアドレスを変更することができます。[ユーザクォータおよびグループクォータの E メールアドレスを生成するルール] ダイアログボックスで指定したルールによって生成された E メールアドレスを上書きする場合は、E メールアドレスを変更できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- を確認しておく必要があります ["ルールの作成に関するガイドライン"](#)。

E メールアドレスを編集すると、ユーザクォータおよびグループクォータの E メールアドレスを生成するルールがクォータに適用されなくなります。指定したルールに従って生成された E メールアドレスに通知を送信するには、E メールアドレスを削除して変更を保存する必要があります。

手順

1. 左側のナビゲーションペインで、* Storage * > * SVMs * をクリックします。
2. * Health : All Storage VMs] ビューで SVM を選択し、* User クォータと Group Quotas * タブをクリックします。
3. タブの行の下にある * 電子メールアドレスの編集 * をクリックします。
4. [電子メールアドレスの編集 *] ダイアログボックスで、適切なアクションを実行します。

状況	作業
指定したルールに従って生成された E メールアドレスに通知を送信する	<ol style="list-style-type: none">a. [Email Address] フィールドの電子メールアドレスを削除します。b. [保存 (Save)] をクリックします。c. F5 キーを押して E メールアドレスの編集ダイアログボックスをリロードし、ブラウザをリフレッシュします。指定したルールによって生成された E メールアドレスが [* E メールアドレス *] フィールドに表示されます。
指定した E メールアドレスに通知を送信する	<ol style="list-style-type: none">a. [Email Address] フィールドで電子メールアドレスを変更します。b. [保存 (Save)] をクリックします。ユーザクォータおよびグループクォータの E メールアドレスを生成するルールがクォータに適用されなくなります。

クォータに関する詳細情報

クォータに関する概念を理解しておく、ユーザクォータとユーザグループクォータを効率的に管理できるようになります。

クォータプロセスの概要

クォータには、ソフトクォータとハードクォータがあります。ソフトクォータ原因 ONTAP では、指定された制限を超過すると通知が送信されますが、ハードクォータでは、指定された制限を超過すると書き込み処理が失敗します。

ONTAP は、FlexVol ボリュームへの書き込み要求をユーザまたはユーザグループから受信すると、そのボリュームでユーザまたはユーザグループに対してクォータがアクティブ化されているかどうかをチェックし、次の点を判断します。

- ハードリミットに到達するかどうか

「はい」の場合は、ハードリミットに達したときに書き込み処理が失敗し、ハードクォータ通知が送信されます。

- ソフトリミットを超過するかどうか

「はい」の場合は、ソフトリミットを超えても書き込み処理が成功し、ソフトクォータ通知が送信されます。

- 書き込み処理でソフトリミットを超えないかどうか

「はい」の場合は、書き込み処理が成功し、通知は送信されません。

クォータについて

クォータを使用すると、ユーザ、グループ、または qtree によって使用されるディスクスペースやファイル数を制限したり、追跡したりできます。クォータは、を使用して指定します `/etc/quotas` ファイル。クォータは、特定のボリュームまたは qtree に適用されます。

クォータの使用目的

クォータは、FlexVol ボリュームのリソース使用量を制限したり、リソース使用量が特定のレベルに達したときに通知したり、リソース使用量を追跡したりするために使用できます。

クォータを指定する理由は次のとおりです。

- ユーザやグループが使用できる、または qtree に格納できる、ディスクスペースの容量やファイル数を制限する場合
- 制限を適用せずに、ユーザ、グループ、または qtree によって使用されるディスクスペースの容量やファイル数を追跡する場合

- ディスク使用率やファイル使用率が高いときにユーザに警告する場合

クォータの概要ダイアログボックス

Health : All Storage VMs ビューの User and Group Quotas タブで適切なオプションを使用して、クォータ関連の問題が発生したときに送信される E メール通知の形式を設定したり、ユーザクォータに基づいて E メールアドレスを指定するルールを設定したりできます。

Email Notification Format ページ

[電子メール通知形式] ページには、クォータ関連の問題が存在するときにユーザーまたはユーザーグループに送信される電子メールのルールが表示されます (ソフトリミットを超過しているか、ハードリミットに達しています)。

E メール通知は、次のユーザまたはユーザグループのクォータイベントが生成された場合にのみ送信されます。ユーザクォータまたはグループクォータのディスクスペースがソフトリミットを超過、ユーザクォータまたはグループクォータのファイル数がソフトリミットを超過、ユーザクォータまたはグループクォータのディスクスペースがハードリミットに達した、またはユーザクォータまたはグループクォータのファイル数がハードリミットを超過しました。

• * から *

Eメールの送信元の E メールアドレスが表示されます。このアドレスは変更が可能です。デフォルトでは、これは、指定された通知ページの電子メールアドレスです。

• * 件名 *

通知メールの件名が表示されます。

• * 電子メールの詳細 *

通知 Eメールのテキストが表示されます。テキストは要件に基づいて変更できます。たとえば、クォータ属性に関する情報を指定して、キーワードの数を減らすことができます。ただし、キーワードは変更しないでください。

有効なキーワードは次のとおりです。

◦ \$event_name

E メール通知の原因となったイベントの名前を示します。

◦ \$QUOTA_TARGET

クォータが適用される qtree またはボリュームを示します。

◦ \$QUOTA_OF_Used% です

ディスクのハードリミット、ディスクのソフトリミット、ファイルのハードリミット、またはファイルのソフトリミットについて、ユーザまたはユーザグループが使用している割合を示します。

- \$QUOTA_limit です

ユーザまたはユーザグループがリミットに達して次のいずれかのイベントが生成されたディスクのハードリミットまたはファイルのハードリミットを示します。

- ユーザクォータまたはグループクォータのディスクスペースがハードリミットに達しました
- ユーザクォータまたはグループクォータのディスクスペースがソフトリミットに達しました
- ユーザクォータまたはグループクォータのファイル数がハードリミットに達しました
- ユーザクォータまたはグループクォータのファイル数がソフトリミットに達しました

- \$QUOTA_Used の値

ユーザまたはユーザグループが使用しているディスクスペースと作成したファイルの数を示します。

- \$QUOTA_USER を選択してください

ユーザまたはユーザグループの名前を示します。

コマンドボタン

各コマンドボタンを使用して、E メール通知の形式に対する変更内容をプレビュー、保存、キャンセルできます。

- * プレビュー *

通知メールのプレビューが表示されます。

- * 工場出荷時のデフォルトに戻します *

通知の形式を工場出荷時のデフォルトに戻すことができます。

- * 保存 *

通知の形式に対する変更内容を保存します。

RulestoGenerateUserandGroupQuotaEmailAddress ヘエシ

Rules to Generate User and Group Quota Email Address ページでは、クラスタ、SVM、ボリューム、qtree、ユーザに関連付けられたユーザクォータに基づいて E メールアドレスを指定するルールを作成できます。またはユーザグループを指定します。クォータに違反が発生すると、指定した E メールアドレスに通知が送信されます。

ルール領域

クォータの E メールアドレスに関するルールを定義する必要があります。ルールを説明するコメントを追加することもできます。

ルールを定義する方法

ルールは実行する順序で入力する必要があります。最初のルールの条件が満たされると、このルールに基づいて E メールアドレスが生成されます。条件が満たされていない場合は、次のルールの条件が考慮されます。行ごとに個別のルールがリストされます。デフォルトのルールはリストの最後のルールです。ルールの優先順位は変更できます。ただし、デフォルトルールの順序は変更できません。

たとえば、qtree1 でのクォータ違反に関する通知を E メールアドレス「qtree1@xyz.com」で受信し、それ以外の qtree については E メールアドレス「admin@xyz.com」を使用する場合は、次の順序でルールを指定する必要があります。

- if (\$qtree='qtree1') then qtree1@xyz.com
- if (\$qtree== *) then admin@xyz.com

指定したルールの条件がどれも満たされていない場合は、デフォルトのルールが使用されます。

```
if ( $user_or_group=* ) then $user_or_group@$domain
```

複数のユーザが同じクォータを使用する場合は、ユーザの名前がカンマで区切って表示され、そのクォータにはルールが適用されません。

コメントを追加する方法

ルールを説明するコメントを追加できます。各コメントの先頭に # を付け、1 行に 1 つずつコメントがリストされるようにしてください。

ルールの構文

ルールの構文には、次のいずれかを使用する必要があります。

- if (valid variableoperator *) をクリックします email ID@domain name

if はキーワードであり、小文字で記述します。演算子は = です。E メール ID には、任意の文字、有効な変数 \$user_or_group、\$user、または \$group、あるいは任意の文字と有効な変数 \$user_or_group、\$user、または \$group の組み合わせを含めることができます。ドメイン名には、任意の文字、有効な変数 \$DOMAIN、または任意の文字と有効な変数 \$DOMAIN の組み合わせを使用できます。有効な変数は大文字と小文字のどちらでもかまいませんが、両方を組み合わせることはできません。たとえば、\$domain と \$domain は有効ですが、\$Domain は有効な変数ではありません。

- if (valid variableoperator `string`) をクリックします email ID@domain name

if はキーワードであり、小文字で記述します。operator には、contains または == を指定できます。E メール ID には、任意の文字、有効な変数 \$user_or_group、\$user、または \$group、あるいは任意の文字と有効な変数 \$user_or_group、\$user、または \$group の組み合わせを含めることができます。ドメイン名には、任意の文字、有効な変数 \$DOMAIN、または任意の文字と有効な変数 \$DOMAIN の組み合わせを使用できます。有効な変数は大文字と小文字のどちらでもかまいませんが、両方を組み合わせることはできません。たとえば、\$domain と \$domain は有効ですが、\$Domain は有効な変数ではありません。

コマンドボタン

コマンドボタンを使用して、作成したルールを保存、検証、またはキャンセルできます。

• * 検証 *

作成したルールの構文を検証します。検証でエラーが発生した場合は、エラーを生成するルールがエラーメッセージとともに表示されます。

• * 工場出荷時のデフォルトに戻します *

アドレスルールを工場出荷時のデフォルト値に戻すことができます。

• * 保存 *

ルールの構文を検証し、エラーがない場合はルールを保存します。検証でエラーが発生した場合は、エラーを生成するルールがエラーメッセージとともに表示されます。

トラブルシューティング

トラブルシューティング情報は、Unified Manager の使用時に発生する問題を特定し、解決する上で役立ちます。

Unified Manager データベースディレクトリにディスクスペースを追加しています

Unified Manager データベースディレクトリには、ONTAP システムから収集された健全性とパフォーマンスのデータがすべて含まれています。状況によっては、データベースディレクトリのサイズの拡張が必要になることがあります。

たとえば、Unified Manager で多数のクラスタからデータを収集している場合、各クラスタに多数のノードがあると、データベースディレクトリがいっぱいになることがあります。データベースディレクトリの使用率が 90% の場合は警告イベントが生成され、ディレクトリの使用率が 95% の場合は重大イベントが生成されます。



ディレクトリの使用率が 95% に達すると、クラスタから追加のデータが収集されなくなります。

データディレクトリの容量を追加する手順は、Unified Manager を VMware ESXi サーバ、Red Hat Linux サーバまたは CentOS Linux サーバ、Microsoft Windows サーバのいずれで実行しているかによって異なります。

VMware 仮想マシンのデータディスクにスペースを追加しています

Unified Manager データベースのデータディスクのスペースを増やす必要がある場合は、インストール後に Unified Manager のメンテナンスコンソールを使用してディスクスペースを増やして容量を追加できます。

• 必要なもの *

- vSphere Client へのアクセス権が必要です。
- 仮想マシンにスナップショットがローカルに格納されていないことが必要です。
- メンテナンスユーザのクレデンシャルが必要です。

仮想ディスクのサイズを拡張する前に仮想マシンをバックアップすることをお勧めします。

手順

1. vSphere Clientで、Unified Manager仮想マシンを選択し、データにディスク容量を追加します disk 3。
詳細については、VMware のドキュメントを参照してください。

Unified Manager の導入で、「ハードディスク 3」ではなく「ハードディスク 2」が使用されることがあります。これが導入環境で発生した場合は、ディスクのサイズを大きくします。データディスクには、常に他のディスクよりも多くの容量があります。

2. vSphere Client で、Unified Manager 仮想マシンを選択し、* Console * タブを選択します。
3. コンソールウィンドウ内をクリックし、ユーザ名とパスワードを使用してメンテナンスコンソールにログインします。
4. * メインメニュー * で、* システム構成 * オプションの番号を入力します。
5. システム構成メニュー * で、[データディスクサイズの増加] オプションの数値を入力します。

Linux ホストのデータディレクトリにスペースを追加しています

に十分なディスクスペースを割り当てていない場合 /opt/netapp/data Unified Managerをサポートするディレクトリ：Linuxホストを最初にセットアップしたあとにUnified Managerをインストールしたときに、のディスクスペースを増やしてインストール後にディスクスペースを追加できます /opt/netapp/data ディレクトリ。

- 必要なもの *

Unified Manager がインストールされている Red Hat Enterprise Linux マシンまたは CentOS Linux マシンへの root ユーザアクセスが必要です。

データディレクトリのサイズを拡張する前に Unified Manager データベースをバックアップすることを推奨します。

手順

1. ディスクスペースを追加する Linux マシンに root ユーザとしてログインします。
2. Unified Manager サービスと関連する MySQL ソフトウェアを次の順序で停止します。systemctl stop ocieau ocie mysqld
3. 一時バックアップフォルダを作成する（例： /backup-data）には、現在のデータを格納できるだけの十分なディスクスペースがあります /opt/netapp/data ディレクトリ。
4. 既存のの内容と権限の設定をコピーします /opt/netapp/data ディレクトリをバックアップデータディレクトリに移動します。

```
cp -arp /opt/netapp/data/* /backup-data
```

5. SE Linux が有効になっている場合：

- a. 既存のフォルダのSE Linuxタイプを取得します /opt/netapp/data フォルダ：

```
se_type=`ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1`
```

次のような情報が返されます。

```
echo $se_type  
mysqlld_db_t
```

- a. を実行します `chcon` バックアップディレクトリに対してSE Linuxタイプを設定するコマンドは、次のとおりです。

```
chcon -R --type=mysqlld_db_t /backup-data
```

6. の内容を削除します `/opt/netapp/data` ディレクトリ：

- a. `cd /opt/netapp/data`
- b. `rm -rf *`

7. のサイズを展開します `/opt/netapp/data` LVMのコマンドを使用するかディスクを追加して、ディレクトリのサイズを150GB以上にします。



を作成した場合は `/opt/netapp/data` ディスクからはマウントしないでください `/opt/netapp/data` NFS共有またはCIFS共有として設定する。このため、ディスクスペースを拡張しようとする、などの一部のLVMコマンドが実行されます `resize` および `extend` 期待どおりに動作しない可能性があります。

8. を確認します `/opt/netapp/data` ディレクトリの所有者（mysql）とグループ（root）は変更されません。

```
ls -ltr /opt/netapp/ | grep data
```

次のような情報が返されます。

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. SE Linuxが有効になっている場合は、のコンテキストを確認します `/opt/netapp/data` ディレクトリが `mysqlld_db_t` に設定されたままである

- a. `touch /opt/netapp/data/abc`
- b. `ls -Z /opt/netapp/data/abc`

次のような情報が返されます。

```
-rw-r--r--. root root unconfined_u:object_r:mysqlld_db_t:s0  
/opt/netapp/data/abc
```

10. ファイルを削除します `abc` この無駄なファイルによって、将来データベースエラーが原因 されなくなります。

11. から内容をコピーします `backup-data` 展開したに戻ります `/opt/netapp/data` ディレクトリ：


```
cp -arp /backup-data/* /opt/netapp/data/
```

12. SE Linux が有効になっている場合は、次のコマンドを実行します。

```
chcon -R --type=mysqlld_db_t /opt/netapp/data
```

13. MySQL サービスを開始します。

```
systemctl start mysqld
```

14. MySQL サービスが開始されたら、ocie サービスと ocieau サービスを次の順序で開始します。

```
systemctl start ocie ocieau
```

15. すべてのサービスが開始されたら、バックアップフォルダを削除します /backup-data :

```
rm -rf /backup-data
```

Microsoft Windows サーバの論理ドライブにスペースを追加する

Unified Manager データベースのディスクスペースを増やす必要がある場合は、Unified Manager がインストールされている論理ドライブに容量を追加できます。

- 必要なもの *

Windows の管理者権限が必要です。

ディスクスペースを追加する前に Unified Manager データベースをバックアップすることを推奨します。

手順

1. ディスクスペースを追加する Windows サーバに管理者としてログインします。
2. スペースを追加する方法に応じて、該当する手順を実行します。

オプション	説明
物理サーバで、Unified Manager server がインストールされている論理ドライブに容量を追加する。	Microsoft の次のトピックの手順に従います。 "基本ボリュームを拡張します"
物理サーバで、ハードディスクドライブを追加します。	Microsoft の次のトピックの手順に従います。 "ハードディスクドライブの追加"
仮想マシンで、ディスクパーティションのサイズを拡張します。	VMware の次のトピックの手順に従います。 "ディスクパーティションのサイズを拡張する"

パフォーマンス統計データの収集間隔を変更する

パフォーマンス統計のデフォルトの収集間隔は 5 分です。大規模なクラスタからの収集がデフォルトの時間内に完了しない場合は、この間隔を 10 分または 15 分に変更できます。この設定は、この Unified Manager インスタンスで監視しているすべてのクラスタからの統計の収集に適用されます。

- 必要なもの *

Unified Manager サーバのメンテナンスコンソールへのログインが許可されているユーザ ID とパスワードが必要です。

パフォーマンス統計の収集が時間内に完了しなかった問題は、バナーメッセージで示されます `Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster <cluster_name>.`

収集間隔の変更が必要になるのは、統計の収集が問題のためです。その他の理由でこの設定を変更しないでください。



この値をデフォルト設定の 5 分から変更すると、Unified Manager でレポートされるパフォーマンスイベントの数や頻度に影響する可能性があります。たとえば、システム定義のパフォーマンスしきい値ポリシーでは、ポリシーを超えた状態が 30 分続くとイベントがトリガーされます。収集間隔が 5 分の場合は、収集間隔が 6 回連続でポリシーの違反となるようにする必要があります。一方、収集間隔が 15 分の場合は、2 回の収集期間のみでポリシーの違反と判断されます。

クラスタセットアップページの下部にあるメッセージは、現在の統計データの収集間隔を示します。

手順

1. SSH を使用して、Unified Manager ホストにメンテナンスユーザとしてログインします。

Unified Manager メンテナンスコンソールのプロンプトが表示されます。

2. 「パフォーマンスポーリング間隔の設定 *」というラベルの付いたメニューオプションの番号を入力し、Enter キーを押します。
3. プロンプトが表示されたら、メンテナンスユーザのパスワードをもう一度入力します。
4. 設定する新しいポーリング間隔の値を入力し、Enter キーを押します。

外部データプロバイダ（Graphite など）への接続を現在設定してある場合は、Unified Manager の収集間隔を 10 分または 15 分に変更したあと、データプロバイダの送信間隔も Unified Manager の収集間隔以上に変更する必要があります。

Unified Manager でイベントデータおよびパフォーマンスデータを保持する期間の変更

Unified Manager には、すべての監視対象クラスタのイベントデータとパフォーマンスデータが 6 カ月間、デフォルトで格納されます。この期間を過ぎると、新しいデータ用のスペースを確保するために古いデータが自動的に削除されます。このデフォルトの期間はほとんどの構成に対して有効ですが、多数のクラスタとノードを含む非常に大規模な構成では、Unified Manager が最適に動作するように保持期間を短縮しなければならな

場合があります。

- 必要なもの *

アプリケーション管理者のロールが必要です。

この 2 種類のデータの保持期間は、Data Retention ページで変更できます。これらの設定は、Unified Manager インスタンスで監視しているすべてのクラスタからのデータの保持に適用されます。



Unified Manager はパフォーマンス統計を 5 分ごとに収集します。毎日、5 分単位の統計が 1 時間単位のパフォーマンス統計に集計されます。5 分ごとのパフォーマンスデータの履歴は 30 日分、1 時間ごとの集計パフォーマンスデータは 6 カ月間保持されます（デフォルト）。

保持期間を短くする必要があるのは、スペースが不足している場合や、バックアップやその他の処理の完了に時間がかかる場合のみです。保持期間を短くした場合の動作は次のとおりです。

- 古いパフォーマンスデータは、午前 0 時を過ぎた時点で Unified Manager データベースから削除されます。
- 古いイベントデータはただちに Unified Manager データベースから削除されます。
- 保持期間の前に発生したイベントはユーザインターフェイスに表示できなくなります。
- 保持期間の前のデータについては、1 時間ごとのパフォーマンス統計が表示される場所には何も表示されません。
- イベントの保持期間がパフォーマンスデータの保持期間より長い場合、古いパフォーマンスイベントには関連するグラフに対応するデータが表示されない可能性があることを示すメッセージがパフォーマンススライダの警告の下に表示されます。

手順

1. 左側のナビゲーションペインで、* ポリシー * > * データ保持 * をクリックします。
2. [* データ保持期間 *] ページで、[イベント保持期間] または [パフォーマンスデータ保持期間] 領域のスライダツールを選択し、データを保持する月数に移動して、[* 保存] をクリックします。

不明な認証エラーです

リモートユーザまたはリモートグループの追加、編集、削除、テストなどの認証に関連する処理を実行すると、次のエラーメッセージが表示される場合があります。 Unknown authentication error.

- 原因 *

この問題は、次のオプションに誤った値を設定した場合に発生することがあります。

- Active Directory 認証サービスの管理者名
- OpenLDAP 認証サービスのバインド識別名
- 是正措置 *

1. 左側のナビゲーションペインで、* 一般 * > * リモート認証 * をクリックします。
2. 選択した認証サービスに基づいて、管理者名またはバインド識別名に適切な情報を入力します。

3. [認証のテスト *] をクリックして、指定した詳細で認証をテストします。

4. [保存 (Save)] をクリックします。

ユーザが見つかりません

リモートユーザまたはリモートグループの追加、編集、削除、テストなどの認証に関連する処理を実行すると、次のエラーメッセージが表示されます。 User not found.

• 原因 *

この問題は、ユーザが AD サーバまたは LDAP サーバに存在し、ベース識別名の値が正しく設定されていない場合に発生する可能性があります。

• 是正措置 *

1. 左側のナビゲーションペインで、 * 一般 * > * リモート認証 * をクリックします。
2. ベース識別名に適切な情報を入力します。
3. [保存 (Save)] をクリックします。

問題で他の認証サービスを使用して **LDAP** を追加

認証サービスとして [その他] を選択すると、ユーザーおよびグループのオブジェクトクラスには、以前に選択したテンプレートの値が保持されます。LDAP サーバが同じ値を使用していないと、処理が失敗することがあります。

• 原因 *

OpenLDAP でユーザが正しく設定されていません。

• 是正措置 *

この問題は、次のいずれかの対処方法によって手動で修正できます。

LDAP のユーザオブジェクトクラスとグループオブジェクトクラスがそれぞれ user と group である場合は、次の手順を実行します。

1. 左側のナビゲーションペインで、 [一般 > リモート認証 *] をクリックします。
2. [* 認証サービス] ドロップダウンメニューで、 [Active Directory*] を選択し、 [* その他 *] を選択します。
3. テキストフィールドに入力します。

LDAP のユーザオブジェクトクラスとグループオブジェクトクラスがそれぞれ posixAccount と posixGroup である場合は、次の手順を実行します。

1. 左側のナビゲーションペインで、 [一般 > リモート認証 *] をクリックします。
2. [* Authentication Service*] ドロップダウンメニューで [* OpenLDAP *] を選択し、 [* Others *] を選択します。
3. テキストフィールドに入力します。

最初の2つの回避策が適用されない場合は、を呼び出します option-set APIを使用してを設定します
auth.ldap.userObjectClass および auth.ldap.groupObjectClass 正しい値を指定します。

イベントとアラートの管理

イベントの管理

イベントによって、監視対象のクラスタ内の問題を特定できます。

Active IQ プラットフォームイベントとは

Unified Manager では、Active IQ プラットフォームで検出されたイベントを表示できます。イベントは、Unified Manager で監視しているすべてのストレージシステムから生成された AutoSupport メッセージに対して一連のルールを実行することで作成されます。

詳細については、を参照してください ["Active IQ プラットフォームイベントの生成方法"](#)。

Unified Manager は新しいルールファイルの有無を自動的にチェックし、ある場合にのみ新しいファイルをダウンロードします。外部ネットワークへのアクセスがないサイトでは、* Storage Management * > * Event Setup * > * Upload Rules * からルールを手動でアップロードする必要があります。

これらの Active IQ イベントは既存の Unified Manager イベントと重複しないため、システム構成、ケーブル配線、ベストプラクティス、可用性の問題に関するインシデントやリスクを特定します。

プラットフォームイベントの有効化の詳細については、を参照してください ["Active IQ ポータルイベントの有効化"](#)。ルールファイルのアップロードの詳細については、を参照してください ["新しい Active IQ ルールファイルをアップロードしています"](#)。

NetApp Active IQ は、ネットアップのハイブリッドクラウド全体にわたってストレージシステムの運用を最適化するのに役立つ、予測分析とプロアクティブなサポートを提供するクラウドベースのサービスです。を参照してください ["NetApp Active IQ の略"](#) を参照してください。

イベント管理システムイベントとは

Event Management System（EMS；イベント管理システム）は、ONTAP カーネルのさまざまな部分からイベントデータを収集し、イベント転送のメカニズムを提供します。Unified Manager では、このような ONTAP イベントを EMS イベントとして報告できます。一元化された監視と管理により、重大な EMS イベントとそれらの EMS イベントに基づくアラート通知を簡単に設定することができます。

Unified Manager にクラスタを追加すると、Unified Manager のアドレスが通知の送信先としてクラスタに追加されます。クラスタでイベントが発生するとすぐに EMS イベントが報告されます。

Unified Manager で EMS イベントを受け取る方法は 2 つあります。

- 一定数の重要な EMS イベントは自動的に報告されます。
- EMS イベントを受け取るように個別に登録することができます。

Unified Manager で生成される EMS イベントの報告方法は、イベントが生成された方法によって異なります。

機能性	自動の EMS メッセージ	登録した EMS メッセージ
使用可能な EMS イベント	一部の EMS イベント	すべての EMS イベント
EMS メッセージがトリガーされたときの名前	Unified Manager のイベント名（EMS のイベント名から変換）	固有でないエラーの EMS を受信しました。詳細なメッセージに実際の EMS イベントをドット表記の形式で記載します
メッセージを受信しました	クラスタが検出されるとすぐに検出されます	必要な各 EMS イベントが Unified Manager に追加されたあと、15 分間隔の次のポーリング時
イベントのライフサイクル	Unified Manager の他のイベントと同じで、「新規」、「確認済み」、「解決済み」、「廃止」の状態があります	クラスタを更新したあと、イベントが作成されてから 15 分後に EMS イベントが廃止されます
Unified Manager が停止しているときのイベントのキャプチャ	システムの起動時に各クラスタと通信して不足しているイベントを取得	いいえ
イベントの詳細	推奨される対処方法を ONTAP から直接インポートして、一貫した解決策を提示します	[イベントの詳細] ページで修正アクションを使用できません



新しい自動 EMS イベントには、過去のイベントが解決されたことを示す情報イベントも含まれます。たとえば、「FlexGroup constituents Space Status all ok」情報イベントは、「FlexGroup constituents have Space Issues」エラーイベントが解決されたことを示します。情報イベントは、他の重大度タイプのイベントと同じライフサイクルを使用して管理することはできませんが、同じボリュームが別の「スペースの問題」エラーイベントを受信した場合、イベントは自動的に廃止されます。

Unified Manager に自動的に追加される **EMS** イベント

次の ONTAP EMS イベントが Unified Manager に自動的に追加されます。これらのイベントは、Unified Manager が監視しているいずれかのクラスタでトリガーされると生成されます。

ONTAP 9.5 以降のソフトウェアを実行しているクラスタの監視では、次の EMS イベントを使用できます。

Unified Manager のイベント名	EMS のイベント名	影響を受けるリソース	Unified Manager の重大度
アグリゲートの再配置でクラウド階層へのアクセスが拒否されました	arl.netra.ca.check.failed	アグリゲート	エラー

Unified Manager のイベント名	EMS のイベント名	影響を受けるリソース	Unified Manager の重大度
ストレージフェイルオーバー時にアグリゲートの再配置でクラウド階層へのアクセスが拒否されました	gb.netra.ca.check.failed	アグリゲート	エラー
FabricPool ミラーレプリケーションの再同期が完了しました	wafl.ca.resync.complete	クラスタ	エラー
FabricPool スペースがほぼフルです	fabricpool.Nearly .full	クラスタ	エラー
NVME の猶予期間 - 開始されました	nvmf.graceperiod.start	クラスタ	警告
NVME の猶予期間 - アクティブ	nvmf.graceperiod.active	クラスタ	警告
NVME の猶予期間 - 終了	nvmf.graceperiod.expired	クラスタ	警告
LUN が破棄されました	lun.destroy	LUN	情報
Cloud AWS メタデータ接続エラー	Cloud.AWS- メタデータの接続に失敗しました	ノード	エラー
Cloud AWS IAM クレデンシャルが期限切れです	Cloud.AWs.iamCredsExpired	ノード	エラー
Cloud AWS IAM クレデンシャルが無効です	Cloud.AWs.iamCredsInvalid	ノード	エラー
Cloud AWS IAM クレデンシャルが見つからない	Cloud.AWs.iamCredsNotFound	ノード	エラー
Cloud AWS IAM クレデンシャルが初期化されていない	Cloud.AWS.iamNotInitialized	ノード	情報
Cloud AWS IAM ロールが無効です	Cloud.AWs.iamRoleInvalid	ノード	エラー
Cloud AWS IAM ロールが見つからない	Cloud.AWs.iamRoleNotFound	ノード	エラー

Unified Manager のイベント名	EMS のイベント名	影響を受けるリソース	Unified Manager の重大度
クラウド階層のホスト解決不可	objstor.host.unresolvable	ノード	エラー
クラウド階層のクラスター間 LIF が停止しています	objstore.interclusterlifDown	ノード	エラー
要求とクラウド階層シグネチャの不一致	OSC.signignatureMismatch	ノード	エラー
NFSv4 プールの 1 つを使い果たしました	Nblade.nfsV4PoolExhaust	ノード	重要
QoS 監視メモリの最大化	QoS 。 monitor.memory.maxed	ノード	エラー
QoS 監視メモリの縮小	QoS .monitor.memory.abated	ノード	情報
NVMe ネームスペースを破棄します	NVMeNS.destroy	ネームスペース	情報
NVMeNS Online	NVMe ネームスペースオンライン	ネームスペース	情報
NVMeNS はオフラインです	NVMe ネームスペースオンライン	ネームスペース	情報
NVMe ネームスペーススペース不足です	NVMe ネームスペース不足です。スペース不足です	ネームスペース	警告
同期レプリケーションが同期されていません	sms.status.out.out.out.sync	SnapMirror 関係	警告
同期レプリケーションがリストアされました	sms.status.in.sync	SnapMirror 関係	情報
同期レプリケーションの自動再同期に失敗しました	sms.resync.attempt 。失敗しました	SnapMirror 関係	エラー
多数の CIFS 接続	Nblade.cifsManyAths	SVM	エラー

Unified Manager のイベント名	EMS のイベント名	影響を受けるリソース	Unified Manager の重大度
最大 CIFS 接続数を超えました	Nblade.cifsMaxOpenSam eFile	SVM	エラー
ユーザあたりの最大 CIFS 接続数を超えました	Nblade.cifsMaxSessPerU srConn	SVM	エラー
CIFS NetBIOS 名が競合しています	Nblade.cifsNbNameConfl ict になっています	SVM	エラー
存在しない CIFS 共有に 対して試行します	Nblade.cifsNoPrivShare	SVM	重要
CIFS シャドウコピー処理 に失敗しました	cifs.shadowcopy.failure	SVM	エラー
AV サーバがウィルスを検 出しました	Nblad. vscanVirusDetected	SVM	エラー
ウィルススキャン用の AV サーバ接続がありません	Nbladen.vscanNoScanner Conn	SVM	重要
AV サーバが登録されてい ません	Nbladet.vscanNoRegdSc anner	SVM	エラー
応答する AV サーバ接続 がありません	Nbladet.vscanConnInactiv e	SVM	情報
AV サーバがビジーのため 新しいスキャン要求の受 け入れ不可	Nbladet.vscanConnBackP ressure です	SVM	エラー
権限のないユーザが AV サーバへのアクセスを試 みました	Nblad.vscanBadUserPriv Access	SVM	エラー
FlexGroup コンスティ チュエントのスペースに問 題あり	flexgroup コンスティ チュエント .have .spac確保 問題	ボリューム	エラー
FlexGroup コンスティ チュエントのスペースステ ータスはすべて正常です	flexgroup コンスティ チュエント。 spac確保。 status.all.ok	ボリューム	情報

Unified Manager のイベント名	EMS のイベント名	影響を受けるリソース	Unified Manager の重大度
FlexGroup 構成要素の inode に問題があります	flexgroup.constituents.hav e.inodes.issues	ボリューム	エラー
FlexGroup コンスティ チュエントの inode ステ ータスはすべて正常です	flexgroup.constituents.ino des.status.all.ok	ボリューム	情報
ボリューム論理スペース はほぼフルです	monitor.vol.nearFull.inc.sa v	ボリューム	警告
ボリューム論理スペース はフルです	monitor.vol.full.inc.sav	ボリューム	エラー
ボリューム論理スペース は正常な状態です	monitor.vol.one.ok.inc.sav	ボリューム	情報
WAFL ボリュームのオート サイズが失敗しました	wافل.vol.autoSize.fail	ボリューム	エラー
WAFL ボリュームのオート サイズ完了	wافل.vol.autoSize.done	ボリューム	情報
WAFL REaddir ファイル 処理タイムアウト	wافل.readdir.expired	ボリューム	エラー

ONTAP EMS イベントに登録する

ONTAP ソフトウェアがインストールされているシステムで生成された Event Management System (EMS ; イベント管理システム) イベントを受け取るように登録することができます。一部の EMS イベントは Unified Manager に自動的に報告されますが、それ以外の EMS イベントは登録している場合にのみ報告されます。

- 必要なもの *

Unified Manager にすでに自動的に追加されている EMS イベントには登録しないでください。同じ問題のイベントを 2 つ受信すると原因で混乱する可能性があります。

EMS イベントはいくつでも登録できます。登録したすべてのイベントが検証され、検証済みのイベントだけが Unified Manager で監視しているクラスタに適用されます。ONTAP 9 EMS イベントカタログ_ は、指定したバージョンの ONTAP 9 ソフトウェアのすべての EMS メッセージに関する詳細情報を提供します。該当するイベントの一覧については、ONTAP 9 製品ドキュメントページで該当するバージョンの _EMS イベントカタログを参照してください。

["ONTAP 9 製品ライブラリ"](#)

登録した ONTAP EMS イベントにアラートを設定したり、それらのイベントに対して実行するカスタムスクリプトを作成したりできます。



登録した ONTAP EMS イベントが届かない場合は、クラスタの DNS 設定が含まれている問題で、クラスタから Unified Manager サーバに到達できなくなっていることが考えられます。クラスタ管理者はこの問題を解決するために、クラスタの DNS 設定を修正してから Unified Manager を再起動する必要があります。これにより、保留中の EMS イベントが Unified Manager サーバにフラッシュされます。

手順

1. 左側のナビゲーションペインで、*** Storage Management *** > *** Event Setup *** をクリックします。
2. Event Setup ページで、*** Subscribe to EMS events *** ボタンをクリックします。
3. [EMS イベントのサブスクライブ (Subscribe to EMS events)] ダイアログボックスで、サブスクライブする ONTAP EMS イベントの名前を入力します。

登録可能な EMS イベントの名前を確認するには、ONTAP クラスタシェルで `event route show` コマンド (ONTAP 9 より前) または `event catalog show` コマンド (ONTAP 9 以降) を使用します。

["Active IQ Unified Manager で ONTAP EMS イベントサブスクリプションからアラートを設定して受信する方法"](#)

4. [追加 (Add)] をクリックします。

EMS イベントはサブスクライブされた EMS イベントのリストに追加されますが、該当する [To Cluster] 列には、追加した EMS イベントのステータスが「Unknown」と表示されます。

5. **Save and Close *** をクリックして、EMS イベントサブスクリプションをクラスタに登録します。
6. もう一度 **[* EMS イベントをサブスクライブ *]** をクリックします。

追加した EMS イベントの [Applicable to Cluster] 列には、ステータス「Yes」が表示されます。

ステータスが「はい」でない場合は、ONTAP EMS イベント名のスペルを確認します。入力した名前に間違いがある場合は、そのイベントを削除して追加し直す必要があります。

ONTAP の EMS イベントが発生すると、イベントが Events ページに表示されます。イベントを選択すると、EMS イベントに関する詳細をイベントの詳細ページで確認できます。イベントの処理を管理したり、イベントのアラートを作成したりすることもできます。

イベント受信時の動作

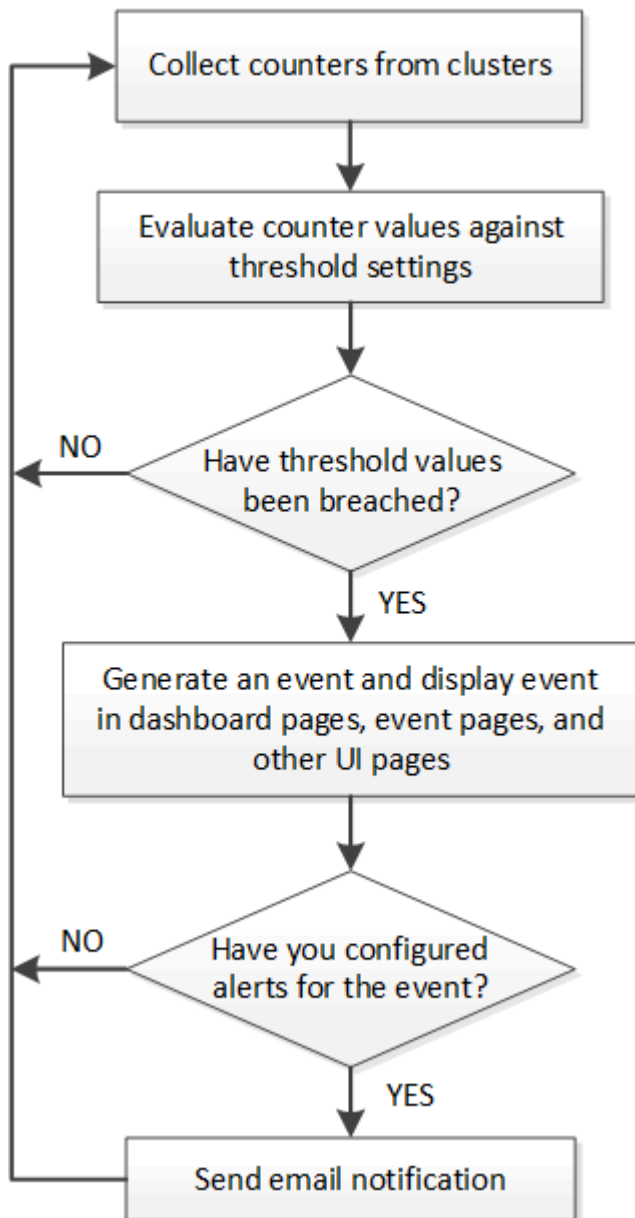
Unified Manager がイベントを受け取ると、ダッシュボードページ、イベント管理インベントリページ、クラスタ / パフォーマンスページの概要タブとエクスプローラタブ、およびオブジェクト固有のインベントリページ（ボリューム / 健全性インベントリページなど）に表示されます。

Unified Manager では、同じクラスタコンポーネントに対する同じ状況についての連続した複数のイベントを検出すると、それらのすべてのイベントを個別のイベントではなく 1 つのイベントとして扱います。イベントが継続している間は、そのイベントがまだアクティブであることを示すために期間が延びていきます。

Alert Setup ページでの設定に応じて、これらのイベントについて他のユーザに通知できます。アラートにより、次の処理が開始されます。

- イベントに関する E メールをすべての Unified Manager 管理者ユーザに送信できます。
- イベントを追加の E メール受信者に送信できます。
- SNMP トラップをトラップレシーバに送信できます。
- アクションを実行するカスタムスクリプトを実行できます。

このワークフローを次の図に示します。



イベントとイベントの詳細を表示する

Unified Manager がトリガーするイベントに関する詳細を表示して、そのイベントに対処することができます。たとえば、健全性イベントである「ボリュームはオフライン」が発生した場合は、そのイベントをクリックして詳細を表示し、対処方法を実行できま

す。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

イベントの詳細には、イベントのソース、イベントの原因、イベントに関連するメモなどの情報が含まれます。

手順

1. 左側のナビゲーションペインで、* イベント管理 * をクリックします。

デフォルトでは、すべてのアクティブなイベントのビューには、影響レベルがインシデントまたはリスクの過去 7 日間に生成された新規と確認済み（アクティブ）のイベントが表示されます。

2. 容量イベントやパフォーマンスイベントなど、特定のカテゴリのイベントを表示するには、* View * をクリックして、イベントタイプのメニューから選択します。
3. 詳細を表示するイベントの名前をクリックします。

イベントの詳細がイベントの詳細ページに表示されます。

未割り当てのイベントを表示する

未割り当てのイベントを表示して、各イベントを解決できるユーザに割り当てることができます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* イベント管理 * をクリックします。

デフォルトでは、新規と確認済みのイベントがイベント管理のインベントリページに表示されます。

2. [* フィルタ * (* Filters *)] パネルの [* 割り当て先 * (Assigned to *)] 領域で [* 未割り当て * (* Unassigned *)] フィルタオプションを選択する。

イベントを確認して解決します

イベントを生成した問題で作業を開始する前に、アラート通知が繰り返し送信されないようにイベントに確認応答する必要があります。特定のイベントに対処したら、そのイベントを解決済みとしてマークします。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

複数のイベントに同時に確認応答して解決することができます。



情報イベントに確認応答することはできません。

手順

1. 左側のナビゲーションペインで、* イベント管理 * をクリックします。
2. イベントのリストで、次の操作を実行してイベントに応答します。

状況	手順
1つのイベントに確認応答して解決済みとしてマークします	<ol style="list-style-type: none">a. イベント名をクリックします。b. イベントの詳細ページで、イベントの原因を確認します。c. [* Acknowledge (確認)] をクリックしd. 適切な方法で対処します。e. [* 解決済みとしてマークする *] をクリックします。
複数のイベントに確認応答して解決済みとしてマークします	<ol style="list-style-type: none">a. それぞれのイベントの詳細ページでイベントの原因を確認します。b. イベントを選択します。c. [* Acknowledge (確認)] をクリックしd. 適切な方法で対処します。e. [* 解決済みとしてマークする *] をクリックします。

解決済みとしてマークされたイベントは、解決済みイベントのリストに移動します。

3. * オプション * : [* Notes and Updates* (メモと更新*)] 領域で、イベントの対処方法に関するメモを追加し、[* Post* (投稿)] をクリックします。

特定のユーザにイベントを割り当てます


未割り当てのイベントは、自分自身またはリモートユーザを含む他のユーザに割り当てることができます。必要に応じて、割り当てられたイベントを別のユーザに再割り当てすることもできます。たとえば、ストレージオブジェクトで頻繁に問題が発生する場合、そのオブジェクトを管理するユーザにそれらの問題に対するイベントを割り当てることができます。

- 必要なもの *
- ユーザの名前と E メール ID が正しく設定されている必要があります。
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* イベント管理 * をクリックします。

2. [* イベント管理 *] インベントリページで、割り当てるイベントを 1 つ以上選択します。
3. 次のいずれかを実行してイベントを割り当てます。

イベントを割り当てるユーザ	操作
自分自身	[* Assign to * > * Me *] をクリックします。
別のユーザ	<p>a. [* Assign to * > * another user* (* 他のユーザに割り当て)] をクリックします</p> <p>b. 所有者の割り当てダイアログボックスで、ユーザ名を入力するか、ドロップダウンリストからユーザを選択します。</p> <p>c. [Assign] をクリックします。</p> <p>ユーザに E メール通知が送信されます。</p> <div>  <p>ユーザ名を入力しない場合、またはドロップダウンリストからユーザを選択し、* assign * をクリックすると、イベントは未割り当てのままになります。</p> </div>

不要なイベントを無効にします

デフォルトでは、すべてのイベントが有効になっています。環境で重要でないイベントについては、グローバルに無効にして通知が生成されないようにすることができます。無効にしたイベントの通知を再開するときは、該当するイベントを有効にすることができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

イベントを無効にすると、システムで以前に生成されたイベントは「廃止」とマークされ、それらのイベントに設定されたアラートはトリガーされなくなります。無効にしたイベントを有効にすると、それらのイベントの通知の生成が次の監視サイクルから開始されます。

オブジェクトのイベント（など）を無効にした場合 vol offline イベント）をクリックし、あとでイベントを有効にした場合、イベントが無効な状態のときにオフラインになったオブジェクトに対しては新しいイベントは生成されません。Unified Manager では、イベントを再度有効にしたあとにオブジェクトの状態に変更があった場合にのみ新規のイベントが生成されます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Event Setup * をクリックします。
2. イベント設定 * ページで、次のいずれかのオプションを選択してイベントを無効または有効にします。

状況	操作
イベントを無効にします	<ul style="list-style-type: none"> a. [Disable] をクリックします。 b. [イベントの無効化] ダイアログボックスで、イベントの重大度を選択します。 c. [Matching Events] カラムで、イベントの重大度に基づいてディセーブルにするイベントを選択し、右矢印をクリックして [Disable Events] カラムに移動します。 d. [保存して閉じる] をクリックします。 e. 無効にしたイベントが Event Setup ページのリストビューに表示されることを確認します。
イベントを有効にします	<ul style="list-style-type: none"> a. 有効にするイベントのチェックボックスを選択します。 b. [Enable] をクリックします。

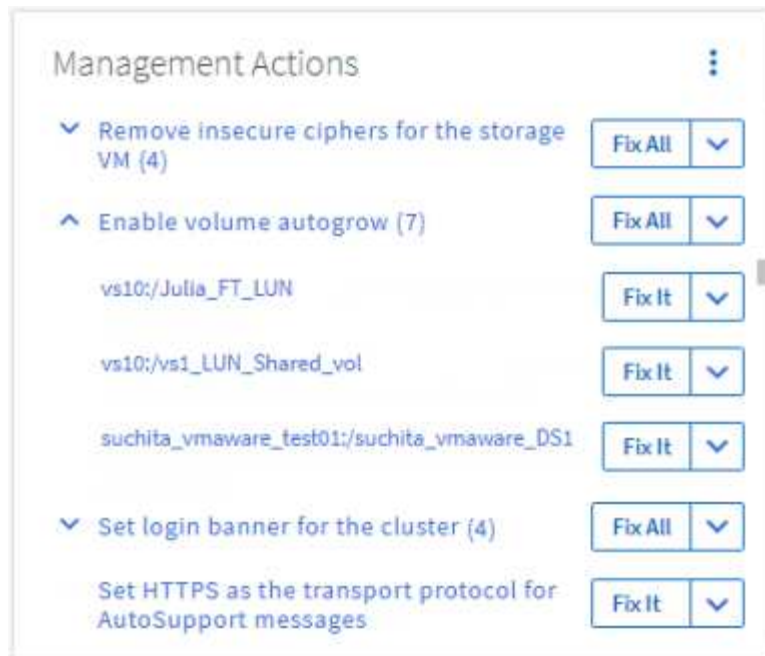
Unified Manager の自動修復を使用して問題を修正します

イベントによっては、Unified Manager の詳細な診断によって、* Fix it * ボタンを使用して単一の解決策が提供されることがあります。解決策がある場合は、ダッシュボード、イベントの詳細ページ、左側のナビゲーションメニューのワークロード分析の順に表示されます。

ほとんどのイベントではイベントの詳細ページにさまざまな解決策が表示されるため、ONTAP システムマネージャまたは ONTAP CLI を使用して最適な解決策を実装できます。問題を修正する解像度が 1 つで、ONTAP の CLI コマンドで解決できることが Unified Manager で確認された場合は、* Fix it * アクションを使用できます。

手順

1. * ダッシュボード * から解決できるイベントを表示するには、* ダッシュボード * をクリックします。



2. Unified Manager で修正可能な問題を解決するには、* 修正 * ボタンをクリックします。複数のオブジェクトに存在する問題を修正するには、* すべて修正 * ボタンをクリックします。

自動修正で解決できる問題については、を参照してください "[Unified Manager で解決可能な問題](#)"。

Active IQ イベントレポートの有効化と無効化

Active IQ プラットフォームイベントは、デフォルトで生成されて Unified Manager ユーザーインターフェイスに表示されます。「ノイジー」が大きすぎる場合や、Unified Manager でこれらのイベントを表示したくない場合は、これらのイベントの生成を無効にすることができます。あとで有効にして、これらの通知の受信を再開することができます。

- 必要なもの *

アプリケーション管理者のロールが必要です。

この機能を無効にすると、Unified Manager は Active IQ プラットフォームイベントの受信をただちに停止します。

この機能を有効にすると、クラスタのタイムゾーンの午前 0 時を過ぎに Unified Manager は Active IQ プラットフォームイベントの受信を開始します。開始時刻は、Unified Manager がいつ各クラスタから AutoSupport メッセージを受信したかによって決まります。

手順

1. 左側のナビゲーションペインで、* 一般 * > * 機能設定 * をクリックします。
2. [* 機能の設定 *] ページで、次のいずれかのオプションを選択して Active IQ プラットフォームイベントを無効または有効にします。

状況	操作
Active IQ プラットフォームイベントを無効にします	Active IQ ポータルイベント * パネルで、スライダーボタンを左に動かします。
Active IQ プラットフォームイベントを有効にします	Active IQ ポータルイベント * パネルで、スライダーボタンを右に動かします。

新しい **Active IQ** ルールファイルをアップロードしています

Unified Managerは、新しいActive IQ イベント（ルール）ファイルの有無を自動的にチェックし、ある場合は新しいファイルをダウンロードします。ただし、外部ネットワークへのアクセスがないサイトでは、ルールファイルを手動でアップロードする必要があります。



Active IQ ルールは、Config Advisor（CA）セキュアルールとも呼ばれます。

ネットワークに接続されていないサイトでUnified Managerをインストールまたはアップグレードすると、バンドルされているActive IQ ルールを自動的にアップロードに使用できるようになります。ただし、更新されたイベントが生成されてストレージシステムが最適な状態を継続できるようにするために、ネットアップサポートサイトから月に約1回は新しいルールファイルをダウンロードすることを推奨します。

- 必要なもの *
- Active IQ ポータルイベントのレポートを有効にする必要があります。この機能はデフォルトで有効になっています。詳細については、を参照してください "[Active IQ ポータルイベントの有効化](#)"。
- ルールファイルをNetApp Support Siteからダウンロードする必要があります。

ルールファイルは次の場所にあります。 https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

手順

1. ネットワークにアクセスできるコンピュータで、NetApp Support Site に移動し、現在のルールをダウンロードします .zip ファイル。

ルールパッケージには、ルールリポジトリ、データソース、およびネットアップの技術情報アーティクルが含まれています。



Windowsシステムでは、ネットワークに接続されていないサイトでは、デフォルトではネットアップの技術情報アーティクルがインストーラにバンドルされていません。サポートサイトから `_secure_rules.zip` ファイルをダウンロードしてアップロードすると、すべてのルールのKB記事を参照できます。

2. ルールファイルをセキュリティエリアに持ち出すことができるメディアに転送し、セキュリティエリアのシステムにコピーします。
3. 左側のナビゲーションペインで、 * Storage Management * > * Event Setup * をクリックします。
4. [* イベントの設定 *] ページで、[* ルールのアップロード *] ボタンをクリックします。

5. [ルールの上ロード (* Upload Rules *)]ダイアログボックスで、ルールに移動して選択します .zip ダウンロードしたファイルで、*アップロード*をクリックします。

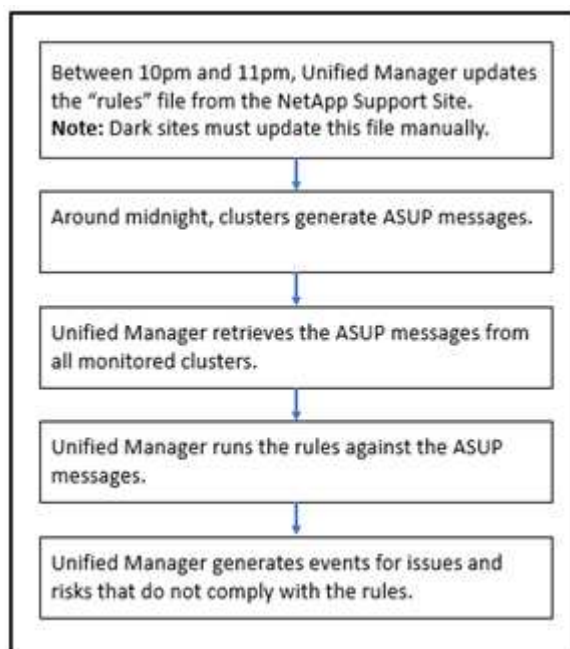
この処理には数分かかることがあります。

ルールファイルが Unified Manager サーバに解凍されます。午前0時を過ぎた時点で管理対象クラスターで AutoSupport ファイルが生成され、Unified Manager がルールファイルに照らしてクラスターをチェックし、必要に応じて新しいリスクイベントとインシデントイベントを生成します。

詳細については、次の技術情報アーティクル (KB) を参照してください。 ["Active IQ Unified Manager で AICASecure ルールを手動で更新する方法"](#)。

Active IQ プラットフォームイベントの生成方法

Active IQ プラットフォームのインシデントとリスクは、次の図に示すように Unified Manager のイベントに変換されます。

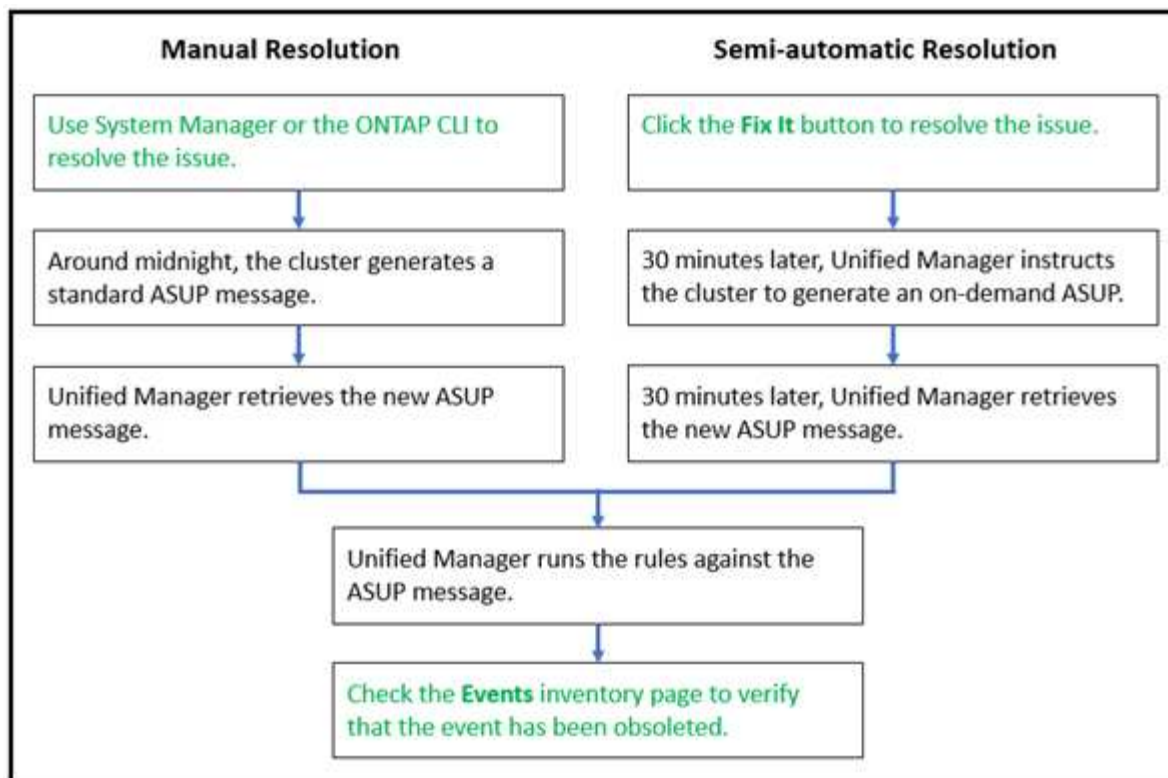


このように、Active IQ プラットフォームで作成されたルールファイルが最新の状態に維持され、クラスターの AutoSupport メッセージが毎日生成され、Unified Manager がイベントのリストを毎日更新します。

Active IQ プラットフォームイベントを解決しています

Active IQ プラットフォームのインシデントとリスクは、Unified Manager の他のイベントと同様に、解決のために他のユーザに割り当て可能で、ステータスの種類も同じです。ただし、[修正] ボタンを使用してこれらのタイプのイベントを解決すると、解決を数時間以内に検証できます。

次の図は、Active IQ プラットフォームで生成されたイベントの解決時にユーザが実行する操作（緑）と Unified Manager で実行される操作（黒）を示しています。



手動で解決する場合は、System Manager または ONTAP コマンドラインインターフェイスにログインして問題を修正する必要があります。問題を検証できるのは、午前 0 時にクラスタで新しい AutoSupport メッセージが生成されたあとです。

[Fix it* (修正)] ボタンを使用して半自動の解決を実行する場合、修正が数時間以内に正常に完了したことを確認できます。

イベント保持を設定しています

イベントが自動的に削除されるまでに Unified Manager サーバでイベントを保持する月数を指定できます。

- 必要なもの *

アプリケーション管理者のロールが必要です。

サーバのパフォーマンスに影響する可能性があるため、イベントの保持期間を 6 カ月以上に設定することは推奨されません。

手順

1. 左側のナビゲーションペインで、* 一般 * > * データ保持 * をクリックします。
2. [* データ保持期間 *] ページで、[イベント保持期間] 領域のスライダを選択し、イベントを保持する月数に移動して、[保存] をクリックします。

Unified Manager のメンテナンス時間とは

Unified Manager のメンテナンス時間を定義することで、クラスタのメンテナンスを計画

している場合に、その期間はイベントやアラートを抑制して不要な通知を受け取らないようにすることができます。

メンテナンス時間が開始されると、「Object Maintenance Window Started」イベントがイベント管理インベントリページに記録されます。このイベントは、メンテナンス時間が終了すると自動的に廃止されます。

メンテナンス時間中も、そのクラスタのすべてのオブジェクトに関連するイベントは引き続き生成されますが、いずれの UI ページにも表示されず、アラートやその他の通知も送信されません。ただし、[イベント管理] インベントリページの [表示] オプションのいずれかを選択すると、保守期間中にすべてのストレージオブジェクトに対して生成されたイベントを表示できます。

メンテナンス時間をスケジュールしたり、スケジュールされたメンテナンス時間の開始時刻や終了時刻を変更したり、スケジュールされたメンテナンス時間をキャンセルしたりできます。

メンテナンス時間のスケジュールによるクラスイベント通知の無効化

クラスタをアップグレードしたり、いずれかのノードを移動したりする場合など、クラスタを計画的に停止するときは、Unified Manager のメンテナンス時間をスケジュールすることで、その間は通常生成されるイベントやアラートを抑制することができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

メンテナンス時間中も、そのクラスタのすべてのオブジェクトに関連するイベントは引き続き生成されますが、イベントページには表示されず、アラートやその他の通知も送信されません。

メンテナンス時間に入力する時刻は Unified Manager サーバの時刻に基づいています。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Cluster Setup * をクリックします。
2. クラスタの「* メンテナンス・モード *」列で、スライダ・ボタンを選択して右に動かします。

カレンダーウィンドウが表示されます。

3. メンテナンス時間の開始日時と終了日時を選択し、* 適用 * をクリックします。

スライダボタンの横に「スケジュール済み」というメッセージが表示されます。

開始時間に達すると、クラスタがメンテナンスモードになり、「Object Maintenance Window Started」イベントが生成されます。

スケジュールされたメンテナンス時間を変更またはキャンセルする

Unified Manager のメンテナンス時間を設定している場合、開始時刻と終了時刻を変更したり、メンテナンス時間をキャンセルしたりできます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

メンテナンス時間中に、スケジュールされたメンテナンス時間の終了時刻よりも前にクラスタのメンテナンスが完了し、クラスタからのイベントやアラートの受信を再開する場合は、現在のメンテナンス時間をキャンセルすると便利です。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Cluster Setup * をクリックします。
2. クラスタの「 * Maintenance Mode * 」列で、次の手順を実行します。

状況	実行する手順
スケジュールされたメンテナンス時間の期間を変更する	<ol style="list-style-type: none">a. スライダボタンの横にある「スケジュール済み」というテキストをクリックします。b. 開始日時または終了日時を変更し、 * 適用 * をクリックします。
アクティブなメンテナンス期間を延長します	<ol style="list-style-type: none">a. スライダボタンの横にある「Active」というテキストをクリックします。b. 終了日時を変更し、 * 適用 * をクリックします。
スケジュールされたメンテナンス時間をキャンセルする	スライダボタンを選択して左に移動します。
アクティブなメンテナンス期間をキャンセルする	スライダボタンを選択して左に移動します。

メンテナンス時間中に発生したイベントの表示

必要に応じて、すべてのストレージオブジェクトについて Unified Manager のメンテナンス時間中に生成されたイベントを確認することができます。ほとんどのイベントは、メンテナンス時間が終了し、すべてのシステムリソースが再び稼働すると、「廃止」の状態になります。

- 必要なもの *

少なくとも 1 回はメンテナンス時間が完了している必要があります。

メンテナンス時間中に発生したイベントは、デフォルトではイベント管理インベントリページに表示されません。

手順

1. 左側のナビゲーションペインで、 * Events * （イベント * ） をクリックします。

デフォルトでは、すべてのアクティブな（新規および確認済みの）イベントがイベント管理インベントリページに表示されます。

2. [表示] ペインで、 [メンテナンス中に生成されたすべてのイベント] オプション * を選択します。

メンテナンス時間のすべてのセッションとすべてのクラスタを対象に、過去 7 日間にトリガーされたイベントのリストが表示されます。

3. 1 つのクラスタに複数のメンテナンス時間がある場合は、* Triggered Time * カレンダーアイコンをクリックして、表示するメンテナンス期間イベントの期間を選択できます。

ホストシステムリソースイベントの管理

Unified Manager には、Unified Manager がインストールされているホストシステムでのリソースの問題を監視するサービスが用意されています。ディスクスペースが不足している場合やホストシステムでメモリが不足している場合など、管理ステーションイベントがトリガーされて UI 上部にバナーメッセージとして表示されることがあります。

管理ステーションイベントは、Unified Manager がインストールされているホストシステムを含む問題を示します。管理ステーションの問題には、たとえば、ホストシステムでのディスクスペースの不足、Unified Manager での定期的なデータ収集サイクルの失敗、次の収集ポーリングが開始されたことによる統計分析の完了または完了の遅れなどがあります。

Unified Manager の他のイベントメッセージとは異なり、管理ステーション固有の警告イベントと重大イベントはバナーメッセージで表示されます。

ステップ

1. 管理ステーションイベント情報を表示するには、次の操作を実行します。

状況	手順
イベントの詳細を表示します	イベントバナーをクリックして、問題の推奨ソリューションを含むイベントの詳細ページを表示します。
管理ステーションのすべてのイベントを表示します	<ol style="list-style-type: none">a. 左側のナビゲーションペインで、* イベント管理 * をクリックします。b. Event Management イベントリページの Filters ペインで、Source Type リストの Management Station のボックスをクリックします。

イベントに関する詳細情報

イベントに関する概念を理解しておく、クラスタおよびクラスタオブジェクトを効率的に管理し、アラートを適切に定義できるようになります。

イベントの状態の定義

イベントの状態を確認すると、対処が必要かどうかを特定するのに役立ちます。イベントの状態は、「新規」、「確認済み」、「解決済み」、「廃止」のいずれかです。「新規」と「確認済み」のイベントの両方がアクティブなイベントとみなされます。

イベントの状態は次のとおりです。

- * 新 *

新しいイベントの状態。

- * 承認済み *

イベントを確認したときの状態。

- * 解決済み *

イベントが解決済みとマークされたときの状態。

- * 廃止 *

イベントが自動的に修正されたとき、またはイベントの原因が無効になったときの状態。



廃止状態のイベントを確認または解決することはできません。

イベントのさまざまな状態の例

次の例は、手動および自動でイベントの状態が変化する様子を示しています。

「Cluster Not Reachable」イベントがトリガーされると、イベントの状態は「New」になります。イベントを確認すると、イベントの状態は「確認済み」に変わります。適切な方法で対処したら、イベントを解決済みとしてマークする必要があります。その後、イベントの状態が「解決済み」に変わります。

「クラスタに到達できません」イベントが生成された原因が停電であった場合は、電源が復旧すると、管理者の介入なしでクラスタが起動します。そのため、「クラスタに到達できません」イベントは有効でなくなり、イベントの状態が次の監視サイクルで「廃止」に変わります。

Unified Manager では、イベントが「Obsolete」または「Resolved」の状態になるとアラートを送信します。アラートの E メール の件名と内容に、イベントの状態に関する情報が記載されます。SNMP トラップには、イベントの状態に関する情報も含まれます。

概要のイベントの重大度タイプ

イベントには、対処する際の優先度を判別できるように、それぞれ重大度タイプが関連付けられています。

- * 重要 *

問題が発生しており、すぐに対処しないとサービスが停止する可能性があります。

パフォーマンスに関する重大イベントは、ユーザ定義のしきい値からのみ生成されます。

- * エラー *

イベントソースは実行中ですが、サービスの停止を回避するために対処が必要です。

- * 警告 *

イベントソースに注意が必要なアラートが発生したか、クラスタオブジェクトのパフォーマンスカウンタが正常な範囲から外れており、重大な問題にならないように監視が必要です。この重大度のイベントでは原因サービスは停止しません。早急な対処も不要です。

パフォーマンスに関する警告イベントは、ユーザ定義のしきい値、システム定義のしきい値、または動的なしきい値から生成されます。

- * 情報 *

新しいオブジェクトが検出されたときやユーザ操作が実行されたときに発生します。たとえば、ストレージオブジェクトが削除された場合や設定に変更があった場合は、情報タイプの重大度のイベントが生成されます。

情報イベントは、設定の変更が検出されたときに ONTAP から直接送信されます。

イベントの影響レベルの概要

イベントには、対処する際の優先度を判別できるように、それぞれに影響レベル（インシデント、リスク、イベント、またはアップグレード）が関連付けられています。

- * インシデント *

インシデントは、クラスタによるクライアントへのデータの提供の停止やデータを格納するスペースの不足を発生させることができる一連のイベントです。影響レベルが「インシデント」のイベントは、最も重大度が高く、サービスの停止を回避するためにすぐに対処する必要があります。

- * リスク *

リスクは、原因クラスタによるクライアントへのデータの提供の停止やデータを格納するスペースの不足を引き起こす可能性がある一連のイベントです。影響レベルが「リスク」のイベントは、原因サービスの停止につながる可能性があります。対処が必要な場合があります。

- * イベント *

イベントは、ストレージオブジェクトとその属性の状態やステータスの変化を示します。影響レベルが「イベント」のイベントは情報提供を目的としたものであり、対処は必要ありません。

- * アップグレード *

アップグレードイベントは、Active IQ プラットフォームから報告される特定のタイプのイベントです。これらのイベントは、ONTAP ソフトウェア、ノードファームウェア、またはオペレーティングシステムソフトウェア（セキュリティアドバイザリ用）のアップグレードが必要な問題を示します。これらの問題については、すぐに対処が必要なものもあれば、スケジュールされた次回のメンテナンスまで待てるものもあります。

イベントの影響領域の概要

イベントは、6つの影響領域（可用性、容量、構成、パフォーマンス、保護、および security）を使用して、管理者が担当するタイプのイベントに集中できるようにしま

す。

- * 利用可能性 *

可用性イベントは、ストレージオブジェクトがオフラインになった場合、プロトコルサービスが停止した場合、ストレージフェイルオーバーを実行した問題が発生した場合、ハードウェアで問題が実行された場合に通知するイベントです。

- * 容量 *

容量イベントは、アグリゲート、ボリューム、LUN、またはネームスペースのサイズがしきい値に近づいているか達した場合、または環境の通常の増加率とかけ離れている場合に通知するイベントです。

- * コンフィグレーション *

構成イベントは、ストレージオブジェクトの検出、削除、追加、または名前変更について通知するイベントです。構成イベントの影響レベルは「イベント」、重大度タイプは「情報」です。

- * パフォーマンス *

パフォーマンスイベントは、監視対象のストレージオブジェクトにおけるデータストレージの入力速度や取得速度に悪影響を及ぼす可能性がある、クラスタのリソース、設定、または処理の状況について通知するイベントです。

- * 保護 *

保護イベントは、SnapMirror 関係に関するインシデントやリスク、デスティネーションの容量の問題、SnapVault 関係の問題、または保護ジョブの問題について通知するイベントです。セカンダリボリュームおよび保護関係をホストする ONTAP オブジェクト（アグリゲート、ボリューム、および SVM）は、いずれもこの影響領域に分類されます。

- * セキュリティ *

セキュリティイベントは、で定義されたパラメータに基づいて、ONTAP クラスタ、Storage Virtual Machine（SVM）、およびボリュームのセキュリティがどの程度確保されるかを通知します ["ONTAP 9 セキュリティ設定ガイド"](#)。

また、この領域には、Active IQ プラットフォームから報告されるアップグレードイベントも含まれます。

オブジェクトステータスの計算方法

オブジェクトステータスは、現在の状態が「新規」または「確認済み」の最も重大度の高いイベントによって決まります。たとえば、オブジェクトステータスが Error の場合は、オブジェクトのいずれかのイベントの重大度タイプが Error となっています。イベントに対処すると、イベントの状態は Resolved になります。

動的なパフォーマンスイベントチャートの詳細

動的なパフォーマンスイベントの場合、イベントの詳細ページのシステム診断セクションに、競合状態のクラスタコンポーネントのレイテンシまたは使用量が最も高い上位の

ワークロードが表示されます。

パフォーマンス統計は、パフォーマンスイベントが検出されてからイベントが最後に分析されるまでの時間に基づいています。このグラフには、競合状態のクラスタコンポーネントの過去のパフォーマンス統計も表示されます。

たとえば、コンポーネントの利用率が高いワークロードを特定して、利用率が低いコンポーネントに移動するワークロードを特定できます。ワークロードを移動すると、現在のコンポーネントでの作業量が減り、コンポーネントの競合状態が解消する可能性があります。このセクションの上部には、イベントが検出されて最後に分析された時刻と日付の範囲が表示されます。アクティブなイベント（新規または確認済みのイベント）の場合、最後に分析された時刻が更新されます。

レイテンシとアクティビティのグラフにカーソルを合わせると、上位のワークロードの名前が表示されます。グラフの右側にあるワークロードのタイプメニューをクリックすると、イベントでのワークロードのロールに基づいてワークロードをソートできます。これには、_Shark、_Bully、_Victim の各ワークロードのレイテンシと競合しているクラスタコンポーネントでの使用状況の詳細が表示されます。実際の値と想定値を比較して、ワークロードがレイテンシまたは使用量の想定範囲を外れたタイミングを確認できます。詳細については、を参照してください ["Unified Manager で監視されるワークロードのタイプ"](#)。



レイテンシのピーク偏差でソートする場合は、システム定義のワークロードがテーブルに表示されません。これは、レイテンシがユーザー定義のワークロードにのみ適用されるためです。レイテンシの値が小さいワークロードはこのテーブルに表示されません。

動的なパフォーマンスしきい値の詳細については、を参照してください ["動的なパフォーマンスしきい値で生成されたイベントを分析する"](#)。

Unified Managerでワークロードをランク付けしてソート順序を決定する方法については、を参照してください ["Unified Manager がイベントによるパフォーマンスへの影響を判定する仕組み"](#)。

グラフ内のデータには、イベントが最後に分析されるまでの 24 時間のパフォーマンス統計が示されます。各ワークロードの実際の値と想定値は、ワークロードがイベントに関連した時刻に基づいています。たとえば、イベントの検出後にワークロードがイベントに関連した可能性があるため、そのパフォーマンス統計がイベント検出時の値と一致しないことがあります。デフォルトでは、レイテンシのピーク（最大）偏差でワークロードがソートされます。



Unified Manager では 5 分ごとのパフォーマンスとイベントの履歴データが最大 30 日分保持されるため、30 日前より古いイベントの場合、パフォーマンスデータは表示されません。

• * ワークロードソート列 *

◦ * レイテンシグラフ *

前回の分析中の、ワークロードのレイテンシに対するイベントの影響が表示されます。

◦ * コンポーネント使用状況列 *

競合状態のクラスタコンポーネントのワークロードの使用量に関する詳細が表示されます。グラフでは、実際の使用量は青い線で表示されます。検出時刻から最後に分析された時刻までのイベント期間が赤いバーで強調表示されます。詳細については、を参照してください ["ワークロードのパフォーマンスの測定値"](#)。



ネットワークコンポーネントの場合は、クラスタ以外のアクティビティに基づいてネットワークパフォーマンス統計が作成されるため、この列は表示されません。

◦ * コンポーネント使用率 *

QoS ポリシーグループコンポーネントのネットワーク処理、データ処理、および集約コンポーネントの使用率の履歴、またはアクティビティの履歴をパーセント単位で表示します。ネットワークコンポーネントまたはインターコネクトコンポーネントについては、このグラフは表示されません。統計にカーソルを合わせると、特定の時点における使用状況を表示できます。

◦ * 書き込み MBps の合計履歴 *

MetroCluster のリソースコンポーネントの場合にのみ、MetroCluster 構成のパートナークラスタにミラーリングされるすべてのボリュームワークロードについて、書き込みスループットの合計が 1 秒あたりのメガバイト数 (MBps) で表示されます。

◦ * イベント履歴 *

競合状態のコンポーネントの過去のイベントを示す赤い影付きの線が表示されます。廃止イベントの場合は、選択したイベントが検出される前に発生したイベントと解決後のイベントがグラフに表示されます。

Unified Manager によって設定の変更が検出されました

Unified Manager では、クラスタの構成の変更が監視され、それが原因で発生したパフォーマンスイベントがないかどうかを判断できます。パフォーマンスエクスプローラのページには、変更イベントアイコン (●) をクリックして、変更が検出された日時を示します。

パフォーマンスエクスプローラのページおよびワークロード分析ページでパフォーマンスチャートを確認して、変更イベントが選択したクラスタオブジェクトのパフォーマンスに影響したかどうかを確認できます。パフォーマンスイベントとほぼ同時に変更が検出された場合、その変更が問題にもたらした可能性があり、イベントのアラートがトリガーされた可能性があります。

Unified Manager では次の変更イベントを検出できます。これらは情報イベントに分類されます。

- ボリュームがアグリゲート間で移動されたとき。

移動が開始されたとき、完了したとき、または失敗したときに Unified Manager で検出されます。ボリュームの移動中に Unified Manager が停止していた場合は、稼働状態に戻ったあとにボリュームの移動が検出され、対応する変更イベントが表示されます。

- 1 つ以上の監視対象ワークロードを含む QoS ポリシーグループのスループット (MBps または IOPS) の制限が変更されたとき。

ポリシーグループ制限を変更原因すると、レイテンシ (応答時間) が一時的に長くなることもあり、ポリシーグループのイベントがトリガーされる可能性もあります。レイテンシは徐々に正常に戻り、発生したイベントは廃止状態になります。

- HA ペアのノードのストレージがパートナーノードにテイクオーバーまたはギブバックされたとき。

テイクオーバー、部分的なテイクオーバー、またはギブバックの処理が完了したときに Unified Manager で検出されます。ノードのパニック状態が原因で発生したテイクオーバーは Unified Manager では検出されません。

- ONTAP のアップグレード処理またはリバート処理が完了しました。

以前のバージョンと新しいバージョンが表示されます。

イベントおよび重大度タイプのリスト

リストに表示されるイベントを使用して、イベントのカテゴリと名前、および Unified Manager に表示される各イベントの重大度タイプを確認することができます。イベントは、オブジェクトカテゴリごとにアルファベット順に一覧表示されます。

アグリゲートイベント

アグリゲートイベントは、アグリゲートのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

アスタリスク（*）は、Unified Manager イベントに変換された EMS イベントを示します。

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
アグリゲートがオフライン（ Document EvtAggregateStateOffline ）	インシデント	アグリゲート	重要
アグリゲートが失敗しました（ Document EvtAggregateStateFailed ）	インシデント	アグリゲート	重要
集約は制限されています（ DocumentEvtAggregateStateRestricted ）	リスク	アグリゲート	警告
アグリゲートの再構築（ Document EvtAggregateRaidStateReconstructing ）	リスク	アグリゲート	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
アグリゲートがデグレード状態になりました（ Document EvtAggregateRaidStateDegraded）	リスク	アグリゲート	警告
クラウド階層に部分的に到達可能（ドキュメントイベントクラウド階層への到達不能）	リスク	アグリゲート	警告
クラウド階層に到達不能（ Document EventCloudTierUnreachable）	リスク	アグリゲート	エラー
アグリゲートの再配置でクラウド階層へのアクセス拒否*（ arlNetraCaCheckFailed）	リスク	アグリゲート	エラー
ストレージフェイルオーバー時のアグリゲートの再配置でクラウド階層へのアクセス拒否*（ gbNetraCaCheckFailed）	リスク	アグリゲート	エラー
MetroCluster の残りのアグリゲート（ ocument MetroClusterAggregateLeftBehind）	リスク	アグリゲート	エラー
MetroCluster アグリゲートのミラーリングがデグレード状態になる（ Document EvtMetroClusterAggregateMirroring Degraded）	リスク	アグリゲート	エラー

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
アグリゲートスペースがほぼフル（ Document EvtAggregateNearlyFull ）	リスク	アグリゲート	警告
アグリゲートスペースがフル（ Document EvtAggregateFull ）	リスク	アグリゲート	エラー
アグリゲートのフルまでの日数（ Document EvtAggregateDaysUntilFullSoon ）	リスク	アグリゲート	エラー
アグリゲートがオーバーコミット（ Document EvtAggregateOvercommitted ）	リスク	アグリゲート	エラー
アグリゲートがほぼオーバーコミット（ Document EvtAggregateAlmostOvercommitted ）	リスク	アグリゲート	警告
アグリゲートの Snapshot リザーブがフル（ Document EvtAggregateSnapReserveFull ）	リスク	アグリゲート	警告
アグリゲートの増加率が異常（ Document EvtAggregateGrowthRateAbnormal ）	リスク	アグリゲート	警告

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
アグリゲートを検出（該当なし）	イベント	アグリゲート	情報
アグリゲートの名前を変更（該当なし）	イベント	アグリゲート	情報

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
アグリゲートが削除されました（該当なし）	イベント	ノード	情報

影響範囲：パフォーマンス

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
アグリゲート IOPS の重大しきい値を超過（ Document AggregateIopsIncident）	インシデント	アグリゲート	重要
アグリゲート IOPS の警告しきい値を超過（ DocumentAggregateIops Warning）	リスク	アグリゲート	警告
アグリゲート MBps の重大しきい値を超過（ Document AggregateMbpsIncident）	インシデント	アグリゲート	重要
アグリゲート MBps の警告しきい値を超過（ Document AggregateMbpsWarning）	リスク	アグリゲート	警告
アグリゲートレイテンシの重大しきい値を超過（ Document AggregateLatencyIncident）	インシデント	アグリゲート	重要
アグリゲートレイテンシの警告しきい値を超過（ DocumentAggregateLatencyWarning）	リスク	アグリゲート	警告
アグリゲート使用済みパフォーマンス容量の重大しきい値を超過（「 AggregatePerfCapacityUsedIncident」）	インシデント	アグリゲート	重要

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
アグリゲート使用済みパフォーマンス容量の警告しきい値を超過（「AggregatePerfCapacityUsedWarning」）	リスク	アグリゲート	警告
アグリゲート利用率の重大しきい値を超過（DocumentAggregateUtilizationIncident）	インシデント	アグリゲート	重要
アグリゲート利用率の警告しきい値を超過（DocumentAggregateUtilizationWarning）	リスク	アグリゲート	警告
利用率の高いアグリゲートディスクのしきい値を超過（DocumentAggregateDisksOverUtilizedWarning）	リスク	アグリゲート	警告
アグリゲート動的しきい値を超過（DocumentAggregateDynamicEventWarning）	リスク	アグリゲート	警告

クラスタイイベント

クラスタイイベントは、クラスタのステータスに関する情報を提供します。これにより、クラスタの潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名、トラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

アスタリスク（*）は、Unified Manager イベントに変換された EMS イベントを示します。

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
クラスタにスペアディスクなし（DocumentEvtDisksNoSpares）	リスク	クラスタ	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
クラスタに到達できません（Document EvtClusterUnreachable）	リスク	クラスタ	エラー
クラスタの監視に失敗しました（Document EvtClusterMonitoringFailed）	リスク	クラスタ	警告
クラスタの FabricPool ライセンス容量制限を超過（Document EvtExternalCapacityTierSpaceFull）	リスク	クラスタ	警告
NVMF の猶予期間 - 開始 *（nvmetfGracePeriodStart）	リスク	クラスタ	警告
NVMF の猶予期間 - アクティブ *（nvmetfGracePeriodActive）	リスク	クラスタ	警告
NVMF の猶予期間 - 終了 *（nvmetfGracePeriodExpired）	リスク	クラスタ	警告
オブジェクトのメンテナンス時間が開始されました（objectMaintenanceWindowStarted）	イベント	クラスタ	重要
オブジェクトのメンテナンス時間が終了しました（objectMaintenanceWindowEnded）	イベント	クラスタ	情報
MetroCluster のスペアディスクが残されている（Document EvtSpareDiskLeftBehind）	リスク	クラスタ	エラー

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
MetroCluster の自動計画外スイッチオーバーが無効（ Document EvtMccAutomaticUnplannedSwitchOverDisabled ）	リスク	クラスタ	警告
クラスタユーザパスワードが変更されました *（ cluster.passwd.changed ）	イベント	クラスタ	情報

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
クラスタ容量の不均衡しきい値を超過（ドキュメント「 ConformanceNodeImbalanceWarning 」）	リスク	クラスタ	警告
クラスタのクラウド階層の計画（ clusterCloudTierPlaningWarning ）	リスク	クラスタ	警告
FabricPool ミラーレプリケーションの再同期が完了 *（ wafCaResyncComplete ）	イベント	クラスタ	警告
FabricPool スペースがほぼフル *（ fabricpoolNearlyFull ）	リスク	クラスタ	エラー

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ノードが追加されました（該当なし）	イベント	クラスタ	情報

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ノードが削除されました（該当なし）	イベント	クラスタ	情報
クラスタが削除されました（該当なし）	イベント	クラスタ	情報
クラスタの追加に失敗（該当なし）	イベント	クラスタ	エラー
クラスタ名が変更されました（該当なし）	イベント	クラスタ	情報
緊急の EMS を受信（該当なし）	イベント	クラスタ	重要
重大な EMS を受信（該当なし）	イベント	クラスタ	重要
アラートの EMS を受信（該当なし）	イベント	クラスタ	エラー
エラーの EMS を受信（該当なし）	イベント	クラスタ	警告
警告の EMS を受信（該当なし）	イベント	クラスタ	警告
デバッグの EMS を受信（該当なし）	イベント	クラスタ	警告
通知の EMS を受信（該当なし）	イベント	クラスタ	警告
情報の EMS を受信（該当なし）	イベント	クラスタ	警告

ONTAP EMS イベントは、Unified Manager イベントの 3 つの重大度レベルに分類されます。

Unified Manager イベントの重大度レベル	ONTAP EMS イベントの重大度レベル
重要	緊急 重要

エラー	アラート
警告	エラー 警告 デバッグ 注意 情報

影響範囲：パフォーマンス

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
クラスタ負荷の不均衡しきい値を超過（）	リスク	クラスタ	警告
クラスタ IOPS の重大しきい値を超過（ドキュメント ClusterIopsIncident）	インシデント	クラスタ	重要
クラスタ IOPS の警告しきい値を超過（ドキュメントクラスタ警告）	リスク	クラスタ	警告
クラスタ MBps の重大しきい値を超過（ドキュメント ClusterMbpsIncident）	インシデント	クラスタ	重要
クラスタ MBps の警告しきい値を超過（ドキュメントクラスタの警告）	リスク	クラスタ	警告
クラスタ動的しきい値を超過（DocumentClusterDynamicEventWarning）	リスク	クラスタ	警告

影響範囲：セキュリティ

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
AutoSupport HTTPS 転送が無効になっています（ドキュメント ASUPHttpsConfiguredDisabled）	リスク	クラスタ	警告
ログ転送が暗号化されていない（ocClusterAuditLogUnencrypted）	リスク	クラスタ	警告
デフォルトのローカル管理者ユーザーが有効になっています（ocClusterDefaultAdminEnabled）	リスク	クラスタ	警告
FIPS モードが無効になっています（ドキュメント ClusterFipsDisabled）	リスク	クラスタ	警告
ログインバナーが無効になっています（ドキュメント ClusterLoginBannerDisabled）	リスク	クラスタ	警告
ログインバナーが変更されました (DocumentClusterLoginBannerChanged)	リスク	クラスタ	警告
ログ転送先が変更されました (DocumentLogForwardDestinationsChanged)	リスク	クラスタ	警告
NTP サーバー名が変更されました（Document NtpServerNamesChanged）	リスク	クラスタ	警告
NTP サーバ数が少ない（securityConfigNTPServerCountLowRisk）	リスク	クラスタ	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
クラスタピア通信が暗号化されていない（Document ClusterPeerEncryptionDisabled）	リスク	クラスタ	警告
SSH でセキュアでない暗号を使用（ocClusterSSH セキュア でない）	リスク	クラスタ	警告
Telnet プロトコルが有効になっている（ocClusterTelnetEnabled）	リスク	クラスタ	警告
一部の ONTAP ユーザアカウントのパスワードで安全性の低い MD5 ハッシュ関数を使用しています（ドキュメント ClusterMD5PasswordHashUsed）	リスク	クラスタ	警告
クラスタで自己署名証明書（ドキュメント ClusterSelfSignedCertificate）を使用する	リスク	クラスタ	警告
クラスタのリモートシェルが有効になっています（Document ClusterRshDisabled）	リスク	クラスタ	警告
クラスタ証明書の有効期限が近づいています（DocumentEvtClusterCertificateAboutToExpire）	リスク	クラスタ	警告
クラスタ証明書の有効期間が終了しました（ドキュメントのEvtClusterCertificateExpired）	リスク	クラスタ	エラー

ディスクイベント

ディスクのイベントは、ディスクのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
フラッシュディスク - スペアブロックがほぼ使用されています（ Document EvtClusterFlashDiskFewerSpareBlockError）	リスク	クラスタ	エラー
フラッシュディスク - スペアブロックなし（ Document EvtClusterFlashDiskNoSpareBlockCritical）	インシデント	クラスタ	重要
一部の未割り当てディスク（ Document EvtClusterUnassignedDiskSome）	リスク	クラスタ	警告
一部のディスクで障害が発生しました（ Document EvtDisksSomeFailed）	インシデント	クラスタ	重要

エンクロージャのイベント

エンクロージャのイベントは、データセンター内のディスクシェルフエンクロージャのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ディスクシェルフのファンに障害が発生しました（ドキュメントシェルフのファンに障害が発生しました）	インシデント	ストレージシェルフ	重要
ディスクシェルフの電源装置に障害が発生しました（ドキュメントエヴァティシェルフの電源装置に障害が発生しました）	インシデント	ストレージシェルフ	重要
<p>ディスクシェルフマルチパスが設定されていません（ document Connectivity NotInMultiPath ）</p> <p>このイベントは次のものには適用されません。</p> <ul style="list-style-type: none"> • MetroCluster 構成のクラスタ • FAS2554 、 FAS2552 、 FAS2520 、 および FAS2240 のプラットフォーム 	リスク	ノード	警告
ディスクシェルフパスの障害（ documentDiskShelfConnectivityPathFailure ）	リスク	ストレージシェルフ	警告

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ディスクシェルフを検出（該当なし）	イベント	ノード	情報
ディスクシェルフが取り外されました（該当なし）	イベント	ノード	情報

ファンのイベント

ファンのイベントは、データセンター内のノードのファンのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
1つ以上のファンに障害が発生しました（ドキュメント EvtFansOneOrMoreFailed）	インシデント	ノード	重要

フラッシュカードイベント

フラッシュカードのイベントは、データセンター内のノードに取り付けられているフラッシュカードのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
フラッシュカードはオフライン（ドキュメント： FlashCardOffline）	インシデント	ノード	重要

inode イベント

inode イベントは、inode がフルまたはほぼフルになったことを通知します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
inode がほぼフル（ Document EvtInodesAlmostFull）	リスク	ボリューム	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
inode がフル（ドキュメントのノードがフル）	リスク	ボリューム	エラー

ネットワークインターフェイス（LIF）イベント

ネットワークインターフェイスイベントは、ネットワークインターフェイス（LIF）のステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ネットワークインターフェイスのステータスが停止しています（ DocumentEvtLifStatusDown）	リスク	インターフェイス	エラー
FC / FCoE ネットワークインターフェイスのステータスが停止（ DocumentEvtFCLifStatusDown）	リスク	インターフェイス	エラー
ネットワークインターフェイスのフェールオーバーができません（ DocumentEvtLifFailoverNotPossible）	リスク	インターフェイス	警告
ホームポートにないネットワークインターフェイス (DocumentEvtLifNotAtHomePort)	リスク	インターフェイス	警告

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ネットワークインターフェイスのルートが設定されていません（該当なし）	イベント	インターフェイス	情報

影響範囲：パフォーマンス

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ネットワークインターフェイス MBps の重大しき値を超過（文書 NetworkLifMbpsIncident）	インシデント	インターフェイス	重要
ネットワークインターフェイス MBps の警告しき値を超過（文書ネットワーク LifMbpsWarning）	リスク	インターフェイス	警告
FC ネットワークインターフェイス MBps の重大しき値を超過（ドキュメント FcpLifMbpsIncident）	インシデント	インターフェイス	重要
FC ネットワークインターフェイス MBps の警告しき値を超過（ドキュメント FcpLifMbpsWarning）	リスク	インターフェイス	警告
NVMf FC ネットワークインターフェイス MBps の重大しき値を超過（ドキュメント NvmfFcLifMbpsIncident）	インシデント	インターフェイス	重要
NVMf FC ネットワークインターフェイス MBps の警告しき値を超過（ドキュメント NvmfFcLifMbpsWarning）	リスク	インターフェイス	警告

LUN イベント

LUN イベントは、LUN のステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

アスタリスク（*）は、Unified Manager イベントに変換された EMS イベントを示します。

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
LUN オフライン（ Document EvtLunOffline）	インシデント	LUN	重要
LUN を破棄*（ lunDestroy）	イベント	LUN	情報
igroup でサポートされていないオペレーティング・システムにマッピングされた LUN（ igroupUnsupportedOsType）	インシデント	LUN	警告
LUN にアクセスするためのアクティブなパスが 1 つ（ Document EvtLunSingleActivePath）	リスク	LUN	警告
LUN にアクセスするためのアクティブなパスがありません（ Document EvtLunNotReachable）	インシデント	LUN	重要
LUN にアクセスするための最適化されたパスがありません（ Document EvtLunOptimizedPathInactive）	リスク	LUN	警告
HA パートナーから LUN にアクセスするためのパスがない（ Document EvtLunHaPathInactive）	リスク	LUN	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
HA ペアの方のノードから LUN にアクセスするためのパスがありません（ocumentEvtLunNodePathStatusDown）	リスク	LUN	エラー

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
LUN Snapshot コピー用の十分なスペースがありません（ocumentLunSnapshotNotPossible）	リスク	ボリューム	警告

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
igroup でサポートされていないオペレーティング・システムにマッピングされた LUN（igroupUnsupportedOsType）	リスク	LUN	警告

影響範囲：パフォーマンス

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
LUN IOPS の重大しきい値を超過（ocLunIopsIncident）	インシデント	LUN	重要
LUN IOPS の警告しきい値を超過（ocLunIopsWarning）	リスク	LUN	警告
LUN MBps の重大しきい値を超過（ocLunMbpsIncident）	インシデント	LUN	重要

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
LUN MBps の警告しきい値を超過（ ocLunMbpsWarning）	リスク	LUN	警告
LUN レイテンシミリ秒 / 処理の重大しきい値を超過（ Document LunLatencyIncident）	インシデント	LUN	重要
LUN レイテンシミリ秒 / 処理の警告しきい値を超過（ ocumentLunLatencyWarning）	リスク	LUN	警告
LUN レイテンシ / LUN IOPS の重大しきい値を超過（ ocLunLatencyIopsIncident）	インシデント	LUN	重要
LUN レイテンシ / LUN IOPS の警告しきい値を超過（ Document LunLatencyIopsWarning）	リスク	LUN	警告
LUN レイテンシ / LUN MBps の重大しきい値を超過（ ocLunLatencyMbpsIncident）	インシデント	LUN	重要
LUN レイテンシ / LUN MBps の警告しきい値を超過（ ocLunLatencyMbpsWarning）	リスク	LUN	警告
LUN レイテンシ / アグリゲート使用済みパフォーマンス容量の重大しきい値を超過（ ocLunLatencyAggregatePerfCapacityUsedIncident）	インシデント	LUN	重要

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
LUN レイテンシ / アグリゲート使用済みパフォーマンス容量の警告しきい値を超過（ ocLunLatencyAggregatePerfCapacityUsedWarning）	リスク	LUN	警告
LUN レイテンシ / アグリゲート利用率の重大しきい値を超過（ ocLunLatencyAggregateUtilizationIncident）	インシデント	LUN	重要
LUN レイテンシ / アグリゲート利用率の警告しきい値を超過（ ocLunLatencyAggregateUtilizationWarning）	リスク	LUN	警告
LUN レイテンシ / ノードの使用済みパフォーマンス容量の重大しきい値を超過（ ocLunLatencyNodePerfCapacityUsedIncident）	インシデント	LUN	重要
LUN レイテンシ / ノードの使用済みパフォーマンス容量の警告しきい値を超過（ Document LunLatencyNodePerfCapacityUsedWarning ）	リスク	LUN	警告
LUN レイテンシ / ノード使用済みパフォーマンス容量 - テイクオーバーの重大しきい値を超過（ Document LunLatencyAggregatePerfCapacityUsedTakeoverIncident）	インシデント	LUN	重要

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
LUN レイテンシ / ノードの使用済みパフォーマンス容量 - テイクオーバーの警告しきい値を超過（Document LunLatencyAggregatePerfCapacityUsedTakeoverWarning）	リスク	LUN	警告
LUN レイテンシ / ノード利用率の重大しきい値を超過（ocLunLatencyNodeUtilizationIncident）	インシデント	LUN	重要
LUN レイテンシ / ノード利用率の警告しきい値を超過（ocLunLatencyNodeUtilizationWarning）	リスク	LUN	警告
QoS LUN 最大 IOPS の警告しきい値を超過（ドキュメントの QosLunMaxIopsWarning）	リスク	LUN	警告
QoS LUN 最大 MBps の警告しきい値を超過（ドキュメントの QosLunMaxMbpsWarning）	リスク	LUN	警告
パフォーマンスサービスレベルポリシーに定義されたワークロードの LUN レイテンシしきい値を超過（ドキュメントのコンフォーマル遅延警告）	リスク	LUN	警告

管理ステーションイベント

管理ステーションイベントは、Unified Manager がインストールされているサーバのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
管理サーバのディスクスペースがほぼフル（ Document EvtUnifiedManagerDiskSpaceNearlyFull）	リスク	管理ステーション	警告
管理サーバのディスクスペースがフル（ Document EvtUnifiedManagerDiskSpaceFull）	インシデント	管理ステーション	重要
管理サーバのメモリが減少（ Document EvtUnifiedManagerMemoryLow）	リスク	管理ステーション	警告
管理サーバのメモリがほとんどない（ Document EvtUnifiedManagerMemoryAlmostOut）	インシデント	管理ステーション	重要
MySQL ログファイルのサイズが増加しました。再起動が必要です（ Document EvtMysqlLogFileSizeWarning）	インシデント	管理ステーション	警告
監査ログサイズ割り当ての合計がフルになります	リスク	管理ステーション	警告
syslog サーバ証明書の有効期限が近づいています	リスク	管理ステーション	警告
syslog サーバ証明書の有効期限が切れました	リスク	管理ステーション	エラー
監査ログファイルが改ざんされました	リスク	管理ステーション	警告
監査ログファイルが削除されました	リスク	管理ステーション	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
syslog サーバ接続エラー	リスク	管理ステーション	エラー
syslog サーバ設定が変更されました	イベント	管理ステーション	警告

影響範囲：パフォーマンス

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
パフォーマンスデータ分析への影響（ Document EvtUnifiedManagerDataMissingAnalyze ）	リスク	管理ステーション	警告
パフォーマンスデータ収集への影響（ Document EvtUnifiedManagerDataMissingCollection ）	インシデント	管理ステーション	重要



最後の 2 つのパフォーマンスイベントは、Unified Manager 7.2 でのみ使用されていたものです。これらのいずれかのイベントが新規の状態で存在している場合、Unified Manager ソフトウェアを新しいバージョンにアップグレードしてもイベントは自動的にパージされません。イベントを手動で解決済みの状態に移行する必要があります。

MetroCluster ブリッジイベント

MetroCluster ブリッジイベントは、ブリッジのステータス情報を提供します。これにより、MetroCluster over FC構成の潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ブリッジに到達不能（ Document EvtBridgeUnreachable ）	インシデント	MetroCluster ブリッジ	重要
ブリッジの温度が異常（ Document EvtBridgeTemperatureAbnormal ）	インシデント	MetroCluster ブリッジ	重要

MetroCluster 接続イベント

接続イベントは、クラスタのコンポーネント間の接続およびMetroCluster over FCおよびMetroCluster over IP構成のクラスタ間の接続に関する情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

両方の構成で共通のイベント

これらの接続イベントは、MetroCluster over FC構成とMetroCluster over IP構成で共通です。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
MetroCluster パートナー間のすべてのリンクが停止（Document EvtMetroClusterAllLinksBetweenPartnersDown）	インシデント	MetroCluster 関係	重要
ピアリングネットワーク経由で MetroCluster パートナーに到達できない（ドキュメント MetroCluster PartnersNotReachableOverPeeringNetwork）	インシデント	MetroCluster 関係	重要
影響を受ける MetroCluster ディザスタリカバリ機能（文書 MetroCluster DRStatusImpacted）	リスク	MetroCluster 関係	重要
MetroCluster 構成がスイッチオーバーされている（MetroClusterDRStatusImpacted）	リスク	MetroCluster 関係	警告

MetroCluster over FC構成

これらのイベントは、MetroCluster over FC構成に関係します。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
すべてのスイッチ間リンクが停止（Document EvtMetroClusterAllISLBetweenSwitchesDown）	インシデント	MetroCluster スイッチ間接続	重要
FC-SAS ブリッジからストレージスタックへのリンクが停止（Document EvtBridgeSasPortDown）	インシデント	MetroCluster ブリッジスタック接続	重要
MetroCluster 構成を部分的にスイッチオーバー（ドキュメント MetroCluster DRStatusPartiallyImpacted）	リスク	MetroCluster 関係	エラー
ノードから FC スイッチへのすべての FC-VI インターコネクトリンクが停止（Document EvtMccNodeSwitchFcvLinksDown）	インシデント	MetroCluster ノードのスイッチ接続	重要
ノードから FC スイッチへの一部の FC イニシエータリンクが停止（Document EvtMccNodeSwitchFcLinksOneOrMoreDown）	リスク	MetroCluster ノードのスイッチ接続	警告
ノードから FC スイッチへのすべての FC イニシエータリンクが停止（Document EvtMccNodeSwitchFcLinksDown）	インシデント	MetroCluster ノードのスイッチ接続	重要
スイッチから FC-SAS ブリッジへの FC リンクが停止（ドキュメント EvtMccSwitchgeFcLinksDown）	インシデント	MetroCluster スイッチのブリッジ接続	重要

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ノード間のすべての FC VI インターコネクトリンクが停止（ Document EvtMccInterNodeLinksDown ）	インシデント	ノード間の接続	重要
ノード間で 1 つ以上の FC VI インターコネクトリンクが停止（ ocument MccInterNodeLinksOneOrMoreDown ）	リスク	ノード間の接続	警告
ノードからブリッジへのリンクが停止（ Document EvtMccNodeBridgeLinksDown ）	インシデント	ノードのブリッジ接続	重要
ノードからストレージスタックへのすべての SAS リンクが停止（ Document EvtMccNodeStackLinksDown ）	インシデント	ノードスタック接続	重要
ノードからストレージスタックへの 1 つ以上の SAS リンクが停止（ ocument MccNodeStackLinksOneOrMoreDown ）	リスク	ノードスタック接続	警告

MetroCluster over IP構成

これらのイベントは、MetroCluster over IP構成に関係します。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
MetroCluster IPサイト間接続ステータスが「停止」（mccIntersitecivityStatusDown）	リスク	MetroCluster 関係	重要

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
MetroCluster - IPノードからスイッチへの接続がオフライン (IpPortStatusOffline)	リスク	ノード	エラー

MetroCluster スイッチイベント

MetroCluster over FC構成のMetroCluster スイッチイベントは、MetroCluster スイッチのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
スイッチの温度が異常（ドキュメント異常）	インシデント	MetroCluster スイッチ	重要
スイッチに到達不能（Document EvtSwitchUnreachable）	インシデント	MetroCluster スイッチ	重要
ファンの切り替えに失敗しました (DocumentEvtSwitchFans OneOrMoreFailed)	インシデント	MetroCluster スイッチ	重要
スイッチの電源装置に障害が発生しました（ドキュメント EvtSwitchPowerSupplies OneOrMoreFailed）	インシデント	MetroCluster スイッチ	重要

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
温度センサーの切り替えに失敗しました（ドキュメント EvtSwitchTemperatureSensorFailed） <div>  <div> このイベントは Cisco スイッチにのみ該当します。 </div> </div>	インシデント	MetroCluster スイッチ	重要

NVMe ネームスペースイベント

NVMe ネームスペースイベントは、ネームスペースのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

アスタリスク（*）は、Unified Manager イベントに変換された EMS イベントを示します。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
NVMeNS オフライン *（nvmespaceStatusOffline）	イベント	ネームスペース	情報
NVMeNS オンライン *（nvmespaceStatusOnline）	イベント	ネームスペース	情報
NVMeNS スペース不足 *（nvmeNamespaceOutOfSpace）	リスク	ネームスペース	警告
NVMe ネームスペースの破棄 *（nvmespaceDestroy）	イベント	ネームスペース	情報

影響範囲：パフォーマンス

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
NVMe ネームスペース IOPS の重大しきい値を超過（ドキュメント NvmeNamesaceIopsIncident）	インシデント	ネームスペース	重要
NVMe ネームスペース IOPS の警告しきい値を超過（ドキュメント NvmeNamesaceIopsWarning）	リスク	ネームスペース	警告
NVMe ネームスペース MBps の重大しきい値を超過（ドキュメント NvmeNamespaceMpsIncident）	インシデント	ネームスペース	重要
NVMe ネームスペース MBps の警告しきい値を超過（ドキュメント NvmeNamespaceMpsWarning）	リスク	ネームスペース	警告
NVMe ネームスペースレイテンシ / 処理の重大しきい値を超過（ドキュメント NvmeNamesaceLatencyIncident）	インシデント	ネームスペース	重要
NVMe ネームスペースレイテンシミリ秒 / 処理の警告しきい値を超過（ドキュメント NvmeNamesaceLatencyWarning）	リスク	ネームスペース	警告
NVMe ネームスペースレイテンシ / IOPS の重大しきい値を超過（ドキュメント NvmeNamespaceLatencyIopsIncident）	インシデント	ネームスペース	重要

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
NVMe ネームスペースレイテンシ / IOPS の警告しきい値を超過（ドキュメント NvmeNamespaceLatencyIopsWarning）	リスク	ネームスペース	警告
NVMe ネームスペースレイテンシ / MBps の重大しきい値を超過（ドキュメント NvmeNamespaceLatencyMbpsIncident）	インシデント	ネームスペース	重要
NVMe ネームスペースレイテンシ / MBps の警告しきい値を超過（ Document NvmeNamespaceLatencyMbpsWarning）	リスク	ネームスペース	警告

ノードイベント

ノードイベントは、ノードのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

アスタリスク（*）は、Unified Manager イベントに変換された EMS イベントを示します。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ノードのルートボリュームのスペースがほぼフル（ Document EvtClusterNodeRootVolumeSpaceNearlyFull）	リスク	ノード	警告
Cloud AWS MetaDataConnFail *（ Document CloudAwsMetadataConnFail）	リスク	ノード	エラー

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
Cloud AWS IAM クレデンシャルが期限切れ *（ Document CloudAwlamCredsExpired）	リスク	ノード	エラー
Cloud AWS IAM クレデンシャルが無効 *（ドキュメント CloudAwslamCredsInvalid）	リスク	ノード	エラー
Cloud AWS IAM クレデンシャルが見つからない *（ドキュメント Cloud AwslamCredsNotFound）	リスク	ノード	エラー
Cloud AWS IAM クレデンシャルが初期化されていない *（ドキュメント CloudAwslamCredsNotInitialized）	イベント	ノード	情報
Cloud AWS IAM ロールが無効 *（ DocumentCloudAwslamRoleInvalid）	リスク	ノード	エラー
Cloud AWS IAM RoleNotFound *（ドキュメント CloudAwslamRoleNotFound）	リスク	ノード	エラー
クラウド階層のホスト解決不可 *（文書 ObjstoreHostUnresolvable）	リスク	ノード	エラー
クラウド階層のクラスター間 LIF が停止している *（ ObjstoreInterClusterLifDown）	リスク	ノード	エラー

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
NFSv4 プールの 1 つを使い果たしました *（ nbladeNfsv4PoolExhaust）	インシデント	ノード	重要
要求とクラウド階層シグネチャの不一致 *（オシレチャ不一致）	リスク	ノード	エラー

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
QoS 監視メモリの最大化 *（文書 QosMonitorMemoryMaxed）	リスク	ノード	エラー
QoS 監視メモリの異常 *（文書化された QosMonitorMemoryAbated）	イベント	ノード	情報

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ノードの名前を変更（該当なし）	イベント	ノード	情報

影響範囲：パフォーマンス

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ノード IOPS の重大しき値を超過（ドキュメントノード lopsIncident）	インシデント	ノード	重要
ノード IOPS の警告しき値を超過（ドキュメントノード lopsWarning）	リスク	ノード	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ノード MBps の重大しき値を超過（ドキュメントノード MbpsIncident）	インシデント	ノード	重要
ノード MBps の警告しき値を超過（ドキュメントノード MbpsWarning）	リスク	ノード	警告
ノードレイテンシミリ秒 / 処理の重大しき値を超過（ドキュメントノードレイテンシインシデント）	インシデント	ノード	重要
ノードレイテンシミリ秒 / 処理の警告しき値を超過（ドキュメントノードレイテンシ警告）	リスク	ノード	警告
ノードの使用済みパフォーマンス容量の重大しき値を超過（ocNodePerfCapacityUsed Incident）	インシデント	ノード	重要
ノードの使用済みパフォーマンス容量の警告しき値を超過（ocNodePerfCapacityUsed Warning）	リスク	ノード	警告
ノードの使用済みパフォーマンス容量 - テイクオーバーの重大しき値を超過（ocNodePerfCapacityUsed TakeoverIncident）	インシデント	ノード	重要
ノードの使用済みパフォーマンス容量 - テイクオーバーの警告しき値を超過（ocNodePerfCapacityUsed TakeoverWarning）	リスク	ノード	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ノード利用率の重大しきい値を超過（ドキュメントノード利用率インシデント）	インシデント	ノード	重要
ノード利用率の警告しきい値を超過（ドキュメントノード利用率の警告）	リスク	ノード	警告
利用率の高いノード HA ペアのしきい値を超過（ocNodeHaPairOverUtilizedInformation）	イベント	ノード	情報
ノードディスク断片化の警告しきい値を超過（Document NodeDiskFragmentation Warning）	リスク	ノード	警告
使用済みパフォーマンス容量のしきい値を超過（ドキュメントノードのオーバー利用率警告）	リスク	ノード	警告
ノード動的しきい値を超過（Document NodeDynamicEventWarning）	リスク	ノード	警告

影響範囲：セキュリティ

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
アドバイザリ ID : NTAP-<_advisory ID__（ドキュメント x）	リスク	ノード	重要

NVRAM バッテリイベント

NVRAM バッテリイベントは、バッテリーのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
NVRAM バッテリ低下（Document EvtNvramBatteryLow）	リスク	ノード	警告
NVRAM バッテリ放電 (Document EvtNvramBatteryDischarged)	リスク	ノード	エラー
NVRAM バッテリ過充電（Document EvtNvramBatteryOverCharge）	インシデント	ノード	重要

ポートイベント

ポートイベントは、クラスタポートに関するステータスを提供します。これにより、ポートが停止しているかどうかなど、ポート上の変更や問題を監視できます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ポートステータス停止 (Document EvtPortStatus Down)	インシデント	ノード	重要

影響範囲：パフォーマンス

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ネットワークポート MBps の重大しきい値を超過（文書 NetworkPortMbpsIncident）	インシデント	ポート	重要
ネットワークポート MBps の警告しきい値を超過（文書ネットワークポートの MbpsWarning）	リスク	ポート	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
FCP ポート MBps の重大しきい値を超過（ドキュメント FcpPortMbpsIncident）	インシデント	ポート	重要
FCP ポート MBps の警告しきい値を超過（ドキュメント FcpPortMbpsWarning）	リスク	ポート	警告
ネットワークポート利用率の重大しきい値を超過（ドキュメント NetworkPortUtilizationIncident）	インシデント	ポート	重要
ネットワークポート利用率の警告しきい値を超過（ドキュメント NetworkPortUtilizationWarning）	リスク	ポート	警告
FCP ポート利用率の重大しきい値を超過（ドキュメント FcpPortUtilizationIncident）	インシデント	ポート	重要
FCP ポート利用率の警告しきい値を超過（ドキュメント FcpPortUtilizationWarning）	リスク	ポート	警告

電源装置イベント

電源装置イベントは、ハードウェアのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
1 つ以上の電源装置に障害が発生しました（ドキュメント EvtPowerSupplyOneOrMoreFailed）	インシデント	ノード	重要

保護イベント

保護イベントは、ジョブの失敗や中止を通知して、問題を監視できるようにします。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：保護

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
保護ジョブが失敗しました (DocumentEvtProtectionJobTaskFailed)	インシデント	ボリュームまたはストレージサービス	重要
保護ジョブが中止されました（Document EvtProtectionJobAborted）	リスク	ボリュームまたはストレージサービス	警告

qtree イベント

qtree イベントは、qtree の容量とファイルとディスクの制限に関する情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
qtree スペースがほぼフル（qtree の qtree eSpaceNearlyFull）	リスク	qtree	警告
qtree スペースがフル（Document QtreeSpaceFull）	リスク	qtree	エラー

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
qtree スペースが正常（ Document qtree eSpaceThresholdOk）	イベント	qtree	情報
qtree のファイル数がハード リミットに到達（ Document EvtQtreeFilesHardLimitReached）	インシデント	qtree	重要
qtree のファイル数がソフト リミットを超過（ Document QtreeFilesSoftLimit超過）	リスク	qtree	警告
qtree のスペースがハード リミットに到達（ Document QtreeSpaceHardLimitReached）	インシデント	qtree	重要
qtree のスペースがソフト リミットを超過（ Document QtreeSpaceSoftLimit超過）	リスク	qtree	警告

サービスプロセッサイベント

サービスプロセッサイベントは、プロセッサのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
サービスプロセッサが設定 されていません（ Document EvtServiceProcessorNotConfigured）	リスク	ノード	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
サービスプロセッサがオフラインです（ Document EvtServiceProcessorOffline）	リスク	ノード	エラー

SnapMirror 関係イベント

SnapMirror 関係イベントは、非同期 SnapMirror 関係と同期 SnapMirror 関係のステータス情報を提供します。これにより、潜在的な問題を監視できます。非同期 SnapMirror 関係イベントは、Storage VM とボリュームの両方に対して生成されますが、同期 SnapMirror 関係イベントはボリューム関係に対してのみ生成されます。Storage VM デザスタリカバリ関係を構成するコンスチチュエントボリュームについては、イベントは生成されません。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：保護

アスタリスク（*）は、Unified Manager イベントに変換された EMS イベントを示します。



SnapMirror 関係のイベントは、Storage VM デザスタリカバリで保護されているが、コンスチチュエントオブジェクト関係については生成されません。

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ミラーレプリケーションが正常でない（ Document SnapmirrorRelationshipUnhealthy）	リスク	SnapMirror 関係	警告
ミラーレプリケーションを切断（ DocumentEvtSnapmirrorRelationshipStateBrokenoff）	リスク	SnapMirror 関係	エラー
ミラーレプリケーションの初期化に失敗しました（ドキュメント SnapMirror 関係の初期化に失敗しました）	リスク	SnapMirror 関係	エラー

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ミラーレプリケーションの更新に失敗しました（ドキュメント：SnapmirrorRelationshipUpdateFailed）	リスク	SnapMirror 関係	エラー
ミラーレプリケーションの遅延エラー（「Document EvtSnapMirrorRelationshipLagError」）	リスク	SnapMirror 関係	エラー
ミラーレプリケーションの遅延警告（「Document」「SnapMirrorRelationshipLagWarning」）	リスク	SnapMirror 関係	警告
ミラーレプリケーションの再同期失敗（ドキュメント：SnapmirrorRelationshipResyncFailed）	リスク	SnapMirror 関係	エラー
同期レプリケーションが同期されていない*（syncSnapmirrorRelationshipOutofsync）	リスク	SnapMirror 関係	警告
同期レプリケーションをリストア*（同期 SnapMirror 関係は InSync）	イベント	SnapMirror 関係	情報
同期レプリケーションの自動再同期失敗*（syncSnapmirrorRelationshipAutoSyncRetryFailed）	リスク	SnapMirror 関係	エラー
ONTAP メディエーターがクラスタに追加されました（SnapmirrorMediatorAdded）	イベント	クラスタ	情報

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ONTAP メディエーターがクラスタから削除されました (snapmirrorMediatorRemoved)	イベント	クラスタ	情報
ONTAP メディエーターがクラスタから到達できません (snapmirrorMediatorUnreachable)	リスク	メディエーター	警告
ONTAP メディエーターにクラスタからアクセスできない (SnapmirrorMediatorMisconfigured)	リスク	メディエーター	エラー
ONTAP メディエーターの接続が再確立され、再同期されてSMBC (snapmirrorMediatorInQuorum) 用の準備が整いました。	イベント	メディエーター	情報

非同期ミラーバックアップ関係イベント

非同期ミラーバックアップ関係イベントは、非同期 SnapMirror 関係とバックアップ関係のステータス情報を提供します。これにより、潜在的な問題を監視できます。非同期ミラーバックアップ関係イベントは、ボリュームと Storage VM の両方の保護関係でサポートされます。ただし、Storage VM ディザスタリカバリではバックアップ関係のみがサポートされません。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：保護



また、Storage VM ディザスタリカバリで保護されているものの、コンスチチュエントオブジェクト関係については生成されません。

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
非同期ミラーバックアップが正常でない（ Document EvtMirrorVaultRelationshipUnhealthy）	リスク	SnapMirror 関係	警告
非同期ミラーバックアップを切断（ Document EvtMirrorRelationshipStateBrokenoff ）	リスク	SnapMirror 関係	エラー
非同期ミラーバックアップの初期化失敗（ Document EvtMirrorVaultRelationshipInitializeFailed ）	リスク	SnapMirror 関係	エラー
非同期ミラーバックアップの更新に失敗しました （ドキュメント EvtMirrorVaultRelationshipUpdateFailed ）	リスク	SnapMirror 関係	エラー
非同期ミラーバックアップの遅延エラー（ Document EvtMirrorVaultRelationshipLagError ）	リスク	SnapMirror 関係	エラー
非同期ミラーバックアップの遅延警告（ Document EvtMirrorVaultRelationshipLagWarning ）	リスク	SnapMirror 関係	警告
非同期ミラーバックアップの再同期失敗（ドキュメント EvtMirrorVaultRelationshipResyncFailed ）	リスク	SnapMirror 関係	エラー



「 SnapMirror update failure 」 イベントは、 Active IQ ポータル（ Config Advisor ） から生成されます。

Snapshot イベント

Snapshot イベントは、Snapshot のステータス情報を提供します。これにより、Snapshot の潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名、トラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
Snapshot の自動削除が無効（該当なし）	イベント	ボリューム	情報
Snapshot の自動削除が有効（該当なし）	イベント	ボリューム	情報
Snapshot の自動削除設定を変更（該当なし）	イベント	ボリューム	情報

SnapVault 関係イベント

SnapVault 関係イベントは、SnapVault 関係のステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：保護

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
非同期バックアップが正常でない（ ocument SnapVaultRelationshipUnhealthy ）	リスク	SnapMirror 関係	警告
非同期バックアップを切断（ Document EvtSnapVaultRelationshipStateBrokenoff ）	リスク	SnapMirror 関係	エラー
非同期バックアップの初期化に失敗しました（ Document EvtSnapVaultRelationshipInitializeFailed ）	リスク	SnapMirror 関係	エラー

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
非同期バックアップの更新に失敗しました（ドキュメント SnapVault 関係更新失敗）	リスク	SnapMirror 関係	エラー
非同期バックアップの遅延エラー（Document EvtSnapVaultRelationship LagError）	リスク	SnapMirror 関係	エラー
非同期バックアップの遅延警告（Document EvtSnapVaultRelationship LagWarning）	リスク	SnapMirror 関係	警告
非同期バックアップの再同期失敗（「Document EvtSnapvaultRelationship ResyncFailed」）	リスク	SnapMirror 関係	エラー

ストレージフェイルオーバー設定のイベント

ストレージフェイルオーバー（SFO）の設定のイベントは、ストレージフェイルオーバーが無効か設定されていないかに関する情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ストレージフェイルオーバーインターコネクトの1つ以上のリンクが停止（Document EvtSfoInterconnectOneOrMoreLinksDown）	リスク	ノード	警告
ストレージフェイルオーバーが無効になっている（Document EvtSfoSettingsDisabled）	リスク	ノード	エラー

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ストレージフェイルオーバーが設定されていません（Document EvtSfoSettingsNotConfigured）	リスク	ノード	エラー
ストレージフェイルオーバーの状態 - テイクオーバー（Document EvtSfoStateTakeover）	リスク	ノード	警告
ストレージフェイルオーバーの状態 - 部分的なギブバック（ドキュメント EvtSfoStatePartialGiveback）	リスク	ノード	エラー
ストレージフェイルオーバーノードのステータスが停止しています（Document EvtSfoNodeStatusDown）	リスク	ノード	エラー
ストレージフェイルオーバーのテイクオーバーを実行できません（ドキュメントエヴァットフォックステイクオーバー可能）	リスク	ノード	エラー

ストレージサービスイベント

ストレージサービスイベントは、ストレージサービスの作成とサブスクリプションに関する情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ストレージサービスを作成（該当なし）	イベント	ストレージサービス	情報

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ストレージサービスをサブスクライブ（該当なし）	イベント	ストレージサービス	情報
ストレージサービスをアンサブスクライブ（該当なし）	イベント	ストレージサービス	情報

影響範囲：保護

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
管理対象 SnapMirror 関係の予期しない削除が発生しました。また、StorageServiceUnsupportedRelationshipDeletion を参照してください	リスク	ストレージサービス	警告
ストレージサービスメンバーボリュームの予期しない削除（Document EvtStorageServiceUnexpectedVolumeDeletion）	インシデント	ストレージサービス	重要

ストレージシェルフイベント

ストレージシェルフイベントは、ストレージシェルフが異常な状態である場合に通知します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
異常な電圧範囲 (Document EvtShelfVoltageAbnormal)	リスク	ストレージシェルフ	警告
異常な電流範囲 (Document EvtShelfCurrentAbnormal)	リスク	ストレージシェルフ	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
異常な温度（ドキュメントシェルフ温度異常）	リスク	ストレージシェルフ	警告

Storage VM イベント

Storage VM（Storage Virtual Machine、SVM）イベントは、Storage VM（SVM）のステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

アスタリスク（*）は、Unified Manager イベントに変換された EMS イベントを示します。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
SVM CIFS サービスが停止（Document EvtVserverCifsServiceStatusDown）	インシデント	SVM	重要
SVM CIFS サービス未設定（該当なし）	イベント	SVM	情報
存在しない CIFS 共有への接続試行*（nbladeCifsNoPrivShare）	インシデント	SVM	重要
CIFS NetBIOS Name Conflict*（nbladeCifsNbNameConflict）	リスク	SVM	エラー
CIFS シャドウコピー処理失敗*（cifsShadowCopyFailure）	リスク	SVM	エラー
多数の CIFS 接続*（nbladeCifsManyAths）	リスク	SVM	エラー

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
最大 CIFS 接続数を超過 *（ nbladeCifsMaxOpenSameFile）	リスク	SVM	エラー
ユーザあたりの最大 CIFS 接続数を超過 *（ nbladeCifsMaxSessPerUserConn）	リスク	SVM	エラー
SVM FC/FCoE サービス停止（Document EvtVserverFcServiceStatusDown）	インシデント	SVM	重要
SVM iSCSI サービスが停止（Document EvtVserverIscsiServiceStatusDown）	インシデント	SVM	重要
SVM NFS サービス停止（Document EvtVserverNfsServiceStatusDown）	インシデント	SVM	重要
SVM FC / FCoE サービス未設定（該当なし）	イベント	SVM	情報
SVM iSCSI サービス未設定（該当なし）	イベント	SVM	情報
SVM NFS サービス未設定（該当なし）	イベント	SVM	情報
SVM が停止しました（Document EvtDown）	リスク	SVM	警告
AV サーバがビジーのため新しいスキャン要求を受け入れることができません *（ nbladeVscanConnBackPressure）	リスク	SVM	エラー

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ウィルススキャン用の AV サーバ接続がありません *（ nbladeVscanNoScannerConn）	インシデント	SVM	重要
AV サーバが登録されていません *（ nbladeVscanNoRegdScanner）	リスク	SVM	エラー
応答する AV サーバ接続がありません *（ nbladeVscanConnInactive）	イベント	SVM	情報
権限のないユーザが AV サーバにアクセスしようとした *（ nbladeVscanBadUserPrivAccess）	リスク	SVM	エラー
AV サーバが検出したウイルス *（ nbladeVscanVirusDetected）	リスク	SVM	エラー

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
SVM を検出（該当なし）	イベント	SVM	情報
SVM が削除されました（ 該当なし）	イベント	クラスタ	情報
SVM の名前が変更されました（該当なし）	イベント	SVM	情報

影響範囲：パフォーマンス

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
SVM IOPS の重大しきい値を超過（ドキュメント：vmIopsIncident）	インシデント	SVM	重要
SVM IOPS の警告しきい値を超過（ドキュメントの注意：警告）	リスク	SVM	警告
SVM MBps の重大しきい値を超過（ドキュメント：vmMbpsIncident）	インシデント	SVM	重要
SVM MBps の警告しきい値を超過（ドキュメントの vmMbpsWarning）	リスク	SVM	警告
SVM レイテンシの重大しきい値を超過（ドキュメント：vmLatencyIncident）	インシデント	SVM	重要
SVM レイテンシの警告しきい値を超過（ドキュメント：vmLatencyWarning）	リスク	SVM	警告

影響範囲：セキュリティ

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
監査ログ無効（VserverAuditLogDisabled）	リスク	SVM	警告
ログインバナーが無効になっています（ドキュメントの LoginBannerDisabled）	リスク	SVM	警告
SSH でセキュアでない暗号を使用（documentVserverSSHSecure）	リスク	SVM	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ログインバナーが変更されました（Document LoginBannerChanged）	リスク	SVM	警告
Storage VM のランサムウェア対策監視が無効（antiRansomwareSvmStateDisabled）	リスク	SVM	警告
Storage VM のランサムウェア対策監視が有効（ラーニングモード）（antiRansomwareSvmStateDryrun）	イベント	SVM	情報
Storage VM：ランサムウェア対策監視（ラーニングモード）（Document EvtSvmArwCandidate）に適している	イベント	SVM	情報

ユーザクォータイベントとグループクォータイベント

ユーザクォータイベントとグループクォータイベントは、ユーザクォータとユーザグループクォータの容量およびファイルとディスクの制限に関する情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ユーザクォータまたはグループクォータのディスクスペースがソフトリミットを超過（Document EvtUserOrGroupQuotaDiskSpaceSoftLimit超過）	リスク	ユーザクォータまたはグループクォータ	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ユーザクォータまたはグループクォータのディスク容量がハードリミットに到達（ Document EvtUserOrGroupQuotaDiskSpaceHardLimitReached ）	インシデント	ユーザクォータまたはグループクォータ	重要
ユーザクォータまたはグループクォータのファイル数がソフトリミットを超過（ Document EvtUserOrGroupQuotaFileCountSoftLimit未 超過）	リスク	ユーザクォータまたはグループクォータ	警告
ユーザクォータまたはグループクォータのファイル数がハードリミットに到達しました（ Document EvtUserOrGroupQuotaFileCountHardLimitReached ）	インシデント	ユーザクォータまたはグループクォータ	重要

ボリュームイベント

ボリュームイベントは、ボリュームのステータスに関する情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名、トラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

アスタリスク（*）は、Unified Manager イベントに変換された EMS イベントを示します。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリュームが制限状態（ Document EvtVolumeRestricted ）	リスク	ボリューム	警告
ボリュームがオフライン（ Document EvtVolumeOffline ）	インシデント	ボリューム	重要

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリュームは一部使用可能（ドキュメント別のボリューム）	リスク	ボリューム	エラー
ボリュームがアンマウントされています（該当なし）	イベント	ボリューム	情報
ボリュームをマウント（該当なし）	イベント	ボリューム	情報
ボリュームを再マウント（該当なし）	イベント	ボリューム	情報
ボリュームジャンクションパスが非アクティブ（Document EvtVolumeFunctionPathInactive）	リスク	ボリューム	警告
ボリュームのオートサイズを有効化（適用不可）	イベント	ボリューム	情報
ボリュームのオートサイズを無効化（該当なし）	イベント	ボリューム	情報
ボリュームのオートサイズの最大容量を変更（該当なし）	イベント	ボリューム	情報
ボリュームのオートサイズの増分サイズを変更（該当なし）	イベント	ボリューム	情報

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
シンプロビジョニングボリュームにスペースリスク（文書化「シンプロビジョニング」の「ボリュームスペースリスク」）	リスク	ボリューム	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリュームスペースがフル（ Document EvtVolumeFull ）	リスク	ボリューム	エラー
ボリュームスペースがほぼフル（ Document EvtVolumeNearlyFull ）	リスク	ボリューム	警告
ボリューム論理スペースがフル*（ volumeLogicalSpaceFull ）	リスク	ボリューム	エラー
ボリューム論理スペースがほぼフル*（ volumeLogicalSpaceNearlyFull ）	リスク	ボリューム	警告
ボリューム論理スペースが正常*（ volumeLogicalSpaceAlloc ）	イベント	ボリューム	情報
ボリュームの Snapshot リザーブスペースがフル（ Document EvtSnapshotFull ）	リスク	ボリューム	警告
Snapshot コピーが多すぎる（ ocumentEvtSnapshotTooMany ）	リスク	ボリューム	エラー
ボリュームの qtree クォータがオーバーコミット（ Document EvtVolumeQtreeQuotaOvercommitted ）	リスク	ボリューム	エラー
ボリュームの qtree クォータがほぼオーバーコミット（ Document EvtVolumeQtreeQuotaAlmostOvercommitted ）	リスク	ボリューム	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリュームの増加率が異常（ Document EvtVolumeGrowthRateAbnormal ）	リスク	ボリューム	警告
ボリュームのフルまでの日数（ Document EvtVolumeDaysUntilFullSoon ）	リスク	ボリューム	エラー
ボリュームのスペースギャランティを無効化（該当なし）	イベント	ボリューム	情報
ボリュームのスペースギャランティを有効化（該当なし）	イベント	ボリューム	情報
ボリュームのスペースギャランティを変更（該当なし）	イベント	ボリューム	情報
ボリュームの Snapshot リザーブのフルまでの日数（ Document EvtVolumeSnapshotReserveDaysUntilFullSoon ）	リスク	ボリューム	エラー
FlexGroup コンスティチュエントのスペースに問題あり * （ flexGroupConstitutsHaveSpaceIssues ）	リスク	ボリューム	エラー
FlexGroup コンスティチュエントのスペースステータスがすべて正常 * （ flexGroupConstitutionsSpaceStatusAllOK ）	イベント	ボリューム	情報
FlexGroup コンスティチュエントの inode に関する問題 * （ flexGroupConstitutionsHaveInodeIssues ）	リスク	ボリューム	エラー

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
FlexGroup コンスティ ュエント inode ステータ スすべて OK *（ flexGroupConstitutionsIno desStatusAllOK）	イベント	ボリューム	情報
WAFL ボリュームのオート サイズが失敗 *（ wafVolAutoSizeFail）	リスク	ボリューム	エラー
WAFL ボリュームのオート サイズ完了 *（ wafVolAutoSizeDone）	イベント	ボリューム	情報
FlexGroup ボリュームの 使用率が 80% を超えてい ます *	インシデント	ボリューム	エラー
FlexGroup ボリュームの 使用率が 90% を超えてい ます *	インシデント	ボリューム	重要
ボリュームのストレージ 効率化に問題があります （ ocVolumeAbnormalStorag eEfficiency Warning）	リスク	ボリューム	警告
利用率の低いボリューム のSnapshotリザーブ （volumeSnaphotReserve UnderutilizedWarning）	イベント	ボリューム	警告
ボリュームのSnapshotリ ザーブの利用率が低い （volumeSnaphotReserve UnderutilizedCleared）	イベント	ボリューム	警告

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリュームの名前を変更 （該当なし）	イベント	ボリューム	情報

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリュームを検出（該当なし）	イベント	ボリューム	情報
ボリュームが削除されました（該当なし）	イベント	ボリューム	情報

影響範囲：パフォーマンス

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
QoS ボリューム最大 IOPS の警告しきい値を超過（ドキュメントの QosVolumeMaxIopsWarning）	リスク	ボリューム	警告
QoS ボリューム最大 MBps の警告しきい値を超過（ドキュメントの QosVolumeMaxMbpsWarning）	リスク	ボリューム	警告
QoS ボリューム最大 IOPS/TB の警告しきい値を超過（ドキュメントの QosVolumeMaxIopsPerTbWarning）	リスク	ボリューム	警告
パフォーマンスサービスレベルポリシーに定義されたワークロードのボリュームレイテンシしきい値を超過（ドキュメントのコンフォーマル遅延警告）	リスク	ボリューム	警告
ボリューム IOPS の重大しきい値を超過（ドキュメントボリューム IopsIncident）	インシデント	ボリューム	重要
ボリューム IOPS の警告しきい値を超過（ドキュメントボリュームの IopsWarning）	リスク	ボリューム	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリューム MBps の重大しきい値を超過（ドキュメントボリュームの MbpsIncident）	インシデント	ボリューム	重要
ボリューム MBps の警告しきい値を超過（ドキュメントボリュームの警告）	リスク	ボリューム	警告
ボリュームレイテンシミリ秒 / 処理の重大しきい値を超過（ドキュメントボリュームレイテンシインシデント）	インシデント	ボリューム	重要
ボリュームレイテンシミリ秒 / 処理の警告しきい値を超過（ドキュメントボリュームレイテンシ警告）	リスク	ボリューム	警告
ボリュームキャッシュミス率の重大しきい値を超過（ドキュメント VolumeCacheMissRatioIncident）	インシデント	ボリューム	重要
ボリュームキャッシュミス率の警告しきい値を超過（ドキュメント VolumeCacheMissRatioWarning）	リスク	ボリューム	警告
ボリュームレイテンシ / IOPS の重大しきい値を超過（ドキュメントボリュームレイテンシ / IOPS の重大しきい値を超過）	インシデント	ボリューム	重要
ボリュームレイテンシ / IOPS の警告しきい値を超過（ドキュメントボリュームレイテンシ / IOPS の警告）	リスク	ボリューム	警告

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリュームレイテンシ / MBps の重大しきい値を超過（ドキュメントボリュームレイテンシ MbpsIncident）	インシデント	ボリューム	重要
ボリュームレイテンシ / MBps の警告しきい値を超過（ドキュメントボリュームレイテンシ MbpsWarning）	リスク	ボリューム	警告
ボリュームレイテンシ / アグリゲートの使用済みパフォーマンス容量の重大しきい値を超過（ocVolumeLatencyAggregatePerfCapacityUsedIncident）	インシデント	ボリューム	重要
ボリュームレイテンシ / アグリゲートの使用済みパフォーマンス容量の警告しきい値を超過（ocVolumeLatencyAggregatePerfCapacityUsedWarning）	リスク	ボリューム	警告
ボリュームレイテンシ / アグリゲート利用率の重大しきい値を超過（ocVolumeLatencyAggregateUtilizationIncident）	インシデント	ボリューム	重要
ボリュームレイテンシ / アグリゲート利用率の警告しきい値を超過（Document VolumeLatencyAggregateUtilizationWarning）	リスク	ボリューム	警告
ボリュームレイテンシ / ノードの使用済みパフォーマンス容量の重大しきい値を超過（文書 VolumeLatencyNodePerfCapacityUsedIncident）	インシデント	ボリューム	重要

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリュームレイテンシ / ノードの使用済みパフォーマンス容量の警告しきい値を超過（ ocVolumeLatencyNodePerfCapacityUsedWarning）	リスク	ボリューム	警告
ボリュームレイテンシ / ノードの使用済みパフォーマンス容量 - テイクオーバーの重大しきい値を超過（文書 VolumeLatencyAggregatePerfCapacityUsedTakeoverIncident）	インシデント	ボリューム	重要
ボリュームレイテンシ / ノードの使用済みパフォーマンス容量 - テイクオーバーの警告しきい値を超過（文書 VolumeLatencyAggregatePerfCapacityUsedTakeoverWarning）	リスク	ボリューム	警告
ボリュームレイテンシ / ノード利用率の重大しきい値を超過（ドキュメント VolumeLatencyNodeUtilizationIncident）	インシデント	ボリューム	重要
ボリュームレイテンシ / ノード利用率の警告しきい値を超過（ ocVolumeLatencyNodeUtilizationWarning）	リスク	ボリューム	警告

影響範囲：セキュリティ

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリュームのランサムウェア対策監視が有効（アクティブモード）（ <code>antiRansomwareVolumeStateEnabled</code> ）	イベント	ボリューム	情報
ボリュームのランサムウェア対策の監視が無効（ <code>antiRansomwareVolumeStateDisabled</code> ）	リスク	ボリューム	警告
ボリュームのランサムウェア対策監視が有効（ラーニングモード）（ <code>antiRansomwareVolumeStateDryrun</code> ）	イベント	ボリューム	情報
ボリュームのランサムウェア対策監視が一時停止（ラーニングモード）（ <code>antiRansomwareVolumeStateDryrunPaused</code> ）	リスク	ボリューム	警告
ボリュームのランサムウェア対策監視が一時停止（アクティブモード）（ <code>antiRansomwareVolumeStateEnablePaused</code> ）	リスク	ボリューム	警告
ボリュームのランサムウェア対策監視が無効化中（ <code>antiRansomwareVolumeStateDisableInProgress</code> ）	リスク	ボリューム	警告
ランサムウェア攻撃の発生（ <code>callHomeRansomwareActivitySeen</code> ）	インシデント	ボリューム	重要
ランサムウェア対策モニタリング（学習モード）に適したボリューム（ <code>DocumentEvtVolumeArwCandidate</code> ）	イベント	ボリューム	情報

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ランサムウェア対策モニタリング（アクティブモード）に適したボリューム（DocumentVolumeSuitedForActiveAntiRansomwareDetection）	リスク	ボリューム	警告
ボリュームでランサムウェア対策によるアラートが発生する（antiRansomwareFeatureNoisyVolume）	リスク	ボリューム	警告

影響範囲：データ保護

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリュームにローカルSnapshot保護が不十分です（volumeLacksLocalProtectionWarning）	リスク	ボリューム	警告
ボリュームにローカルSnapshot保護が不十分です（volumeLacksLocalProtectionCleared）	リスク	ボリューム	警告

ボリューム移動ステータスイベント

ボリューム移動のステータスのイベントは、ボリューム移動のステータスについて通知します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソースタイプ、および重大度が表示されます。

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリューム移動ステータス：実行中（該当なし）	イベント	ボリューム	情報

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ボリューム移動ステータス - 失敗（Document EvtVolumeMoveFailed）	リスク	ボリューム	エラー
ボリューム移動ステータス：完了（該当なし）	イベント	ボリューム	情報
ボリューム移動 - カットオーバー保留（Document EvtVolumeMoveCutoverDeffered）	リスク	ボリューム	警告

イベントウィンドウとダイアログボックスの概要

環境内の問題はイベントを通じて通知されます。イベント管理のインベントリページおよびイベントの詳細ページを使用して、すべてのイベントを監視できます。通知設定オプションダイアログボックスを使用して通知を設定できます。イベントの設定ページを使用して、イベントを無効または有効にすることができます。

通知ページ

Unified Manager サーバでは、イベントが生成されたときやユーザに割り当てられたときに通知を送信するように設定することができます。通知メカニズムを設定することもできます。たとえば、通知を E メールや SNMP トラップとして送信できます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

E メール

この領域では、アラート通知に関する次の E メール設定を行うことができます。

• * 送信元アドレス *

アラート通知の送信元 E メールアドレスを指定します。この値は、共有時にレポートの送信元アドレスとしても使用されます。送信元アドレスに「ActiveIQUnifiedManager@localhost.com」というアドレスがあらかじめ入力されている場合は、実際の作業用 E メールアドレスに変更して、すべての E メール通知が正常に配信されるようにしてください。

SMTP サーバ

この領域では、次の SMTP サーバ設定を行うことができます。

• * ホスト名または IP アドレス *

SMTP ホストサーバのホスト名を指定します。このホスト名は、指定した受信者へのアラート通知の送信

に使用されます。

- * ユーザー名 *

SMTP ユーザ名を指定します。SMTP ユーザ名は、SMTP サーバで SMTPAUTH が有効になっている場合にのみ必要です。

- * パスワード *

SMTP パスワードを指定します。SMTP ユーザ名は、SMTP サーバで SMTPAUTH が有効になっている場合にのみ必要です。

- * ポート *

アラート通知を送信する SMTP ホストサーバで使用されるポートを指定します。

デフォルト値は 25. です。

- * START/TLS* を使用します

このチェックボックスをオンにすると、TLS/SSL プロトコル（start_tls および StartTLS とも表記）を使用して SMTP サーバと管理サーバの間のセキュアな通信が確立されます。

- * SSL * を使用します

このチェックボックスをオンにすると、SSL プロトコルを使用して SMTP サーバと管理サーバの間のセキュアな通信が確立されます。

SNMP

この領域では、次の SNMP トラップ設定を行うことができます。

- * バージョン *

必要なセキュリティのタイプに応じて、使用する SNMP のバージョンを指定します。オプションには、バージョン 1、バージョン 3、認証を使用するバージョン 3、認証と暗号化を使用するバージョン 3 があります。デフォルト値はバージョン 1 です。

- * トラップ送信先ホスト *

管理サーバによって送信される SNMP トラップを受信するホスト名または IP アドレス（IPv4 または IPv6）を指定します。複数のトラップ送信先を指定するには、各ホストをカンマで区切ります。



「バージョン」や「アウトバウンドポート」などの他の SNMP 設定は、リスト内のすべてのホストで同じでなければなりません。

- * アウトバウンドトラップポート *

管理サーバによって送信されるトラップを SNMP サーバが受信する際に使用するポートを指定します。

デフォルト値は 162. です。

- * コミュニティ *

ホストにアクセスするためのコミュニティストリングです。

- * エンジン ID *

SNMP エージェントの一意の識別子を指定します。この識別子は、管理サーバによって自動的に生成されます。エンジン ID は、SNMP バージョン 3、認証付き SNMP バージョン 3、認証および暗号化付き SNMP バージョン 3 で使用できます。

- * ユーザー名 *

SNMP ユーザ名を指定します。ユーザ名は、SNMP バージョン 3、認証を使用する SNMP バージョン 3、および認証と暗号化を使用する SNMP バージョン 3 で使用できます。

- * 認証プロトコル *

ユーザの認証に使用するプロトコルを指定します。プロトコルオプションには MD5 と SHA があります。MD5 がデフォルト値です。認証プロトコルは、認証および暗号化を使用する SNMP バージョン 3 で使用できます。

- * 認証パスワード *

ユーザの認証時に使用するパスワードを指定します。認証パスワードは、SNMP バージョン 3（認証あり）および SNMP バージョン 3（認証および暗号化あり）で使用できます。

- * プライバシープロトコル *

SNMP メッセージの暗号化に使用するプライバシープロトコルを指定します。プロトコルのオプションには、AES 128 と DES があります。デフォルト値は AES 128 です。プライバシープロトコルは、認証および暗号化を使用する SNMP バージョン 3 で使用できます。

- * プライバシーパスワード *

プライバシープロトコルを使用する場合のパスワードを指定します。プライバシーパスワードは、認証と暗号化を使用する SNMP バージョン 3 で使用できます。

SNMP のオブジェクトとトラップの詳細については、をダウンロードしてください "[Active IQ Unified Manager MIB です](#)" NetApp Support Site から。

Event Management のインベントリページ

Event Management インベントリページでは、現在のイベントとそのプロパティのリストを表示できます。イベントについて、確認、解決、割り当てなどのタスクを実行することができます。特定のイベントに対するアラートを追加することもできます。

このページの情報は 5 分ごとに自動的に更新され、最新のイベントが表示されます。

フィルタコンポーネント

イベントリストに表示される情報をカスタマイズできます。次のコンポーネントを使用して、イベントのリストを絞り込むことができます。

- [表示] メニューでは、事前定義されたフィルタ選択のリストから選択できます。

これには、すべてのアクティブなイベント（新規および確認済みのイベント）、アクティブなパフォーマンスイベント、自分（ログインしているユーザ）に割り当てられているイベント、メンテナンス時間中に生成されたすべてのイベントなどの項目が含まれます。

- 検索ペインでキーワードの全体または一部を入力して、イベントのリストを絞り込むことができます。
- [フィルタ] ペインを起動する [フィルタ] ボタン。使用可能なすべてのフィールドとフィールド属性から選択して、イベントのリストを絞り込むことができます。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * 「*」に割り当てます

イベントを割り当てるユーザを選択できます。イベントをユーザに割り当てると、イベントリストの選択したイベントの該当するフィールドに、そのユーザの名前とイベントを割り当てた時刻が追加されます。

- 私

現在ログインしているユーザにイベントを割り当てます。

- 別のユーザ

[所有者の割り当て] ダイアログボックスが表示されますこのダイアログボックスでは ' イベントを他のユーザーに割り当てたり ' 再割り当てしたりできます所有権のフィールドを空白にすると、イベントの割り当てを解除できます。

- * 確認 *

選択したイベントを確認します。

イベントを確認すると、イベントリストの選択したイベントの該当するフィールドに、自分のユーザ名とイベントを確認した時刻が追加されます。確認したイベントについては、自分で対処する必要があります。



情報イベントに確認応答することはできません。

- * 解決済みとしてマーク *

イベントの状態を解決済みに変更できます。

イベントを解決すると、イベントリストの選択したイベントの該当するフィールドに、自分のユーザ名とイベントを解決した時刻が追加されます。イベントに対処したら、そのイベントを解決済みとしてマークする必要があります。

- * アラートの追加 *

アラートの追加ダイアログボックスが表示され、選択したイベントのアラートを追加できます。

- * レポート *

現在のイベントビューの詳細をカンマ区切り値（.csv）ファイルまたは PDF ドキュメントとしてエクスポートできます。

- * 列セレクトの表示 / 非表示 *

ページに表示する列とその表示順序を選択できます。

イベントのリスト





すべてのイベントの詳細がトリガーされた時刻の順に表示されます。

デフォルトでは、すべてのアクティブなイベントの表示には、影響レベルがインシデントまたはリスクである過去 7 日間の「新規」と「確認済み」のイベントが表示されます。

- * トリガー日時 *

イベントが生成された時刻。

- * 重大度 *

イベントの重大度：Critical（）、エラー（）、警告（）、および情報（）。

- * 状態 *

イベントの状態：新規、確認済み、解決済み、廃止。

- * 影響レベル *

イベントの影響レベル：インシデント、リスク、イベント、アップグレード。

- * 影響領域 *

イベントの影響領域：可用性、容量、パフォーマンス、保護、構成、または Security を選択します。

- * 名前 *

イベント名。名前を選択して、そのイベントのイベントの詳細ページを表示できます。

- * 出典 *

イベントが発生したオブジェクトの名前。名前を選択して、そのオブジェクトの健全性またはパフォーマンスの詳細ページを表示できます。

共有 QoS ポリシーの違反の場合、このフィールドには、IOPS または MBps が高い上位のワークロードオブジェクトのみが表示されます。このポリシーを使用する他のワークロードは、イベントの詳細ページに表示されます。

- * ソースタイプ *

イベントが関連付けられているオブジェクトのタイプ（Storage VM、ボリューム、qtree など）。

- * 割り当て先 *

イベントが割り当てられているユーザの名前。

- * イベントの発生元 *

イベントの生成元が「Active IQ ポータル」であるか、「Active IQ Unified Manager」から直接であるか。

- * アノテーション名 *

ストレージオブジェクトに割り当てられたアノテーションの名前。

- * メモ *

イベントに追加されたメモの数。

- * 未処理日数 *

イベントが最初に生成されてからの経過日数。

- * 割り当て時間 *

イベントがユーザに割り当てられてからの経過時間。1 週間を過ぎたイベントには、割り当て時のタイムスタンプが表示されます。

- * 承認者 *

イベントを確認したユーザの名前。イベントが確認されていない場合は空白になります。

- * 承認時間 *

イベントが確認されてからの経過時間。1 週間を過ぎたイベントには、承認時のタイムスタンプが表示されます。

- * 解決者 *

イベントを解決したユーザの名前。イベントが解決されていない場合は空白になります。

- * 解決時間 *

イベントが解決されてからの経過時間。1 週間を過ぎたイベントには、解決時のタイムスタンプが表示されます。

- * 廃止時刻 *

イベントの状態が「廃止」になった時刻。

イベントの詳細ページ

イベントの詳細ページでは、選択したイベントの重大度、影響レベル、影響領域、イベントソースなどの詳細を確認できます。問題を解決するための考えられる対処方法について、追加情報を確認することもできます。

- * イベント名 *

イベントの名前と最終確認時刻。

パフォーマンスイベント以外のイベントの場合は、状態が「新規」または「確認済み」のときは最終確認時刻が不明なため、この情報は表示されません。

- * イベント概要 *

イベントの簡単な概要。

イベント概要には、イベントがトリガーされた理由が含まれる場合があります。

- * 競合状態のコンポーネント *

動的なパフォーマンスイベントについて、クラスタの論理コンポーネントと物理コンポーネントを表すアイコンが表示されます。コンポーネントが競合状態にある場合は、アイコンが赤い丸で強調表示されます。

表示されるコンポーネントの概要については、「_ クラスタコンポーネントとその競合の原因」を参照してください。

「イベント情報」、「システム診断」、および「推奨処置」の各セクションについては、他のトピックで説明しています。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * メモアイコン *

イベントに関するメモを追加または更新したり、他のユーザが残したすべてのメモを確認したりできます。

- アクションメニュー *

- * 自分に割り当て *

イベントを自分に割り当てます。

- * 他のユーザーに割り当て *

[所有者の割り当て] ダイアログボックスが開きますこのダイアログボックスで ' イベントを他のユーザーに割り当てたり ' 再割り当てしたりできます

イベントをユーザに割り当てると、イベントリストの選択したイベントの該当するフィールドに、ユーザの名前とイベントが割り当てられた時刻が追加されます。

所有権のフィールドを空白にすると、イベントの割り当てを解除できます。

- * 確認 *

選択したイベントに確認応答し、アラート通知が繰り返し送信されないようにします。

イベントを確認すると、ユーザ名とそのイベントを確認した時刻が、選択したイベントのイベントリスト（確認済みのイベントのリスト）に追加されます。確認したイベントについては、自分で対処する必要があります。

- * 解決済みとしてマーク *

イベントの状態を解決済みに変更できます。

イベントを解決すると、イベントリスト（で解決）に選択したイベントのユーザ名と解決時刻が追加されます。イベントに対処したら、そのイベントを解決済みとしてマークする必要があります。

- * アラートの追加 *

アラートの追加ダイアログボックスが表示され、選択したイベントにアラートを追加できます。

[Event Information] セクションに表示される内容

イベントの詳細ページのイベント情報セクションでは、選択したイベントについて、イベントの重大度、影響レベル、影響領域、イベントソースなどの詳細を確認できます。

イベントタイプに該当しないフィールドは表示されません。イベントに関する次の詳細を確認できます。

- * イベントトリガー時間 *

イベントが生成された時刻。

- * 状態 *

イベントの状態：新規、確認済み、解決済み、廃止。

- * 原因を廃止 *

問題が修正されたなど、イベントを廃止する原因となった操作。

- * イベント期間 *

アクティブなイベント（新規および確認済みのイベント）の場合は、イベントが検出されてから最後に分析されるまでの時間です。廃止イベントの場合は、イベントが検出されてから解決されるまでの時間です。

このフィールドは、すべてのパフォーマンスイベントに対して表示されます。その他のタイプのイベントについては、解決されるか廃止になったあとにのみ表示されます。

- * 最終発生日 *

イベントがアクティブだった最終日時。

パフォーマンスイベントの場合は、イベントがアクティブであるかぎり、パフォーマンスデータの新しい収集が実行されるたびにこのフィールドが更新されるため、この値はイベントトリガー時間よりも新しい可能性があります。その他のタイプのイベントの場合は、状態が「新規」または「確認済み」のときは内容が更新されないため、このフィールドは非表示になります。

- * 重大度 *

イベントの重大度： Critical (❌)、エラー (❗)、警告 (⚠)、および情報 (ℹ)。

- * 影響レベル *

イベントの影響レベル：インシデント、リスク、イベント、アップグレード。

- * 影響領域 *

イベントの影響領域：可用性、容量、パフォーマンス、保護、構成、または Security を選択します。

- * 出典 *

イベントが発生したオブジェクトの名前。

共有 QoS ポリシーのイベントの詳細を表示している場合、このフィールドには、IOPS または MBps が高い上位のワークロードオブジェクトが最大 3 つ表示されます。

ソース名のリンクをクリックすると、そのオブジェクトの健全性またはパフォーマンスの詳細ページを表示できます。

- * ソースアノテーション *

イベントが関連付けられているオブジェクトのアノテーションの名前と値が表示されます。

このフィールドは、クラスタ、SVM、およびボリュームの健全性イベントに対してのみ表示されます。

- * ソースグループ *

該当オブジェクトがメンバーになっているすべてのグループの名前が表示されます。

このフィールドは、クラスタ、SVM、およびボリュームの健全性イベントに対してのみ表示されます。

- * ソースタイプ *

イベントが関連付けられているオブジェクトのタイプ (SVM、ボリューム、qtree など)。

- * クラスタ上 *

イベントが発生したクラスタの名前。

クラスタ名のリンクをクリックすると、そのクラスタの健全性またはパフォーマンスの詳細ページを表示できます。

- * 影響を受けるオブジェクト数 *

イベントの影響を受けるオブジェクトの数。

オブジェクトのリンクをクリックすると、インベントリページが表示され、現在このイベントの影響を受けているオブジェクトを確認できます。

このフィールドは、パフォーマンスイベントに対してのみ表示されます。

- * 影響を受けるボリューム *

このイベントの影響を受けるボリュームの数。

このフィールドは、ノードまたはアグリゲートのパフォーマンスイベントに対してのみ表示されます。

- * トリガーされたポリシー *

イベントを発行したしきい値ポリシーの名前。

ポリシー名にカーソルを合わせると、しきい値ポリシーの詳細を確認できます。アダプティブ QoS ポリシーの場合は、定義されているポリシー、ブロックサイズ、および割り当てのタイプ（割り当てスペースまたは使用スペース）も表示されます。

このフィールドは、パフォーマンスイベントに対してのみ表示されます。

- * ルール ID *

Active IQ プラットフォームイベントの場合、イベントの生成をトリガーされたルールの番号です。

- * 承認者 *

イベントに確認応答したユーザの名前と応答時刻。

- * 解決者 *

イベントを解決したユーザの名前と解決時刻。

- * 割り当て先 *

イベントに対応するように割り当てられているユーザーの名前。

- * アラート設定 *

アラートに関する次の情報が表示されます。

- 選択したイベントに関連付けられているアラートがない場合は、* アラートの追加 * リンクが表示されます。

リンクをクリックすると、[Add Alert] ダイアログボックスを開くことができます。

- 選択したイベントにアラートが 1 つ関連付けられている場合は、そのアラートの名前が表示されます。

リンクをクリックすると、[Edit Alert] ダイアログボックスを開くことができます。

- 選択したイベントにアラートが複数関連付けられている場合は、アラートの数が表示されます。

リンクをクリックすると、アラートセットアップページが開き、アラートの詳細が表示されます。

無効になっているアラートは表示されません。

- * 最後に送信された通知 *

最新のアラート通知が送信された日時。

- * 送信者 *

アラート通知の送信に使用されたメカニズム（E メールまたは SNMP トラップ）。

- * 前回のスクリプト実行 *

アラートが生成されたときに実行されたスクリプトの名前。

【提案されたアクション】セクションの表示内容

[イベントの詳細] ページの [提案されたアクション] セクションには、イベントの考えられる理由が表示され、独自の方法でイベントを解決できるようにいくつかのアクションが提案されます。推奨される対処方法は、イベントのタイプまたは超過したしきい値のタイプに基づいてカスタマイズされます。

この領域は、一部のタイプのイベントに対してのみ表示されます。

特定のアクションを実行するための手順など、推奨される多くのアクションについて追加情報を参照する * Help * リンクがページに表示される場合があります。一部の対処方法では、Unified Manager、ONTAP System Manager、OnCommand Workflow Automation、ONTAP CLI コマンド、またはこれらのツールの組み合わせを使用する場合があります。

これらの推奨される対処方法は、このイベントを解決するための一般的なガイダンスであることに注意してください。このイベントを解決するための対処方法は、環境に応じて決める必要があります。

オブジェクトやイベントを詳しく分析するには、* ワークロードの分析 * ボタンをクリックしてワークロードの分析ページを表示します。

イベントによっては、Unified Manager の詳細な診断によって 1 つの解決策が提供されることがあります。解決策がある場合は、* Fix it * ボタンで表示されます。このボタンをクリックすると、Unified Manager によってイベントの原因となっている問題が修正されます。

Active IQ プラットフォームイベントの場合、問題と解決策について解説したネットアップのナレッジベースの記事へのリンクがこのセクションに表示されることがあります。外部ネットワークへのアクセスがないサイトでは、ナレッジベースの記事の PDF がローカルで開きます。この PDF は、Unified Manager インスタンスに手動でダウンロードしたルールファイルに含まれています。

「システム診断」セクションの表示内容

イベント詳細ページのシステム診断セクションには、イベントに関連する問題の診断に役立つ情報が記載されています。

この領域は、一部のイベントに対してのみ表示されます。

一部のパフォーマンスイベントについては、トリガーされたイベントに関連するグラフが表示されます。通常は、過去 10 日間の IOPS または MBps のグラフとレイテンシのグラフです。これらのグラフを確認することで、イベントがアクティブなときにレイテンシに影響している、または影響を受けているストレージコンポーネントを特定できます。

動的なパフォーマンスイベントについては、次のグラフが表示されます。

- ワークロードレイテンシ - 競合状態のコンポーネントの Victim、Bully、Shark の上位のワークロードについて、レイテンシの履歴が表示されます。
- ワークロードアクティビティ - 競合状態のクラスタコンポーネントのワークロードの使用量に関する詳細が表示されます。
- リソースアクティビティ - 競合状態のクラスタコンポーネントの過去のパフォーマンス統計が表示されます。

一部のクラスタコンポーネントが競合状態にある場合は、これ以外のグラフが表示されます。

その他のイベントについては、ストレージオブジェクトに対して実行されている分析タイプの簡単な概要が表示されます。複数のパフォーマンスカウンタを分析するシステム定義のパフォーマンスポリシーについて、分析されたコンポーネントごとに 1 行以上の行が表示されることがあります。このシナリオでは、診断の横に、その診断で問題が見つかったかどうかを示す緑または赤のアイコンが表示されます。

Event Setup ページ

[Event Setup] ページに、無効なイベントのリストが表示され、関連するオブジェクトタイプやイベントの重大度などの情報が提供されます。イベントのグローバルな無効化や有効化などのタスクを実行することもできます。

このページにアクセスできるのは、アプリケーション管理者ロールまたはストレージ管理者ロールが割り当てられている場合のみです。

コマンドボタン

選択したイベントについて、各コマンドボタンを使用して次のタスクを実行できます。

• * 無効 *

[イベントの無効化] ダイアログボックスが開きます。このダイアログボックスを使用して、イベントを無効にできます。

• * 有効 *

以前に無効にするように選択したイベントを有効にします。

• * ルールのアップロード *

ルールのアップロードダイアログボックスを表示します。このダイアログボックスで、外部ネットワークアクセスのないサイトから Active IQ ルールファイルを Unified Manager に手動でアップロードできます。これらのルールがクラスタの AutoSupport メッセージに対して実行され、Active IQ プラットフォームで定義されているシステム構成、ケーブル配線、ベストプラクティス、および可用性についてのイベントが生成されます。

• * EMS イベント * を購読しなさい

[EMS イベントのサブスクライブ (Subscribe to EMS Events)] ダイアログボックスを開きます。このダイアログボックスでは、監視しているクラスタから特定の Event Management System (EMS ; イベント管理システム) イベントを受け取るようにサブスクライブできます。EMS では、クラスタで発生したイベントに関する情報を収集します。サブスクライブした EMS イベントに関する通知を受信すると、

適切な重大度を使用して Unified Manager イベントが生成されます。

リストビュー

リストビューには、無効になっているイベントに関する情報が表形式で表示されます。列のフィルタを使用して、表示するデータをカスタマイズできます。

- * イベント *

無効なイベントの名前が表示されます。

- * 重大度 *

イベントの重大度が表示されます。重大、エラー、警告、情報のいずれかです。

- * ソースタイプ *

イベントが生成されるソースタイプが表示されます。

DisableEvents ダイアログボックス

[イベントの無効化] ダイアログボックスには、イベントを無効にできるイベントタイプのリストが表示されます。イベントタイプの特定の重大度のイベントを無効にしたり、一連のイベントを無効にしたりできます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

[イベントのプロパティ] 領域

Event Properties 領域では、次のイベントプロパティを指定します。

- * イベントの重大度 *

重大度タイプに基づいてイベントを選択できます。タイプは、「重大」、「エラー」、「警告」、「情報」のいずれかになります。

- * イベント名に * が含まれています

名前に指定した文字を含むイベントをフィルタできます。

- * 一致イベント *

指定した重大度タイプとテキスト文字列に一致するイベントのリストが表示されます。

- * イベントを無効にする *

無効にするように選択したイベントのリストが表示されます。

イベント名に加えてイベントの重大度も表示されます。

選択したイベントについて、各コマンドボタンを使用して次のタスクを実行できます。

- * 保存して閉じる *

イベントタイプを無効にしてダイアログボックスを閉じます。

- * キャンセル *

変更内容を破棄してダイアログボックスを閉じます。

アラートの管理

特定のイベントまたは特定の重大度タイプのイベントが発生したときに自動的に通知を送信するアラートを設定できます。アラートをスクリプトに関連付けて、アラートがトリガーされたときにスクリプトが実行されるようにすることもできます。

アラートとは

イベントが継続的に発生している状況では、イベントが指定したフィルタ条件を満たす場合にのみ、Unified Manager はアラートを生成します。アラートを生成するイベントを選択できます。たとえば、スペースのしきい値を超えた場合やオブジェクトがオフラインになった場合などです。アラートをスクリプトに関連付けて、アラートがトリガーされたときにスクリプトが実行されるようにすることもできます。

フィルタ条件には、オブジェクトクラス、名前、またはイベントの重大度が含まれます。

アラート E メールに含まれる情報

Unified Manager のアラート E メールには、イベントのタイプ、イベントの重大度、イベントを原因で通知するために違反したポリシーまたはしきい値の名前、およびイベントの概要が記載されています。また、UI でイベントの詳細ページを確認できるように、各イベントのハイパーリンクも E メールメッセージ内に記載されています。

アラート E メールは、アラートを受け取るようにサブスクライブしているすべてのユーザに送信されます。

パフォーマンスカウンタ原因や容量の値が収集期間内に大きく変わった場合、同じしきい値ポリシーに対して重大イベントと警告イベントの両方が同時にトリガーされることがあります。この場合、警告イベント用と重大イベント用の E メールが 1 通ずつ届きます。これは、Unified Manager では、警告と重大のしきい値違反に対するアラートを受信するように個別に登録できるためです。

アラート Eメールの例を次に示します。

From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:

<https://10.11.12.13:443/events/94>

Source details:

<https://10.11.12.13:443/health/volumes/106>

Alert details:

<https://10.11.12.13:443/alerting/1>

アラートの追加

特定のイベントが生成されたときに通知するようにアラートを設定できます。アラートは、単一のリソース、リソースのグループ、または特定の重大度タイプのイベントについて設定することができます。通知を受け取る頻度を指定したり、アラートにスクリプトを関連付けたりできます。

- 必要なもの *
- イベント生成時に Active IQ Unified Manager サーバからユーザに通知を送信できるように、通知に使用するユーザの E メールアドレス、SMTP サーバ、SNMP トラップホストなどを設定しておく必要があります。
- アラートをトリガーするリソースとイベント、および通知するユーザのユーザ名または E メールアドレスを確認しておく必要があります。
- イベントに基づいてスクリプトを実行する場合は、Scripts ページを使用して Unified Manager にスクリプトを追加しておく必要があります。
- アプリケーション管理者またはストレージ管理者のロールが必要です。

アラートは、ここで説明するように、Alert Setup ページからアラートを作成するだけでなく、イベントを受信した後に Event Details ページから直接作成できます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Alert Setup * をクリックします。

2. [* Alert Setup*] ページで、[* Add] をクリックします。
3. [* アラートの追加*] ダイアログボックスで、[* 名前*] をクリックし、アラートの名前と概要を入力します。
4. [* リソース] をクリックし、アラートに含めるリソースまたはアラートから除外するリソースを選択します。

[* 次を含む名前 (* Name Contains)] フィールドでテキスト文字列を指定してフィルタを設定し、リソースのグループを選択できます。指定したテキスト文字列に基づいて、フィルタルールに一致するリソースのみが使用可能なリソースのリストに表示されます。指定するテキスト文字列では、大文字と小文字が区別されます。

あるリソースが対象に含めるルールと除外するルールの両方に該当する場合は、除外するルールが優先され、除外されたリソースに関連するイベントについてはアラートが生成されません。

5. [*Events] をクリックし、アラートをトリガーするイベント名またはイベントの重大度タイプに基づいてイベントを選択します。



複数のイベントを選択するには、Ctrl キーを押しながら選択します。

6. [*Actions] をクリックし、通知するユーザを選択し、通知頻度を選択し、SNMP トラップをトラップレシーバに送信するかどうかを選択し、アラートが生成されたときに実行するスクリプトを割り当てます。



ユーザに対して指定されている E メールアドレスを変更し、アラートを再び開いて編集しようとする、変更した E メールアドレスが以前に選択したユーザにマッピングされていないため、名前フィールドは空白になります。また、選択したユーザの E メールアドレスを Users ページで変更した場合、変更後の E メールアドレスは反映されません。

SNMP トラップを使用してユーザに通知することもできます。

7. [保存 (Save)] をクリックします。

アラートの追加例

この例は、次の要件を満たすアラートを作成する方法を示しています。

- アラート名： HealthTest
- リソース：名前に「abc」が含まれるすべてのボリュームを対象に含め、名前に「xyz」が含まれるすべてのボリュームを対象から除外する
- イベント：健全性に関するすべての重大なイベントを含みます
- アクション：「sample@domain.com」、「Test」スクリプトが含まれ、15 分ごとにユーザに通知する必要があります

[Add Alert] ダイアログボックスで、次の手順を実行します。

1. [名前] をクリックし、と入力します *HealthTest* を入力します。
2. [* リソース] をクリックし、[含める] タブで、ドロップダウン・リストから [* ボリューム] を選択します。
 - a. 入力するコマンド **abc***名前に「」を含むフィールドには、「abc」を含むボリュームが表示されま

す。

- b. 「* +」を選択します[All Volumes whose name contains 'abc']+* を使用可能なリソース領域から選択したリソース領域に移動します。
 - c. [除外する]をクリックし、と入力します **xyz**[名前に*が含まれています]フィールドで、[*追加]をクリックします。
3. [* イベント] をクリックし、[イベントの重要度] フィールドから [クリティカル *] を選択します。
 4. [Matching Events] 領域から [*All Critical Events] を選択し、 [Selected Events] 領域に移動します。
 5. [アクション]をクリックし、と入力します **sample@domain.com** [これらのユーザーにアラートを送信] フィールドに入力します。
 6. 15 分ごとにユーザに通知するには、「* 15 分ごとに通知する」を選択します。

指定した期間、受信者に繰り返し通知を送信するようにアラートを設定できます。アラートに対してイベント通知をアクティブにする時間を決める必要があります。

7. 実行するスクリプトの選択メニューで、* テスト * スクリプトを選択します。
8. [保存 (Save)] をクリックします。

アラートの追加に関するガイドライン

アラートは、クラスタ、ノード、アグリゲート、ボリュームなどのリソース、および特定の重大度タイプのイベントに基づいて追加できます。ベストプラクティスとして、重要なオブジェクトが属するクラスタを追加したあと、それらのすべてのオブジェクトについてのアラートを追加することを推奨します。

アラートを作成する際は、システムを効率的に管理できるように次のガイドラインと考慮事項を参考にしてください。

- Alert 概要の略

アラートを効果的に追跡できるように、概要をアラートに設定する必要があります。

- リソース

アラートが必要な物理リソースまたは論理リソースを決める必要があります。必要に応じて、リソースを追加したり除外したりできます。たとえば、アラートを設定してアグリゲートを詳細に監視する場合は、リソースのリストから必要なアグリゲートを選択する必要があります。

リソースのカテゴリを選択した場合（* + など）[All User or Group Quotas]+* を指定すると、そのカテゴリのすべてのオブジェクトに関するアラートが送信されます。



リソースとしてクラスタを選択しても、そのクラスタ内のストレージオブジェクトは自動的に選択されません。たとえば、すべてのクラスタのすべての重大イベントに対するアラートを作成した場合、受信するアラートの対象はクラスタの重大イベントのみです。ノードやアグリゲートなどの重大イベントに対するアラートは受信しません。

- イベントの重大度

イベントの重大度（重大、エラー、警告）ごとにアラートをトリガーするかどうかを決め、アラートをト

リガーする重大度を指定する必要があります。

- 選択したイベント

生成されるイベントのタイプに基づいてアラートを追加する場合は、アラートが必要なイベントを決める必要があります。

イベントの重大度を選択し、個々のイベントを選択しなかった場合（「選択したイベント」列を空白にした場合）は、カテゴリのすべてのイベントに関するアラートが表示されます。

- アクション

通知を受信するユーザのユーザ名と E メールアドレスを指定する必要があります。通知のモードとして SNMP トラップを指定することもできます。アラートが生成されたときに実行されるように、アラートにスクリプトを関連付けることができます。

- 通知の頻度

指定した期間、受信者に繰り返し通知を送信するようにアラートを設定できます。アラートに対してイベント通知をアクティブにする時間を決める必要があります。イベントが確認されるまでイベント通知を再送する場合は、通知を再送する頻度を決める必要があります。

- スクリプトを実行します

アラートにスクリプトを関連付けることができます。スクリプトはアラートが生成されると実行されます。

パフォーマンスイベントのアラートを追加しています

パフォーマンスイベントのアラートは、Unified Manager で受信する他のイベントと同様に、イベントごとに個別に設定することができます。また、すべてのパフォーマンスイベントを同じように扱い、同じユーザに E メールを送信する場合は、重大または警告のパフォーマンスイベントがトリガーされたときに通知する共通のアラートを作成することもできます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

次の例は、レイテンシ、IOPS、および MBps のすべての重大イベントに対するイベントを作成する方法を示しています。同じ方法で、すべてのパフォーマンスカウンタからイベントを選択したり、すべての警告イベントに対してイベントを選択したりできます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Alert Setup * をクリックします。
2. [* Alert Setup*] ページで、[* Add] をクリックします。
3. [* アラートの追加 *] ダイアログボックスで、[* 名前 *] をクリックし、アラートの名前と概要を入力します。
4. [* リソース] ページでは、リソースを選択しないでください。

リソースを選択していないため、クラスタ、アグリゲート、ボリュームなど、何に対するイベントを受信したかに関係なく、すべてのリソースにアラートが適用されます。

5. [* Events (イベント)] をクリックして、次の操作を実行します。
 - a. イベントの重大度リストで、* クリティカル * を選択します。
 - b. [Event Name Contains] フィールドに、と入力します *latency* をクリックし、矢印をクリックして一致するすべてのイベントを選択します。
 - c. [Event Name Contains] フィールドに、と入力します *iops* をクリックし、矢印をクリックして一致するすべてのイベントを選択します。
 - d. [Event Name Contains] フィールドに、と入力します *mbps* をクリックし、矢印をクリックして一致するすべてのイベントを選択します。
6. [* アクション *] をクリックし、[これらのユーザーに警告] フィールドで警告メールを受信するユーザーの名前を選択します。
7. SNMP トラップの発行やスクリプトの実行など、このページの他のオプションを設定します。
8. [保存 (Save)] をクリックします。

アラートのテスト

アラートをテストして、アラートが正しく設定されていることを確認できます。イベントがトリガーされるとアラートが生成され、設定した受信者にアラート E メールが送信されます。テストアラートを使用して、通知が送信されるかどうか、およびスクリプトが実行されるかどうかを確認できます。

- 必要なもの *
- 受信者の E メールアドレス、SMTP サーバ、SNMP トラップなどの通知を設定しておく必要があります。

Unified Manager サーバはこれらの設定を使用して、イベントが生成されたときにユーザに通知を送信します。

- スクリプトを割り当てて、アラートが生成されたときに実行するようにスクリプトを設定しておく必要があります。
- アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Alert Setup * をクリックします。
2. [* アラート設定 *] ページで、テストするアラートを選択し、[* テスト *] をクリックします。

アラートの作成時に指定した E メールアドレスにテストアラート E メールが送信されます。

解決済み / 廃止状態のイベントに対するアラートの有効化 / 無効化

アラートを送信するように設定したすべてのイベントについて、使用可能なすべての状態（新規、確認済み、解決済み、廃止）に移行したときにアラートメッセージが送信されます。イベントが解決済み / 廃止状態に移行したときにアラートを受信したくない場

合は、アラートを抑制するようグローバルに設定できます。

・必要なもの*

アプリケーション管理者またはストレージ管理者のロールが必要です。

デフォルトでは、イベントが解決済み / 廃止状態に移行する際にアラートは送信されません。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Alert Setup * をクリックします。
2. [* アラートの設定 * (* Alert Setup *)] ページで、項目の横にあるスライダコントロールを使用して、解決済み / 廃止イベントのアラート*を使用して、次のいずれかのアクションを実行します。

目的	手順
イベントが解決済みまたは廃止状態に移行したときのアラートの送信を停止します	スライダコントロールを左に移動します
イベントが解決済みまたは廃止状態に移行したときのアラートの送信を開始します	スライダコントロールを右に移動します

ディザスタリカバリのデスティネーションボリュームをアラート生成対象から除外します

ボリュームアラートを設定するときに、ボリュームまたはボリュームグループを識別する文字列をアラートダイアログボックスで指定できます。ただし、SVM のディザスタリカバリを設定している場合は、ソースボリュームとデスティネーションボリュームの名前が同じであるため、両方のボリュームについてアラートを受け取ることになります。

・必要なもの*

アプリケーション管理者またはストレージ管理者のロールが必要です。

ディザスタリカバリのデスティネーションボリュームに対するアラートを無効にするには、デスティネーション SVM の名前を含むボリュームを除外します。これは、ボリュームイベントの識別子に SVM 名とボリューム名の両方が「<svm_name> : /<volume_name>」の形式で含まれていることを確認したものです。

次の例は、プライマリ SVM 「vs1」上のボリューム「vol1」に対するアラートを作成し、SVM 「vs1-dr」にある同じ名前のボリュームはアラート生成の対象から除外する方法を示しています。

[Add Alert] ダイアログボックスで、次の手順を実行します。

手順

1. [* 名前 *] をクリックして、アラートの名前と概要を入力します。
2. [* リソース (* Resources)] をクリックし、[* 含める * (* Include *)] タブを選択します。
 - a. ドロップダウンリストから「* Volume 」を選択し、と入力します ***vol1***名前に「」を含むフィールドには、名前に「vol1」を含むボリュームが表示されます。

- b. 「* +」を選択します[All Volumes whose name contains 'vol1']**[Available Resources]** 領域から **[Selected Resources]** 領域に移動します。
 3. [除外]タブを選択し、[ボリューム]を選択して、と入力します **vs1-dr**[名前に*が含まれています]フィールドで、[*追加]をクリックします。
- SVM 「vs1-dr」のボリューム「vol1」については、アラートは生成されません。
4. 「* Events」をクリックして、ボリュームに適用するイベントを選択します。
 5. [* アクション*]をクリックし、[これらのユーザーに警告]フィールドで警告メールを受信するユーザーの名前を選択します。
 6. SNMP トラップを発行してスクリプトを実行するために、このページの他のオプションを設定し、* Save * をクリックします。

アラートの表示

さまざまなイベントに対して作成されたアラートのリストは、[Alert Setup] ページで表示できます。アラートのプロパティとして、アラート概要、通知の方法と頻度、アラートをトリガーするイベント、アラートの E メール受信者、クラスタ、アグリゲート、ボリュームなどの影響を受けるリソースなどを表示することもできます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ステップ

1. 左側のナビゲーションペインで、* Storage Management * > * Alert Setup * をクリックします。

アラートのリストは、Alert Setup ページに表示されます。

アラートの編集

関連付けられているリソース、イベント、受信者、通知オプション、通知頻度など、アラートのプロパティを編集することができます。 および関連するスクリプト。

- 必要なもの *

アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Alert Setup * をクリックします。
2. [* アラート設定 * (* Alert Setup *)] ページで、編集するアラートを選択し、[* 編集 * (* Edit *)] をクリックします。
3. [* アラートの編集*] ダイアログボックスで、名前、リソース、イベント、アクションの各セクションを編集します。必要に応じて。

アラートに関連付けられているスクリプトについては、変更と削除が可能です。

4. [保存 (Save)] をクリックします。

アラートの削除

不要になったアラートを削除できます。たとえば、特定のリソースが Unified Manager の監視対象でなくなった場合、そのリソースに対して作成されたアラートを削除できます。

- 必要なもの *

アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Alert Setup * をクリックします。
2. [* アラート設定 * (* Alert Setup *)] ページで、削除するアラートを選択し、[* 削除 * (* Delete *)] をクリックします。
3. [はい] をクリックして、削除要求を確定します。

概要のアラートウィンドウとダイアログボックス

[Add Alert] ダイアログボックスを使用して、イベントに関する通知を受信するようにアラートを設定する必要があります。アラートのリストは、Alert Setup ページからも表示できます。

Alert Setup ページ

[Alert Setup] ページには、アラートのリストが表示され、アラート名、ステータス、通知方法、および通知頻度に関する情報が提供されます。また、このページでアラートを追加、編集、削除、有効化、無効化することもできます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

コマンドボタン

- * 追加 *。

アラートの追加ダイアログボックスが表示され、新しいアラートを追加できます。

- * 編集 *。

アラートの編集ダイアログボックスが表示され、選択したアラートを編集できます。

- * 削除 *

選択したアラートを削除します。

- * 有効 *

選択したアラートを有効にして通知を送信します。

- * 無効 *

通知の送信を一時的に停止する場合に、選択したアラートを無効にします。

- * テスト *

選択したアラートをテストして、アラートの追加後または編集後にその設定を検証します。



- * 解決済み / 廃止状態のイベントに関するアラート *

イベントが解決済みまたは廃止状態に移行した場合のアラートの送信を有効または無効にすることができます。これにより、ユーザは不要な通知を受信できます。

リストビュー

リストビューには、作成されたアラートに関する情報が表形式で表示されます。列のフィルタを使用して、表示するデータをカスタマイズできます。アラートを選択して、そのアラートに関する詳細を詳細領域に表示することもできます。

- * ステータス *

アラートが有効になっているかどうかを示します () または無効 () 。

- * 警告 *

アラートの名前が表示されます。

- * 概要 *

アラートの概要が表示されます。

- * 通知方法 *

アラートに対して選択された通知方式が表示されます。E メールまたは SNMP トラップを使用してユーザに通知できます。

- * 通知頻度 *

イベントが確認または解決されるか、廃止状態に設定されるまでの間、管理サーバが通知を送信する頻度 (分) を示します。

詳細領域

詳細領域には、選択したアラートに関する詳細情報が表示されます。

- * アラート名 *

アラートの名前が表示されます。

- * Alert 概要 *

アラートの概要が表示されます。

- * イベント *

アラートをトリガーするイベントが表示されます。

- * リソース *

アラートをトリガーするリソースが表示されます。

- * が含まれます

アラートをトリガーするリソースのグループが表示されます。

- * 除外 *

アラートをトリガーしないリソースのグループが表示されます。

- * 通知方法 *

アラートの通知方式が表示されます。

- * 通知頻度 *

イベントが確認または解決されるか、廃止状態に設定されるまでの間、管理サーバがアラート通知を送信する頻度が表示されます。

- * スクリプト名 *

選択したアラートに関連付けられているスクリプトの名前が表示されます。このスクリプトはアラートが生成されたときに実行されます。

- * 電子メール受信者 *

アラート通知を受信するユーザの E メールアドレスが表示されます。

Add Alert ダイアログボックス

アラートを作成すると、特定のイベントが生成されたときに通知されるため、問題にすばやく対処し、環境への影響を最小限に抑えることができます。アラートは、単一のリソース、一連のリソース、および特定の重大度タイプのイベントについて作成することができます。アラートの通知方式と通知頻度を指定することもできます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

名前

この領域では、アラートの名前と概要を指定できます。

- * アラート名 *

アラート名を指定できます。

• * Alert 概要 *

アラートの概要を指定できます。

リソース

この領域では、アラートをトリガーする対象のリソースを個別に選択したり、動的ルールに基づいてリソースをグループ化したりできます。a_dynamic rule_ は、指定したテキスト文字列に基づいてフィルタリングされるリソースのセットです。ドロップダウンリストからリソースタイプを選択してリソースを検索するか、正確なリソース名を指定して特定のリソースを表示できます。

いずれかのストレージオブジェクトの詳細ページからアラートを作成する場合は、ストレージオブジェクトが自動的にアラートに含まれます。

• * インクルード *

アラートをトリガーする対象に含めるリソースを指定できます。テキスト文字列を指定すると、その文字列に一致するリソースをグループ化し、そのグループをアラートの対象として選択できます。たとえば、「abc」という文字列が名前に含まれるすべてのボリュームをグループ化できます。

• * 除外 *

アラートをトリガーする対象から除外するリソースを指定できます。たとえば、「xyz」という文字列が名前に含まれるすべてのボリュームを除外することができます。

除外 (Exclude) タブは ' 特定のリソースタイプのすべてのリソース () を選択した場合にのみ表示されます <<All Volumes>> または <<All Volumes whose name contains 'xyz'>>[]

あるリソースが対象に含めるルールと除外するルールの両方に該当する場合は、除外するルールが優先され、イベントについてはアラートが生成されません。

イベント

この領域では、アラートを作成するイベントを選択できます。アラートは特定の重大度のイベントに対して作成するか、一連のイベントについて作成することができます。

複数のイベントを選択するには、Ctrl キーを押しながら選択します。

• * イベントの重大度 *

重大度タイプに基づいてイベントを選択できます。タイプは、「重大」、「エラー」、「警告」のいずれかになります。

• * イベント名に * が含まれています

名前に指定した文字を含むイベントを選択できます。

アクション

この領域では、アラートがトリガーされたときに通知するユーザを指定できます。通知方式と通知頻度を指定することもできます。

- * これらのユーザーに警告 *

通知を受信するユーザの E メールアドレスまたはユーザ名を指定できます。

ユーザに対して指定されている E メールアドレスを変更し、アラートを再び開いて編集しようとする、変更した E メールアドレスが以前に選択したユーザにマッピングされていないため、名前フィールドは空白になります。また、選択したユーザの E メールアドレスを Users ページで変更した場合、変更した E メールアドレスはそのユーザに対して更新されません。

- * 通知頻度 *

イベントが確認または解決されるか、廃止状態に設定されるまでの間、管理サーバが通知を送信する頻度を指定できます。

次のいずれかの通知方式を選択できます。

- 1 回だけ通知します
- 指定した頻度で通知します
- 指定した期間内の指定した頻度で通知します

- * 問題 SNMP トラップ *

このチェックボックスをオンにすると、グローバルに設定された SNMP ホストに SNMP トラップを送信するかどうかを指定できます。

- * スクリプトの実行 *

アラートにカスタムスクリプトを追加できます。このスクリプトはアラートが生成されたときに実行されます。



この機能がユーザインターフェイスに表示されない場合は、管理者によって無効にされています。この機能は、必要に応じて、* Storage Management * > * Feature Settings * から有効にできます。

コマンドボタン

- * 保存 *

アラートを作成してダイアログボックスを閉じます。

- * キャンセル *

変更内容を破棄してダイアログボックスを閉じます。

EditAlert ダイアログボックス

関連付けられているリソース、イベント、スクリプト、通知オプションなど、アラートのプロパティを編集することができます。

名前

この領域では、アラートの名前と概要を編集できます。

- * アラート名 *

アラート名を編集できます。

- * Alert 概要 *

アラートの概要を指定できます。

- * アラートの状態 *

アラートを有効または無効にできます。

リソース

この領域では、アラートをトリガーする対象のリソースを個別に選択したり、動的ルールに基づいてリソースをグループ化したりできます。ドロップダウンリストからリソースタイプを選択してリソースを検索するか、正確なリソース名を指定して特定のリソースを表示できます。

- * インクルード *

アラートをトリガーする対象に含めるリソースを指定できます。テキスト文字列を指定すると、その文字列に一致するリソースをグループ化し、そのグループをアラートの対象として選択できます。たとえば、「vol0」という文字列が名前に含まれるすべてのボリュームをグループ化することができます。

- * 除外 *

アラートをトリガーする対象から除外するリソースを指定できます。たとえば、「xyz」という文字列が名前に含まれるすべてのボリュームを除外することができます。



除外 (Exclude) タブは '特定のリソースタイプのすべてのリソース (+ など) を選択した場合にのみ表示されます[[All Volumes](#)]+ または <<All Volumes whose name contains 'xyz'>>[]

イベント

この領域では、アラートをトリガーするイベントを選択できます。アラートは特定の重大度のイベントに対してトリガーするか、一連のイベントを指定してトリガーできます。

- * イベントの重大度 *

重大度タイプに基づいてイベントを選択できます。タイプは、「重大」、「エラー」、「警告」のいずれかになります。

- * イベント名に * が含まれています

名前に指定した文字を含むイベントを選択できます。

アクション

この領域では、通知方式と通知頻度を指定できます。

- * これらのユーザーに警告 *

通知を受け取る E メールアドレスまたはユーザ名を編集できます。新しい E メールアドレスまたはユーザ名を指定することもできます。

- * 通知頻度 *

イベントが確認または解決されるか、廃止状態に設定されるまでの間、管理サーバが通知を送信する頻度を編集できます。

次のいずれかの通知方式を選択できます。

- 1 回だけ通知します
- 指定した頻度で通知します
- 指定した期間内の指定した頻度で通知します

- * 問題 SNMP トラップ *

グローバルに設定された SNMP ホストに SNMP トラップを送信するかどうかを指定できます。

- * スクリプトの実行 *

アラートにスクリプトを関連付けることができます。このスクリプトはアラートが生成されたときに実行されます。

コマンドボタン

- * 保存 *

変更内容を保存してダイアログボックスを閉じます。

- * キャンセル *

変更内容を破棄してダイアログボックスを閉じます。

スクリプトの管理

Unified Manager で複数のストレージオブジェクトを自動的に変更または更新するスクリプトを作成することができます。スクリプトはアラートに関連付けられます。イベントによってアラートがトリガーされるとスクリプトが実行されます。カスタムスクリプトをアップロードし、アラートが生成されたときの動作をテストすることができます。

スクリプトを Unified Manager にアップロードして実行する機能は、デフォルトで有効になっています。セキュリティ上の理由からこの機能を許可しない場合は、* ストレージ管理 * > * 機能設定 * からこの機能を無効にできます。

- 関連情報 *

"スクリプトアップロード機能の有効化と無効化"

スクリプトとアラートの連携方法

Unified Manager でイベントに対するアラートが発生したときにスクリプトが実行されるように、スクリプトにアラートを関連付けることができます。スクリプトを使用して、ストレージオブジェクトの問題を解決したり、イベントの生成元のストレージオブジェクトを特定したりできます。

Unified Manager でイベントに対するアラートが生成されると、指定した受信者にはアラート E メールが送信されます。アラートがスクリプトに関連付けられている場合は、そのスクリプトが実行されます。スクリプトに渡された引数の詳細をアラート E メールから取得できます。



カスタムスクリプトを作成し、そのスクリプトを特定のイベントタイプのアラートに関連付けた場合、そのイベントタイプのカスタムスクリプトに基づいて操作が実行されます。 * Fix it * アクションは、デフォルトでは管理アクションページまたは Unified Manager ダッシュボードで使用できません。

スクリプトの実行には次の引数が使用されます。

- -eventID
- -eventName
- -eventSeverity
- -eventSourceID
- -eventSourceName
- -eventSourceType
- -eventState
- -eventArgs

これらの引数をスクリプトで使用して、関連するイベントの情報を収集したり、ストレージオブジェクトを変更したりできます。

スクリプトから引数を取得する例

```
`print "$ARGV[0] : $ARGV[1]\n"`  
`print "$ARGV[7] : $ARGV[8]\n"`
```

アラートが生成されると、このスクリプトが実行され、次の出力が表示されます。

```
-`eventID : 290`  
-`eventSourceID : 4138`
```


スクリプトの追加

Unified Manager でスクリプトを追加し、アラートに関連付けることができます。アラートが生成されるとこれらのスクリプトが自動的に実行されるため、イベントが生成されたストレージオブジェクトに関する情報を取得できます。

- 必要なもの *
- Unified Manager サーバに追加するスクリプトを作成して保存しておく必要があります。
- サポートされるスクリプトのファイル形式は、Perl、Shell、PowerShell、Python、およびです .bat ファイル。

Unified Manager がインストールされているプラットフォーム	サポートされている言語
VMware	Perl / シェルスクリプト
Linux の場合	Perl、Python、シェルの各スクリプト
Windows の場合	PowerShell、Perl、Python、.bat スクリプト

- Perl スクリプトを使用するには、Perl が Unified Manager サーバにインストールされている必要があります。VMware 環境には Perl 5 がデフォルトでインストールされ、Perl 5 のサポート対象のみがスクリプトでサポートされます。Unified Manager のあとに Perl をインストールした場合は、Unified Manager サーバを再起動する必要があります。
- PowerShell スクリプトを使用するには、スクリプトを実行するための適切な PowerShell 実行ポリシーが Windows サーバで設定されている必要があります。



スクリプトでログファイルを作成してアラートスクリプトの進捗を追跡する場合は、ログファイルが Unified Manager のインストールフォルダ内に作成されないようにする必要があります。

- アプリケーション管理者またはストレージ管理者のロールが必要です。

カスタムスクリプトをアップロードし、アラートに関するイベントの詳細を収集できます。



この機能がユーザインターフェイスに表示されない場合は、管理者によって無効にされています。この機能は、必要に応じて、* Storage Management * > * Feature Settings * から有効にできます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Scripts * をクリックします。
2. [* スクリプト *] ページで、[* 追加] をクリックします。
3. [スクリプトの追加 *] ダイアログボックスで、[* 参照 *] をクリックしてスクリプトファイルを選択します。
4. 選択したスクリプトの概要を入力します。
5. [追加 (Add)] をクリックします。

- 。関連情報 *

"スクリプトアップロード機能の有効化と無効化"

スクリプトの削除

不要または無効になったスクリプトは、 Unified Manager から削除できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- スクリプトがアラートに関連付けられていないことを確認する必要があります。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Scripts * をクリックします。
2. [* スクリプト *] ページで、削除するスクリプトを選択し、 [* 削除] をクリックします。
3. [警告 *] ダイアログボックスで、 [はい] をクリックして削除を確認します。

スクリプトの実行テスト

ストレージオブジェクトに対してアラートが生成されたときにスクリプトが正しく実行されるかどうかを確認することができます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- サポートされるファイル形式のスクリプトを Unified Manager にアップロードしておく必要があります。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Scripts * をクリックします。
2. [* Scripts] ページで、テストスクリプトを追加します。
3. 左側のナビゲーションペインで、 * Storage Management * > * Alert Setup * をクリックします。
4. [* Alert Setup*] ページで、次のいずれかの操作を実行します。

目的	手順
アラートを追加します	<ol style="list-style-type: none">a. [追加（Add）] をクリックします。b. [アクション] セクションで、アラートをテストスクリプトに関連付けます。
アラートを編集する	<ol style="list-style-type: none">a. アラートを選択し、 * 編集 * をクリックします。b. [アクション] セクションで、アラートをテストスクリプトに関連付けます。

5. [保存（ Save ）] をクリックします。
 6. [* アラート設定 *] ページで、追加または変更したアラートを選択し、[* テスト *] をクリックします。
- 「-test」引数を指定してスクリプトが実行され、アラートの作成時に指定した E メールアドレスに通知アラートが送信されます。

Unified Manager の CLI コマンドがサポートされています

ストレージ管理者は、CLI コマンドを使用して、クラスタ、アグリゲート、ボリューム、qtree、および LUN：CLI コマンドを使用して、Unified Manager の内部データベースと ONTAP データベースを照会できます。CLI コマンドは、処理の開始時または終了時に実行されるスクリプト、アラートがトリガーされたときに実行されるスクリプトでも使用できます。

すべてのコマンドの前にコマンドを入力する必要があります `um cli login` 認証用の有効なユーザ名とパスワードを指定します。



`_um run_command`を実行するには、アカウントに`_console_application`アクセス権があることを確認します。

CLI コマンド	説明	出力
<code>um cli login -u <username> [-p <password>]</code>	CLI にログインします。セキュリティ上の理由から、「-u」オプションのあとにはユーザ名のみを入力してください。この方法でパスワードを入力すると、パスワードの入力を求められます。パスワードは履歴テーブルまたはプロセステーブルには保存されません。セッションはログインしてから 3 時間が経過すると期限切れになり、3 時間が経過するとユーザは再度ログインする必要があります。	対応するメッセージを表示します。
<code>um cli logout</code>	CLI からログアウトします。	対応するメッセージを表示します。
<code>um help</code>	第 1 レベルのすべてのサブコマンドを表示します。	第 1 レベルのすべてのサブコマンドを表示します。

CLI コマンド	説明	出力
<code>um run cmd [-t <timeout>] <cluster> <command></code>	1 つ以上のホストでコマンドを実行する最も簡単な方法です。主に、アラートのスクリプト化を使用して ONTAP で処理を取得または実行します。オプションの <code>timeout</code> 引数で、コマンドがクライアントで完了するのを待機する最大時間（秒）を設定できます。デフォルトは 0（無期限に待機）です。	ONTAP から受け取ったとおり。
<code>um run query <sql command></code>	SQL クエリを実行します。データベースからの読み取りが許可されるクエリのみです。更新、挿入、削除の各操作はサポートされていません。	結果は表形式で表示されます。空のセットが返された場合、または構文エラーや無効な要求がある場合は、該当するエラーメッセージが表示されます。
<code>um datasource add -u <username> -P <password> [-t <protocol>] [-p <port>] <hostname-or-ip></code>	管理対象ストレージシステムのリストにデータソースを追加します。データソースは、ストレージシステムへの接続方法を定義したものです。データソースを追加するときは、 <code>-u</code> （ユーザ名）オプションと <code>-P</code> （パスワード）オプションを必ず指定する必要があります。オプションの <code>-t</code> （プロトコル）では、クラスタとの通信に使用するプロトコル（ <code>http</code> または <code>https</code> ）を指定します。プロトコルが指定されていない場合は、両方のプロトコルが試行されます。オプションの <code>-p</code> （ポート）では、クラスタとの通信に使用するポートを指定します。ポートが指定されていない場合は、該当するプロトコルのデフォルト値が試行されます。このコマンドは、ストレージ管理者のみが実行できます。	ユーザに証明書の承認を求めるプロンプトを表示し、対応するメッセージを出力します。
<code>um datasource list [<datasource-id>]</code>	管理対象ストレージシステムのデータソースを表示します。	次の値が表形式で表示されます。 ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message。

CLI コマンド	説明	出力
<code>um datasource modify [-h <hostname-or-ip>] [-u <username>] [-P <password>] [-t <protocol>] [-p <port>] <datasource-id></code>	1 つ以上のデータソースオプションを変更します。ストレージ管理者のみが実行できます。	対応するメッセージを表示します。
<code>um datasource remove <datasource-id></code>	Unified Manager からデータソース（クラスタ）を削除します。	対応するメッセージを表示します。
<code>um option list [<option> ..]</code>	に、set コマンドを使用して設定できるすべてのオプションを示します。	次の値が表形式で表示されます。 Name, Value, Default Value, and Requires Restart.
<code>um option set <option-name>=<option-value> [<option-name>=<option-value> ...]</code>	1 つまたは複数のオプションを設定します。このコマンドは、ストレージ管理者のみが実行できます。	対応するメッセージを表示します。
<code>um version</code>	Unified Manager ソフトウェアのバージョンを表示します。	Version ("9.6")
<code>um lun list [-q] [-ObjectType <object-id>]</code>	<p>指定したオブジェクトでフィルタリングした LUN のリストを表示します。-q は、ヘッダーを表示しないすべてのコマンドに適用されます。ObjectType には、lun、qtree、cluster、volume、quota、または SVM を選択します。</p> <p>例：</p> <p>um lun list -cluster 1</p> <p>この例では、objectType が「-cluster」で、objectId が「1」です。このコマンドを実行すると、ID が 1 のクラスタに含まれるすべての LUN のリストが表示されます。</p>	次の値が表形式で表示されます。 ID and LUN path.

CLI コマンド	説明	出力
um svm list [-q] [-ObjectType <object-id>]	<p>指定したオブジェクトでフィルタリングした Storage VM のリストを表示します。ObjectType には、lun、qtree、cluster、volume、quota、または SVM を選択します。</p> <p>例：</p> <p>um svm list -cluster 1</p> <p>この例では、objectType が「-cluster」で、objectId が「1」です。このコマンドを実行すると、ID が 1 のクラスタに含まれるすべての Storage VM のリストが表示されます。</p>	<p>次の値が表形式で表示されます。 Name and Cluster ID.</p>
um qtree list [-q] [-ObjectType <object-id>]	<p>指定したオブジェクトでフィルタリングした qtree のリストを表示します。-q は、ヘッダーを表示しないすべてのコマンドに適用されます。ObjectType には、lun、qtree、cluster、volume、quota、または SVM を選択します。</p> <p>例：</p> <p>um qtree list -cluster 1</p> <p>この例では、objectType が「-cluster」で、objectId が「1」です。このコマンドを実行すると、ID が 1 のクラスタに含まれるすべての qtree のリストが表示されます。</p>	<p>次の値が表形式で表示されます。 Qtree ID and Qtree Name.</p>

CLI コマンド	説明	出力
um disk list [-q] [-ObjectType <object-id>]	<p>指定したオブジェクトでフィルタリングしたディスクのリストを表示します。ObjectType には、disk、aggr、node、cluster のいずれかを指定できます。</p> <p>例：</p> <p>um disk list -cluster 1</p> <p>この例では、objectType が「-cluster」で、objectId が「1」です。このコマンドを実行すると、ID が 1 のクラスタに含まれるすべてのディスクのリストが表示されます。</p>	<p>次の値が表形式で表示されます ObjectType and object-id。</p>
um cluster list [-q] [-ObjectType <object-id>]	<p>指定したオブジェクトでフィルタリングしたクラスタのリストを表示します。ObjectType には、disk、aggr、node、cluster、lun、qtree、ボリューム、クォータ、または SVM。</p> <p>例：</p> <p>um cluster list -aggr 1</p> <p>この例では、objectType が「-aggr」で、objectId が「1」です。このコマンドを実行すると、ID が 1 のアグリゲートが属するクラスタが表示されます。</p>	<p>次の値が表形式で表示されます。 Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key。</p>

CLI コマンド	説明	出力
um cluster node list [-q] [-ObjectType <object-id>]	<p>指定したオブジェクトでフィルタリングしたクラスタノードのリストを表示します。ObjectType には、disk、aggr、node、cluster のいずれかを指定できます。</p> <p>例：</p> <pre>um cluster node list -cluster 1</pre> <p>この例では、objectType が「-cluster」で、objectId が「1」です。このコマンドを実行すると、ID が 1 のクラスタに含まれるすべてのノードのリストが表示されます。</p>	<p>次の値が表形式で表示されます Name and Cluster ID。</p>
um volume list [-q] [-ObjectType <object-id>]	<p>指定したオブジェクトでフィルタリングしたボリュームのリストを表示します。ObjectType には、lun、qtree、cluster、volume、quota、SVM またはアグリゲート。</p> <p>例：</p> <pre>um volume list -cluster 1</pre> <p>この例では、objectType が「-cluster」で、objectId が「1」です。このコマンドを実行すると、ID が 1 のクラスタに含まれるすべてのボリュームのリストが表示されます。</p>	<p>次の値が表形式で表示されます Volume ID and Volume Name。</p>

CLI コマンド	説明	出力
um quota user list [-q] [-ObjectType <object-id>]	<p>指定したオブジェクトでフィルタリングしたクォータユーザのリストを表示します。ObjectType には、qtree、cluster、volume、quota、svm のいずれかを指定できます。</p> <p>例：</p> <pre>um quota user list -cluster 1</pre> <p>この例では、objectType が「-cluster」で、objectId が「1」です。このコマンドを実行すると、ID が 1 のクラスタに含まれるすべてのクォータユーザのリストが表示されます。</p>	次の値が表形式で表示されます ID, Name, SID and Email。
um aggr list [-q] [-ObjectType <object-id>]	<p>指定したオブジェクトでフィルタリングしたアグリゲートのリストを表示します。ObjectType には、disk、aggr、node、cluster、volume のいずれかを指定できます。</p> <p>例：</p> <pre>um aggr list -cluster 1</pre> <p>この例では、objectType が「-cluster」で、objectId が「1」です。このコマンドを実行すると、ID が 1 のクラスタに含まれるすべてのアグリゲートのリストが表示されます。</p>	次の値が表形式で表示されます Aggr ID, and Aggr Name。
um event ack <event-ids>	1 つ以上のイベントに確認応答します。	対応するメッセージを表示します。
um event resolve <event-ids>	1 つ以上のイベントを解決します。	対応するメッセージを表示します。
um event assign -u <username> <event-id>	ユーザにイベントを割り当てます。	対応するメッセージを表示します。

CLI コマンド	説明	出力
<code>um event list [-s <source>] [-S <event-state-filter-list>..] [<event-id> ..]</code>	システムまたはユーザによって生成されたイベントのリストが表示されます。ソース、状態、および ID に基づいてイベントをフィルタリングします。	次の値が表形式で表示されます Source, Source type, Name, Severity, State, User and Timestamp。
<code>um backup restore -f <backup_file_path_and_name></code>		対応するメッセージを表示します。

スクリプトのウィンドウとダイアログボックスの概要

Scripts ページを使用して、Unified Manager にスクリプトを追加できます。

[スクリプト] ページ

Scripts ページを使用して、Unified Manager にカスタムスクリプトを追加できます。これらのスクリプトをアラートに関連付けると、ストレージオブジェクトが自動的に再設定されます。

Scripts ページを使用して、Unified Manager に対してスクリプトを追加または削除できます。

コマンドボタン

- * 追加 *

スクリプトの追加ダイアログボックスが表示されます。このダイアログボックスで、スクリプトを追加できます。

- * 削除 *

選択したスクリプトを削除します。

リストビュー

リストビューには、Unified Manager に追加したスクリプトが表形式で表示されます。

- * 名前 *

スクリプトの名前が表示されます。

- * 概要 *

スクリプトの概要を表示します。

【スクリプトの追加】ダイアログボックス

スクリプトの追加ダイアログボックスでは、Unified Manager にスクリプトを追加できます。スクリプトを使用して、ストレージオブジェクトに対して生成されたイベントを自動的に解決するようにアラートを設定することができます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

- * スクリプトファイルを選択 *

アラート用のスクリプトを選択できます。

- * 概要 *

スクリプトの概要を指定できます。

クラスタのパフォーマンスを監視および管理する

Active IQ Unified Manager によるパフォーマンス監視の概要

Active IQ Unified Manager（旧 OnCommand Unified Manager）は、NetApp ONTAP ソフトウェアを実行するシステムを対象に、パフォーマンス監視機能とパフォーマンスイベントの根本原因分析機能を提供します。

Unified Manager では、クラスタコンポーネントを過剰に消費しているワークロードや、クラスタ上のその他のワークロードのパフォーマンスを低下させているワークロードを特定できます。パフォーマンスしきい値ポリシーを定義して特定のパフォーマンスカウンタの最大値を指定し、しきい値を超えたときにイベントが生成されるようにすることもできます。Unified Manager は、管理者がイベントに対処してパフォーマンスを平常時のレベルに戻すことができるよう、このようなパフォーマンスイベントに関するアラートをユーザに通知します。Unified Manager の UI でイベントを表示および分析できます。

Unified Manager は、次の 2 種類のワークロードのパフォーマンスを監視します。

- ユーザ定義のワークロード

このワークロードは、クラスタに作成した FlexVol ボリュームと FlexGroup ボリュームで構成されます。

- システム定義のワークロード

このワークロードは、内部のシステムアクティビティで構成されます。

Unified Manager のパフォーマンス監視機能

Unified Manager は、ONTAP ソフトウェアを実行しているシステムからパフォーマンス統計を収集して分析します。このツールは、動的なパフォーマンスしきい値とユーザ定義のパフォーマンスしきい値を使用して、多数のクラスタコンポーネントにわたるさまざまなパフォーマンスカウンタを監視します。

長い応答時間（レイテンシ）は、ストレージオブジェクト（ボリュームなど）の実行速度が通常よりも遅いことを示しています。また、この問題は、ボリュームを使用しているクライアントアプリケーションのパフォーマンスが低下したことも示します。Unified Manager はパフォーマンス問題が存在するストレージコンポーネントを特定し、そのパフォーマンス問題に対処するための推奨される対処策を提示します。

Unified Manager には次の機能があります。

- ONTAP ソフトウェアを実行しているシステムからワークロードのパフォーマンス統計を監視して分析します。
- クラスタ、ノード、アグリゲート、ポート、SVM のパフォーマンスカウンタを追跡します。ボリューム、LUN、NVMe ネームスペース、およびネットワークインターフェイス（LIF）。
- IOPS（処理数）、MBps（スループット）、レイテンシ（応答時間）、利用率など、ワークロードのアクティビティを時系列で示す詳細なグラフを表示します。パフォーマンス容量とキャッシュ比率：
- しきい値を超えた場合にイベントをトリガーして E メールアラートを送信する、ユーザ定義のパフォーマンスしきい値ポリシーを作成できます。

- システム定義のしきい値とワークロードのアクティビティを学習する動的なパフォーマンスしきい値を使用して、パフォーマンスの問題を特定してアラートを送信します。
- ボリュームおよび LUN に適用されるサービス品質（QoS）ポリシーとパフォーマンスサービスレベルポリシー（PSL）を特定します。
- 競合状態のクラスタコンポーネントを特定します。
- クラスタコンポーネントを過剰に消費しているワークロードと、アクティビティの増加によってパフォーマンスが影響を受けたワークロードを特定します。

ストレージシステムのパフォーマンスを管理するために使用される **Unified Manager** インターフェイス

ここでは、Active IQ Unified Manager でデータストレージの容量、可用性、保護に関する問題をトラブルシューティングするための2つのユーザインターフェイスについて説明します。2種類のUIとは、Unified Manager Web UI とメンテナンスコンソールです。

Unified Manager の保護機能を使用する場合は、OnCommand Workflow Automation（WFA）もインストールして設定する必要があります。

Unified Manager Web UI

Unified Manager Web UI では、管理者がデータストレージの容量、可用性、保護に関連するクラスタの問題を監視してトラブルシューティングすることができます。

これらのセクションでは、管理者がUnified Manager Web UIに表示されるストレージ容量、データの可用性、または保護に関する問題をトラブルシューティングする際に従う共通のワークフローについて説明します。

メンテナンスコンソール

Unified Manager のメンテナンスコンソールでは、管理者が Unified Manager サーバ自体に関連するオペレーティングシステムの問題、バージョンアップグレードの問題、ユーザアクセスの問題、およびネットワークの問題を監視し、診断し、対処することができます。Unified Manager Web UI を使用できない場合は、メンテナンスコンソールが Unified Manager にアクセスする唯一の手段となります。

この情報は、メンテナンスコンソールにアクセスしてUnified Managerサーバの機能に関連する問題を解決するために使用します。

クラスタの構成とパフォーマンスのデータの収集アクティビティ

クラスタ構成 data_is の収集間隔は 15 分です。たとえば、クラスタを追加したあと、そのクラスタの詳細が Unified Manager の UI に表示されるまでに 15 分かかります。クラスタに対する変更を行った場合にも同じ間隔が適用されます。

たとえば、クラスタ内の SVM に 2 つの新しいボリュームを追加した場合、それらの新しいオブジェクトが UI に表示されるのは次のポーリング間隔のあとであるため、最大で 15 分後になります。

Unified Manager は、監視対象のすべてのクラスタから 5 分間隔で current_performance_statistics_ を収集します。そのデータを分析することでパフォーマンスイベントや潜在的な問題を特定します。5 分ごとのパフォーマンスデータについては 30 日分、1 時間ごとのパフォーマンスデータについては 180 日分のデータが履歴として保持されます。これにより、過去 1 カ月間の非常にきめ細かなパフォーマンスの詳細と最大 1 年間の

パフォーマンスの傾向を確認できます。

収集のポーリングは、各クラスタからのデータが同時に送信されてパフォーマンスに影響することがないように数分ずつオフセットされます。

次の表に、Unified Manager で実行される収集アクティビティを示します。

アクティビティ	時間間隔	説明
パフォーマンス統計のポーリング	5 分ごと	各クラスタからリアルタイムのパフォーマンスデータを収集します。
統計分析	5 分ごと	<p>Unified Manager では、統計のポーリングが完了するたびに、収集したデータをユーザ定義のしきい値、システム定義のしきい値、および動的なしきい値と比較します。</p> <p>パフォーマンスしきい値の違反が見つかったと、Unified Manager はイベントを生成し、設定されている場合は該当のユーザに E メールを送信します。</p>
構成のポーリング	15 分ごと	各クラスタから詳細なインベントリ情報を収集して、すべてのストレージオブジェクト（ノード、SVM、ボリュームなど）を特定します。
要約	1 時間ごと	<p>5 分ごとに収集した最新の 12 回分のパフォーマンスデータを集計して 1 時間の平均を求めます。</p> <p>1 時間の平均値は UI のいくつかのページで使用され、180 日間保持されます。</p>
予測分析とデータの削除	毎日午前 0 時から	<p>クラスタのデータを分析し、次の 24 時間のボリュームのレイテンシと IOPS の動的なしきい値を設定します。</p> <p>30 日を経過した 5 分ごとのパフォーマンスデータをデータベースから削除します。</p>

アクティビティ	時間間隔	説明
データの削除	毎日午前 2 時から	180 日を経過したイベントおよび 180 日を経過した動的しきい値をデータベースから削除します。
データの削除	毎日午前 3 時 30 分から	180 日を経過した 1 時間ごとのパフォーマンスデータをデータベースから削除します。

データの継続性収集サイクルとは

データの継続性収集サイクルは、リアルタイムのクラスタパフォーマンス収集サイクルの外部で、デフォルトでは 5 分ごとにパフォーマンスデータを取得します。データの継続性収集により、Unified Manager がリアルタイムのデータを収集できなかった期間の統計データを補完することができます。

Unified Manager は、次のイベントが発生したときにデータの継続性収集による履歴パフォーマンスデータのポーリングを実行します。

- クラスタが最初に Unified Manager に追加されたとき。

Unified Manager は、過去 15 日間の履歴パフォーマンスデータを収集します。これにより、クラスタが追加されてから数時間で 2 週間分の履歴パフォーマンス情報を表示できます。

また、該当する期間にシステム定義のしきい値のイベントが発生していた場合はそれらのイベントも報告されます。

- 現在のパフォーマンスデータ収集サイクルが所定の時間に完了しない。

リアルタイムのパフォーマンスのポーリングが 5 分間隔の収集期間を超えると、データの継続性収集サイクルが開始され、収集されなかった期間の情報が収集されます。データの継続性収集が実行されなかった場合、次の収集期間がスキップされます。

- 次の状況により、Unified Manager に一時的にアクセスできなくなり、そのあとオンラインに戻ったとき。
 - 再起動された。
 - ソフトウェアのアップグレードやバックアップファイルの作成のために Unified Manager がシャットダウンされた。
 - ネットワーク停止から復旧した。
- 次の状況により、クラスタに一時的にアクセスできなくなり、そのあとオンラインに戻ったとき。
 - ネットワーク停止から復旧した。
 - 低速なワイドエリアネットワーク接続が原因で、通常のパフォーマンスデータの収集に遅延が生じた。

データの継続性収集サイクルは、最大 24 時間の履歴データを収集できます。Unified Manager が停止した状態が 24 時間以上続くと、UI のページにパフォーマンスデータが表示されない期間が発生します。

データの継続性収集サイクルとリアルタイムのデータ収集サイクルを同時に実行することはできません。データの継続性収集サイクルが完了してからでないと、リアルタイムのパフォーマンスデータ収集は開始されません。1 時間以上の履歴データを収集するためにデータの継続性収集が必要な場合は、Notifications ペインの上部に、そのクラスタのバナーメッセージが表示されます。

収集されたデータとイベントのタイムスタンプの意味

収集された健全性とパフォーマンスのデータに表示されるタイムスタンプやイベントの検出時間に表示されるタイムスタンプは、ONTAP クラスタの時間に基づいて、Web ブラウザで設定されているタイムゾーンに調整されます。

ネットワークタイムプロトコル（NTP）サーバを使用して、Unified Manager サーバ、ONTAP クラスタ、および Web ブラウザの時間を同期することを強く推奨します。



特定のクラスタのタイムスタンプが正しく表示されない場合は、そのクラスタの時間が正しく設定されていることを確認してください。

Unified Manager の GUI で実行するパフォーマンスワークフロ

Unified Manager インターフェイスには、パフォーマンス情報を収集、表示するためのページが多数あります。左側のナビゲーションパネルを使用して各ページに移動し、ページ上のタブとリンクを使用して情報を表示および設定します。

クラスタのパフォーマンス情報を監視し、トラブルシューティングを行うには、次のすべてのページを使用します。

- ダッシュボードページ
- ストレージおよびネットワークオブジェクトのインベントリページ
- ストレージオブジェクトの詳細ページ（パフォーマンスエクスプローラを含む）
- 設定および設定ページ
- イベントページ

UI にログインします

Unified Manager の UI には、サポートされている Web ブラウザからログインできます。

- 必要なもの *
- Web ブラウザが最小要件を満たしている必要があります。

詳細については、Interoperability Matrix を参照してください "mysupport.netapp.com/matrix" をクリックして、サポートされているブラウザバージョンの一覧を表示します。

- Unified Manager サーバの IP アドレスまたは URL が必要です。

1 時間何も操作を行わないと、セッションから自動的にログアウトされます。この時間枠は、* 一般 * > * 機能設定 * で設定できます。

手順

1. Web ブラウザに、下記の形式で URL を入力します。url は、Unified Manager サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）です。

- IPv4 の場合：https://URL/
- IPv6 の場合：https://[URL]/

自己署名のデジタル証明書がサーバで使用されている場合、信頼されていない証明書であることを示す警告がブラウザ画面に表示されることがあります。リスクを承認してアクセスを続行するか、認証局（CA）の署名のあるデジタル証明書をインストールしてサーバを認証します。。ログイン画面で、ユーザ名とパスワードを入力します。

Unified Manager のユーザインターフェイスへのログインが SAML 認証で保護されている場合は、Unified Manager のログインページではなくアイデンティティプロバイダ（IdP）のログインページでクレデンシャルを入力します。

ダッシュボードページが表示されます。



Unified Manager サーバが初期化されていない場合は、新しいブラウザウィンドウに初期設定ウィザードが表示されます。このウィザードで、E メールアラートの受信者および E メール通信を処理する SMTP サーバを入力し、AutoSupport で Unified Manager に関する情報のテクニカルサポートへの送信が有効になっているかどうかを指定します。この情報の入力を完了すると、Unified Manager の UI が表示されます。

グラフィカルインターフェイスと操作手順

Unified Manager は柔軟性に優れており、複数のタスクをさまざまな方法で実行できます。Unified Manager を実際に使用してみると、操作手順が多数あることがわかります。使用できる操作手順をすべて紹介することは不可能ですが、ここでは、代表的な操作手順をいくつか紹介します。

クラスタオブジェクト監視時の操作

Unified Manager で管理しているクラスタ内のすべてのオブジェクトのパフォーマンスを監視できます。ストレージオブジェクトの監視では、クラスタとオブジェクトのパフォーマンスの概要を確認し、パフォーマンスイベントを監視します。パフォーマンスとイベントの総合的な情報を表示することも、オブジェクトのパフォーマンスとパフォーマンスイベントの詳しいデータを表示して調査することもできます。

次に、クラスタオブジェクトを監視する際の操作例を紹介します。

1. ダッシュボードページで、パフォーマンス容量パネルの詳細を確認して使用済みパフォーマンス容量が最も多いクラスタを特定し、棒グラフをクリックしてそのクラスタのノードのリストに移動します。
2. 使用済みパフォーマンス容量の値が最も高いノードを特定し、そのノードをクリックします。
3. ノード / パフォーマンスエクスプローラページで、表示と比較メニューからこのノード上のアグリゲートをクリックします。

4. 使用済みパフォーマンス容量が最も多いアグリゲートを特定し、そのアグリゲートをクリックします。
5. アグリゲート / パフォーマンスエクスプローラページで、表示と比較メニューから、このアグリゲート上の * ボリュームをクリックします。
6. IOPS が最も高いボリュームを特定します。

特定したボリュームを調べて、QoS ポリシーまたはパフォーマンスサービスレベルポリシーを適用するかどうかを判断するか、またはポリシーの設定を変更し、これらのボリュームが使用する IOPS の割合が少なくなるようにします。

Dashboard All Clusters

Management Actions

- Enable takeover on panic (2)
- Disable telnet (2)
- Enable volume autogrow (9)

Capacity

31 events (No new in past 24 hours)

CLUSTER	USED	DAYS TO FULL	REDUCTION
opm-sl...icity	40.5 TB	< 1 month	13.0:1
umeng...1-02	83.6 TB	51 days	8.0:1
sysmgr...0-1-8	33 TB	140 days	6.3:1

Performance Capacity

No new events

CLUSTER	USED	DAYS TO FULL
umeng-aff220-01-02	83%	< 1 month
sysmgr-fas8060-1-8	49%	< 1 month
fas8040-206-21	46%	77 days

Nodes Last updated: Nov 15, 2019, 10:48 AM

VIEW Nodes on umeng-aff220-01-02 Search Nodes Filter Hardware Inventory Report

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports Show / Hide

Status	Node	Latency	IOPS	MB/s	Performance Capacity Used	Utilization	Fr
✖	umeng-aff220-01	21.7 ms/op	27,333 IOPS	221 MB/s	73%	50%	3.1
✖	umeng-aff220-02	8.33 ms/op	83.4 IOPS	102 MB/s	53%	43%	6.1

Node / Performance : umeng-aff220-01

Summary Explorer Failover Planning Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Aggregates on this Node Filter

Aggregate	Latency	IOPS	MB/s	Perf...
NSLM12_002	12.4 ...	47.51...	5.6 M...	8%
NSLM12_001	11.4 ...	216 L...	4.33 ...	5%

Aggregate / Performance : NSLM12_002

Summary Explorer Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Volumes on this Aggregate Filter

Volume	Latency	IOPS	MB/s
suchita_vmware_d...	6.38 ms...	76.8 IOPS	2.55 MB/s
suchita_vmware_d...	5.82 ms...	4,775 L...	18.7 MB/s
aiqum_scale_do_no...	0.114 m...	< 1 IOPS	< 1 MB/s

Unified Manager で管理しているすべてのクラスタのパフォーマンスを監視できます。クラスタの監視では、クラスタとオブジェクトのパフォーマンスの概要を確認し、パフォーマンスイベントを監視します。パフォーマンスとイベントの総合的な情報を表示することも、クラスタとオブジェクトのパフォーマンスおよびパフォーマンスイベントの詳細なデータを表示して調査することもできます。

次に、クラスタパフォーマンスを監視する際の操作例を紹介します。

1. 左側のナビゲーションペインで、* Storage * > * Aggregates * をクリックします。
2. これらのアグリゲートのパフォーマンスに関する情報を表示するには、パフォーマンス：すべてのアグリゲートビューを選択します。
3. 調査するアグリゲートを特定し、そのアグリゲート名をクリックして、アグリゲート / パフォーマンスエクスプローラのページに移動します。
4. 必要に応じて、[表示と比較 (View and Compare)] メニューでこのアグリゲートと比較する他のオブジェクトを選択し、比較ペインにオブジェクトの 1 つを追加します。

両方のオブジェクトの統計が、比較できるようにカウンタグラフに表示されます。

5. エクスプローラページの右側にある比較ペインで、いずれかのカウンタチャートの * ズームビュー * をクリックすると、そのアグリゲートのパフォーマンス履歴の詳細が表示されます。

Aggregates

Last updated: Nov 15, 2019, 1:18 PM

VIEW **Performance: All Aggregates** Search Aggregates Filter

Assign Performance Threshold Policy Clear Performance Threshold Policy

Scheduled Reports Show / Hide

	Status	Aggregate	Type	Latency	IOPS	MB/s	Performance Capacity Used	Utilization
		aggr_evt	SSD	0.29 ms/op	3.79 IOPS	< 1 MB/s	< 1%	< 1%
		aggr4	HDD	5.74 ms/op	14.4 IOPS	1.31 MB/s	6%	5%
		aggr3	HDD	5.06 ms/op	3.06 IOPS	< 1 MB/s	6%	5%
		meg_aggr2	HDD	10.4 ms/op	52.9 IOPS	7.28 MB/s	3%	2%

Aggregate / Performance : aggr4

Switch to Health View Last updated: Nov 15, 2019, 1:20 PM

Summary Explorer Information

Compare the performance of associated objects and display detailed charts

TIME RANGE Last 72 Hours

VIEW AND COMPARE **Aggregates on same Node** Filter

Aggregate	Latency	IOPS	MB/s	Perf...
aggr3	5.06 ...	3.06 ...	< 1 M...	6%
aggr_evt	0.29 ...	3.79 ...	< 1 M...	< 1%
aggr_automation	0.27...	6.35 ...	< 1 M...	< 1%

Comparing
1 Additional Object
aggr4
aggr3

Events for Aggregate: aggr4
No data to display

Latency
Latency - Total view (ms/op)
aggr4
aggr3
Nov 14, 2019, 6:39 AM
12:00 AM Nov 15, 2019, 12:00 AM
Zoom View

Latency for Aggregate: aggr4

Last updated: Nov 15, 2019, 1:23 PM

Event Timeline: aggr4
Critical Events
Error Events
Warning Events
Information Events
No data to display

Comparing Objects
aggr4
aggr3
Latency - Total view (ms/op)
aggr4
aggr3
Nov 14, 2019, 1:24 AM
Nov 15, 2019, 12:00 AM Nov 15, 2019, 12:00 PM Nov 15, 2019, 12:00 PM Nov 15, 2019, 12:00 AM Nov 15, 2019, ...

Unified Manager のイベント詳細ページには、パフォーマンスイベントに関する詳しい情報が表示されます。トラブルシューティングやシステムパフォーマンスの微調整を行う際に、このページでパフォーマンスイベントを調査できます。

パフォーマンスイベントのタイプに応じて、次のいずれかのイベント詳細ページが表示されます。

- ユーザ定義およびシステム定義のしきい値ポリシーイベントのイベントの詳細ページ
- 動的しきい値ポリシーのイベントの詳細ページ

次に、イベントを調査する際の手順の一例を示します。

1. 左側のナビゲーションペインで、* イベント管理 * をクリックします。
2. [表示] メニューの [アクティブなパフォーマンスイベント *] をクリックします。
3. 調査するイベントの名前をクリックすると、イベントの詳細ページが表示されます。
4. イベントの概要を表示し、提案されたアクション（使用可能な場合）を確認して、問題の解決に役立つイベントの詳細を確認します。分析ワークロード * ボタンをクリックすると、問題の詳細な分析に役立つ詳細なパフォーマンスチャートを表示できます。

VIEW Active performance events

Search Events



Filter +

Assign To

Acknowledge

Mark as Resolved

Add Alert



Show / Hide

Triggered Time	Severity	State	Impact Lev	Impact Area	Name	Source	Source Ty
Nov 14, 2019, 11:39 AM	Warning	New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs7:/julia_feb12_vol1	Volume
Nov 14, 2019, 11:39 AM	Warning	New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs7:/julia_non_shared_3	Volume
Nov 15, 2019, 5:04 AM	Warning	New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	suchita_vmwvar...nt_delete_01	Volume
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency...Service Level Policy	iscsi_boot/ia.../ocum-c220-01	LUN
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency...Service Level Policy	iscsi_boot/ia.../ocum-c220-07	LUN



Event: QoS Volume Peak IOPS/TB Warning Threshold Breached ⓘ

(Last Seen: Nov 15, 2019, 11:19 AM)

IOPS value of 570 IOPS on policy group NSLM_vs7_Performance_2_0 has triggered a WARNING event to identify performance problems for the workloads in this policy group.



Actions

Suggested Actions to Fix The Issue ⓘ

Troubleshoot

Analyze Workload

Take Action

This is an Adaptive QoS Policy that might be used by other workloads in the system.

If it is acceptable that changes you make to the QoS setting will be applied to other workloads that are using this policy,

- Increase the threshold to 4950 IOPS/TB for this Adaptive QoS Policy.

If you are satisfied with the current limitation on workload throughput,

- Leave the QoS configuration setting as it is.

Event Information ⓘ

EVENT TRIGGER TIME

Nov 14, 2019, 11:39 AM

SEVERITY

Warning

SOURCE

vs7:/julia_non_shared_3

STATE

New

IMPACT LEVEL

Risk

SOURCE TYPE

Volume

EVENT DURATION

1 day 40 minutes

IMPACT AREA

Performance

ION CLUSTER

ocum-mobility-01-02

LAST SEEN

Nov 15, 2019, 11:19 AM

AFFECTED OBJECTS COUNT

1

TRIGGERED POLICY

QoS Peak IOPS/TB threshold ⓘ

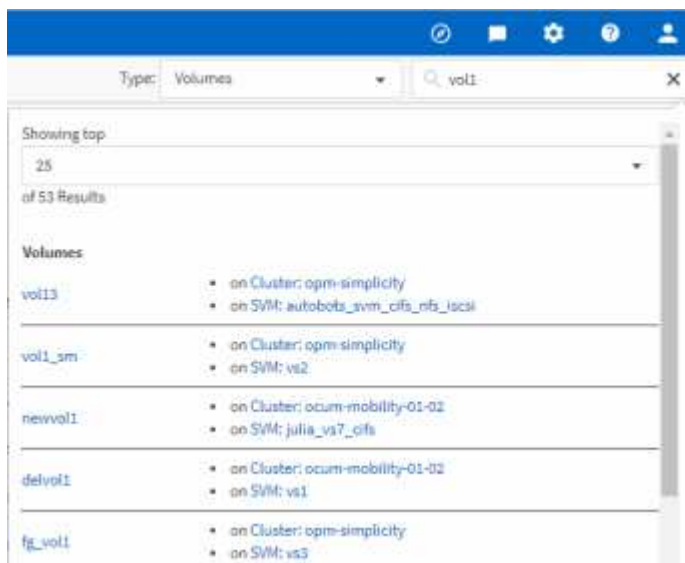
ストレージオブジェクトを検索しています

特定のオブジェクトにすばやくアクセスするには、メニューバーの上部にある「すべてのストレージオブジェクトの検索」フィールドを使用します。すべてのオブジェクトをグローバルに検索する方法を使用すると、特定のオブジェクトをタイプ別にすばやく見つけることができます。検索結果はストレージオブジェクトのタイプ別に表示され、ドロップダウンメニューを使用してフィルタできます。検索キーワードは3文字以上にする必要があります。

グローバル検索では、検索結果の総数は表示されますが、アクセスできるのは上位 25 件のみです。そのため、グローバル検索機能は、すばやく検索したい項目がわかっている場合に特定の項目を検索するためのショートカットツールと考えることができます。検索結果をすべて表示するには、オブジェクトのインベントリページで検索を実行するか、関連するフィルタリング機能を使用します。

ドロップダウンボックスをクリックして「すべて *」を選択すると、すべてのオブジェクトとイベントを同時に検索できます。または、ドロップダウンボックスをクリックしてオブジェクトタイプを指定することもできます。[すべてのストレージオブジェクトの検索] フィールドにオブジェクトまたはイベント名の 3 文字以上を入力し、**Enter** キーを押して、次のような検索結果を表示します。

- クラスタ：クラスタ名
- nodes：ノード名
- アグリゲート：アグリゲート名
- SVMs：SVM 名
- volumes：ボリューム名
- LUN：LUN パス



LIF とポートはグローバル検索バーでは検索できません。

この例では、ドロップダウンボックスでボリュームオブジェクトタイプが選択されています。[Search All Storage Objects] フィールドに「vol」と入力すると、名前にこれらの文字が含まれるすべてのボリュームのリストが表示されます。オブジェクトの検索では、任意の検索結果をクリックして、そのオブジェクトのパフォーマンスエクスペローラページに移動できます。イベント検索では、検索結果内の項目をクリックすると、[イベントの詳細] ページが表示されます。

インベントリページの内容のフィルタリング

Unified Manager でインベントリページのデータをフィルタリングして、特定の条件に基づいてデータをすばやく特定できます。フィルタリングを使用すると、Unified Manager のページの内容を絞り込んで、関心のある結果だけを表示できます。そのため、関心のあるデータだけを効率的に表示できます。

環境設定に基づいてグリッド表示をカスタマイズするには、* フィルタリング * を使用します。使用可能なフィルタオプションは、グリッドで表示しているオブジェクトタイプによって異なります。フィルタが現在適用されている場合は、[フィルタ (Filter)] ボタンの右側に適用されたフィルタの数が表示されます。

3 種類のフィルタパラメータがサポートされています。

パラメータ	検証
文字列 (テキスト)	演算子は、* contains *、* starts with *、* ends with *、および * does not contain * です。
番号	演算子は、* より大きい *、* より小さい *、* の最後の *、および * の間です。
列挙 (テキスト)	演算子は * は * で、* は * ではありません。

各フィルタには、列、演算子、および値のフィールドが必要です。使用可能なフィルタは、現在のページのフィルタ可能な列に基づいています。適用できるフィルタは 4 つまでです。フィルタパラメータの組み合わせに基づいてフィルタされた結果が表示されます。フィルタされた結果は、現在表示されているページだけでなく、フィルタ処理された検索のすべてのページに適用されます。

フィルタパネルを使用してフィルタを追加できます。

1. ページの上部にある * Filter * ボタンをクリックします。フィルタリングパネルが表示されます。
2. 左側のドロップダウンリストをクリックし、Cluster、パフォーマンスカウンタなどのオブジェクトを選択します。
3. 中央のドロップダウンリストをクリックし、使用する演算子を選択します。
4. 最後のリストで値を選択または入力して、そのオブジェクトのフィルタを完成させます。
5. 別のフィルタを追加するには、[* + フィルタの追加 *] をクリックします。追加のフィルタフィールドが表示されます。前述の手順に従って、このフィルタを設定します。4 番目のフィルタを追加すると、[* + フィルタを追加 *] ボタンは表示されなくなります。
6. [フィルタを適用 (Apply Filter)] をクリックする。フィルタオプションがグリッドに適用され、フィルタボタンの右側にフィルタの数が表示されます。
7. フィルタパネルを使用して、削除するフィルタの右側にあるゴミ箱アイコンをクリックして、個々のフィルタを削除します。
8. すべてのフィルターを削除するには、フィルターパネルの下部にある * リセット * をクリックします。

フィルタリングの例

次の図は、フィルタパネルと 3 つのフィルタを示しています。フィルタを最大 4 つまでしか使用できない場合は、「* + フィルタを追加 *」ボタンが表示されます。

MBps	greater than	5	MBps	
Node	name starts with	test		
Type	is	FCP Port		
<input type="button" value="+ Add Filter"/>				
				<input type="button" value="Cancel"/> <input type="button" value="Apply Filter"/>

[フィルタの適用（Apply Filter）] をクリックすると、[フィルタ（Filtering）] パネルが閉じ、フィルタが適用され、適用されているフィルタの数が表示されます（ 3 ）。

ダッシュボードからのクラスタパフォーマンスの監視

Unified Manager のダッシュボードには、Unified Manager の現在のインスタンスで監視しているすべてのクラスタのパフォーマンスステータスの概要が、いくつかのパネルに分けて表示されます。管理対象クラスタの全体的なパフォーマンスを評価し、特定のイベントをすばやく把握して特定し、解決策を適用することができます。

ダッシュボードのパフォーマンスパネルについて

Unified Manager のダッシュボードには、環境内の監視対象のすべてのクラスタのパフォーマンスステータスの概要が、複数のパネルに分けて表示されます。すべてのクラスタまたは個々のクラスタのステータスを表示できます。

ほとんどのパネルには、パフォーマンス情報に加えて、そのカテゴリのアクティブイベントの数および過去 24 時間に追加された新しいイベントの数が表示されます。この情報から、報告されたイベントを解決するために詳細な分析が必要なクラスタを決定できます。イベントをクリックすると、上位数件のイベントが表示され、そのカテゴリのイベントをフィルタリングして表示するイベント管理インベントリページへのリンクが表示されます。

次のパネルにはパフォーマンスステータスが表示されます。

• * パフォーマンス容量パネル *

すべてのクラスタを表示している場合、このパネルには、各クラスタのパフォーマンス容量（過去 1 時間の平均）とパフォーマンス容量が上限に達するまでの日数（日次増加率に基づく）が表示されます。棒グラフをクリックすると、そのクラスタのノードインベントリページが表示されます。ノードのインベントリページには過去 72 時間のパフォーマンス容量の平均が表示されるため、この値がダッシュボードの値と一致しないことがあります。

単一のクラスタを表示している場合、このパネルには、そのクラスタのパフォーマンス容量、合計 IOPS、合計スループットが表示されます。

• * ワークロード IOPS パネル *

ワークロードのアクティブ管理が有効になっていて、単一のクラスタを表示している場合、このパネルに

は、特定の範囲の IOPS で現在実行されているワークロードの総数が表示されます。

• * ワークロードパフォーマンスパネル *

ワークロードのアクティブ管理が有効になっている場合、このパネルには、定義された各パフォーマンスサービスレベルに割り当てられている準拠ワークロードと非準拠ワークロードの総数が表示されます。棒グラフをクリックすると、そのポリシーに割り当てられているワークロードがワークロードページに表示されます。

• * 使用状況の概要パネル *

すべてのクラスタを表示している場合、IOPS またはスループット（MBps）が高い順にクラスタを表示できます。

単一のクラスタを表示している場合は、そのクラスタのワークロードを IOPS またはスループット（MBps）が高い順に表示できます。

パフォーマンスのバナーメッセージと説明

Unified Manager の通知ページ（通知ベルから）にバナーメッセージが表示されて、特定のクラスタのステータスの問題を通知することができます。

バナーメッセージ	説明	解決策：
No performance data is being collected from cluster <code>cluster_name</code> . Restart Unified Manager to correct this issue.	Unified Manager の収集サービスが停止しており、どのクラスタからでもパフォーマンスデータが収集されていません。	この問題を解決するには、Unified Manager を再起動します。それでも問題が修正されない場合は、テクニカルサポートにお問い合わせください。
More than x hour(s) of historical data is being collected from cluster <code>cluster_name</code> . Current data collections will start after all historical data is collected.	リアルタイムのクラスタパフォーマンス収集サイクル以外に、データの継続性収集サイクルによるパフォーマンスデータの収集が実行中です。	対処は不要です。現在のパフォーマンスデータは、データの継続性収集サイクルの完了後に収集されます。 データの継続性収集サイクルが実行されるのは、新しいクラスタが追加されたときや、Unified Manager が何らかの理由で現在のパフォーマンスデータを収集できなくなったときです。

パフォーマンス統計データの収集間隔を変更する

パフォーマンス統計のデフォルトの収集間隔は 5 分です。大規模なクラスタからの収集がデフォルトの時間内に完了しない場合は、この間隔を 10 分または 15 分に変更できます。この設定は、この Unified Manager インスタンスで監視しているすべてのクラスタからの統計の収集に適用されます。

- 必要なもの *

Unified Manager サーバのメンテナンスコンソールへのログインが許可されているユーザ ID とパスワードが必要です。

パフォーマンス統計の収集が時間内に完了しなかった問題は、バナーメッセージで示されます Unable to consistently collect from cluster <cluster_name> または Data collection is taking too long on cluster <cluster_name>。

収集間隔の変更が必要になるのは、統計の収集が問題のためです。その他の理由でこの設定を変更しないでください。



この値をデフォルト設定の 5 分から変更すると、Unified Manager でレポートされるパフォーマンスイベントの数や頻度に影響する可能性があります。たとえば、システム定義のパフォーマンスしきい値ポリシーでは、ポリシーを超えた状態が 30 分続くとイベントがトリガーされます。収集間隔が 5 分の場合は、収集間隔が 6 回連続でポリシーの違反となるようにする必要があります。一方、収集間隔が 15 分の場合は、2 回の収集期間のみでポリシーの違反と判断されます。

クラスタセットアップページの下部にあるメッセージは、現在の統計データの収集間隔を示します。

手順

1. SSH を使用して、Unified Manager ホストにメンテナンスユーザとしてログインします。

Unified Manager メンテナンスコンソールのプロンプトが表示されます。

2. 「パフォーマンスポーリング間隔の設定 *」というラベルの付いたメニューオプションの番号を入力し、Enter キーを押します。
3. プロンプトが表示されたら、メンテナンスユーザのパスワードをもう一度入力します。
4. 設定する新しいポーリング間隔の値を入力し、Enter キーを押します。

外部データプロバイダ（Graphite など）への接続を現在設定してある場合は、Unified Manager の収集間隔を 10 分または 15 分に変更したあと、データプロバイダの送信間隔も Unified Manager の収集間隔以上に変更する必要があります。


Workload Analyzer を使用したワークロードのトラブルシューティング

Workload Analyzer は、1 つのワークロードに関する健全性とパフォーマンスの重要な条件を 1 つのページに表示して、トラブルシューティングを支援します。ワークロードの現在と過去のイベントをすべて表示することで、ワークロードにパフォーマンス問題または容量 が割り当てられている理由をより正確に把握できます。

また、このツールを使用すると、ストレージがアプリケーションのパフォーマンスの問題の原因かどうか、あるいは問題がネットワークやその他の関連問題に起因しているかどうかを判断できます。

この機能は、ユーザインターフェイスのさまざまな場所から開始できます。

- 左側のナビゲーションメニューの [ワークロード分析] を選択します

- [イベントの詳細] ページで、[ワークロードの分析] ボタンをクリックします
- 任意のワークロードインベントリページ（ボリューム、LUN、ワークロード、NFS 共有、SMB / CIFS 共有）から、[詳細] アイコンをクリックします  をクリックし、* 分析ワークロード * を実行します
- [仮想マシン] ページで、任意のデータストアオブジェクトの [ワークロードの分析] ボタンをクリックします

左側のナビゲーションメニューからツールを起動した場合、分析するワークロードの名前を入力し、トラブルシューティングを行う期間を選択できます。いずれかのワークロードまたは仮想マシンのインベントリページからツールを起動した場合、ワークロードの名前は自動的に入力され、デフォルトの 2 時間分のワークロードデータが表示されます。イベントの詳細ページからツールを起動すると、ワークロードの名前が自動的に入力され、10 日間のデータが表示されます。

Workload Analyzer で表示されるデータは何ですか

Workload Analyzer ページには、ワークロードに影響している可能性のある現在のイベントに関する情報、イベントの原因となっている問題を修正するための推奨事項、およびパフォーマンスと容量の履歴を分析するためのグラフが表示されます。

ページの上部では、分析するワークロード（ボリュームまたは LUN）の名前と、統計情報を表示する期間を指定します。表示する期間はいつでも短縮または延長することができます。

ページの他の領域には、分析結果およびパフォーマンスと容量のグラフが表示されます。



LUN のワークロードグラフに表示される統計情報レベルは、ボリュームのワークロードグラフと同じではないため、これら 2 種類のワークロードで異なる値が表示されることもあります。

• * イベントサマリ領域 *

期間中に発生したイベントの数とタイプの概要が表示されます。さまざまな影響領域（パフォーマンスや容量など）のイベントがある場合は、この情報が表示され、関心のあるイベントタイプの詳細を選択できます。イベントタイプをクリックすると、イベント名のリストが表示されます。

期間中にイベントが 1 つしかない場合、一部のイベントについては、問題を修正するための推奨事項のリストが表示されます。

• * イベントタイムライン *

指定した期間内に発生したすべてのイベントが表示されます。各イベントにカーソルを合わせると、イベント名が表示されます。

イベントの詳細ページから * ワークロードの分析 * ボタンをクリックしてこのページを表示した場合は、選択したイベントのアイコンが大きく表示され、イベントを特定できます。

• * パフォーマンスチャート領域 *

選択した期間のレイテンシ、スループット（IOPS と MBps の両方）、利用率（ノードとアグリゲートの両方）のグラフが表示されます。さらに分析を行う場合は、View performance details リンクをクリックしてワークロードの Performance Explorer ページを表示できます。

- * Latency * は選択した期間のワークロードのレイテンシを表示します。このグラフには、次の 3 つの

ビューがあります。

- * 合計 * レイテンシ
- * 内訳 * レイテンシ（読み取り、書き込み、その他のプロセスによる内訳）
- * クラスタコンポーネント * レイテンシ（クラスタコンポーネント別）

を参照してください ["クラスタコンポーネントとその競合要因"](#) 表示されるクラスタコンポーネントの概要の場合。* **Throughput** * には、選択した期間におけるワークロードの **IOPS** と **MBps** の両方のスループットが表示されます。このグラフには 4 つのビューがあり、それぞれ以下を確認できます。* 合計スループット * 内訳 * スループット（読み取り、書き込み、その他のプロセスによる内訳）* クラウドスループット *（クラウドへのデータの書き込みとクラウドからのデータの読み取りに使用される MBps。容量をクラウドに階層化しているワークロードの場合）* 予測付き **IOPS** *（**IOPS** スループットの上限と下限の値が時間枠を超えて想定される予測）このチャートには、サービス品質（**QoS**）の最大スループットと最小スループットのしきい値の設定も表示されます（設定されている場合）。そのため、**QoS** ポリシーによって意図的にスループットが制限されているかどうかを確認することができます。* **Utilization** * には、選択した期間にワークロードが実行されているアグリゲートとノードの両方の利用率が表示されます。ここから、アグリゲートまたはノードが過剰に使用され、レイテンシが高くなっていないかどうかを確認できます。FlexGroup ボリュームを分析している場合は、利用率グラフに複数のノードと複数のアグリゲートが表示されます。

• * 容量チャート領域 *

過去 1 カ月のワークロードに対するデータ容量と Snapshot 容量のグラフが表示されます。

ボリュームについては、容量の詳細の表示リンクをクリックして、詳細な分析を行う場合に備えてワークロードの健全性の詳細ページを表示できます。LUN の健全性の詳細ページがないため、LUN ではこのリンクは表示されません。

- * 容量ビュー *：ワークロードに割り当てられている使用可能な合計スペースと使用済みの論理スペースが表示されます（ネットアップによるすべての最適化の完了後）。
- * Snapshot ビュー * には、Snapshot コピー用にリザーブされているスペースの合計と、現在使用されているスペースの量が表示されます。LUN には Snapshot ビューがありません。
- * クラウド階層ビュー * には、ローカルのパフォーマンス階層で使用されている容量とクラウド階層で使用されている容量が表示されます。これらのグラフには、このワークロードの容量がフルになるまでの推定残り時間が表示されます。この情報は過去の使用状況に基づいており、最低 10 日間のデータが必要です。Unified Manager は、容量が 30 日未満になるとストレージを「ほぼフル」とみなします。


Workload Analyzer を使用するタイミング

Workload Analyzer は、ユーザから報告されたレイテンシ問題のトラブルシューティングを行う場合、報告されたイベントやアラートを詳しく分析する場合、動作に異常があるワークロードについて調べる場合に使用します。

アプリケーションの実行速度が非常に遅いという連絡をユーザから受けた場合は、アプリケーションが実行されているワークロードのレイテンシ、スループット、利用率の各グラフを調べて、ストレージがパフォーマンス問題の原因かどうかを確認できます。ONTAP システムで容量の使用率が 85% を超えると原因のパフォーマンスの問題が生じる可能性があるため、容量グラフを使用して使用率が低下していないかどうかを確認することもできます。これらのグラフから、問題の原因がストレージであるか、ネットワークであるか、またはその他の関連する問題であるかを判断できます。

Unified Manager でパフォーマンスイベントが生成された場合に問題の原因をより詳細に確認するには、イベ

ントの詳細ページでワークロード分析ツールを起動し、「ワークロードの分析」ボタンをクリックしてレイテンシ、スループット、ワークロードの容量のトレンドを表示します。

ワークロードのインベントリページ（ボリューム、LUN、ワークロード、NFS 共有、SMB / CIFS 共有）でワークロードが異常に処理されていることがわかりした場合、[詳細]アイコンをクリックできます  に移動し、* Analyze Workload * をクリックしてワークロードの分析ページを開き、ワークロードの詳細を確認します。

Workload Analyzer の使用

Workload Analyzer は、ユーザインターフェイスからさまざまな方法で起動できます。ここでは、左側のナビゲーションペインからツールを起動する方法について説明します。

手順

1. 左側のナビゲーションペインで、* ワークロード分析 * をクリックします。

ワークロード分析ページが表示されます。

2. ワークロード名がわかっている場合は入力します。完全な名前がわからない場合は、3 文字以上入力すると、その文字列に一致するワークロードのリストが表示されます。
3. デフォルトの 2 時間よりも長い統計を表示する場合は時間範囲を選択し、* 適用 * をクリックします。
4. サマリ領域を表示して、期間中に発生したイベントを確認します。
5. パフォーマンスと容量のグラフを表示して指標値が異常な期間を確認し、その期間に発生しているイベントがないかどうかを確認します。

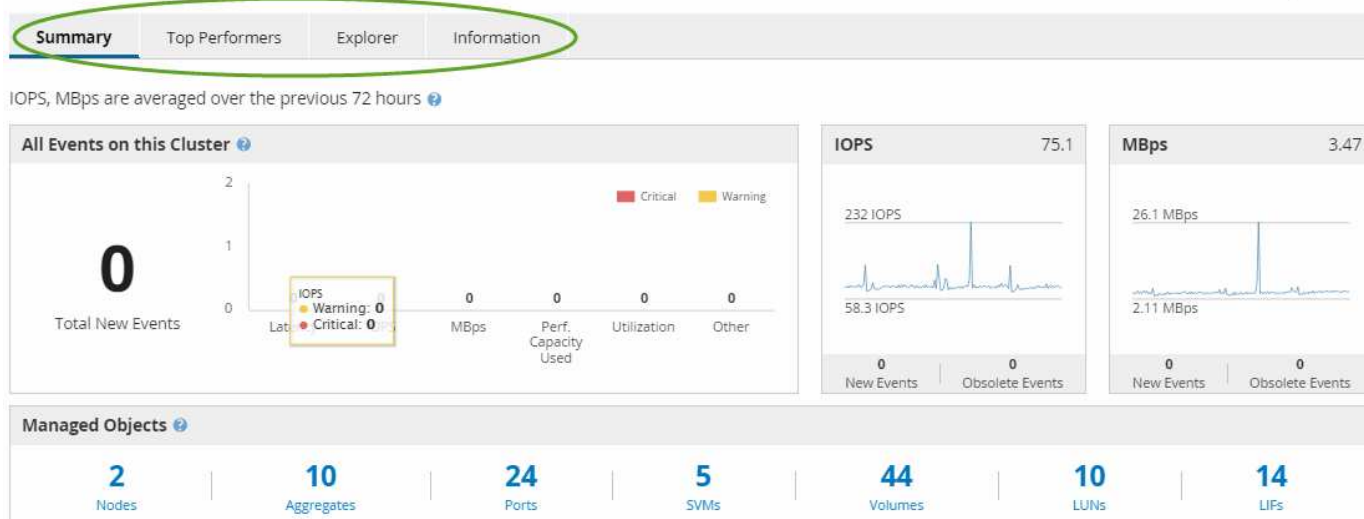
パフォーマンスクラスタランディングページからのクラスタパフォーマンスの監視

パフォーマンスクラスタランディングページには、Unified Manager のインスタンスによって監視されている、選択したクラスタのパフォーマンスステータスの概要が表示されます。このページでは、特定のクラスタの全体的なパフォーマンスを評価し、特定されたクラスタ固有のイベントをすばやく把握して特定し、解決策を適用することができます。

パフォーマンスクラスタランディングページについて

パフォーマンスクラスタのランディングページでは、選択したクラスタのパフォーマンスの概要が、クラスタ内の上位 10 個のオブジェクトのパフォーマンスステータスとともに表示されます。パフォーマンスの問題は、ページの上部の [このクラスタのすべてのイベント] パネルに表示されます。

パフォーマンスクラスタランディングページには、Unified Manager のインスタンスで管理される各クラスタの概要が表示されます。このページでは、イベントとパフォーマンスに関する情報が提供され、クラスタの監視とトラブルシューティングを行うことができます。次の図は、OPM によるモビリティというクラスタのパフォーマンスクラスタランディングページの例を示しています。



クラスタサマリページのイベント数がパフォーマンスイベントインベントリページのイベント数と一致しない可能性があります。これは、組み合わせしきい値ポリシーに違反したときにクラスタの概要ページのレイテンシと利用率のバーにそれぞれ 1 つのイベントが表示され、パフォーマンスイベントのインベントリページで組み合わせポリシーに違反したときに表示されるイベントは 1 つだけであるためです。



クラスタが Unified Manager の管理対象から除外されると、ページ上部のクラスタ名の右側にステータス * Removed * が表示されます。

パフォーマンスクラスタランディングページ

パフォーマンスクラスタのランディングページには、選択したクラスタのパフォーマンスステータスの概要が表示されます。このページから、選択したクラスタ上のストレージオブジェクトの各パフォーマンスカウンタの詳細にアクセスできます。

パフォーマンスクラスタのランディングページには、クラスタの詳細を 4 つの情報領域に分けて表示するタブが 4 つあります。

- サマリページ
 - クラスタイイベントペイン
 - MBps と IOPS のパフォーマンスチャート
 - [Managed Objects] ペイン
- ハフォーマンスシヨウイヘエシ
- Explorer ページ
- 情報ページ

Performance Cluster Summary ページ

Performance Cluster Summary ページには、クラスタのアクティブなイベント、IOPS パフォーマンス、および MBps パフォーマンスの概要が表示されます。このページには、クラスタ内のストレージオブジェクトの総数も表示されます。

クラスタパフォーマンスイベントのペインには、クラスタのパフォーマンス統計およびアクティブなすべてのイベントが表示されます。これは、クラスタおよびクラスタ関連のすべてのパフォーマンスとイベントを監視する場合に最も役立ちます。



このクラスタペインのすべてのイベント

このクラスタペインの「すべてのイベント」には、過去 72 時間のアクティブなクラスタパフォーマンスイベントがすべて表示されます。アクティブなイベントの合計数は左端に表示されます。この値は、このクラスタ内のすべてのストレージオブジェクトについて、「新規」と「確認済み」のすべてのイベントの合計数を示します。Total Active Events リンクをクリックすると、Events Inventory ページが表示されます。このページにはフィルタリングされてイベントが表示されます。

クラスタの Total Active Events バーのグラフには、アクティブな重大イベントと警告イベントの総数が表示されます。

- レイテンシ（ノード、アグリゲート、SVM、ボリューム、LUN の合計、ネームスペース）
- IOPS（クラスタ、ノード、アグリゲート、SVM、ボリュームの合計、LUN、ネームスペース）
- MBps（クラスタ、ノード、アグリゲート、SVM、ボリュームの合計、LUN、ネームスペース、ポート、LIF）
- 使用済みパフォーマンス容量（ノードとアグリゲートの合計）
- 利用率（ノード、アグリゲート、ポートの合計）
- その他（ボリュームのキャッシュミス率）

リストには、ユーザ定義のしきい値ポリシー、システム定義のしきい値ポリシー、および動的なしきい値からトリガーされたアクティブなパフォーマンスイベントが含まれます。

グラフのデータ（カウンタの縦棒）は、赤で表示されます（）をクリックします（）をクリックします。各カウンタの縦棒にカーソルを合わせると、イベントの実際のタイプと数が表示されます。カウンタパネルのデータを更新するには、* Refresh * をクリックします。

凡例で * クリティカル * と * 警告 * のアイコンをクリックすると、アクティブイベントの合計パフォーマンスグラフで重大イベントと警告イベントの表示と非表示を切り替えることができます。特定のイベントタイプを非表示にした場合、凡例のアイコンがグレーで表示されます。

カウンタパネル

カウンタパネルには、過去 72 時間のクラスタのアクティビティとパフォーマンスイベントが表示されます。次のカウンタがあります。

• * IOPS カウンタパネル *

IOPS は、クラスタの 1 秒あたりの入出力処理数の動作速度を示します。このカウンタパネルでは、過去 72 時間のクラスタの IOPS の概要を確認できます。グラフ上のラインにカーソルを合わせると、その時点の IOPS の値が表示されます。

• * MBps カウンタパネル *

MBps は、クラスタとの間で転送されたデータの量を 1 秒あたりのメガバイト数で示します。このカウン

タパネルでは、過去 72 時間のクラスタの MBps の概要を確認できます。グラフ上のラインにカーソルを合わせると、その時点の MBps の値が表示されます。

グラフ右上のグレーのバーに表示される数字は、過去 72 時間の平均値です。トレンドグラフの上下に表示される数字は、過去 72 時間の最小値と最大値です。グラフ下のグレーのバーには、過去 72 時間のアクティブなイベント（新規および確認済みのイベント）と廃止イベントの件数が表示されます。

カウンタパネルには、次の 2 種類のイベントが表示されます。

- * アクティブ *

現在アクティブなパフォーマンスイベント（新規または確認済みのイベント）を示します。自己修復または解決されていないイベントを引き起こしている問題。ストレージオブジェクトのパフォーマンスカウンタがパフォーマンスしきい値を超えたままになっているものです。

- * 廃止 *

アクティブではなくなったイベントを示します。自己修復または解決されたイベントである問題。ストレージオブジェクトのパフォーマンスカウンタがパフォーマンスしきい値を上回らなくなったものです。

- アクティブイベント * の場合、イベントアイコンにカーソルを合わせ、イベント番号をクリックすると、該当する [イベントの詳細] ページにリンクできます。複数のイベントがある場合は、[すべてのイベントを表示] をクリックして [イベントインベントリ] ページを表示できます。このページには、選択したオブジェクトカウンタタイプのすべてのイベントが表示されます。

[Managed Objects] ペイン

Performance Summary タブの Managed Objects ペインには、クラスタのストレージオブジェクトタイプと数の概要が表示されます。このペインでは、各クラスタ内のオブジェクトのステータスを追跡できます。

管理対象オブジェクトの数は、前回の収集期間以降のポイントインタイムデータです。新しいオブジェクトは 15 分間隔で検出されます。

いずれかのオブジェクトタイプのリンクされた番号をクリックすると、そのオブジェクトタイプのオブジェクトパフォーマンスインベントリページが表示されます。オブジェクトのインベントリページには、このクラスタ上のオブジェクトだけが表示されます。

管理対象オブジェクトは次のとおりです。

- * ノード * :

クラスタ内の物理システム。

- * アグリゲート *

保護およびプロビジョニングの際に 1 つのユニットとして管理可能な、複数の Redundant Array of Independent Disks （ RAID ） グループの集まりです。

- * ポート * :

ネットワーク上の他のデバイスへの接続に使用されるノード上の物理接続ポイント。

- * ストレージ VMs *

一意のネットワークアドレスでネットワークアクセスを提供する仮想マシン。SVM は、固有のネームスペースからデータを提供でき、クラスタの残りのエンティティとは別に管理することができます。

- * ボリューム *

サポートされているプロトコルを使用してアクセス可能なユーザデータを格納する論理エンティティ。数には FlexVol と FlexGroup の両方のボリュームが含まれます。FlexGroup コンスティチュエントは含まれません。

- * LUN*

Fibre Channel（FC）論理ユニットまたは iSCSI 論理ユニットの識別子。通常、論理ユニットはストレージボリュームに対応し、コンピュータオペレーティングシステム内ではデバイスとして表されます。

- * ネットワーク・インターフェイス *

ノードへのネットワークアクセスポイントを表す論理ネットワークインターフェイス。数にはすべてのインターフェイスタイプが含まれます。

パフォーマンスシヨウイヘエシ

パフォーマンス上位ページには、選択したパフォーマンスカウンタに基づいて、パフォーマンスが最大または最小のストレージオブジェクトが表示されます。たとえば、Storage VM カテゴリには、IOPS が最大、レイテンシが最大、または MBps が最小の SVM を表示できますまた、パフォーマンスが上位のオブジェクトでアクティブなパフォーマンスイベント（新規または確認済みのイベント）が発生しているかどうか也表示されます。

[パフォーマンスのトップ] ページには、各オブジェクトの最大 10 個が表示されます。Volume オブジェクトには、FlexVol ボリュームと FlexGroup ボリュームの両方が含まれます。

- * 時間範囲 *

上位のオブジェクトを表示する期間を選択できます。選択した期間環境のすべてのストレージオブジェクトが表示されます。使用可能な時間範囲：

- 過去 1 時間
- 過去 24 時間
- 過去 72 時間（デフォルト）
- 過去 7 日間

- * メートル法 *

[*Metric] メニューをクリックして別のカウンタを選択します。カウンタのオプションはオブジェクトタイプによって異なります。たとえば、* Volumes * オブジェクトで使用可能なカウンタは、* Latency *、* IOPS *、* MB/s * です。カウンタを変更すると、パネルのデータがリロードされ、選択したカウンタに基づいて上位のオブジェクトが表示されます。



使用可能なカウンタ：

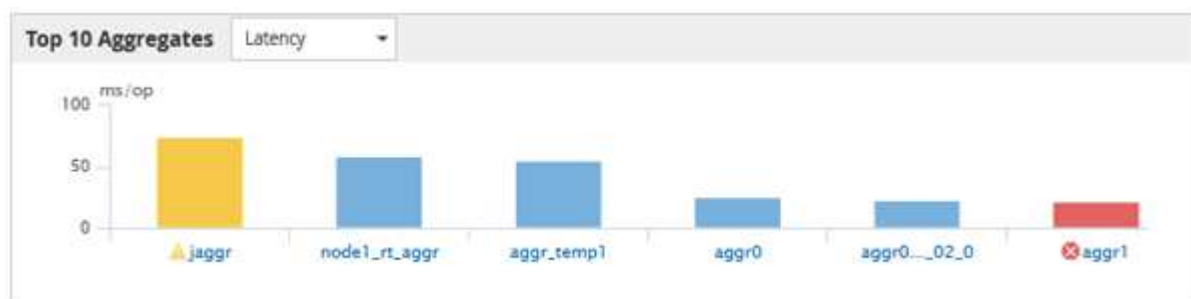
- レイテンシ
- IOPS
- MB/s
- 使用済みパフォーマンス容量（ノードとアグリゲートの場合）
- 利用率（ノードとアグリゲートの場合）

• * 並べ替え *

[* 並べ替え *] メニューをクリックして、選択したオブジェクトとカウンタの昇順または降順の並べ替えを選択します。オプションは、 * highest ~ lowest * および * lowest ~ highest * です。これらのオプションを使用すると、パフォーマンスが高いオブジェクトとパフォーマンスが低いオブジェクトを表示できます。



• * カウンターバー *

グラフのカウンタバーには、各オブジェクトのパフォーマンス統計が棒グラフで表示されます。棒グラフは色分けされ、カウンタがパフォーマンスしきい値に違反していない場合は青で表示されます。しきい値の違反がアクティブ（新規または確認済みのイベント）な場合、バーはそのイベントの色で表示されます。警告イベントは黄色（) をクリックすると、重大イベントが赤で表示されます（）。しきい値の違反は、警告イベントと重大イベントの重大度イベントインジケータアイコンでさらに細かく示されます。



各グラフの X 軸には、選択したオブジェクトタイプの上位のオブジェクトが表示されます。Y 軸には、選択したカウンタに適用可能な単位が表示されます。各垂直棒グラフ要素の下にあるオブジェクト名のリンクをクリックすると、選択したオブジェクトのパフォーマンスランディングページに移動します。

• * イベントの重大度インジケータ *

アクティブなクリティカルなオブジェクト名の左側には、 * 重大度イベント * インジケータアイコンが表示されます（）または warning（）上位のオブジェクトグラフのイベント。[Severity Event] インジケータアイコンをクリックすると、次の項目が表示されます。

- * 1 つのイベント *

そのイベントのイベント詳細ページに移動します。

- * 2 つ以上のイベント *

選択したオブジェクトのすべてのイベントを表示するためにフィルタされたイベントインベントリページに移動します。

- * 「エクスポート」 ボタン *

を作成します。CSV カウンタバーに表示されるデータを含むファイル。表示している単一のクラスタについてのファイルのほか、データセンターのすべてのクラスタについてのファイルを作成することもできます。

パフォーマンスインベントリページを使用したパフォーマンスの監視

オブジェクトインベントリパフォーマンスページには、オブジェクトタイプカテゴリ内のすべてのオブジェクトのパフォーマンス情報、パフォーマンスイベント、およびオブジェクトの健全性が表示されます。すべてのノードやすべてのボリュームなど、クラスタ内の各オブジェクトのパフォーマンスステータスの概要が一目でわかります。

オブジェクトインベントリパフォーマンスページでは、オブジェクトステータスの概要を確認し、すべてのオブジェクトの全体的なパフォーマンスを評価してオブジェクトのパフォーマンスデータを比較できます。オブジェクトインベントリページの内容を絞り込むには、検索、ソート、フィルタリングを実行します。パフォーマンスの問題があるオブジェクトをすばやく特定してトラブルシューティングプロセスを開始できるため、オブジェクトのパフォーマンスを監視および管理する場合に便利です。

Nodes - Performance / All Nodes Last updated: Jan 17, 2019, 7:54 AM

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

View All Nodes

<input type="checkbox"/>	Status	Node	Latency	IOPS	MBps	Flash Cache Reads	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster
<input type="checkbox"/>	!	ocum-mobility-02	10.2 ms/op	18,884 IOPS	156 MBps	N/A	81%	35%	16.6 TB	23.2 TB	ocum-mobility-01-02
<input checked="" type="checkbox"/>	!	opm-simplicity-01	2.01 ms/op	39,358 IOPS	153 MBps	<1%	119%	88%	4.88 TB	18.3 TB	opm-simplicity
<input type="checkbox"/>	✓	ocum-mobility-01	0.018 ms/op	<1 IOPS	18.2 MBps	N/A	23%	18%	8.69 TB	15.7 TB	ocum-mobility-01-02
<input type="checkbox"/>	✓	opm-simplicity-02	17 ms/op	14,627 IOPS	124 MBps	<1%	29%	20%	212 GB	5.88 TB	opm-simplicity

パフォーマンスインベントリページのオブジェクトは、デフォルトでは、オブジェクトのパフォーマンスの重大度に基づいてソートされます。新しい重大なパフォーマンスイベントが報告されたオブジェクトが最初に表示され、そのあとに警告イベントが報告されたオブジェクトが表示されます。これにより、対処が必要な問題を簡単に特定できます。パフォーマンスデータはいずれも 72 時間の平均値です。

オブジェクト名の列でオブジェクト名をクリックすると、オブジェクトインベントリパフォーマンスページからオブジェクトの詳細ページに簡単に移動できます。たとえば、Performance/AllNodes インベントリヘエシで、* Nodes * 列のノードオブジェクトをクリックします。オブジェクトの詳細ページには、アクティブなイベントを並べた比較など、選択したオブジェクトの詳細情報が表示されます。

すべてのストレージオブジェクトのパフォーマンスインベントリページを表示する

パフォーマンスインベントリページでは、クラスタ、アグリゲート、ボリュームなど、使用可能な各ストレージオブジェクトに関するパフォーマンス情報の概要を確認できます。パフォーマンスオブジェクト詳細ページへのリンクを使用して、特定のオブジェクトの詳細情報を表示できます。

ビューページ内のオブジェクトは、デフォルトでは、イベントの重大度に基づいてソートされます。重大イベントが報告されたオブジェクトが最初に表示され、そのあとに警告イベントが報告されたオブジェクトが表示されます。これにより、対処が必要な問題を簡単に特定できます。

これらのページのデータをカンマ区切り値でエクスポートできます (.csv) ファイル、Microsoft Excel ファイル (.xlsx) 、または (.pdf) *Reports* ボタンを使用して文書化し、エクスポートしたデータを使用してレポートを作成します。また、ページをカスタマイズしてから、定期的に作成して E メールで送信するようにレポートをスケジュール設定することもできます。その場合は、 * Scheduled Reports * ボタンを使用します。

これらのページ上のすべてのフィールドは、カスタムビューとレポートで使用できます。一部のフィールドは関連ページにリンクされており、より詳細な表示が可能です。

パフォーマンス：すべてのクラスタビュー

Performance : All Clusters ビューには、Unified Manager のインスタンスによって監視されている各クラスタのパフォーマンスイベント、データ、および設定情報の概要が表示されます。このページでは、クラスタのパフォーマンスを監視し、パフォーマンスの問題やしきい値イベントをトラブルシューティングすることができます。

パフォーマンスしきい値ポリシーは、オブジェクトインベントリページの任意のオブジェクトに、*パフォーマンスしきい値ポリシーの割り当て* ボタンと *パフォーマンスしきい値ポリシーのクリア* ボタンを使用して割り当てまたはクリアできます。

Performance : All Clusters ビューのいくつかの重要なフィールドを次に示します。

- Cluster FQDN : クラスタの完全修飾ドメイン名 (FQDN) 。
- IOPS : クラスタでの1秒あたりの入出力処理数。
- MBps : クラスタのスループット。1秒あたりのMiBで測定されます。
- 容量のフィールド : GiB単位の空き容量と合計容量。
- Host Name or IP Address : クラスタ管理LIFのホスト名またはIPアドレス (IPv4またはIPv6) 。
- OS Version : クラスタにインストールされているONTAP ソフトウェアのバージョン。



クラスタ内の各ノードに異なるバージョンのONTAP ソフトウェアがインストールされている場合は、最も低いバージョン番号が表示されます。各ノードにインストールされているONTAP のバージョンは、Performance : All Nodes ビューで確認できます。

- しきい値ポリシー : このストレージオブジェクトでアクティブなユーザ定義のパフォーマンスしきい値ポリシー。ポリシー名に省略記号 (...) が含まれている場合、ポリシー名にカーソルを合わせると完全なポリシー名または割り当てられているポリシー名のリストが表示されます。左端のチェックボックスをクリックしてオブジェクトを選択するまで、Assign Performance Threshold Policy ボタンと Clear Performance Threshold Policy ボタンは無効のままです。

Performance : All Volumes ビュー

Performance : All Volumes ビューには、Unified Manager のインスタンスによって監視されている各 FlexVol ボリュームおよび FlexGroup ボリュームのパフォーマンスイベント、カウンタデータ、および設定情報の概要が表示されます。このページでは、ボリュームのパフォーマンスを簡単に監視し、パフォーマンスの問題やしきい値イベントをトラブルシューティングすることができます。

特定のオブジェクトのレイテンシとスループットを分析するには、その他のオプションボタンをクリックしま

す。その後* Workload *を分析すると、Workload Analysisページにパフォーマンスと容量のグラフを表示できます。System Managerの有効なクレデンシャルがあれば、System Managerで詳細を確認することができます。



データ保護 (DP) ボリュームについては、ユーザが生成したトラフィックのカウンタ値のみが表示されます。ルートボリュームはこのページに表示されません。

Performance : All Volumesビューのいくつかの重要なフィールドを次に示します。

- 形式：FlexVol またはFlexGroup。
- Latency：FlexVol ボリュームの場合は、すべてのI/O要求のボリュームの平均応答時間で、処理あたりのミリ秒で表されます。FlexGroup ボリュームの場合は、すべてのコンスティチュエントボリュームの平均レイテンシです。
- IOPS/TB：ワークロードで消費されている合計スペースに基づく1秒あたりの入出力処理数。テラバイト単位で表示されます。このカウンタは、特定のストレージ容量で提供可能なパフォーマンスを測定します。
- IOPS：FlexVol ボリュームの場合、ボリュームでの1秒あたりの入出力処理数。FlexGroup ボリュームの場合は、すべてのコンスティチュエントボリュームの合計IOPS。
- MBps：FlexVol ボリュームの場合、ボリュームのスループットです。1秒あたりのメガバイト数で測定されます。FlexGroup ボリュームの場合は、すべてのコンスティチュエントボリュームの合計MBps。
- 容量のフィールド：GiB単位の空き容量と合計容量。

詳細については、次のリンクを参照してください。

- ["ストレージオブジェクトにパフォーマンスしきい値ポリシーを割り当てます"](#)
- ["ストレージオブジェクトからパフォーマンスしきい値ポリシーを削除する"](#)
- ["Unified Manager で監視されるワークロードのタイプ"](#)
- ["特定のボリュームまたは LUN に適用されている QoS ポリシーグループ設定を表示する"](#)
- ["Unified Manager によるクラウドへのデータの階層化の推奨について理解していること"](#)
- ["パフォーマンスチャートを表示して、同じ QoS ポリシーグループ内のボリュームまたは LUN を比較できます"](#)

パフォーマンス：すべてのアグリゲートが表示されます

Performance : All aggregatesビューには、Unified Managerのインスタンスによって監視されている各アグリゲートのパフォーマンスイベント、データ、および設定情報の概要が表示されます。このページでは、アグリゲートのパフォーマンスを監視し、パフォーマンスの問題やしきい値イベントをトラブルシューティングすることができます。

パフォーマンスのいくつかの重要なフィールドを次に示します。すべてのアグリゲートビュー。

- type：アグリゲートのタイプ。
 - HDD
 - ハイブリッドHDDとSSDの組み合わせですが、Flash Poolは有効になっていません。
 - Hybrid (Flash Pool)：HDDとSSDの組み合わせで、Flash Poolが有効になっています。

- SSD の場合
- SSD (FabricPool) : SSDとクラウド階層の組み合わせです
- HDD (FabricPool) HDDとクラウド階層の組み合わせです
- VMDisk (SDS) : 仮想マシン内の仮想ディスク
- VMディスク (FabricPool) : 仮想ディスクとクラウド階層の組み合わせです
- LUN (FlexArray)
- Inactive Data Reporting : このアグリゲートでInactive Data Reporting機能が有効になっているかどうか。有効にすると、このアグリゲートのボリュームのPerformance : All Volumesビューにコールドデータの量が表示されます。Inactive Data ReportingをサポートしていないONTAP のバージョンでは、このフィールドの値は「N/A」です。
- しきい値ポリシー : このストレージオブジェクトでアクティブなユーザ定義のパフォーマンスしきい値ポリシー。ポリシー名に省略記号 (...) が含まれている場合、ポリシー名にカーソルを合わせると完全なポリシー名または割り当てられているポリシー名のリストが表示されます。左端のチェックボックスをクリックしてオブジェクトを選択するまで、Assign Performance Threshold PolicyボタンとClear Performance Threshold Policyボタンは無効のままです。詳細については、次のリンクを参照してください。
- ["ストレージオブジェクトにパフォーマンスしきい値ポリシーを割り当てます"](#)
- ["ストレージオブジェクトからパフォーマンスしきい値ポリシーを削除する"](#)

Performance : All Nodesビュー

Performance : All Nodesビューには、Unified Managerのインスタンスによって監視されている各ノードのパフォーマンスイベント、データ、および設定情報の概要が表示されます。このページでは、ノードのパフォーマンスを簡単に監視し、パフォーマンスの問題やしきい値イベントをトラブルシューティングすることができます。



Flash Cache読み取りでは、ノードに対する読み取り処理の割合がディスクから返されるのではなく、キャッシュで対応されます。Flash Cache のデータは、ノードに Flash Cache モジュールがインストールされている場合にのみ表示されます。

レポート*メニューには、Unified Managerとその管理対象クラスタが外部ネットワークに接続されていないサイトにインストールされている場合に、*ハードウェアインベントリレポート*オプションが表示されます。このボタンを使用すると、ハードウェアのモデル番号とシリアル番号、ディスクのタイプと数、インストールされているライセンスなど、クラスタとノードのすべての情報を含む.csvファイルが生成されます。このレポート機能は、NetApp Active IQ プラットフォームに接続されていないセキュアなサイトでの契約更新に役立ちます。パフォーマンスしきい値ポリシーは、オブジェクトインベントリページの任意のオブジェクトに、*パフォーマンスしきい値ポリシーの割り当て*ボタンと*パフォーマンスしきい値ポリシーのクリア*ボタンを使用して割り当てまたはクリアできます。

詳細については、次のリンクを参照してください。

- ["ストレージオブジェクトにパフォーマンスしきい値ポリシーを割り当てます"](#)
- ["ストレージオブジェクトからパフォーマンスしきい値ポリシーを削除する"](#)
- ["契約更新用のハードウェアインベントリレポートの生成"](#)

Performance : All Storage VMビュー

Performance : All Storage VMビューには、Unified Managerのインスタンスによって監視されている各Storage Virtual Machine (SVM) のパフォーマンスイベント、データ、および設定情報の概要が表示されます。このページでは、SVMのパフォーマンスを簡単に監視し、パフォーマンスの問題やしきい値イベントをトラブルシューティングすることができます。このページのLatencyフィールドは、すべてのI/O要求の平均応答時間を処理あたりのミリ秒で表示します。




このページに表示されるSVMは、データSVMとクラスタSVMだけです。Unified Managerでは、管理SVMとノードSVMが使用されず、表示もされません。

詳細については、次のリンクを参照してください。

- ["ストレージオブジェクトにパフォーマンスしきい値ポリシーを割り当てます"](#)
- ["ストレージオブジェクトからパフォーマンスしきい値ポリシーを削除する"](#)

Performance : All LUNsビュー

Performance : All LUNsビューには、Unified Managerのインスタンスによって監視されている各LUNのパフォーマンスイベント、データ、および設定情報の概要が表示されます。このページでは、LUNのパフォーマンスを簡単に監視し、パフォーマンスの問題やしきい値イベントをトラブルシューティングすることができます。

特定のオブジェクトのレイテンシとスループットを分析するには、詳細アイコンをクリックします  をクリックし、*ワークロードの分析*を実行すると、パフォーマンスと容量のグラフを*ワークロード分析*のページで確認できます。

詳細については、次のリンクを参照してください。

- ["コンシステンシグループ関係の LUN を監視しています"](#)
- ["LUN のプロビジョニング"](#)
- ["ストレージオブジェクトにパフォーマンスしきい値ポリシーを割り当てます"](#)
- ["ストレージオブジェクトからパフォーマンスしきい値ポリシーを削除する"](#)
- ["同じ QoS ポリシーグループ内のボリュームまたは LUN の表示"](#)
- ["特定のボリュームまたは LUN に適用されている QoS ポリシーグループ設定を表示する"](#)
- ["APIを使用したLUNのプロビジョニング"](#)

パフォーマンス：すべてのNVMeネームスペースビュー

Performance : All NVMeネームスペースビューには、Unified Managerのインスタンスによって監視されている各NVMeネームスペースのパフォーマンスイベント、データ、および設定情報の概要が表示されます。このページでは、ネームスペースのパフォーマンスと健全性を簡単に監視し、問題やしきい値イベントをトラブルシューティングすることができます。

特に、次の情報が報告されます。ネームスペースの現在の状態。オフライン-ネームスペースへの読み取り/書き込みアクセスが許可されていません。*オンライン-ネームスペースへの読み取り/書き込みアクセスが許可されています。NVFail - NVRAMの障害が原因でネームスペースが自動的にオフラインになっています。*スペースエラー-ネームスペースのスペースが不足しています。

詳細については、次のリンクを参照してください。

- ["ストレージオブジェクトにパフォーマンスしきい値ポリシーを割り当てます"](#)
- ["ストレージオブジェクトからパフォーマンスしきい値ポリシーを削除する"](#)

パフォーマンス：すべてのネットワークインターフェイスビュー

Performance：All Network Interfacesビューには、Unified Managerの現在のインスタンスで監視している各ネットワークインターフェイス（LIF）のパフォーマンスイベント、データ、および設定情報の概要が表示されます。このページでは、インターフェイスのパフォーマンスを簡単に監視し、パフォーマンスの問題やしきい値イベントをトラブルシューティングすることができます。Performance：All Network Interfacesビューのいくつかの重要なフィールドを次に示します。

- IOPS：1秒あたりの入出力処理数。NFS LIFとCIFS LIFにはIOPSは適用されず、これらのタイプではN/Aと表示されます。
- Latency：すべてのI/O要求の平均応答時間。処理あたりのミリ秒数で表されます。レイテンシはNFS LIFとCIFS LIFには該当せず、これらのタイプではN/Aと表示されます。
- ホームの場所：インターフェイスのホームの場所。ノード名とポート名をコロン（:）で区切った形式で表示されます。場所が省略記号（...）とともに表示される場合は、場所の名前にカーソルを合わせると場所全体が表示されます。
- Current Location：インターフェイスの現在の場所。ノード名とポート名をコロン（:）で区切った形式で表示されます。場所が省略記号（...）とともに表示される場合は、場所の名前にカーソルを合わせると場所全体が表示されます。
- ロール：インターフェイスのロール：「データ」、「クラスタ」、「ノード管理」、「クラスタ間」のいずれかです。



このページに表示されるインターフェイスには、データLIF、クラスタLIF、ノード管理LIF、クラスタ間LIFがあります。Unified ManagerではシステムLIFが使用されず、表示もされません。

Performance：All Portsビュー

Performance：All Portsビューには、Unified Managerのインスタンスによって監視されている各ポートのパフォーマンスイベント、データ、および設定情報の概要が表示されます。このページでは、ポートのパフォーマンスを簡単に監視し、パフォーマンスの問題やしきい値イベントをトラブルシューティングすることができます。ポートロールについては、「Data」または「Cluster」のいずれかのネットワークポート機能が表示されます。FCPポートにはロールを指定できないため、「N/A」と表示されます



パフォーマンスカウンタの値は物理ポートについてのみ表示されます。VLANまたはインターフェイスグループのカウンタ値は表示されません。

詳細については、次のリンクを参照してください。

- ["ストレージオブジェクトにパフォーマンスしきい値ポリシーを割り当てます"](#)
- ["ストレージオブジェクトからパフォーマンスしきい値ポリシーを削除する"](#)

Performance：QoS Policy Groupsビュー

QoSポリシーグループビューには、Unified Managerが監視しているクラスタで使用可能なQoSポリシーグループが表示されます。これには、従来のQoSポリシー、アダプティブQoSポリシー、およびパフォーマンスサービスレベルを使用して割り当てられたQoSポリシーが含まれます。

Performance：QoS Policy Groupsビューのいくつかの重要なフィールドを次に示します。

- QoS Policy Group：QoSポリシーグループの名前。Unified Manager 9.7以降にインポートされたNetApp Service Level Manager（NSLM）1.3ポリシーの場合、ここに表示される名前には、SVM名、およびパフォーマンスサービスレベルがNSLMで定義された時点では名前に含まれていないその他の情報が含まれます。たとえば「NSLM_vs6_Performance_2_0」という名前は、SVM「vs6」に作成された、想定レイテンシが「2ミリ秒/処理」のNSLMシステム定義の「パフォーマンス」PSLポリシーであることを意味します。
- SVM：QoSポリシーグループが属するStorage VM（SVM）。Storage VM名をクリックすると、そのStorage VMの詳細ページが表示されます。管理Storage VMにQoSポリシーが作成されている場合、このStorage VMタイプはクラスタを表すため、このフィールドは空白になります。
- Min Throughput：ポリシーグループで提供される最小スループット（IOPS）。アダプティブポリシーの場合、ボリュームまたはLUNに割り当てられる最小想定IOPS/TBで、ストレージオブジェクトの割り当てサイズに基づきます。
- Max Throughput：ポリシーグループの最大スループット（IOPSまたはMB/秒）。このフィールドが空白の場合、ONTAPに定義されている最大スループットは制限されていません。アダプティブポリシーの場合、ボリュームまたはLUNに割り当てられる最大（ピーク）IOPS/TBで、ストレージオブジェクトの割り当てサイズまたは使用済みサイズに基づきます。
- 絶対最小IOPS：アダプティブポリシーの場合、想定IOPSがこの値より低い場合に上書き値として使用される絶対最小IOPS値です。
- Block Size：QoSアダプティブポリシーに指定されているブロックサイズ。
- 最小割り当て：最大スループット（ピーク）IOPSを決定するために「割り当てスペース」と「使用済みスペース」のどちらを使用するか。
- 想定レイテンシ：ストレージの入出力処理の想定平均レイテンシ。
- Shared：従来のQoSポリシーの場合、ポリシーグループに定義されたスループット値を複数のオブジェクトで共有するかどうか。
- Associated Objects：QoSポリシーグループに割り当てられているワークロードの数。展開ボタン（▼）をクリックし、ポリシーグループに関する詳細情報を表示します。
- Allocated Capacity：QoSポリシーグループ内のオブジェクトが現在使用しているスペースの量。
- 関連付けられているオブジェクト：QoSポリシーグループに割り当てられているワークロードの数。ボリュームとLUNに分けて表示されます。数字をクリックすると、選択したボリュームまたはLUNに関する詳細情報を表示するページに移動できます。

詳細については、のトピックを参照してください ["QoS ポリシーグループ情報を使用したパフォーマンスの管理"](#)。

パフォーマンスインベントリページの内容の改善

パフォーマンスオブジェクトのインベントリページには、オブジェクトインベントリデータのコンテンツを絞り込むためのツールが含まれており、特定のデータをすばやく簡単に見つけることができます。

パフォーマンスオブジェクトのインベントリページに格納される情報は多岐にわたる場合があり、複数のページにまたがるがよくあります。この種の包括的なデータは、パフォーマンスの監視、追跡、改善には非常に役立ちますが、特定のデータを特定するには、探しているデータをすばやく特定するためのツールが必要です。したがって、パフォーマンスオブジェクトのインベントリページには、検索、ソート、およびフィルタリングの機能が含まれています。また、検索とフィルタリングを組み合わせ、結果をさらに絞り込むこともで

きます。

オブジェクトインベントリのパフォーマンスページで検索しています

オブジェクトインベントリのパフォーマンスページで文字列を検索できます。ページの右上にある * Search * フィールドを使用して、オブジェクト名またはポリシー名に基づいてデータをすばやく検索できます。これにより、特定のオブジェクトとその関連データをすばやく特定したり、ポリシーを特定して関連するポリシーオブジェクトデータを表示したりできます。

ステップ

1. 検索条件に基づいて、次のいずれかのオプションを実行します。

検索対象	入力する内容
特定のオブジェクト	[* 検索 * (* Search *)] フィールドのオブジェクト名を入力し、[* 検索 * (* Search *)] をクリックする。該当するオブジェクトとその関連データが表示されます。
ユーザ定義のパフォーマンスしきい値ポリシー	ポリシー名のすべてまたは一部を * Search * フィールドに入力し、* Search * をクリックします。該当するポリシーに割り当てられているオブジェクトが表示されます。

オブジェクトインベントリのパフォーマンスページでソートします

オブジェクトインベントリパフォーマンスページのすべてのデータを任意の列で昇順または降順でソートできます。オブジェクトインベントリデータをすばやく特定できるため、パフォーマンスの調査時やトラブルシューティングの開始時に役立ちます。

ソート用に選択した列は、列見出し名が強調表示され、ソート方向を示す矢印アイコンが名前の右側に表示されます。上矢印は昇順、下矢印は降順を示します。デフォルトのソート順序は、ステータス * (イベントの重要度) が降順、重大度が最も高いパフォーマンスイベントが最初に表示されます。

ステップ

1. 列名をクリックすると、昇順または降順で列のソート順序を切り替えることができます。

Object Inventory Performance ページの内容は、選択した列に基づいて昇順または降順でソートされません。

オブジェクトインベントリのパフォーマンスページでのデータのフィルタリング

オブジェクトインベントリのパフォーマンスページでデータをフィルタリングして、特定の条件に基づいてデータをすばやく特定できます。フィルタリングを使用すると、オブジェクトインベントリのパフォーマンスページの内容を絞り込んで、指定した結果だけを表示できます。そのため、関心のあるパフォーマンスデータだけを効率的に表示で

きます。

フィルタリングパネルを使用して、プリファレンスに基づいてグリッドビューをカスタマイズできます。使用可能なフィルタオプションは、グリッドで表示しているオブジェクトタイプによって異なります。フィルタが現在適用されている場合は、[フィルタ (Filter)] ボタンの右側に適用されたフィルタの数が表示されます。

3 種類のフィルタパラメータがサポートされています。

パラメータ	検証
文字列 (テキスト)	演算子は、 * contains * 、 * starts with * 、 * ends with * 、 および * does not contain * です。
番号	演算子は、 * より大きい * 、 * より小さい * 、 * の最後の * 、 および * の間です。
列挙 (テキスト)	演算子は * は * で、 * は * ではありません。

各フィルタには、列、演算子、および値のフィールドが必要です。使用可能なフィルタは、現在のページのフィルタ可能な列に基づいています。適用できるフィルタは 4 つまでです。フィルタパラメータの組み合わせに基づいてフィルタされた結果が表示されます。フィルタされた結果は、現在表示されているページだけでなく、フィルタ処理された検索のすべてのページに適用されます。

フィルタパネルを使用してフィルタを追加できます。

1. ページの上部にある * Filter * ボタンをクリックします。フィルタリングパネルが表示されます。
2. 左側のドロップダウンリストをクリックし、 *Cluster* 、パフォーマンスカウンタなどのオブジェクトを選択します。
3. 中央のドロップダウンリストをクリックし、使用する演算子を選択します。
4. 最後のリストで値を選択または入力して、そのオブジェクトのフィルタを完成させます。
5. 別のフィルタを追加するには、 [* + フィルタの追加 *] をクリックします。追加のフィルタフィールドが表示されます。前述の手順に従って、このフィルタを設定します。4 番目のフィルタを追加すると、 [* + フィルタを追加 *] ボタンは表示されなくなります。
6. [フィルタを適用 (Apply Filter)] をクリックする。フィルタオプションがグリッドに適用され、フィルタボタンの右側にフィルタの数が表示されます。
7. フィルタパネルを使用して、削除するフィルタの右側にあるゴミ箱アイコンをクリックして、個々のフィルタを削除します。
8. すべてのフィルターを削除するには、フィルターパネルの下部にある * リセット * をクリックします。

フィルタリングの例

次の図は、フィルタパネルと 3 つのフィルタを示しています。フィルタを最大 4 つまでしか使用できない場合は、「 * + フィルタを追加 * 」ボタンが表示されます。

MBps	greater than	5	MBps	
Node	name starts with	test		
Type	is	FCP Port		
+ Add Filter				
				<div>Cancel</div> <div>Apply Filter</div>

[フィルタの適用 (Apply Filter)] をクリックすると、[フィルタ (Filtering)] パネルが閉じ、フィルタが適用され、適用されているフィルタの数が表示されます (3) 。

Unified Manager によるクラウドへのデータの階層化の推奨について理解していること

Performance : All Volumes ビューには、ボリ्यूームに格納されているアクセス頻度の低いユーザデータ (コールドデータ) のサイズに関する情報が表示されます。Unified Manager が、特定のボリ्यूームについて、アクセス頻度の低いデータを FabricPool 対応アグリゲートのクラウド階層 (クラウドプロバイダまたは StorageGRID) に階層化することを推奨することがあります。



FabricPool は ONTAP 9.2 で導入されたため、9.2 より前のバージョンの ONTAP ソフトウェアを使用している場合、Unified Manager によるデータの階層化の推奨を有効にするには、ONTAP ソフトウェアのアップグレードが必要になります。また、も参照してください **auto** 階層化ポリシーは ONTAP 9.4 およびに導入されました **all** 階層化ポリシーは ONTAP 9.6 で導入されたため、auto 階層化ポリシーの使用が推奨される場合は、ONTAP 9.4 以降にアップグレードする必要があります。

Performance : All Volumes ビューの次の 3 つのフィールドは、アクセス頻度の低いデータをクラウド階層に移動することでストレージシステムのディスク使用率の改善やパフォーマンス階層のスペースの削減が可能かどうかに関する情報を提供します。

• * 階層化ポリシー *

階層化ポリシーによって、ボリ्यूームのデータを高パフォーマンス階層に残すか、あるいは一部のデータをパフォーマンス階層からクラウド階層に移動するかが決まります。

このフィールドには、ボリ्यूームに対して設定されている階層化ポリシーが、ボリ्यूームが現在 FabricPool アグリゲートにない場合も含めて表示されます。階層化ポリシーが適用されるのは、ボリ्यूームが FabricPool アグリゲートにある場合のみです。

• * コールドデータ *

ボリ्यूームに格納されているアクセス頻度の低いユーザデータ (コールドデータ) のサイズが表示されます。

この値は、ONTAP 9.4 以降のソフトウェアを使用している場合にのみ表示されます。ボリ्यूームを導入するアグリゲートにが含まれている必要があるためです **inactive data reporting parameter** をに設定します **enabled**、を使用しているボリ्यूームで、クーリング日数のしきい値の最小値に達していること

`snapshot-only` または **auto** 階層化ポリシー)。それ以外の場合、値は「N/A」と表示されます。

• * クラウドの推奨事項 *

ボリュームのデータアクティビティに関して十分な情報が収集されると、Unified Manager は、対処が不要か、またはアクセス頻度の低いデータをクラウド階層に移動することでパフォーマンス階層のスペースを削減できるかを判断することができます。



コールドデータフィールドは 15 分ごとに更新されますが、ボリュームでコールドデータ分析が実行されると、クラウドの推奨事項フィールドが 7 日ごとに更新されます。したがって、コールドデータの正確な量はフィールド間で異なる場合があります。Cloud Recommendation フィールドには、分析が実行された日付が表示されます。

Inactive Data Reporting が有効になっている場合は、コールドデータフィールドにはアクセス頻度の低いデータの正確な量が表示されます。Inactive Data Reporting 機能を使用できない場合、Unified Manager はパフォーマンス統計に基づいてアクセス頻度の低いデータがボリュームにあるかどうかを判断します。アクセス頻度の低いデータの量はこの場合のコールドデータフィールドには表示されませんが、クラウドに関する推奨事項を表示するために「* ティア *」という単語にカーソルを合わせると表示されます。

クラウドに関する推奨事項は次のとおりです。

- * 学習中 *。推奨事項を利用できるだけの十分なデータが収集されていません。
- * 階層 *。分析の結果、アクセス頻度の低いコールドデータがボリュームにあり、そのデータをクラウド階層に移動するようにボリュームを設定することが推奨されます。一部のケースでは、ボリュームをまず FabricPool 対応アグリゲートに移動する必要があります。ボリュームがすでに FabricPool アグリゲートにあれば、階層化ポリシーの変更だけで済みます。
- * アクションなし *。ボリュームにアクセス頻度の低いデータがほとんどないか、ボリュームが FabricPool アグリゲートですでに「auto」階層化ポリシーに設定されているか、ボリュームがデータ保護ボリュームです。この値は、ボリュームがオフラインの場合や MetroCluster 構成で使用されている場合にも表示されます。

ボリュームを移動したり、ボリュームの階層化ポリシーやアグリゲートの Inactive Data Reporting の設定を変更するには、ONTAP System Manager、ONTAP の CLI コマンド、またはこの 2 つを組み合わせ使用します。

アプリケーション管理者またはストレージ管理者のロールで Unified Manager にログインしている場合は、「* 階層 *」にカーソルを合わせるとクラウドに関する推奨事項の「ボリュームの設定 *」リンクが表示されます。このボタンをクリックすると、System Manager の Volumes（ボリューム）ページが開き、推奨される変更が行われます。

パフォーマンスエクスプローラページを使用したパフォーマンスの監視

パフォーマンスエクスプローラページには、クラスタ内の各オブジェクトのパフォーマンスに関する詳細情報が表示されます。すべてのクラスタオブジェクトのパフォーマンスの詳細を表示でき、さまざまな期間にわたる特定のオブジェクトのパフォーマンスデータを選択して比較できます。

また、すべてのオブジェクトの全体的なパフォーマンスを評価したり、オブジェクトのパフォーマンスデータ

を並べて比較したりできます。

ルートオブジェクトについて

ルートオブジェクトは、他のオブジェクトを比較する際のベースラインです。他のオブジェクトのデータを表示してルートオブジェクトと比較し、パフォーマンスデータを分析してオブジェクトのパフォーマンスのトラブルシューティングや向上に利用できます。

ルートオブジェクト名は、比較ペインの上部に表示されます。その他のオブジェクトはルートオブジェクトの下に表示されます。[比較 (Comparing)] パネルに追加できる追加オブジェクトの数に制限はありませんが、許可されるルートオブジェクトは 1 つだけです。ルートオブジェクトのデータは、カウンタグラフペインのグラフに自動的に表示されます。

ルートオブジェクトは変更できません。常に表示しているオブジェクトページに設定されます。たとえば、ボリューム 1 のボリュームパフォーマンスエクスプローラページを開くと、ボリューム 1 がルートオブジェクトになり、変更できなくなります。別のルートオブジェクトと比較する場合は、オブジェクトのリンクをクリックして、そのランディングページを開く必要があります。



イベントとしきい値はルートオブジェクトに対してのみ表示されます。

フィルタによるグリッドの関連オブジェクトのリストの絞り込み

フィルタを使用してグリッドに表示されるオブジェクトのサブセットを絞り込むことができます。たとえば、グリッドにボリュームが 25 個ある場合、フィルタを使用することで、それらのボリュームの中からスループットが 90MBps 未満のボリュームのみを表示したり、レイテンシが 1 ミリ秒 / 処理を超えるボリュームだけを表示したりできます。

関連オブジェクトの期間の指定

パフォーマンスエクスプローラページの時間範囲セレクタを使用して、オブジェクトデータを比較する期間を指定できます。時間範囲を指定すると、パフォーマンスエクスプローラのページの内容が調整され、指定した期間内のオブジェクトデータのみが表示されます。

期間を絞り込むと、関心のあるパフォーマンスデータだけを効率的に表示できます。事前定義の期間を選択するか、カスタムの期間を指定できます。デフォルトの期間は過去 72 時間です。

事前定義の期間を選択します

事前定義の期間を選択すると、クラスタオブジェクトのパフォーマンスデータを表示する際に、すばやく効率的にデータ出力をカスタマイズして絞り込むことができます。事前定義の期間を選択する場合、最大 13 カ月分のデータを使用できます。

手順

1. パフォーマンスエクスプローラ * ページの右上にある * 時間範囲 * をクリックします。
2. 時間範囲の選択 * (* Time Range Selection *) パネルの右側で、事前定義された時間範囲を選択しま

す。

3. [* 範囲の適用 *] をクリックします。

カスタムの期間を指定する

パフォーマンスエクスプローラページでは、パフォーマンスデータの日時範囲を指定できます。カスタムの期間を指定すると、クラスタオブジェクトのデータを絞り込む際に、事前定義の期間を使用するよりも柔軟に設定できます。

期間は 1 時間から 390 日の間で選択できます。1 カ月は 30 日としてカウントされるため、390 日は 13 カ月に相当します。日時の範囲を指定すると、特定のパフォーマンスイベントや一連のイベントにフォーカスして詳細を確認することができます。また、日時の範囲を指定すると、パフォーマンスイベントに関連するデータがより詳しく表示されるため、潜在的なパフォーマンスの問題のトラブルシューティングにも役立ちます。事前定義された日付と時間の範囲を選択するには、* Time Range* コントロールを使用します。また、独自の日時の範囲を 390 日まで指定することもできます。事前に定義された時間範囲のボタンは、* 過去 1 時間 * から * 過去 13 カ月 * までの間で異なります。

「過去 13 カ月」オプションを選択するか、30 日を超えるカスタムの日付範囲を指定すると、5 分ごとのデータポーリングではなく 1 時間ごとの平均値で 30 日を超える期間について表示されるパフォーマンスデータが示されるダイアログボックスが表示されます。そのため、タイムラインには要約された情報が表示される可能性があります。ダイアログボックスで * 再表示しない * オプションをクリックした場合、* 過去 13 カ月 * オプションを選択したとき、または 30 日を超えるカスタム日付範囲を指定したときに、メッセージは表示されません。期間が 30 日以内でも、現在の日付から 1 つ以上あとの日時が期間に含まれている場合には要約データが表示されます。

選択した期間（カスタムまたは事前定義）が 30 日以内の場合、5 分ごとのデータサンプルに基づいてデータが表示されます。30 日を超える場合は、1 時間ごとのデータサンプルに基づいてデータが表示されます。

The screenshot displays a 'Time Range' selection interface. It features two side-by-side calendar pickers for April 2015. The left calendar, labeled 'From', shows the 12th as the start date. The right calendar, labeled 'To', shows the 15th as the end date. Below each calendar is a 'Time' dropdown menu, both currently set to '6:00 am'. To the right of the calendars is a vertical list of predefined time range buttons: 'Last Hour', 'Last 24 Hours', 'Last 72 Hours', 'Last 7 Days', 'Last 30 Days', 'Last 13 Months', and 'Custom Range'. At the bottom right of the dialog are 'Cancel' and 'Apply Range' buttons.

1. [* 時間範囲 * (Time Range *)] ドロップダウンボックスをクリックすると、[時間範囲 (Time Range)] パネルが表示されます。
2. 事前定義された時間範囲を選択するには、* 時間範囲 * パネルの右側にある * 最後 ... * ボタンのいずれかををクリックします。事前定義の期間を選択する場合、最大 13 カ月分のデータを使用できます。選択した事前定義の時間範囲ボタンが強調表示され、対応する日と時間がカレンダーと時間セレクタに表示されます。
3. カスタムの日付範囲を選択するには、左側の * 開始日 * カレンダーで開始日をクリックします。カレンダー内を前後に移動するには、「*」または「*」をクリックします。終了日を指定するには、右側の * か

ら * のカレンダーで日付をクリックします。別の終了日を指定しないかぎり、デフォルトの終了日は今日です。時間範囲パネルの右側にある * カスタム範囲 * ボタンが強調表示され、カスタム日付範囲が選択されていることを示します。

4. カスタムの時間範囲を選択するには、* 開始 * カレンダーの下にある * 時間 * コントロールをクリックし、開始時間を選択します。終了時刻を指定するには、右側の * To * カレンダーの下にある * Time * コントロールをクリックし、終了時刻を選択します。時間範囲パネルの右側にある * カスタム範囲 * ボタンが強調表示され、カスタム時間範囲が選択されていることを示します。
5. 事前定義された日付範囲を選択する際に、開始時間と終了時間を指定することもできます。前述の説明に従って事前定義された日付範囲を選択し、前述のように開始時間と終了時間を選択します。選択した日付がカレンダーで強調表示され、指定した開始時刻と終了時刻が * Time * コントロールに表示され、* Custom Range * ボタンが強調表示されます。
6. 日付と時間の範囲を選択したら、* 適用範囲 * をクリックします。その期間のパフォーマンス統計がグラフとイベントタイムラインに表示されます。

比較グラフ用の関連オブジェクトのリストを定義する

カウンタグラフペインでは、データとパフォーマンスの比較の関連オブジェクトのリストを定義できます。たとえば、Storage Virtual Machine（SVM）でパフォーマンス問題が発生した場合は、SVM 内のすべてのボリュームを比較して、問題の原因となったボリュームを特定できます。


関連オブジェクトグリッド内の任意のオブジェクトを比較ペインとカウンタチャートペインに追加できます。これにより、複数のオブジェクトおよびルートオブジェクトのデータを表示して比較できます。関連オブジェクトグリッドとの間でオブジェクトを追加および削除できますが、比較ペインのルートオブジェクトは削除できません。




多くのオブジェクトを比較ペインに追加すると、パフォーマンスが低下する可能性があります。パフォーマンスを維持するには、データ比較用グラフの数を制限する必要があります。

手順

1. オブジェクトグリッドで、追加するオブジェクトを探し、* 追加 * ボタンをクリックします。

[**Add**] ボタンがグレーに変わり、[**比較**] ペインの追加オブジェクトリストにオブジェクトが追加されます。オブジェクトのデータがカウンタグラフペインのグラフに追加されます。オブジェクトの目のアイコンの色（）は、グラフ内のオブジェクトのデータラインの色に一致します。

2. * オプション：* 選択したオブジェクトのデータを表示または非表示にします。

作業	対処方法
選択したオブジェクトを非表示にします	選択したオブジェクトの目のアイコン（  ）を比較ペインに表示します。オブジェクトのデータが非表示になり、そのオブジェクトの目のアイコンがグレーに変わります。

作業	対処方法
非表示のオブジェクトを表示します	<p>比較ペインで選択したオブジェクトの灰色の目のアイコンをクリックします</p> <p>目のアイコンが元の色に戻り、オブジェクトデータがカウンタグラフペインのグラフに再度追加されます。</p>

3. * オプション： * Comparing * ペインから選択したオブジェクトを削除します。

作業	対処方法
選択したオブジェクトを削除します	比較ペインで選択したオブジェクトの名前の上にカーソルを移動して、オブジェクトを削除ボタン（* X *）を表示し、ボタンをクリックします。オブジェクトが比較ペインから削除され、そのデータがカウンタチャートからクリアされます。
選択したオブジェクトをすべて削除します	比較ペインの上部にあるすべてのオブジェクトの削除ボタン（* X *）をクリックします。選択したすべてのオブジェクトとそのデータが削除され、ルートオブジェクトだけが残ります。

カウンタグラフの概要

カウンタグラフペインのグラフでは、ルートオブジェクトのパフォーマンスデータと、関連オブジェクトグリッドから追加したオブジェクトのパフォーマンスデータを表示および比較できます。これは、パフォーマンスの傾向を把握して、パフォーマンスの問題を特定および解決するのに役立ちます。

デフォルトで表示されるカウンタグラフは、イベント、レイテンシ、IOPS、および MBps です。オプションで表示できるグラフは、利用率、使用済みパフォーマンス容量、使用可能な IOPS、IOPS/TB、キャッシュミス率です。また、レイテンシ、IOPS、MBps、および使用済みパフォーマンス容量の各グラフの合計値と内訳値を表示することもできます。

パフォーマンスエクスプローラには、デフォルトで特定のカウンタグラフが表示されます。それらがすべてサポートされているかどうかは関係ありません。サポートされていないカウンタグラフは空で、メッセージが表示されます Not applicable for <object> が表示されます

チャートには、ルートオブジェクトと、比較ペインで選択したすべてのオブジェクトのパフォーマンスの傾向が表示されます。各グラフのデータは次のように配置されています。

• * X 軸 *

指定した期間が表示されます。期間を指定しなかった場合のデフォルトの期間は過去 72 時間です。

• * Y 軸 *

選択したオブジェクトに固有のカウンタ単位が表示されます。

傾向線の色は、比較ペインに表示されるオブジェクト名の色と一致します。任意のラインの特定のポイントにカーソルを合わせると、そのポイントの時間と値の詳細を確認できます。

グラフ内の特定の期間について調査するには、次のいずれかの方法を使用します。

- 「* < *」 ボタンを使用して、カウンタチャートペインを展開し、ページの幅を広げます。
- カーソルを使用して（虫眼鏡に変わる）チャート内の一部の期間を選択し、拡大する。[グラフのズームをリセット] をクリックすると、グラフをデフォルトの期間に戻すことができます。
- 拡大した詳細やしきい値インジケータを含む大きなカウンタチャートを表示するには、* Zoom View * ボタンを使用します。



ラインが途切れて表示されることがあります。その期間は Unified Manager がストレージシステムからパフォーマンスデータを収集できなかったか、Unified Manager が停止していた可能性があります。

パフォーマンスカウンタグラフのタイプ

標準のパフォーマンスグラフには、選択したストレージオブジェクトのカウンタの値が表示されます。内訳カウンタグラフには、合計値が読み取り、書き込み、およびその他のカテゴリに分けて表示されます。さらに、一部の内訳カウンタグラフでは、ズームビューでグラフを表示すると詳細が表示されます。

次の表は、使用可能なパフォーマンスカウンタグラフを示しています。

使用可能なチャート	Chart 概要（チャート）
イベント	ルートオブジェクトの統計グラフに関連し、重大、エラー、警告、情報のイベントが表示されます。パフォーマンスイベントに加えて健全性イベントも表示されるため、パフォーマンスに影響する可能性がある原因を総合的に確認できます。
レイテンシ - 合計	アプリケーションの要求に応答するまでのミリ秒数。平均レイテンシの値は、I/O の重み付きの値です。
レイテンシ - 内訳	Latency Total に表示される同じ情報が、パフォーマンスデータが読み取り、書き込み、その他のレイテンシに分けて表示されます。このグラフは、選択したオブジェクトが SVM、ノード、アグリゲート、ボリューム、LUN である場合にのみ表示されます。またはネームスペースです。

使用可能なチャート	Chart 概要（チャート）
Latency - クラスタコンポーネント	Latency Total に表示される同じ情報が、パフォーマンスデータがクラスタコンポーネントごとのレイテンシに分けて表示される。このグラフは、選択したオブジェクトがボリュームの場合にのみ表示されます。
IOPS - 合計	1 秒あたりの入出力処理数。ノードに対して表示される場合、「Total」を選択すると、そのノードを経由する（ローカルノードまたはリモートノード上の）データの IOPS が表示されます。「Total（Local）」を選択すると、現在のノード上のデータの IOPS が表示されます。
IOPS - 内訳	<p>IOPS の合計に表示される情報は同じですが、パフォーマンスデータが読み取り、書き込み、その他の IOPS に分けて表示されます。このグラフは、選択したオブジェクトが SVM、ノード、アグリゲート、ボリューム、LUN である場合にのみ表示されます。またはネームスペースです。</p> <p>ズームビューで表示した場合、QoS の最小スループットと最大スループットの値が ONTAP で設定されていれば、それらの値が表示されます。</p> <p>ノードに対して表示される場合、「内訳」を選択すると、そのノードを経由する（ローカルノードまたはリモートノード上の）データの IOPS の内訳が表示されます。「内訳（ローカル）」を選択すると、現在のノード上のデータの IOPS の内訳が表示されます。</p>
IOPS - プロトコル	IOPS の合計に表示される情報は同じですが、パフォーマンスデータは、CIFS、NFS、FCP、NVMe、iSCSI のプロトコルトラフィックの個々のグラフに分けて表示されます。このグラフは、選択したオブジェクトが SVM の場合にのみ表示されます。
IOPS/TB - 合計	<p>ワークロードで消費されている合計スペースに基づいて 1 秒あたりの入出力処理数（テラバイト単位）。I/O 密度とも呼ばれ、所定のストレージ容量で提供可能なパフォーマンスを表します。ズームビューで表示した場合、ONTAP で設定されている場合、ボリュームのグラフには QoS の想定スループットとピークスループットの値が表示されます。</p> <p>このグラフは、選択したオブジェクトがボリュームの場合にのみ表示されます。</p>

使用可能なチャート	Chart 概要（チャート）
MBps - 合計	1 秒あたりにオブジェクトとの間で転送されたデータのメガバイト数。
MBps - 内訳	<p>MBps グラフにも同じ情報が表示されますが、スループットデータがディスク読み取り、Flash Cache 読み取り、書き込み、その他に分けて表示されます。ズームビューで表示した場合、QoS 最大スループットの値が ONTAP で設定されていれば、ボリュームのグラフに表示されます。</p> <p>このグラフは、選択したオブジェクトが SVM、ノード、アグリゲート、ボリューム、LUN である場合にのみ表示されます。またはネームスペースです。</p> <div>  <p>Flash Cache のデータは、ノードに Flash Cache モジュールがインストールされている場合にのみ表示されます。</p> </div>
使用済みパフォーマンス容量 - 合計	ノードまたはアグリゲートによるパフォーマンス容量の消費率。
使用済みパフォーマンス容量 - 内訳	使用済みパフォーマンス容量。ユーザプロトコルおよびシステムのバックグラウンドプロセスに分けて表示されます。また、空きパフォーマンス容量が表示されます。
使用可能な IOPS - 合計	このオブジェクトで現在使用可能な（空き）1 秒あたりの入出力処理数。この数値は、Unified Manager がオブジェクトで実行可能と計算する合計 IOPS から現在使用されている IOPS を引いた結果です。このグラフは、選択したオブジェクトがノードまたはアグリゲートの場合にのみ表示されます。
Utilization - 合計	オブジェクトの使用可能なリソースの使用率。利用率は、ノードのノード利用率、アグリゲートのディスク利用率、およびポートの帯域幅利用率を示します。このグラフは、選択したオブジェクトがノード、アグリゲート、またはポートの場合にのみ表示されます。
キャッシュミス率 - 合計	クライアントアプリケーションからの読み取り要求に対してキャッシュからではなくディスクからデータが返される割合。このグラフは、選択したオブジェクトがボリュームの場合にのみ表示されます。

表示するパフォーマンスチャートを選択しています

グラフの選択ドロップダウンリストでは、カウンタグラフペインに表示するパフォーマンスカウンタグラフのタイプを選択できます。これにより、パフォーマンス要件に基づいて特定のデータとカウンタを表示できます。

手順

1. カウンタグラフ * ペインで、* グラフの選択 * ドロップダウンリストをクリックします。
2. グラフを追加または削除します。

目的	手順
チャートを個別に追加または削除します	表示または非表示にするグラフの横にあるチェックボックスをオンにします
すべてのチャートを追加します	[* すべて選択 *] をクリックします
すべてのチャートを削除します	• すべて選択解除 * をクリックします

選択したチャートがカウンタチャートペインに表示されます。チャートを追加すると、新しいチャートがカウンタチャートペインに挿入され、チャートの選択ドロップダウンリストに表示されるチャートの順序が一致します。チャートを選択するにはスクロールが必要な場合があります。

カウンタグラフペインを展開します

カウンタグラフペインを展開すると、グラフをより大きくて読みやすくすることができます。

比較オブジェクトとカウンタの時間範囲を定義すると、大きなカウンタグラフペインが表示されます。パフォーマンスエクスプローラウィンドウの中央にある * < * ボタンを使用してペインを展開します。

ステップ

1. カウンタグラフ * ペインを展開または縮小します。

目的	手順
カウンタグラフペインを展開して、ページの幅に合わせます	「 * < * 」 ボタンをクリックします
カウンタグラフペインをページの右半分に減らします	[>] ボタンをクリックします

カウンタグラフに表示する期間を短くする

マウスを使用して期間を短縮し、[カウンタグラフ] ペインまたは[カウンタグラフズームビュー] ウィンドウで特定の期間にフォーカスを切り替えることができます。これに

より、タイムラインの任意の部分について、パフォーマンスデータ、イベント、およびしきい値をより細かく確認することができます。

- 必要なもの *

この機能がアクティブであることを示すために、カーソルを虫眼鏡に変更する必要があります。



この機能を使用すると、より詳細な表示に対応する値を表示するようにタイムラインが変更され、* 時間範囲 * セレクターの日時範囲はグラフの元の値から変更されません。

手順

1. 特定の期間を拡大して表示するには、虫眼鏡を使用してクリックしてドラッグし、詳細を表示する部分を囲みます。

選択した期間のカウンタの値が、カウンタチャートに拡大して表示されます。

2. 時間範囲 * セレクターで設定した元の時間に戻すには、* グラフズームのリセット * ボタンをクリックします。

カウンタグラフは元の状態で表示されます。

イベントタイムラインでイベントの詳細を表示する

パフォーマンスエクスプローラのイベントタイムラインペインで、すべてのイベントとその関連情報を確認できます。指定した期間内にルートオブジェクトで発生したすべての健全性イベントとパフォーマンスイベントをすばやく効率的に表示できるため、パフォーマンスの問題のトラブルシューティングに役立ちます。

イベントタイムラインペインには、選択した期間中にルートオブジェクトで発生したクリティカル、エラー、警告、および情報イベントが表示されます。イベントの重大度ごとに独自のタイムラインがあります。単一または複数のイベントがタイムライン上に点で表されます。イベントを示す点にカーソルを合わせると、イベントの詳細を確認できます。複数のイベントをより詳細に表示するには、期間を縮小します。複数のイベントが複数の単一のイベントとして表示されるため、各イベントを個々に表示して確認することができます。

イベントタイムラインの各パフォーマンスイベントドットは、イベントタイムラインの下に表示されるカウンタグラフのトレンドラインの急増に対応して縦に並んでいます。イベントと全体的なパフォーマンスの間に直接的な相関関係があることを確認できます。健全性イベントもタイムラインに表示されますが、これらのタイプのイベントはいずれかのパフォーマンスグラフのイベントが急増しているポイントと揃うとはかぎりません。

手順

1. [* イベントタイムライン *] ペインで、タイムライン上のイベントドットにカーソルを合わせると、そのイベントポイントでのイベントのサマリーが表示されます。

イベントタイプ、イベントが発生した日時、状態、およびイベントの期間に関する情報がポップアップダイアログに表示されます。

2. 1 つまたは複数のイベントの詳細を表示します。

作業	オプション
1つのイベントの詳細を表示します	<ul style="list-style-type: none"> ポップアップダイアログでイベントの詳細を表示*。
複数のイベントの詳細を表示します	<ul style="list-style-type: none"> ポップアップダイアログでイベントの詳細を表示*。 <div>  <p>複数イベントダイアログで1つのイベントをクリックすると、該当するイベントの詳細ページが表示されます。</p> </div>

カウンタグラフズームビュー

カウンタグラフにはズームビューが用意されており、指定した期間のパフォーマンスの詳細を拡大できます。これによりパフォーマンスの詳細やイベントをより細かく確認できるため、パフォーマンスの問題のトラブルシューティングを行うときに便利です。

ズームビューで表示した場合、一部の内訳グラフでは、ズームビュー以外では表示されない追加情報が表示されます。たとえば、IOPS、IOPS/TB、および MBps の内訳グラフのズームビューページには、ONTAP で設定されている場合、ボリュームおよび LUN の QoS ポリシーの値が表示されます。



システム定義のパフォーマンスしきい値ポリシーの場合、[Policies] リストから使用できるポリシーは、「Node resources over-utilized」ポリシーと「QoS Throughput limit over資料 的」ポリシーのみです。システム定義のその他のしきい値ポリシーは、現時点では使用できません。

カウンタグラフズームビューの表示

カウンタグラフズームビューを使用すると、選択したカウンタグラフとそれに関連付けられたタイムラインの詳細がさらに細かく表示されます。カウンタグラフのデータが拡大して表示され、パフォーマンスイベントやその原因を詳しく調べることができます。

カウンタグラフズームビューは、任意のカウンタグラフに対して表示できます。

手順

1. 選択したグラフを新しいブラウザウィンドウで開くには、*ズームビュー*をクリックします。
2. 内訳グラフを表示している場合は、*ズームビュー*をクリックすると、内訳グラフがズームビューに表示されます。表示オプションを変更する場合は、ズームビューで*合計*を選択できます。

ズームビューで期間を指定します

カウンタグラフズームビューウィンドウの*時間範囲*コントロールを使用すると、選択したグラフの日付と時間の範囲を指定できます。これにより、設定済みの期間またはカスタムの期間に基づいてデータをすばやく特定できます。

期間は 1 時間から 390 日の間で選択できます。1 カ月は 30 日としてカウントされるため、390 日は 13 カ月に相当します。日時の範囲を指定すると、特定のパフォーマンスイベントや一連のイベントにフォーカスして詳細を確認することができます。また、日時の範囲を指定すると、パフォーマンスイベントに関連するデータがより詳しく表示されるため、潜在的なパフォーマンスの問題のトラブルシューティングにも役立ちます。事前定義された日付と時間の範囲を選択するには、* Time Range* コントロールを使用します。また、独自の日時の範囲を 390 日まで指定することもできます。事前に定義された時間範囲のボタンは、* 過去 1 時間 * から * 過去 13 カ月 * までの間で異なります。

「過去 13 カ月」オプションを選択するか、30 日を超えるカスタムの日付範囲を指定すると、5 分ごとのデータポーリングではなく 1 時間ごとの平均値で 30 日を超える期間について表示されるパフォーマンスデータが表示されるダイアログボックスが表示されます。そのため、タイムラインには要約された情報が表示される可能性があります。ダイアログボックスで * 再表示しない * オプションをクリックした場合、* 過去 13 カ月 * オプションを選択したとき、または 30 日を超えるカスタム日付範囲を指定したときに、メッセージは表示されません。期間が 30 日以内でも、現在の日付から 1 つ以上あとの日時が期間に含まれている場合には要約データが表示されます。

選択した期間（カスタムまたは事前定義）が 30 日以内の場合、5 分ごとのデータサンプルに基づいてデータが表示されます。30 日を超える場合は、1 時間ごとのデータサンプルに基づいてデータが表示されます。

1. [* 時間範囲 * (Time Range *)] ドロップダウンボックスをクリックすると、[時間範囲 (Time Range)] パネルが表示されます。
2. 事前定義された時間範囲を選択するには、* 時間範囲 * パネルの右側にある * 最後 ... * ボタンのいずれかをクリックします。事前定義の期間を選択する場合、最大 13 カ月分のデータを使用できます。選択した事前定義の時間範囲ボタンが強調表示され、対応する日と時間がカレンダーと時間セレクタに表示されます。
3. カスタムの日付範囲を選択するには、左側の * 開始日 * カレンダーで開始日をクリックします。カレンダー内を前後に移動するには、「*」または「*」をクリックします。終了日を指定するには、右側の * から * のカレンダーで日付をクリックします。別の終了日を指定しないかぎり、デフォルトの終了日は今日です。時間範囲パネルの右側にある * カスタム範囲 * ボタンが強調表示され、カスタム日付範囲が選択されていることを示します。
4. カスタムの時間範囲を選択するには、* 開始 * カレンダーの下にある * 時間 * コントロールをクリックし、開始時間を選択します。終了時刻を指定するには、右側の * To * カレンダーの下にある * Time * コントロールをクリックし、終了時刻を選択します。時間範囲パネルの右側にある * カスタム範囲 * ボタンが強調表示され、カスタム時間範囲が選択されていることを示します。
5. 事前定義された日付範囲を選択する際に、開始時間と終了時間を指定することもできます。前述の説明に従って事前定義された日付範囲を選択し、前述のように開始時間と終了時間を選択します。選択した日付がカレンダーで強調表示され、指定した開始時刻と終了時刻が * Time * コントロールに表示され、*

Custom Range * ボタンが強調表示されます。

6. 日付と時間の範囲を選択したら、* 適用範囲 * をクリックします。その期間のパフォーマンス統計がグラフとイベントタイムラインに表示されます。

カウンタグラフズームビューでパフォーマンスしきい値を選択します

カウンタグラフズームビューでしきい値を適用すると、該当するパフォーマンスしきい値イベントに関する詳細が表示されます。しきい値を適用または削除してすぐに結果を表示でき、トラブルシューティングが必要かどうかを判断する際に役立ちます。

カウンタグラフズームビューでしきい値を選択すると、パフォーマンスしきい値イベントに関する正確なデータを確認できます。カウンタグラフズームビューの * Policies * 領域に表示されるしきい値を適用できます。

カウンタグラフズームビューでは、オブジェクトに一度に 1 つずつポリシーを適用できます。

ステップ

1. を選択または選択解除します  ポリシーに関連付けられているもの。

選択したしきい値がカウンタグラフズームビューに適用されます。重大のしきい値は赤の線、警告のしきい値は黄色の線が表示されます。

クラスタコンポーネント別のボリュームレイテンシを表示します

ボリュームの詳細なレイテンシ情報を表示するには、ボリュームパフォーマンスエクスプローラのページを使用します。Latency - Total カウンタグラフはボリュームの合計レイテンシを表示し、Latency - Breakdown カウンタグラフはボリュームへの読み取りと書き込みのレイテンシが及ぼす影響を特定するのに役立ちます。

また、Latency - Cluster Components チャートには各クラスタコンポーネントのレイテンシの詳細な比較が表示され、各コンポーネントがボリュームの合計レイテンシにどのように影響しているかを確認できます。表示されるクラスタコンポーネントは次のとおりです。


- ネットワーク
- 最大 QoS
- 最小 QoS
- ネットワーク処理
- クラスターインターコネクト
- データ処理
- アグリゲートの処理
- ボリュームのアクティブ化
- MetroCluster リソース
- クラウドレイテンシ
- 同期 SnapMirror

手順

1. 選択したボリュームの * ボリュームパフォーマンスエクスプローラ * ページで、レイテンシチャートからドロップダウンメニューから * クラスタコンポーネント * を選択します。

Latency - Cluster Components (レイテンシ - クラスタコンポーネント) グラフが表示されます。

2. グラフのより大きなバージョンを表示するには、「* ズームビュー *」を選択します。

クラスタコンポーネント別のグラフが表示されます。を選択または選択解除して、比較対象を調整することができます  各クラスタコンポーネントに関連付けられている。

3. 特定の値を表示するには、グラフ領域にカーソルを合わせてポップアップウィンドウを表示します。

プロトコル別の SVM の IOPS トラフィックの表示

Performance/SVMExplorer ヘエシを使用すると、SVM の詳細な IOPS 情報を表示できます。IOPS の合計カウンタグラフは SVM の合計 IOPS 使用量を示し、IOPS - 内訳カウンタグラフは、SVM に対する読み取り、書き込み、およびその他の IOPS の影響を特定する際に役立ちます。

また、IOPS - プロトコルグラフには、SVM で使用されている各プロトコルの IOPS トラフィックの詳細な比較が表示されます。使用できるプロトコルは次のとおりです。


- CIFS
- NFS
- FCP
- iSCSI
- NVMe

手順

1. 選択した SVM の * パフォーマンス / SVM エクスプローラ * ページで、IOPS チャートから、ドロップダウンメニューから * プロトコル * を選択します。

IOPS - プロトコルグラフが表示されます。

2. グラフのより大きなバージョンを表示するには、「* ズームビュー *」を選択します。

IOPS のプロトコル比較の詳細チャートが表示されます。を選択または選択解除して、比較対象を調整することができます  プロトコルに関連付けられている。

3. 特定の値を表示するには、いずれかのチャートのチャート領域にカーソルを合わせてポップアップウィンドウを表示します。

ボリュームおよび LUN のレイテンシグラフでパフォーマンス保証を確認

「パフォーマンス保証」プログラムに登録したボリュームと LUN を表示して、レイテンシが保証されたレベルを超えていないことを確認できます。

レイテンシパフォーマンス保証は、1 処理あたりのミリ秒の値であり、超えてはなりません。値は、デフォ

ルトの 5 分間のパフォーマンス収集期間ではなく、1 時間あたりの平均値です。

手順

1. パフォーマンス：すべてのボリューム * 表示または * パフォーマンス：すべての LUN * 表示で、関心のあ
るボリュームまたは LUN を選択します。
2. 選択したボリュームまたは LUN の * パフォーマンスエクスプローラ * ページで、* セレクタの統計の表
示から * 毎時平均 * を選択します。

レイテンシグラフの表示が 5 分間隔の収集データから 1 時間あたりの平均値に変わり、グラフの振れ幅が
少なくなります。

3. 同じアグリゲートにパフォーマンス保証の対象となるボリュームがほかにもある場合は、それらのボリ
ュームを追加して同じグラフでレイテンシの値を確認できます。

オール SAN アレイクラスタのパフォーマンスの表示

Performance : All SAN Array クラスタのパフォーマンスステータスは、Performance
: All Clusters ビューを使用して表示できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

オール SAN アレイクラスタの概要情報は、パフォーマンス：すべてのクラスタビューで確認できます。詳細
については、クラスタ / パフォーマンスエクスプローラのページを参照してください。

手順

1. 左側のナビゲーションペインで、* Storage * > * Clusters * をクリックします。
2. 「パーソナリティ」列が * 正常性：すべてのクラスタ * ビューに表示されていることを確認するか、* 表
示 / 非表示 * コントロールを使用して追加します。

この列には 'すべての SAN アレイクラスタのすべての SAN アレイが表示されます

3. これらのクラスタのパフォーマンスに関する情報を表示するには、「* パフォーマンス：すべてのクラス
タ *」ビューを選択します。

オール SAN アレイクラスタのパフォーマンス情報を表示します。

4. これらのクラスタのパフォーマンスに関する詳細情報を表示するには、オール SAN アレイクラスタの名
前をクリックします。
5. [* エクスプローラ *] タブをクリックします。
6. [* クラスタ / パフォーマンスエクスプローラ *] ページで、[* 表示と比較 *] メニューから [このクラス
タ上のノード *] を選択します。

このクラスタの両方のノードのパフォーマンス統計を比較して、両方のノードの負荷がほぼ同じであるこ
とを確認できます。2 つのノードの間に大きな差がある場合は、2 つ目のノードをグラフに追加し、もっ
と長い期間の値を比較することで、構成の問題を特定できます。

ローカルノード上にのみ存在するワークロードに基づくノード IOPS の表示

ノードの IOPS カウンタグラフでは、リモートノード上のボリュームに対する読み取り / 書き込み処理を実行するために、処理がネットワーク LIF を使用してローカルノードのみを経由する箇所を特定できます。IOPS の「Total (Local)」グラフと「Breakdown (Local)」グラフには、現在のノード上のみのローカルボリュームに存在するデータの IOPS が表示されます。

これらのカウンタ・チャートの「ローカル」バージョンは ' ローカル・ボリューム上に存在するデータの統計のみを表示するため ' パフォーマンス容量と使用率のノード・チャートに似ています

これらのカウンタグラフの「ローカル」バージョンと、通常の合計バージョンのカウンタグラフを比較することで、ローカルノードを経由してリモートノード上のボリュームにアクセスしているトラフィックが大量にあるかどうかを確認できます。ローカルノードを経由してリモートノード上のボリュームにアクセスしている処理が多すぎると原因のパフォーマンスの問題が報告される可能性があります。このような場合は、ボリュームをローカルノードに移動したり、ホストからそのボリュームにアクセスしているトラフィックを接続可能なリモートノードに LIF を作成したりすることができます。

手順

1. 選択したノードの * パフォーマンス / ノードエクスプローラ * ページで、IOPS チャートから、ドロップダウンメニューから * 合計 * を選択します。

IOPS の合計グラフが表示されます。

2. [* ズームビュー *] をクリックすると、新しいブラウザタブにグラフのより大きなバージョンが表示されます。
3. パフォーマンス / ノードエクスプローラ * ページに戻り、IOPS チャートから、ドロップダウンメニューから * 合計 (ローカル) * を選択します。

IOPS の合計 (ローカル) グラフが表示されます。

4. [* ズームビュー *] をクリックすると、新しいブラウザタブにグラフのより大きなバージョンが表示されます。
5. グラフを並べて表示し、IOPS 値が大きく異なっている領域を特定します。
6. これらの領域にカーソルを合わせると、特定の時点におけるローカルと合計の IOPS が比較されます。

オブジェクトランディングページのコンポーネント

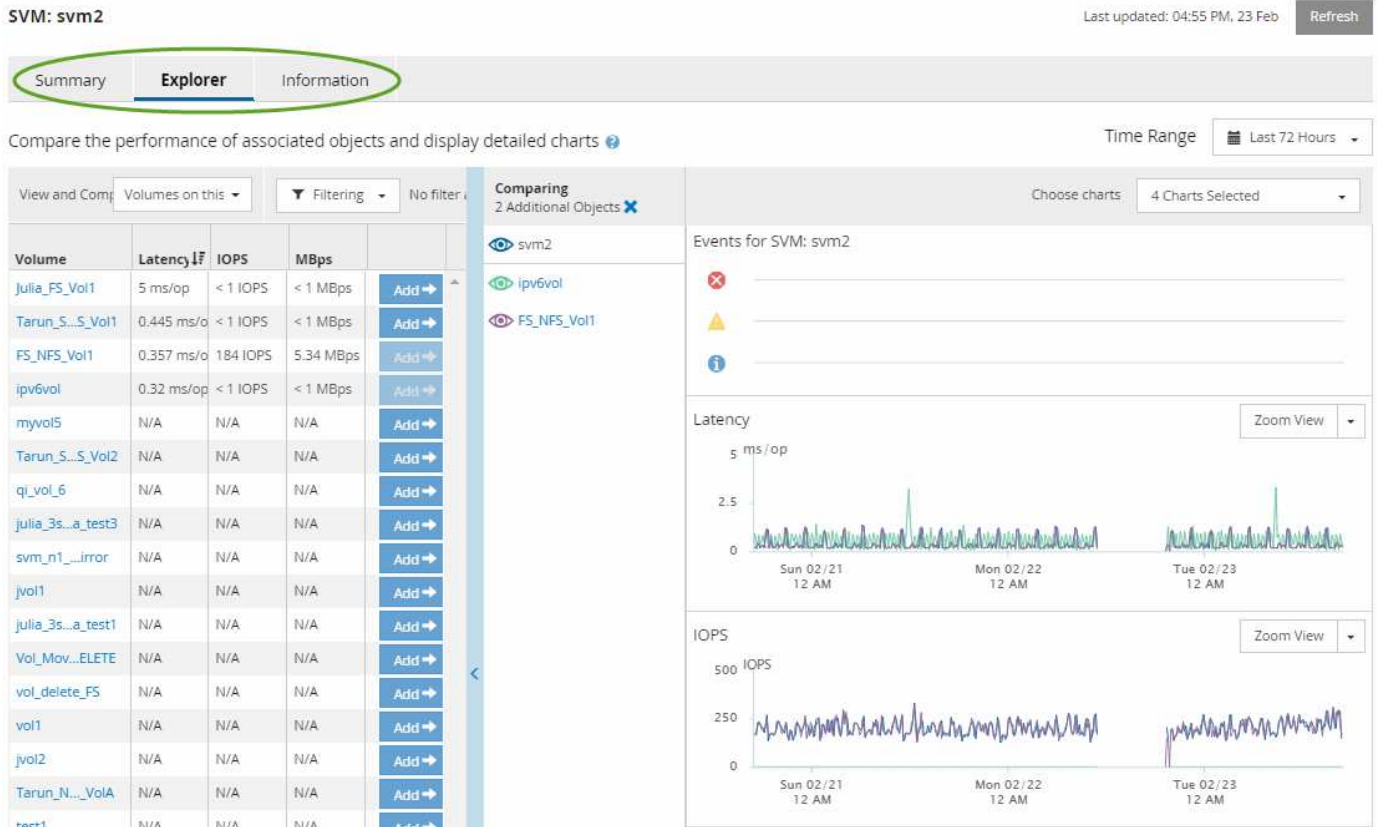
オブジェクトのランディングページには、すべての重大イベント、警告イベント、情報イベントに関する詳細が表示されます。すべてのクラスタオブジェクトのパフォーマンスの詳細が表示され、個々のオブジェクトを選択してさまざまな期間のデータを比較することができます。

オブジェクトランディングページでは、すべてのオブジェクトの全体的なパフォーマンスを調べ、オブジェクトのパフォーマンスデータを並べて比較することができます。これは、パフォーマンスの評価やイベントのトラブルシューティングを行う場合に役立ちます。



カウンタサマリーパネルとカウンタグラフに表示されるデータは、5 分間のサンプリング間隔に基づいています。ページの左側にあるオブジェクトのインベントリグリッドに表示されるデータは、1 時間のサンプリング間隔に基づいています。

次の図は、エクスプローラの情報を表示するオブジェクトランディングページの例を示しています。



表示しているストレージオブジェクトに応じて、オブジェクトのランディングページにはオブジェクトに関するパフォーマンスデータを表示する次のタブが表示されます。

- まとめ

各オブジェクトの過去 72 時間のイベントやパフォーマンスを示すカウンタグラフが 3 つか 4 つ表示されます。チャートには、その期間の高い値と低い値の傾向を示す線も表示されます。

- エクスプローラ (Explorer)

現在のオブジェクトに関連するストレージオブジェクトがグリッド形式で表示され、現在のオブジェクトと関連オブジェクトのパフォーマンスの値を比較することができます。このタブには、最大 11 個のカウンタチャートと期間セレクトが表示され、さまざまな比較を実行できます。

- 情報

ストレージオブジェクトに関するパフォーマンス以外の構成の属性が表示されます。インストールされている ONTAP ソフトウェアのバージョン、HA パートナーの名前、ポートや LIF の数などが含まれます。

- パフォーマンス上位

クラスタの場合：選択したパフォーマンスカウンタに基づいて、パフォーマンスが上位または下位のスト

レージオブジェクトが表示されます。

- フェイルオーバープラン

ノードの場合：ノードの HA パートナーで障害が発生した場合のノードのパフォーマンスへの影響の推定値が表示されます。

- 詳細

ボリュームの場合：選択したボリュームのワークロードに対するすべての I/O アクティビティと処理について、詳細なパフォーマンス統計が表示されます。このタブは、FlexGroup ボリューム、FlexVol ボリューム、および FlexGroup のコンスチチュエントに対して表示されます。

サマリページ

概要ページには、過去 72 時間のオブジェクトごとのイベントとパフォーマンスの詳細が表示されます。このデータは自動では更新されず、最後にページがロードされた時点のデータです。サマリページのグラフ回答 the question _do I need to look further ? _

グラフとカウンタの統計情報

サマリグラフには、過去 72 時間の概要が表示され、さらに調査が必要な潜在的な問題の特定に役立ちます。

概要ページのカウンタの統計がグラフに表示されます。

グラフ上のラインにカーソルを合わせると、その時点のカウンタの値を確認できます。サマリグラフには、以下のカウンタについて、過去 72 時間のアクティブな重大イベントと警告イベントの合計数も表示されます。

- * 遅延 *

すべての I/O 要求の平均応答時間。処理あたりのミリ秒で表されます。

すべてのオブジェクトタイプについて表示されます。

- * IOPS *

平均処理速度。1 秒あたりの入出力処理数で表されます。

すべてのオブジェクトタイプについて表示されます。

- * MB/ 秒 *

平均スループット。1 秒あたりのメガバイト数で表されます。

すべてのオブジェクトタイプについて表示されます。

- * 使用済みパフォーマンス容量 *

ノードまたはアグリゲートによるパフォーマンス容量の消費率。

ノードとアグリゲートについてのみ表示されます。

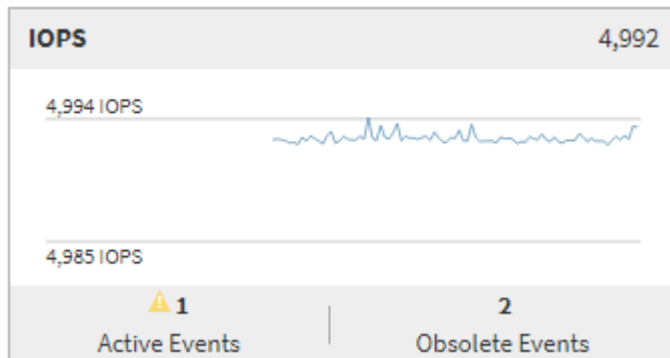
- * 利用率 *

ノードとアグリゲートのオブジェクト利用率、またはポートの帯域幅利用率。

ノード、アグリゲート、およびポートについてのみ表示されます。

アクティブイベントのイベント数にカーソルを合わせると、イベントのタイプと数が表示されます。重大イベントは赤で表示されます (■)、および警告イベントが黄色で表示されます (■)。

グラフ右上のグレーのバーに表示される数字は、過去 72 時間の平均値です。トレンドグラフの上下に表示される数字は、過去 72 時間の最小値と最大値です。グラフ下のグレーのバーには、過去 72 時間のアクティブなイベント (新規および確認済みのイベント) と廃止イベントの件数が表示されます。



- * レイテンシ・カウンタ・チャート *

レイテンシカウンタグラフには、過去 72 時間のオブジェクトレイテンシの概要が表示されます。レイテンシは、すべての I/O 要求の平均応答時間です。処理あたりのミリ秒数、サービス時間、待機時間、または対象となるクラスタストレージコンポーネント内のデータパケットまたはブロックで発生した時間の両方を表します。

- 上 (カウンタ値) : * ヘッダーの数字は過去 72 時間の平均値です。
- 中央 (パフォーマンスグラフ) : グラフの下部に表示される数字は、下が過去 72 時間のレイテンシの最小値で上が最大値です。グラフ上のラインにカーソルを合わせると、その時点のレイテンシの値が表示されます。
- 下部 (イベント) : * カーソルを合わせると、イベントの詳細がポップアップに表示されます。グラフの下にある * Active Events * リンクをクリックして Events Inventory ページに移動し、イベントの詳細を確認します。
- * IOPS カウンタグラフ *

IOPS カウンタグラフには、過去 72 時間のオブジェクトの IOPS の概要が表示されます。IOPS は、ストレージシステムの 1 秒あたりの入出力処理数です。

- 上 (カウンタ値) : * ヘッダーの数字は過去 72 時間の平均値です。
- 中央 (パフォーマンスグラフ) : グラフの上下の数字は、下が過去 72 時間の IOPS の最小値で上が最大値です。グラフ上のラインにカーソルを合わせると、その時点の IOPS の値が表示されます。
- 下部 (イベント) : * カーソルを合わせると、イベントの詳細がポップアップに表示されます。グラフの下にある * Active Events * リンクをクリックして Events Inventory ページに移動し、イベントの詳細を確認します。

- * MBps カウンタチャート *

MBps カウンタグラフには、オブジェクトの MBps パフォーマンスと、オブジェクトとの間で転送されたデータの量が 1 秒あたりのメガバイト数で表示されます。MBps カウンタグラフには、過去 72 時間のオブジェクトの MBps の概要が表示されます。

- 上（カウンタ値）：* ヘッダーの数字は過去 72 時間の MBps の平均値です。
- 中央（パフォーマンスグラフ）：グラフの下部の値は MBps の最小値で、グラフの上部の値は過去 72 時間の MBps の最大値です。グラフ上のラインにカーソルを合わせると、その時点の MBps の値が表示されます。
- 下部（イベント）：* カーソルを合わせると、イベントの詳細がポップアップに表示されます。グラフの下にある * Active Events * リンクをクリックして Events Inventory ページに移動し、イベントの詳細を確認します。
- * 使用済みパフォーマンス容量カウンタグラフ *

使用済みパフォーマンス容量のカウンタグラフには、オブジェクトで消費されているパフォーマンス容量の割合が表示されます。

- 上（カウンタ値）：* ヘッダーの数字は過去 72 時間のパフォーマンス容量使用率の平均値です。
- 中央（パフォーマンスグラフ）：グラフの下部の値は、使用済みパフォーマンス容量の割合が最も低い値、グラフの上部の値は過去 72 時間のパフォーマンス容量の使用率の最大値です。グラフ上のラインにカーソルを合わせると、その時点の使用済みパフォーマンス容量の値が表示されます。
- 下部（イベント）：* カーソルを合わせると、イベントの詳細がポップアップに表示されます。グラフの下にある * Active Events * リンクをクリックして Events Inventory ページに移動し、イベントの詳細を確認します。
- * 利用率カウンタグラフ *

Utilization カウンタグラフには、オブジェクトの利用率が表示されます。Utilization カウンタグラフには、過去 72 時間のオブジェクトまたは帯域幅の使用率の概要が表示されます。

- 上（カウンタ値）：* ヘッダーの数字は過去 72 時間の利用率の平均値です。
- 中央（パフォーマンスグラフ）：グラフの下部の値は、利用率が最も低い値で上が 72 時間の最大値です。グラフ上のラインにカーソルを合わせると、その時点の利用率の値が表示されます。
- 下部（イベント）：* カーソルを合わせると、イベントの詳細がポップアップに表示されます。グラフの下にある * Active Events * リンクをクリックして Events Inventory ページに移動し、イベントの詳細を確認します。

イベント

該当する場合、イベント履歴テーブルには、そのオブジェクトで発生した最新のイベントが表示されます。イベント名をクリックすると、Event Details ページにイベントの詳細が表示されます。

パフォーマンスエクスプローラページのコンポーネント

パフォーマンスエクスプローラページでは、クラスタ内の同様のオブジェクトについて、たとえばクラスタ内のすべてのボリュームなどのパフォーマンスを比較できます。これは、パフォーマンスイベントのトラブルシューティングやオブジェクトのパフォーマンスの微調整を行う際に便利です。また、オブジェクトを他のオブジェクトとの比較

でベースラインとなるルートオブジェクトと比較することもできます。

- 健全性ビューに切り替え * ボタンをクリックすると、このオブジェクトの健全性の詳細ページを表示できます。このオブジェクトのストレージ設定に関して、問題のトラブルシューティングに役立つ重要な情報が得られる場合があります。

パフォーマンスエクスプローラページには、クラスタオブジェクトとそのパフォーマンスデータのリストが表示されます。このページには、同じタイプのすべてのクラスタオブジェクト（ボリュームとそのオブジェクト固有のパフォーマンス統計など）が表形式で表示されます。このビューで、クラスタオブジェクトのパフォーマンスの概要を効率的に確認できます。



テーブルの任意のセルに「N/A」と表示される場合は、そのオブジェクトに I/O がいないため、そのカウンタの値を使用できないことを意味します。

パフォーマンスエクスプローラページには、次のコンポーネントが含まれています。

- * 時間範囲 *

オブジェクトデータの期間を選択できます。

事前定義の範囲を選択することも、独自のカスタム期間を指定することもできます。

- * 表示と比較 *

グリッドに表示する関連オブジェクトのタイプを選択できます。

使用可能なオプションは、ルートオブジェクトのタイプと使用可能なデータによって異なります。[表示と比較 (View and Compare)] ドロップダウンリストをクリックして、オブジェクトタイプを選択できます。選択したオブジェクトタイプがリストに表示されます。

- * フィルタリング *

受け取るデータの量を設定に基づいて絞り込むことができます。

IOPS が 4 を超えるオブジェクトに限定するなど、オブジェクトデータに適用するフィルタを作成することができます。最大 4 つのフィルタを同時に追加できます。

- * 比較 *

ルートオブジェクトと比較するために選択したオブジェクトのリストが表示されます。

比較ペインのオブジェクトのデータがカウンタチャートに表示されます。

- * 統計情報を * で表示します

ボリュームおよび LUN の統計を各収集サイクル（デフォルトは 5 分）後に表示するか、または 1 時間あたりの平均として表示するかを選択できます。この機能を使用して、ネットアップの「パフォーマンス保証」プログラムの状況を確認するためにレイテンシグラフを表示することができます。

- * カウンタチャート *

オブジェクトのパフォーマンスのカテゴリ別にグラフ形式のデータが表示されます。

通常、デフォルトではグラフが 3 つか 4 つだけ表示されます。グラフの選択コンポーネントを使用すると、グラフを追加で表示したり、特定のグラフを非表示にしたりできます。イベントタイムラインの表示と非表示を選択することもできます。

• * イベントタイムライン *

期間コンポーネントで選択したタイムライン全体で発生しているパフォーマンスイベントと健全性イベントが表示されます。

QoS ポリシーグループ情報を使用したパフォーマンスの管理

Unified Manager では、監視しているすべてのクラスタで使用可能な QoS ポリシーグループを表示できます。ポリシーは、ONTAP ソフトウェア（System Manager または ONTAP CLI）または Unified Manager のパフォーマンスサービスレベルポリシーを使用して定義されたものです。Unified Manager には、QoS ポリシーグループが割り当てられているボリュームと LUN も表示されます。

QoS設定の調整の詳細については、を参照してください ["パフォーマンス管理の概要"](#)

ストレージ **QoS** がワークロードスループットを制御する仕組み

QoS ポリシーグループを作成して、ポリシーグループに含まれるワークロードの 1 秒あたりの I/O 処理数（IOPS）やスループット（MBps）の上限を制御できます。デフォルトのポリシーグループなど、ワークロードに制限が設定されていないポリシーグループに含まれている場合や、設定された制限がニーズに合わない場合は、制限を増やしたり、希望する制限が設定された新しいポリシーグループまたは既存のポリシーグループにワークロードを移動したりできます。

「従来の」QoS ポリシーグループは、単一のボリュームや LUN など、個々のワークロードに割り当てることができます。この場合、ワークロードはスループットを上限まで使用できます。また、QoS ポリシーグループを複数のワークロードに割り当てすることもできます。この場合、ワークロードのスループットの上限は「赤」です。たとえば、3 つのワークロードに 9、000 IOPS の QoS 制限を割り当てた場合、IOPS の合計が 9、000 IOPS を超えないように制限されます。

アダプティブ QoS ポリシーグループは、個々のワークロードまたは複数のワークロードに割り当てることができます。ただし、複数のワークロードに割り当てられている場合も、スループットの値を他のワークロードと共有するのではなく、各ワークロードでスループットが上限まで使用されます。また、アダプティブ QoS ポリシーは、スループットの設定をワークロードごとにボリュームサイズに基づいて自動的に調整し、ボリュームサイズが変わっても容量に対する IOPS の比率を維持します。たとえば、アダプティブ QoS ポリシーでピークが 5、000 IOPS/TB に設定されている場合、10TB のボリュームの最大スループットは 50、000 IOPS になります。ボリュームのサイズが 20TB に変更されると、アダプティブ QoS によって最大値が 100、000 IOPS に調整されます。

ONTAP 9.5 以降では、アダプティブ QoS ポリシーを定義する際にブロックサイズを指定できます。これにより、ワークロードが非常に大きなブロックサイズを使用していて、その結果スループットの大半を使用しているケースでは、ポリシーのしきい値が IOPS/TB から MBps に変換されます。

グループで QoS ポリシーを共有している場合、ポリシーグループ内のすべてのワークロードの IOPS または MBps が設定された上限を超えると、ワークロードが調整されてそのアクティビティが制限されます。その結

果、ポリシーグループ内のすべてのワークロードのパフォーマンスが低下することがあります。ポリシーグループの調整によって動的なパフォーマンスイベントが生成されると、イベント概要に関するポリシーグループの名前が表示されます。

パフォーマンス：すべてのボリュームビューで、影響を受けたボリュームを IOPS と MBps でソートすると、イベントの原因となった可能性がある使用率が最も高いワークロードを確認できます。Performance/Volumes Explorer ヘエシでは、ボリューム上の他のボリュームまたは LUN を選択して、影響を受けるワークロードの IOPS または MBps スループットの使用率と比較できます。

ノードリソースを過剰に消費しているワークロードは、より制限の厳しいポリシーグループに割り当てます。これにより、ポリシーグループによる調整でワークロードのアクティビティが制限されて、そのノードでのリソースの使用が削減されます。ただし、ワークロードで使用できるノードのリソースを増やす場合は、ポリシーグループの値を大きくすることができます。

System Manager、ONTAP コマンド、または Unified Manager のパフォーマンスサービスレベルを使用してポリシーグループを管理できます。これには次のタスクが含まれます。

- ポリシーグループを作成する
- ポリシーグループ内のワークロードの追加または削除
- ポリシーグループ間でワークロードを移動する
- ポリシーグループのスループット制限を変更する
- 別のアグリゲートやノードへのワークロードの移動

すべてのクラスタで使用可能なすべての **QoS** ポリシーグループを表示する

Unified Manager が監視しているクラスタで使用可能なすべての QoS ポリシーグループのリストを表示できます。これには、従来の QoS ポリシー、アダプティブ QoS ポリシー、および Unified Manager のパフォーマンスサービスレベルポリシーで管理される QoS ポリシーが含まれます。

手順

1. 左側のナビゲーションペインで、* Storage * > * QoS Policy Groups * をクリックします。

Performance : Traditional QoS Policy Groups ビューがデフォルトで表示されます。

2. 使用可能な従来の各 QoS ポリシーグループの詳細な設定を表示します。
3. 展開ボタン (▼) をクリックし、ポリシーグループに関する詳細情報を表示します。
4. 表示メニューで、いずれかの追加オプションを選択してすべてのアダプティブ QoS ポリシーグループを表示するか、Unified Manager のパフォーマンスサービスレベルを使用して作成されたすべての QoS ポリシーグループを表示します。

同じ **QoS** ポリシーグループ内のボリュームまたは **LUN** の表示

同じ QoS ポリシーグループに割り当てられているボリュームと LUN のリストを表示できます。

複数のボリュームを「赤」で表した従来の QoS ポリシーグループでは、特定のボリュームがポリシーグループに定義されたスループットであるかどうかを確認するのに役立ちます。また、他のボリュームに悪影響を及

ばすことなくポリシーグループにボリュームを追加できるかどうかを判断することもできます。

アダプティブ QoS ポリシーと Unified Manager のパフォーマンスサービスレベルポリシーの場合は、これは、ポリシーグループを使用しているすべてのボリュームまたは LUN を表示して、QoS ポリシーの設定を変更した場合に影響を受けるオブジェクトを確認するのに役立ちます。

手順

1. 左側のナビゲーションペインで、* Storage * > * QoS Policy Groups * をクリックします。

Performance : Traditional QoS Policy Groups ビューがデフォルトで表示されます。

2. 従来のポリシーグループに関心がある場合は、このページを表示したままにします。それ以外の場合は、追加の View オプションを 1 つ選択して、Unified Manager のパフォーマンスサービスレベルによって作成されたすべてのアダプティブ QoS ポリシーグループまたはすべての QoS ポリシーグループを表示します。
3. 目的の QoS ポリシーで、展開ボタン (▼) をクリックしてください。

Quality of Service - Performance / Adaptive QoS Policy Groups ?

Last updated: Jan 31, 2019, 1:56 PM

View

Adaptive QoS Policy Groups

Search Quality of Service

Schedule Report

QoS Policy Group	Cluster	SVM	Min Through...	Max Through...	Absolute Min...	Block Size	Asso
julia_vs2_cifs_Performance	opm-simplicity	julia_vs2_cifs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		1
julia_vs1_nfs_Performance	opm-simplicity	julia_vs1_nfs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		2

Details

Allocated Capacity

0.99 TB

1.15 TB

Associated Objects

2 Volumes

0 LUNs

Events

None

julia_nfs_extreme_Extreme_Performance	ocum-mobility-01-02	julia_nfs_extreme	6144.0 IOPS/TB	12288.0 IOPS/TB	1000IOPS	any	1
julia_extreme_jan16_aqos	ocum-mobility-01-02	julia_nfs_extreme	10000.0 IOPS/TB	12000.0 IOPS/TB	1000IOPS	any	1

4. ボリュームまたは LUN のリンクをクリックし、この QoS ポリシーを使用しているオブジェクトを表示します。

ボリュームまたは LUN のパフォーマンスインベントリページが、QoS ポリシーを使用しているオブジェクトのソート済みリストとともに表示されます。

特定のボリュームまたは **LUN** に適用されている **QoS** ポリシーグループ設定を表示する

ボリュームおよび LUN に適用されている QoS ポリシーグループを表示したり、パフォーマンス / QoS ポリシーグループビューにリンクして、各 QoS ポリシーの詳細な設定を表示したりできます。

ボリュームに適用されている QoS ポリシーを表示する手順を次に示します。LUN についても同様です。

手順

1. 左側のナビゲーションペインで、* Storage * > * Volumes * をクリックします。

デフォルトでは、Health : All Volumes（健全性：すべてのボリューム）ビューが表示されます。

2. [表示]メニューで、[* パフォーマンス：QoS ポリシーグループ内のボリューム]を選択します。*
3. 確認するボリュームを見つけ、* QoS ポリシーグループ * 列が表示されるまで右にスクロールします。
4. QoS ポリシーグループ名をクリックします。

対応する QoS ページは、従来の QoS ポリシー、アダプティブ QoS ポリシー、または Unified Manager のパフォーマンスサービスレベルを使用して作成された QoS ポリシーに応じて表示されます。

5. QoS ポリシーグループの詳細な設定を表示します。
6. 展開ボタン（▼）をクリックし、ポリシーグループに関する詳細情報を表示します。

パフォーマンスチャートを表示して、同じ **QoS** ポリシーグループ内のボリュームまたは **LUN** を比較できます

同じ QoS ポリシーグループ内のボリュームと LUN を表示して、単一の IOPS、MBps、または IOPS/TB チャートでパフォーマンスを比較し、問題がないかどうかを確認できます。

同じ QoS ポリシーグループ内のボリュームのパフォーマンスを比較する手順を次に示します。LUN についても同様です。

手順

1. 左側のナビゲーションペインで、* Storage * > * Volumes * をクリックします。

デフォルトでは、Health : All Volumes（健全性：すべてのボリューム）ビューが表示されます。

2. [表示]メニューで、[* パフォーマンス：QoS ポリシーグループ内のボリューム]を選択します。*
3. 確認するボリュームの名前をクリックします。

ボリュームのパフォーマンスエクスプローラページが表示されます。

4. View and Compare メニューで、**Volumes in Same QoS Policy Group** を選択します。

同じ QoS ポリシーを共有する他のボリュームが下の表に表示されます。

5. グラフにこれらのボリュームを追加して、グラフ内で選択したすべてのボリュームの IOPS、MBps、IOPS/TB、およびその他のパフォーマンスカウンタを比較できるようにします。

パフォーマンスを表示する期間はデフォルトの 72 時間以外に変更できます。

スループットグラフでの各種 **QoS** ポリシーの表示形式

パフォーマンスエクスプローラおよびワークロード分析の IOPS、IOPS/TB、および MBps の各グラフで、ボリュームや LUN に適用されている ONTAP 定義のサービス品質（QoS）ポリシーの設定を確認することができます。グラフに表示される情報は、ワークロードに適用されている QoS ポリシーのタイプによって異なります。

最大スループット（または「ピーク」）設定は、ワークロードが消費できる最大スループットを定義し、システムリソースに対する競合するワークロードへの影響を制限します。最小スループット（または「予測」）設定は、ワークロードに必要な最小スループットを定義するもので、競合するワークロードによる要求に関係なく、重要なワークロードが最小スループットターゲットを満たすようにします。

IOPS および MBps の共有および非共有 QoS ポリシーでは、「最小」および「最大」という用語を使用してフロアと上限を定義します。ONTAP 9.3 で導入された IOPS/TB のアダプティブ QoS ポリシーでは、「予想」と「ピーク」という用語を使用して、床と天井を定義します。

ONTAP ではこの 2 種類の QoS ポリシーを作成できますが、パフォーマンスグラフには、ワークロードへの適用方法に応じて 3 種類の方法で QoS ポリシーが表示されます。

ポリシーのタイプ	機能性	Unified Manager インターフェイスでの表示
単一のワークロードに割り当てられた共有の QoS ポリシー、単一のワークロードまたは複数のワークロードに割り当てられた非共有の QoS ポリシー	指定されたスループット設定を各ワークロードが消費できます	「(QoS)」を表示します。
複数のワークロードに割り当てられた共有の QoS ポリシー	指定されたスループット設定をすべてのワークロードが共有します	「(QoS 共有)」と表示します。
単一のワークロードまたは複数のワークロードに割り当てられたアダプティブ QoS ポリシー	指定されたスループット設定を各ワークロードが消費できます	「(QoS アダプティブ)」を表示します。

次の図は、カウンタグラフでの 3 つのオプションの表示例を示したものです。



IOPS で定義された標準の QoS ポリシーがワークロードの IOPS/TB チャートに表示される場合、ONTAP は IOPS 値を IOPS/TB 値に変換し、Unified Manager は IOPS/TB チャートにそのポリシーを「QoS、で定義」というテキストとともに表示します。

IOPS/TB で定義されているアダプティブ QoS ポリシーがワークロードの IOPS グラフに表示される場合、ONTAP は IOPS/TB の値を IOPS 値に変換し、Unified Manager はそのポリシーを IOPS グラフに「QoS アダプティブ - 使用済み」というテキストとともに表示します。ピーク IOPS 割り当て設定の構成に応じて、「IOPS/TB」または「QoS アダプティブ割り当て」で定義されます。割り当て設定が「allocated-space」に設定されている場合は、ボリュームのサイズに基づいてピーク IOPS が計算されます。割り当て設定が「used-space」に設定されている場合は、ストレージの効率性を考慮し、ボリュームに格納されているデータの量に基づいてピーク IOPS が計算されます。



IOPS/TB グラフには、ボリュームで使用されている論理容量が 128GB 以上の場合にのみパフォーマンスデータが表示されます。選択した期間に使用済み容量が 128GB を下回る期間がある場合、その間のデータはグラフに表示されません。

パフォーマンスエクスプローラでワークロードの **QoS** の下限と上限の設定を確認します

パフォーマンスエクスプローラのグラフで、ボリュームまたは LUN に対する ONTAP 定義のサービス品質（QoS）ポリシーの設定を確認できます。最大スループット設定は、競合するワークロードによるシステムリソースへの影響を抑制するために使用されます。最小スループット設定は、競合するワークロードによる要求に関係なく、重要なワークロードに最小限のスループットを確保するために使用されます。

QoS スループット「最小」および「最大」IOPS および MBps の設定は、ONTAP で設定されている場合にのみカウンタチャートに表示されます。最小スループット設定は、ONTAP 9.2 以降のソフトウェアを実行しているシステムでのみ使用できます。AFF システムでのみ使用でき、現時点では IOPS についてのみ設定できます。

アダプティブ QoS ポリシーは ONTAP 9.3 以降で使用でき、IOPS の代わりに IOPS/TB が使用されます。アダプティブポリシーは、QoS ポリシーの値をワークロードごとにボリュームサイズに基づいて自動的に調整し、ボリュームサイズが変わっても容量に対する IOPS の比率を維持します。アダプティブ QoS ポリシーグループはボリュームにのみ適用できます。QoS の用語 "expected" と "peak" は、最小と最大ではなくアダプティブ QoS ポリシーに使用されます。

Unified Manager では、定義されている QoS 最大ポリシーの設定を超えるワークロードが過去 1 時間の各パフォーマンス収集期間で見つかった場合に、QoS ポリシーの違反とみなして警告イベントを生成します。ワークロードのスループットが各収集期間に短時間だけ QoS のしきい値を超えることがありますが、Unified Manager のグラフには収集期間中の「平均」のスループットが表示されます。そのため、QoS のイベントが表示された場合でも、グラフではワークロードのスループットがポリシーのしきい値を超えていないように見ることがあります。

手順

- 1. 選択したボリュームまたは LUN の * パフォーマンスエクスプローラ * ページで、次の操作を実行して QoS の上限と下限の設定を表示します。

状況	手順
IOPS の上限（QoS 最大）を表示する	IOPS の合計または内訳グラフで、* ズームビュー * をクリックします。
MBps の上限（QoS 最大）を表示する	MBps の合計または内訳グラフで、* ズームビュー * をクリックします。

状況	手順
IOPS の下限（QoS 最小）を表示する	IOPS の合計または内訳グラフで、*ズームビュー* をクリックします。
IOPS/TB の上限（QoS ピーク）を表示する	ボリュームの場合は、IOPS/TB チャートで * Zoom View * をクリックします。
IOPS/TB の下限（QoS 想定）を表示する	ボリュームの場合は、IOPS/TB チャートで * Zoom View * をクリックします。

横方向の点線は、ONTAP で設定された最大または最小のスループット値を示します。QoS 値に対する変更がいつ実装されたかを確認することもできます。

2. IOPS および MBps の具体的な値を QoS 設定と比較して確認するには、グラフ領域にカーソルを合わせてポップアップウィンドウを参照します。

特定のボリュームまたは LUN の IOPS や MBps が非常に高く、システムリソースを圧迫している場合は、System Manager または ONTAP CLI を使用して、それらのワークロードが他のワークロードのパフォーマンスに影響しないように QoS 設定を調整することができます。

QoS設定の調整の詳細については、を参照してください ["パフォーマンス管理の概要"](#)

パフォーマンス容量と使用可能な IOPS の情報を使用してパフォーマンスを管理する

Performance capacity リソースの有用なパフォーマンスを超過しないで、リソースから引き出すことのできるスループットの量を示します。既存のパフォーマンスカウンタを使用した場合、レイテンシが問題になる前に、ノードまたはアグリゲートを最大限利用できるポイントがパフォーマンス容量です。

Unified Manager は、各クラスタ内のノードとアグリゲートからパフォーマンス容量の統計を収集します。_使用済みパフォーマンス容量_ は現在使用されているパフォーマンス容量の割合です。_performance capacity free_ は使用可能な残りのパフォーマンス容量の割合です。

空きパフォーマンス容量からは使用可能な残りのリソースの割合が提供されますが、利用可能な IOPS_ には、最大パフォーマンス容量に達するまでにリソースに追加できる IOPS の数が示されます。この指標を使用すると、あらかじめ決めた数の IOPS のワークロードを確実にリソースに追加できます。

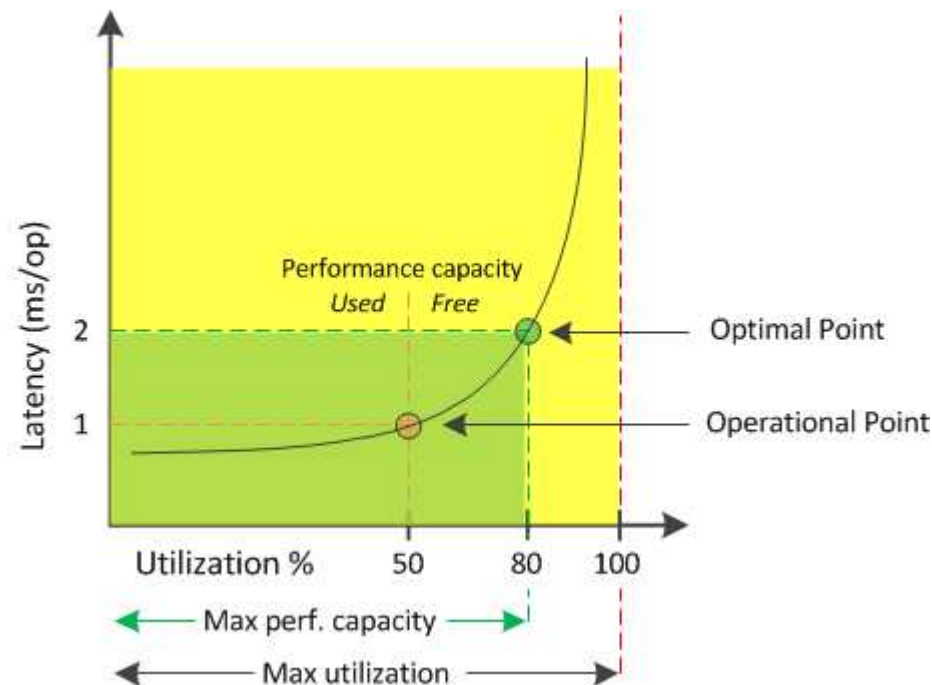
パフォーマンス容量情報を監視する利点は次のとおりです。

- ワークフローのプロビジョニングとバルランシングに役立つ。
- ノードの過負荷や、ノードのリソースが最適ポイントを超えるのを回避して、トラブルシューティングの必要性を減らす。
- ストレージ機器の追加が必要なケースを正確に判断できます。

使用済みパフォーマンス容量とは

使用済みパフォーマンス容量カウンタは、ワークロードが増加した場合にパフォーマンスが低下する可能性があるポイントにノードまたはアグリゲートのパフォーマンスが達していないかどうかを特定するのに役立ちます。また、特定の期間のノードまたはアグリゲートの使用率が高すぎないかどうかを調べることもできます。使用済みパフォーマンス容量は利用率と似ていますが、特定のワークロードに使用できる物理リソースのパフォーマンス容量に関するより詳しい情報を提供します。

ノードまたはアグリゲートの利用率とレイテンシ（応答時間）が最適で、効率的に使用されているポイントが、使用済みパフォーマンス容量の最適ポイントとなります。アグリゲートのレイテンシと利用率の関係を示す曲線の例を次の図に示します。



この例では、*operational point* は、アグリゲートの現在の利用率が 50% で、レイテンシが 1.0 ミリ秒 / 処理であることを示します。アグリゲートからキャプチャされた Unified Manager の統計によると、このアグリゲートでは追加のパフォーマンス容量を利用できます。この例では、アグリゲートの利用率が 80% で、レイテンシが 2.0 ミリ秒 / 処理のポイントとして、*_optimal_point_is* を特定します。したがって、このアグリゲートにボリュームや LUN を追加することで、システムをより効率的に使用することができます。

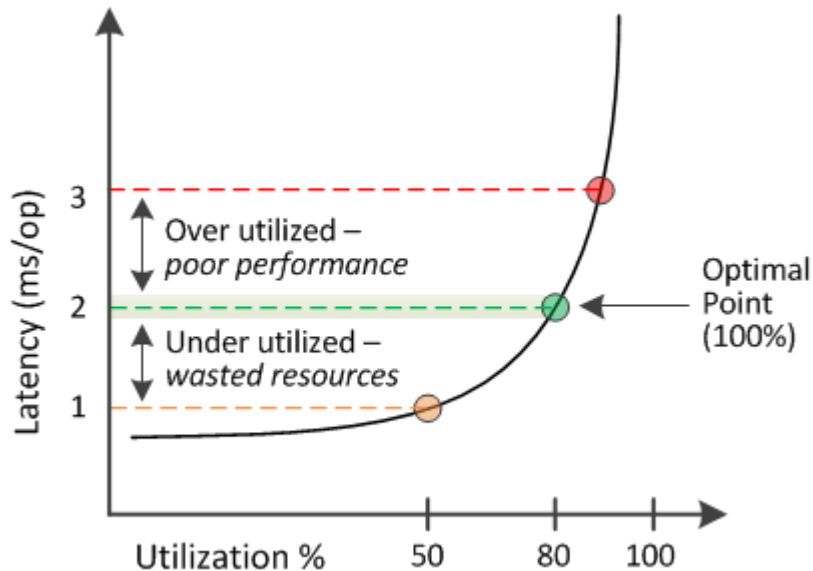
パフォーマンス容量にはレイテンシへの影響があるため、使用されるパフォーマンス容量カウンタは「利用率」カウンタよりも大きい値になることが予想されます。たとえば、ノードまたはアグリゲートの使用率が 70% の場合、使用済みパフォーマンス容量の値はレイテンシの値に応じて 80~100% になると想定されます。

ただし、ダッシュボードページの利用率カウンタの値が大きくなることがあります。これは、このダッシュボードには、Unified Manager のユーザインターフェイスの他のページのような一定期間の平均値ではなく、各収集期間の最新のカウンタの値が更新されて表示されるためです。使用済みパフォーマンス容量カウンタは一定期間のパフォーマンスの平均を確認するのに適した指標であり、利用率カウンタは特定の時点でのリソースの使用状況を確認するのに適した指標です。

使用済みパフォーマンス容量の値の意味

使用済みパフォーマンス容量の値は、利用率が高い状態や低い状態のノードやアグリゲートを特定するのに役立ちます。これにより、ストレージリソースをより効率的に活用できるようにワークロードを再配分することができます。

次の図は、リソースのレイテンシと利用率の関係を示す曲線を示したものです。現在の運用ポイントを色付きの3つの点で示してあります。



- 使用済みパフォーマンス容量が 100% の状態が最適ポイントです。

この時点で、リソースは効率的に使用されています。

- 使用済みパフォーマンス容量が 100% を超えている場合は、ノードまたはアグリゲートの利用率が高く、ワークロードのパフォーマンスが最適な状態ではないことを示します。

新しいワークロードをリソースに追加することは推奨されず、既存のワークロードの再配分が必要になる可能性があります。

- 使用済みパフォーマンス容量が 100% 未満の場合は、ノードまたはアグリゲートの利用率が低く、リソースが効率的に使用されていないことを示します。

リソースにワークロードをさらに追加することができます。



利用率とは異なり、使用済みパフォーマンス容量は 100% を超えることがあります。この値に上限はありませんが、一般に、リソースの利用率が高いときで 110~140% ほどになります。この値が大きいほど、リソースの問題が深刻であることを示します。

使用可能な IOPS とは

使用可能な IOPS カウンタは、リソースの上限に達するまでにノードまたはアグリゲートに追加できる残りの IOPS の数を示します。

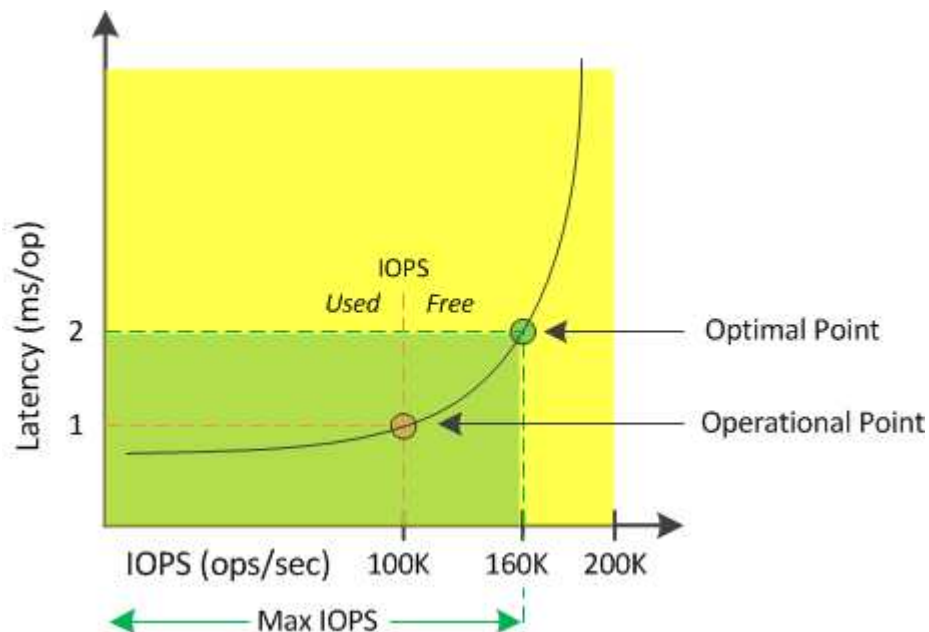
ノードで提供可能な合計 IOPS は、CPU の数、CPU の速度、RAM の容量など、ノードの物理仕様に基づきます。アグリゲートで提供可能な合計 IOPS は、ディスクが SATA、SAS、SSD のいずれであるかなど、ディスクの物理特性に基づきます。

アグリゲート内のすべてのボリュームの合計 IOPS がアグリゲートの合計 IOPS と一致しない場合があります。これについては、次のナレッジベースの記事「KB」で説明しています ["アグリゲート内のすべてのボリュームの IOPS の合計がアグリゲートの IOPS と一致しないのはなぜですか。"](#)

空きパフォーマンス容量カウンタは使用可能な残りのリソースの割合を示すのに対し、使用可能な IOPS カウンタは最大パフォーマンス容量に達するまでにリソースに追加できる IOPS（ワークロード）の正確な数を示します。

たとえば、FAS2520 と FAS8060 のストレージシステムを使用している場合、空きパフォーマンス容量の値が 30% であれば、空きパフォーマンス容量がいくらか残っていることがわかります。ただし、この値からは、それらのノードに導入できるワークロードの数はわかりません。使用可能な IOPS カウンタの場合は、使用可能な IOPS が FAS8060 には 500 あり、FAS2520 には 100 だけのように、正確な数が示されます。

ノードのレイテンシと IOPS の関係を示す曲線の例を次の図に示します。



リソースで提供可能な最大 IOPS は、使用済みパフォーマンス容量カウンタが 100%（最適ポイント）の時点の IOPS の数です。運用ポイントから、このノードの現在の IOPS は 100K で、レイテンシは 1.0 ミリ秒 / 処理です。ノードからキャプチャされた Unified Manager の統計によると、このノードの最大 IOPS は 160K であり、あと 60K の IOPS を利用できます。したがって、このノードにさらにワークロードを追加することで、システムをより効率的に使用することができます。



ユーザアクティビティが少ないリソースについては、一般的なワークロードを想定し、CPU コアあたりの IOPS を約 4、500 として使用可能な IOPS の値が計算されます。これは、提供されるワークロードの特性を正確に見積もるためのデータが Unified Manager で得られないためです。

ノードとアグリゲートの使用済みパフォーマンス容量の値の表示

クラスタ内のすべてのノードまたはアグリゲートの使用済みパフォーマンス容量の値、

または、1つのノードまたはアグリゲートの詳細を表示できます。

使用済みパフォーマンス容量の値は、ダッシュボード、パフォーマンスインベントリページ、パフォーマンスパフォーマンスストップページ、しきい値ポリシーの作成ページ、パフォーマンスエクスペローラページ、および詳細グラフに表示されます。たとえば、Performance : All aggregates ページには、使用済みパフォーマンス容量の列が表示されます。この列には、すべてのアグリゲートの使用済みパフォーマンス容量の値が表示されます。

Aggregates ⓘ

Last updated: 04:11 PM, 08 Feb Refresh

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

Filtering ▾ No filter applied

Search Aggregates Data Search

Assign Threshold Policy Clear Threshold Policy

<input type="checkbox"/>	Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
<input type="checkbox"/>	✓	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
<input type="checkbox"/>	✓	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
<input type="checkbox"/>	✓	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
<input type="checkbox"/>	✓	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
<input type="checkbox"/>	✓	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
<input type="checkbox"/>	✓	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
<input type="checkbox"/>	✓	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
<input type="checkbox"/>	✓	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-io...vity	opm-io...ty-01	aggr_IOPS
<input type="checkbox"/>	⚠	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-io...vity	opm-io...ty-01	aggr_IOPS

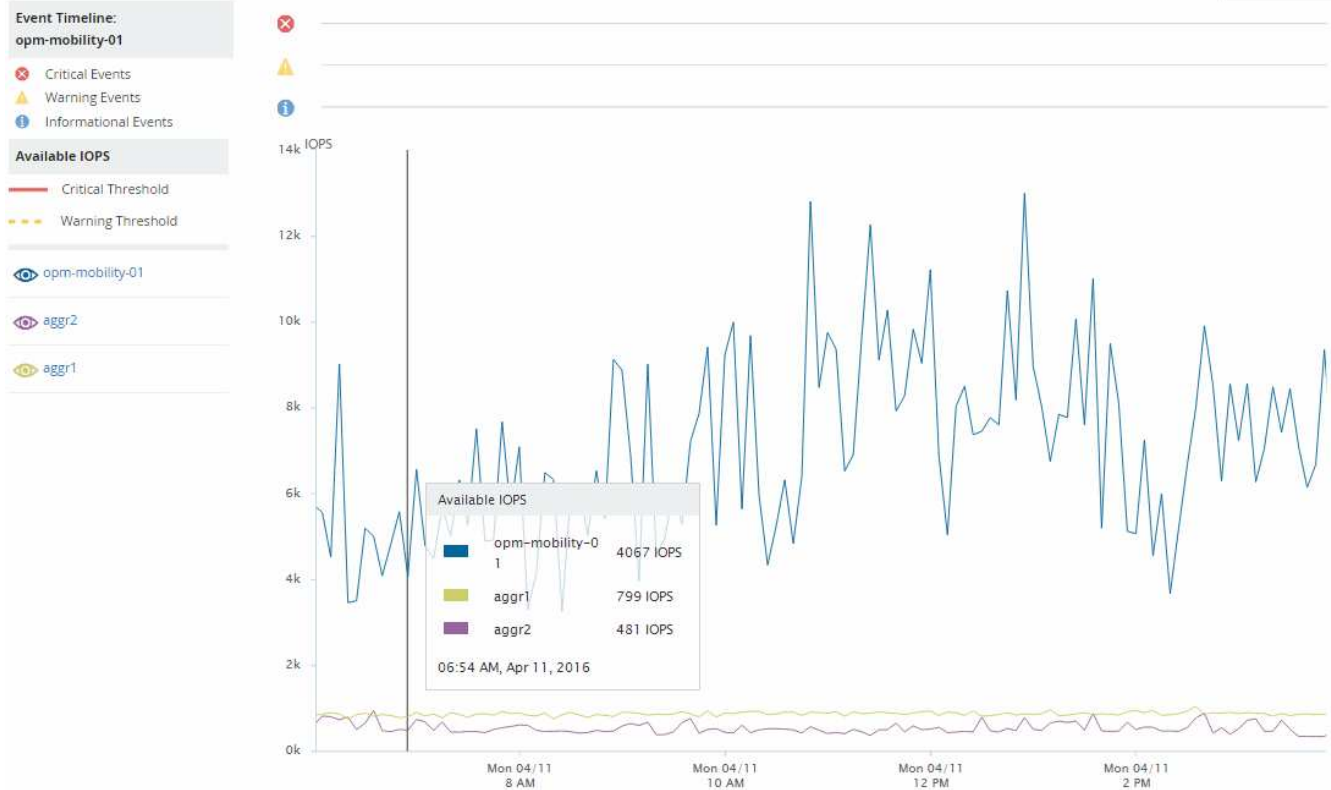
使用済みパフォーマンス容量のカウンタを監視すると、次の項目を特定できます。

- クラスタ上に使用済みパフォーマンス容量の値が大きいノードまたはアグリゲートがないかどうか
- クラスタ上にアクティブな使用済みパフォーマンス容量のイベントが発生しているノードまたはアグリゲートがないかどうか
- 使用済みパフォーマンス容量の値がクラスタ内で最も大きい、または小さいノードとアグリゲート
- 使用済みパフォーマンス容量の値が高いノードまたはアグリゲートと組み合わせたレイテンシと利用率のカウンタ値
- HA ペアの一方向のノードに障害が発生した場合のノードの使用済みパフォーマンス容量への影響
- 使用済みパフォーマンス容量の値が大きいアグリゲート上の最も負荷の高いボリュームと LUN

ノードとアグリゲートの使用可能な IOPS の値の表示

クラスタ内のすべてのノードまたはアグリゲートの使用可能な IOPS の値、または、1つのノードまたはアグリゲートの詳細を表示できます。

使用可能な IOPS の値は、パフォーマンスインベントリページおよびパフォーマンスエクスペローラページのノードとアグリゲートのグラフに表示されます。たとえば、ノード / パフォーマンスエクスペローラページでノードを表示しているときに、リストから「使用可能な IOPS」カウンタチャートを選択すると、そのノードおよびそのノード上の複数のアグリゲートの使用可能な IOPS 値を比較できます。



使用可能な IOPS カウンタを監視することで、次の項目を特定できます。

- 使用可能な IOPS の値が最も大きいノードまたはアグリゲート。今後ワークロードを導入可能な場所を判断します。
- 使用可能な IOPS の値が最も小さいノードまたはアグリゲート。今後発生する可能性のあるパフォーマンスの問題について監視が必要なリソースを特定します。
- 使用可能な IOPS の値が小さいアグリゲート上の最も負荷の高いボリュームと LUN。

問題を特定するためのパフォーマンス容量カウンタグラフの表示

ノードやアグリゲートの使用済みパフォーマンス容量グラフは、パフォーマンスエクスプローラのページで確認できます。選択したノードとアグリゲートの特定の期間にわたる詳細なパフォーマンス容量データを確認できます。

標準のカウンタグラフには、選択したノードまたはアグリゲートの使用済みパフォーマンス容量の値が表示されます。内訳カウンタグラフには、ルートオブジェクトのパフォーマンス容量の値の合計が、ユーザプロトコルとバックグラウンドのシステムプロセスに分けて表示されます。また、空きパフォーマンス容量も表示されます。

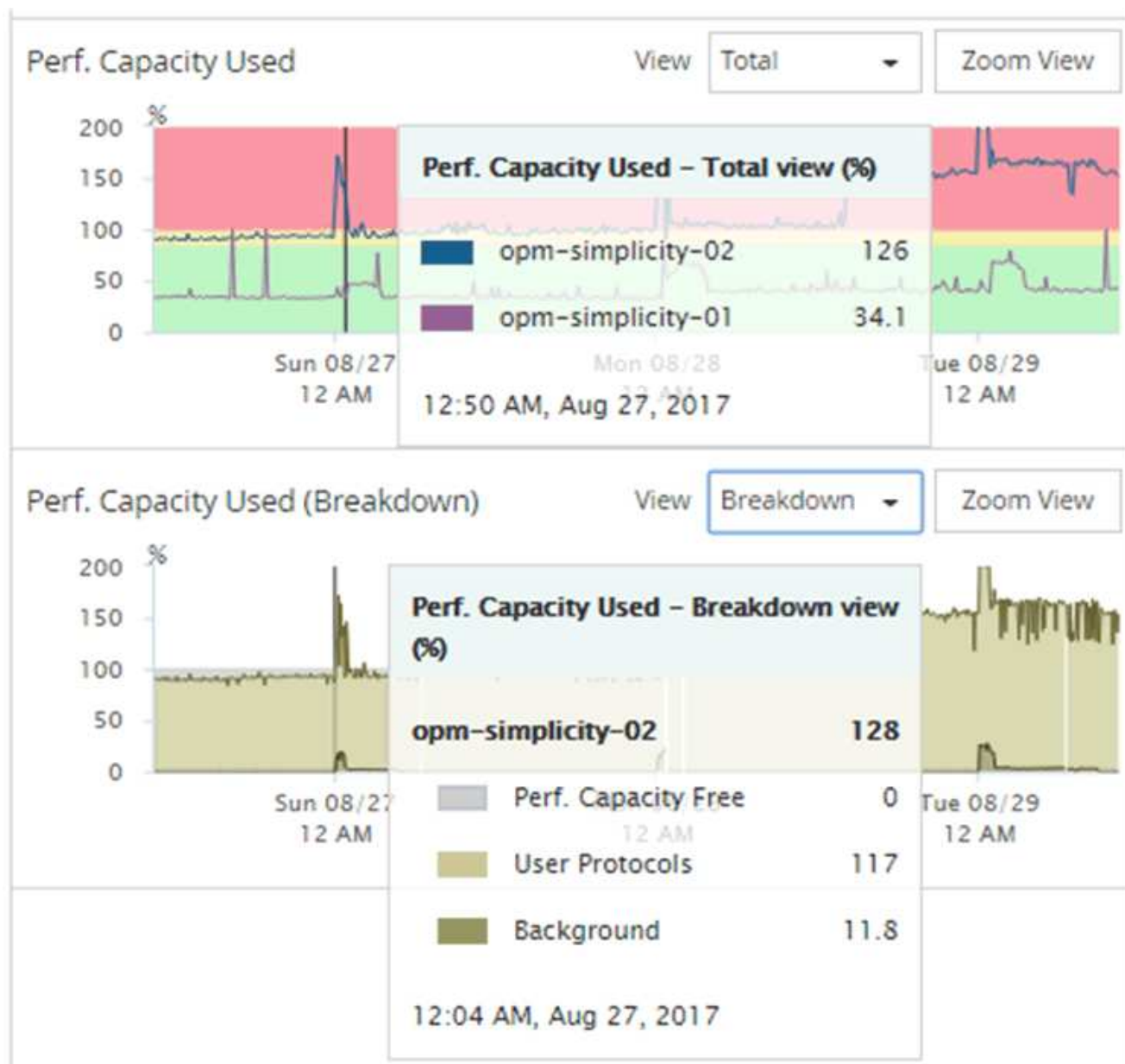


システムとデータの管理に関連する一部のバックグラウンドアクティビティはユーザワークロードとみなされ、ユーザプロトコルに分類されるため、これらのプロセスの実行時にはユーザプロトコルの割合が一時的に高く見ることがあります。通常、これらのプロセスはクラスタの使用量が少ない午前 0 時頃に実行されます。ユーザプロトコルのアクティビティが午前 0 時頃に急増している場合は、その時間にクラスタのバックアップジョブまたはその他のバックグラウンドアクティビティの実行が設定されていないかどうかを確認してください。

手順

1. ノードまたはアグリゲートのランディング * ページから * エクスプローラ * タブを選択します。
2. カウンタグラフ * ペインで、* グラフの選択 * をクリックし、* Perf を選択します。Capacity Used * チャート。
3. チャートが表示されるまで下にスクロールします。

標準チャートには、最適な範囲内のオブジェクトは黄色、利用率が低いオブジェクトは緑、利用率が高いオブジェクトは赤で表示されます。内訳グラフには、ルートオブジェクトのみの詳細なパフォーマンス容量の詳細が表示されます。



4. いずれかのグラフをフルサイズで表示する場合は、* ズームビュー * をクリックします。

この方法で、複数のカウンタグラフを別々のウィンドウで開き、使用済みパフォーマンス容量の値を同じ期間に IOPS または MBps の値と比較できます。

使用済みパフォーマンス容量のパフォーマンスしきい値条件

ユーザ定義のパフォーマンスしきい値ポリシーを作成して、ノードまたはアグリゲートの使用済みパフォーマンス容量の値が定義されている使用済みパフォーマンス容量しきい値の設定を超えたときにイベントがトリガーされるようにすることができます。

また、ノードには「Performance capacity used takeover」しきい値ポリシーを設定することもできます。このしきい値ポリシーは、HA ペアの両方のノードの使用済みパフォーマンス容量の統計を合計して、一方のノードで障害が発生した場合にもう一方のノードの容量が不足するかどうかを判断します。フェイルオーバー中のワークロードは2つのパートナーノードのワークロードの組み合わせであるため、両方のノードに同じ使用済みパフォーマンス容量のテイクオーバーポリシーを適用できます。



ノード間では、一般に使用済みパフォーマンス容量は同等になります。ただし、フェイルオーバーパートナー経由でいずれかのノード宛てのノード間トラフィックが大幅に多い場合は、一方のパートナーノードですべてのワークロードを実行したときともう一方のパートナーノードでワークロードを実行したときで、使用されている合計パフォーマンス容量が、障害が発生したノードによって若干異なることがあります。

LUN とボリュームのしきい値を定義する場合は、使用済みパフォーマンス容量の条件をセカンダリのパフォーマンスしきい値の設定として使用して、組み合わせしきい値ポリシーを作成することもできます。使用済みパフォーマンス容量の条件は、ボリュームや LUN が配置されているアグリゲートまたはノードに適用されます。たとえば、次の条件を使用して組み合わせしきい値ポリシーを作成できます。

ストレージオブジェクト	パフォーマンスカウンタ	警告しきい値	重大のしきい値	期間
ボリューム	レイテンシ	15 ミリ秒 / 処理	25 ミリ秒 / 処理	20 分
アグリゲート	使用済みパフォーマンス容量	80%	95%	

組み合わせしきい値ポリシー原因期間全体で両方の条件に違反した場合にのみイベントが生成されます。

使用済みパフォーマンス容量カウンタを使用してパフォーマンスを管理する

通常、組織では、使用済みパフォーマンス容量の割合を 100% 未満に抑えて、リソースを効率的に使用しつつ、ピーク時の需要に対応するパフォーマンス容量を確保する必要があります。しきい値ポリシーを使用して、使用済みパフォーマンス容量の値が高い場合にアラートを送信するタイミングを設定できます。

パフォーマンス要件に基づいて具体的な目標を設定できます。たとえば、金融機関では、取引をタイミングよく実行するために、より多くのパフォーマンス容量を確保することが考えられます。このような企業は、使用済みパフォーマンス容量のしきい値を 70~80% の範囲に設定する必要があります。小規模な製造業で、IT コストを適切に管理するためにパフォーマンスを犠牲にしてもよいと考えている場合、確保するパフォーマンス容量を少なくすることもできます。このような企業では、使用済みパフォーマンス容量のしきい値を 85~95% の範囲に設定する必要があります。

使用済みパフォーマンス容量の値がユーザ定義のしきい値ポリシーで設定された割合を超えると、Unified Manager はアラート E メールを送信し、イベントをイベントインベントリページに追加します。これにより、パフォーマンスに影響が及ぶ前に潜在的な問題に対処できます。これらのイベントを、ノードやアグリゲ

ート内でワークロードを移動および変更するインジケータとして使用することもできます。

ノードフェイルオーバープランの概要と使用方法ページ

ノードのハイアベイラビリティ（HA）パートナーノードに障害が発生した場合のノードのパフォーマンスへの影響は、Performance/NodeFailover Planning ページで概算できます。Unified Manager は、HA ペアの各ノードのパフォーマンス履歴に基づいて見積もりを行います。

フェイルオーバーのパフォーマンスへの影響を見積もることで、次のシナリオに備えて計画することができます。

- フェイルオーバーによって、テイクオーバーノードの推定パフォーマンスが常に許容できないレベルまで低下する場合は、フェイルオーバーによるパフォーマンスへの影響を軽減する対処策を実施することを検討できます。
- ハードウェアのメンテナンスタスクを実行するために手動フェイルオーバーを開始する前に、フェイルオーバーがテイクオーバーノードのパフォーマンスに及ぼす影響を見積もって、タスクを実行する最適なタイミングを判断できます。

ノードフェイルオーバープランのシナリオ

Performance / Node Failover Planning ページに表示原因された情報に基づいて、フェイルオーバーが HA ペアのパフォーマンスを許容可能なレベルよりも低下しないように対処できます。

たとえば、フェイルオーバーによって予測されるパフォーマンスへの影響を軽減するために、一部のボリュームまたは LUN を HA ペアのノードからクラスタ内の他のノードに移動できます。これにより、プライマリノードはフェイルオーバー後も許容されるパフォーマンスを引き続き提供できます。

Node Failover Planning ページのコンポーネント

Performance / Node Failover Planning ページのコンポーネントが、グリッドと Comparing ペインに表示されます。これらのセクションで、ノードのフェイルオーバーによるテイクオーバーノードのパフォーマンスへの影響を評価できます。

パフォーマンス統計グリッド

Performance/NodeFailover Planning ページには、レイテンシ、IOPS、利用率、使用済みパフォーマンス容量の統計を含むグリッドが表示されます。



このページおよび Performance/NodePerformance Explorer ページに表示されるレイテンシと IOPS の値は一致しないことがあります。異なるパフォーマンスカウンタを使用してノードフェイルオーバーを予測するために値が計算されるためです。

グリッドでは、各ノードに次のいずれかのロールが割り当てられます。

- プライマリ

HA パートナーで障害が発生した場合にパートナーをテイクオーバーするノードです。ルートオブジェクトは常にプライマリノードです。

- パートナー

フェイルオーバーシナリオで障害が発生したノードです。

- 推定テイクオーバー

プライマリノードと同じ。このノードに対して表示されるパフォーマンス統計は、障害が発生したパートナーをテイクオーバーしたあとのテイクオーバーノードのパフォーマンスを示します。



テイクオーバーノードのワークロードはフェイルオーバー後の両方のノードのワークロードの合計に相当しますが、推定テイクオーバーノードの統計はプライマリノードとパートナーノードの統計の合計にはなりません。たとえば、プライマリノードのレイテンシが 2 ミリ秒 / 処理でパートナーノードのレイテンシが 3 ミリ秒 / 処理の場合に、推定テイクオーバーノードのレイテンシが 4 ミリ秒 / 処理になることがありますこの値は Unified Manager で計算されます。

パートナーノードをルートオブジェクトにする場合は、そのノードの名前をクリックします。Performance/NodePerformance Explorer ヘシが表示されたら、* Failover Planning * タブをクリックして、このノード障害シナリオにおけるパフォーマンスの変化を確認できます。たとえば、Node1 がプライマリノードで Node2 がパートナーノードの場合、Node2 をクリックしてプライマリノードに切り替えることができます。これにより、どちらのノードで障害が発生したかに応じて、予想されるパフォーマンスの変化を確認することができます。

比較ペイン

デフォルトでは ' 比較ペインに表示される構成部品は次のとおりです

- * イベントチャート *

これらの値は、Performance/NodePerformance Explorer ページと同じ形式で表示されます。プライマリノードのみが対象になります。

- * カウンタチャート *

グリッドに表示されるパフォーマンスカウンタの過去の統計が表示されます。各チャートの推定テイクオーバーノードのグラフには、フェイルオーバーが特定の時点で発生した場合の推定パフォーマンスが表示されます。

たとえば、利用率のチャートに、推定テイクオーバーノードの 2 月 3 日の午前 11 時の利用率が 73% と表示されているとします2 月 8 日に。その時点でフェイルオーバーが発生した場合は、テイクオーバーノードの利用率は 73% になります。

過去の統計は、テイクオーバーノードに過大な負荷をかけずにフェイルオーバーを開始する最適な時刻を特定するのに役立ちます。テイクオーバーノードの予測パフォーマンスを確認して、許容される時間にフェイルオーバーをスケジュールすることができます。

デフォルトでは、ルートオブジェクトとパートナーノードの両方の統計情報が比較ペインに表示されます。Performance/NodePerformance Explorer ページとは異なり、このページには統計比較用のオブジェクトを追加するための **Add** ボタンは表示されません。

[Performance/Node Performance Explorer] ページで行うのと同じ方法で、[Comparing（比較）] ペインをカスタマイズできます。グラフをカスタマイズする例を次に示します。

- ・ ノード名をクリックすると、カウンタグラフでそのノードの統計の表示と非表示が切り替わります。
- ・ 特定のカウンタの詳細なグラフを新しいウィンドウに表示するには、* Zoom View * をクリックします。

Node Failover Planning ページでしきい値ポリシーを使用します

ノードしきい値ポリシーを作成して、フェイルオーバーが発生する可能性があるとき、テイクオーバーノードのパフォーマンスが許容できないレベルまで低下する場合に、Performance/NodeFailover Planning ページで通知されるようにすることができます。

「Node HA pair over-utilized」という名前のシステム定義のパフォーマンスしきい値ポリシーは、6 回の収集期間（30 分）に連続してしきい値を超えた場合に警告イベントを生成します。HA ペアのノードの使用済みパフォーマンス容量の合計が 200% を超えると、しきい値を超えたと認識されます。

システム定義原因のしきい値ポリシーで生成されたイベントは、フェイルオーバーによってテイクオーバーノードのレイテンシが許容できないレベルまで上昇することを警告します。特定のノードについてこのポリシーで生成されたイベントが表示された場合は、そのノードの Performance/NodeFailover Planning ページに移動して、フェイルオーバーによる予測レイテンシ値を確認できます。

このシステム定義のしきい値ポリシーの使用に加えて、「Performance Capacity Used - Takeover」カウンタを使用してしきい値ポリシーを作成し、選択したノードにそのポリシーを適用できます。200% を下回るしきい値を指定すると、システム定義のポリシーのしきい値を超える前にイベントを受け取ることができます。システム定義のポリシーイベントが生成される前に通知を受け取るには、しきい値を超えた最低期間を 30 分未満に指定することもできます。

たとえば、HA ペアのノードの使用済みパフォーマンス容量の合計が 10 分以上にわたって 175% を超えた場合に警告イベントが生成されるようにしきい値ポリシーを定義できます。HA ペアの Node1 と Node2 にこのポリシーを適用できます。ノード 1 またはノード 2 の警告イベント通知を受け取ったら、そのノードのパフォーマンス / ノードフェイルオーバー計画ページを表示して、テイクオーバーノードへのパフォーマンスの影響を推定できます。フェイルオーバーが発生した場合は、テイクオーバーノードの過負荷を回避するための対処を実行できます。ノードの使用済みパフォーマンス容量の合計が 200% を下回っている間に対処を行うと、この期間にフェイルオーバーが発生してもテイクオーバーノードのレイテンシが許容できないレベルに到達することはありません。

フェイルオーバー計画に使用済みパフォーマンス容量の内訳グラフを使用する

詳細な使用済みパフォーマンス容量 - 内訳グラフには、プライマリノードとパートナーノードの使用済みパフォーマンス容量が表示されます。また、推定テイクオーバーノードの空きパフォーマンス容量も表示されます。この情報から、パートナーノードで障害が発生した場合にパフォーマンス問題が確保されるかどうかを判断できます。

内訳グラフでは、ノードの使用済みパフォーマンス容量の合計に加えて、各ノードの値がユーザプロトコルとバックグラウンドプロセスに分けて表示されます。

- ・ ユーザプロトコルは、ユーザアプリケーションとクラスタとの間の I/O 処理です。
- ・ バックグラウンドプロセスは、ストレージ効率化、データレプリケーション、およびシステム健全性に関連する内部システムプロセスです。

この詳細レベルにより、パフォーマンス問題の原因が、ユーザのアプリケーションアクティビティであるか、重複排除、RAID 再構築、ディスククラビング、SnapMirror コピーなどのバックグラウンドのシステムプロセスであるかを判別できます。

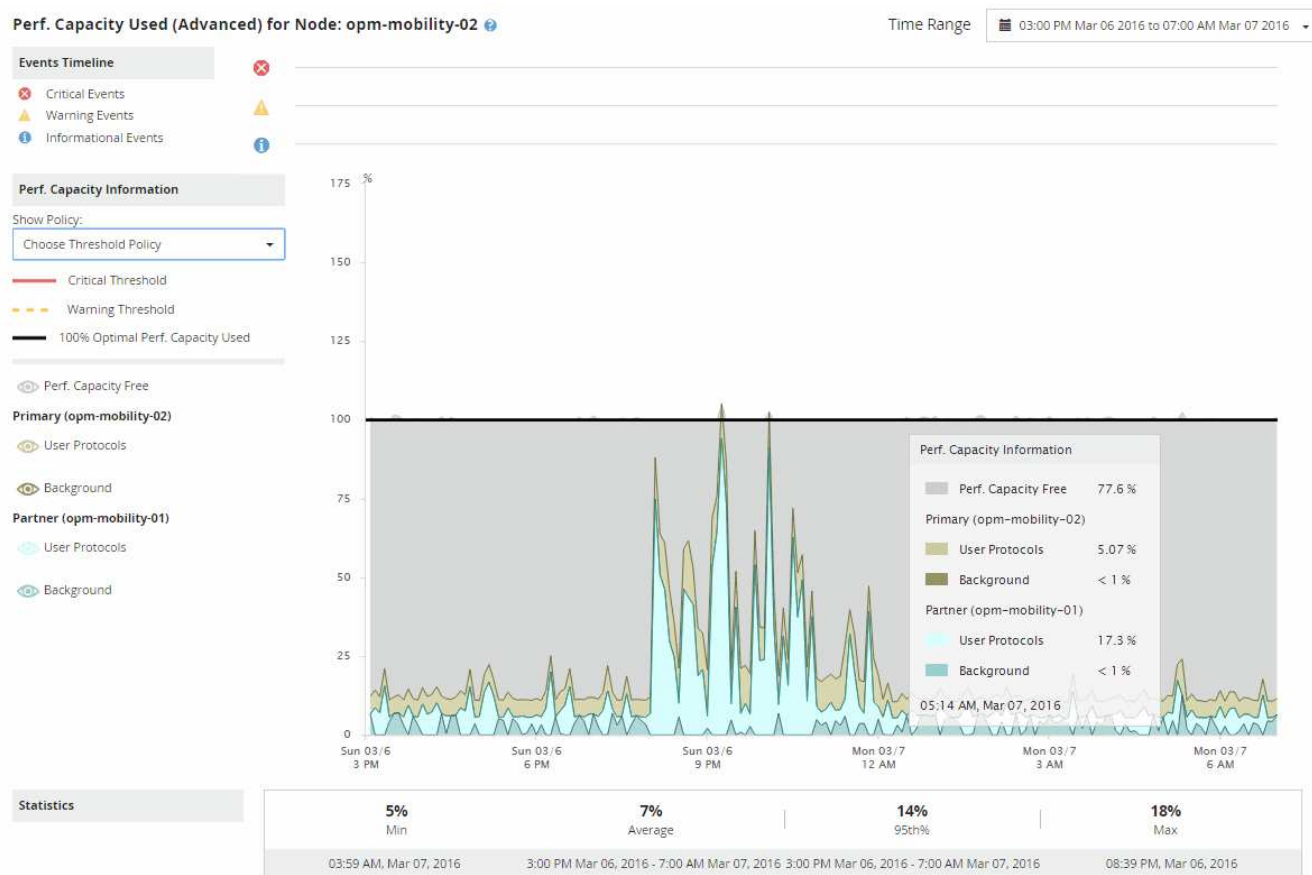
手順

1. 推定テイクオーバーノードとして機能するノードの * パフォーマンス / ノードフェイルオーバー計画 * ページに移動します。
2. * Time Range * セレクタから、カウンタグリッドおよびカウンタチャートに履歴統計を表示する期間を選択します。

カウンタグラフにプライマリノード、パートナーノード、推定テイクオーバーノードの統計が表示されます。

3. [グラフの選択 *] リストから、[*Perf] を選択します。使用済みパフォーマンス容量 *。
4. 使用済み使用済み容量 * グラフで、* 内訳 * を選択し、* ズームビュー * をクリックします。

パフォーマンスの詳細チャート。使用済みパフォーマンス容量] が表示されます。



5. 詳細チャートにカーソルを合わせると、ポップアップウィンドウに使用されているパフォーマンス容量の情報が表示されます。

パフォーマンスCapacity Free] の割合は、Estimated Takeover ノードで使用可能なパフォーマンス容量です。これは、フェイルオーバー後にテイクオーバーノードに残っているパフォーマンス容量を示します。0% の場合は、フェイルオーバーによってレイテンシが原因に増加し、テイクオーバーノードが許容できないレベルまで増加します。

6. その場合、空きパフォーマンス容量の割合の低下を回避するための対処を検討します。

ノードのメンテナンスのためにフェイルオーバーを開始する予定の場合は、空きパフォーマンス容量の割合が 0 でない時間帯にパートナーノードを停止するようにしてください。

データを収集してワークロードのパフォーマンスを監視

Unified Manager では、ワークロードアクティビティを 5 分間隔で収集および分析してパフォーマンスイベントを特定するほか、構成の変更を 15 分間隔で検出します。5 分ごとのパフォーマンスとイベントの履歴データが最大 30 日分保持され、そのデータを使用して監視対象のすべてのワークロードの想定レイテンシ範囲が予測されます。

Unified Manager では、少なくとも 3 日分のワークロードアクティビティを収集して分析してから、ワークロードの分析ページおよびイベントの詳細ページに I/O 応答時間のレイテンシ予測を表示する必要があります。このアクティビティを収集して表示されるレイテンシ予測には、ワークロードアクティビティにおける変化がすべて反映されるわけではありません。3 日間のアクティビティを収集したあと、Unified Manager ではレイテンシ予測を 24 時間ごとに午前 12 時に調整し、ワークロードアクティビティの変化が反映された、より正確で動的なパフォーマンスしきい値を設定します。

Unified Manager でワークロードの監視を開始してから最初の 4 日間に、前回のデータ収集からの経過時間が 24 時間を超える期間がある場合、そのワークロードのレイテンシ予測はレイテンシのグラフに表示されません。前回の収集よりも前に検出されたイベントは引き続き表示されます。



システム時間が夏時間（DST）に切り替わると、監視しているワークロードのパフォーマンスの統計で使用するレイテンシ予測が変わります。Unified Manager は、レイテンシ予測の修正を即座に開始しますが、完了までに 15 日間ほどかかります。その間も Unified Manager の使用は継続できますが、Unified Manager はレイテンシ予測を使用して動的イベントを検出するため、一部のイベントは正確でなくなる可能性があります。時間の変更前に検出されたイベントは影響を受けません。

Unified Manager で監視されるワークロードのタイプ

Unified Manager では、ユーザ定義とシステム定義の 2 種類のワークロードのパフォーマンスを監視できます。

• *_ ユーザ定義のワークロード _*

アプリケーションからクラスタへの I/O スループット。読み取り要求と書き込み要求に関連するプロセスです。ボリューム、LUN、NFS 共有、SMB / CIFS 共有、およびワークロードはユーザ定義のワークロードです。



Unified Manager は、クラスタ内のワークロードだけを監視します。アプリケーション、クライアント、またはアプリケーションとクラスタ間のパスは監視しません。

次の条件が 1 つ以上該当するワークロードは、Unified Manager で監視できません。

- 。読み取り専用モードのデータ保護（DP）コピーである。（DP ボリュームについてはユーザ生成のトラフィックが監視されます）。

- ボリュームがオフラインデータクローンである。
- ボリュームが MetroCluster 構成のミラーボリュームである。
- * _ システム定義のワークロード _ *

次のストレージ効率化、データレプリケーション、およびシステム健全性に関連する内部プロセスです。

- 重複排除などのストレージ効率
- ディスクの健全性。RAID の再構築、ディスクスクラビングなどが含まれます
- SnapMirror コピーなどのデータレプリケーション
- 管理アクティビティ
- ファイルシステムの健全性。さまざまな WAFL アクティビティが含まれます
- WAFL スキャンなどのファイルシステムスキャナ
- VMware ホストからのオフロードされたストレージ効率化処理などのコピーオフロード
- ボリューム移動やデータ圧縮などのシステムヘルス
- 監視対象外のボリューム

システム定義のワークロードのパフォーマンスデータは、これらのワークロードで使用するクラスタコンポーネントが競合状態の場合にのみ表示されます。たとえば、システム定義のワークロードの名前を検索して、そのパフォーマンスデータを表示することはできません。

ワークロードのパフォーマンスの測定値

Unified Manager では、過去の統計値と想定される統計値から決定されるワークロードの値のレイテンシ予測に基づいて、クラスタのワークロードのパフォーマンスを測定します。ワークロードの実際の統計値をレイテンシ予測と比較することで、ワークロードのパフォーマンスが高すぎたり低すぎたりしないかが判別されます。ワークロードのパフォーマンスが想定される範囲外になった場合、動的なパフォーマンスイベントがトリガーされてユーザに通知されます。

次の図では、期間内の実際のパフォーマンス統計が赤で表示されています。この実測値はパフォーマンスしきい値を超えており、レイテンシ予測の上限よりも上に表示されています。ピークは期間内における実測値の最大値です。偏差は想定値（予測）と実測値の差を測定したもので、ピーク偏差は想定値と実測値の差の最大値を示します。



次の表に、ワークロードのパフォーマンスの測定値を示します。

測定値	説明
アクティビティ	<p>ポリシーグループ内のワークロードで使用されている QoS 制限の割合。</p> <div> <p>i</p> <p>ボリュームの追加や削除、QoS 制限の変更など、ポリシーグループに対する変更が Unified Manager で検出されると、実測値や想定値が設定された上限の 100% を超えることがあります。設定された上限の 100% を超える値は、「>100%」と表示されます。設定された上限の 1% 未満の値は、1% として表示されます。</p> </div>
実際	特定の時間に測定された特定のワークロードのパフォーマンス値。
偏差（Deviation）	<p>想定値と実測値の差です。想定範囲の上限値から想定値を引いた値を実測値から想定値を引いた値で割った比率で示されます。</p> <div> <p>i</p> <p>負の偏差値はワークロードのパフォーマンスが想定より低く、正の偏差値はワークロードのパフォーマンスが想定より大きいことを示します。</p> </div>
必要です	特定のワークロードについての過去のパフォーマンスデータの分析に基づく想定値です。Unified Manager では、これらの統計値を分析して値の想定範囲（レイテンシ予測）を決定します。

測定値	説明
レイテンシ予測（想定範囲）	レイテンシ予測とは、特定の時間に想定されるパフォーマンスの上限と下限の値です。ワークロードのレイテンシについては、パフォーマンスしきい値を上回る値です。実測値がパフォーマンスしきい値を超えると、Unified Manager によって動的なパフォーマンスイベントがトリガーされます。
ピーク	一定の期間に測定された最大値です。
ピーク偏差	一定の期間に測定された偏差の最大値です。
キューの深さ	インターコネクトコンポーネントで待機している保留中の I/O 要求の数。
利用率	ネットワーク処理、データ処理、およびアグリゲートコンポーネントのワークロード処理を完了するためにビジー状態になる一定期間における時間の割合です。たとえば、ネットワーク処理やデータ処理のコンポーネントで I/O 要求を処理するのにかかる時間の割合や、アグリゲートで読み取りや書き込みの要求に対応するのにかかる時間の割合などがあります。
書き込みスループット	MetroCluster 構成におけるローカルクラスタのワークロードからパートナークラスタへの書き込みスループットです。1 秒あたりのメガバイト数（MBps）で示されます。

パフォーマンスの想定範囲

レイテンシ予測とは、特定の時間に想定されるパフォーマンスの上限と下限の値です。ワークロードのレイテンシについては、パフォーマンスしきい値を上回る値です。実測値がパフォーマンスしきい値を超えると、Unified Manager によって動的なパフォーマンスイベントがトリガーされます。

たとえば、午前 9 時から午後 5 時までの通常の営業時間の間などですほとんどの従業員は、午前 9 時から午後 5 時まで E メールをチェックすることができますチェックするとしますこの期間、E メールサーバの負荷が増加すると、バックエンドストレージのワークロードアクティビティが増加します。従業員の E メールクライアントからの応答時間が長くなる可能性があります。

昼食の時間は午後 12 時からとなっている午後 1 時までオープン午後 5 時以降の勤務日の終わりには、ほとんどの従業員がコンピュータから離れている可能性があります。一般に、E メールサーバの負荷は軽減され、バックエンドストレージの負荷も軽減されます。または、ストレージのバックアップやウィルススキャンなどのワークロード処理を午後 5 時以降に実行するようにスケジュールしている場合もありますバックエンドストレージのアクティビティが増加します。

ワークロードアクティビティの増加と減少を数日間にわたって監視した結果から、アクティビティの想定範囲

（レイテンシ予測）が特定され、ワークロードの上限と下限が決まります。オブジェクトに対する実際のワークロードアクティビティが上限と下限の範囲から外れ、その状態が一定の期間にわたって続く場合は、オブジェクトの使用率が高すぎるか低すぎる可能性があります。

レイテンシ予測の生成方法

Unified Manager では、少なくとも 3 日分のワークロードアクティビティを収集して分析してから、GUI に表示する I/O 応答時間のレイテンシ予測を決定します。この期間で収集されるデータには、ワークロードアクティビティにおける変化がすべて反映されるわけではありません。最初の 3 日間のアクティビティを収集したあと、Unified Manager はレイテンシ予測を 24 時間ごとに午前 12 時に調整します。ワークロードアクティビティの変化を反映し、より正確な動的なパフォーマンスしきい値を設定する。



システム時間が夏時間（DST）に切り替わると、監視しているワークロードのパフォーマンスの統計で使用するレイテンシ予測が変わります。Unified Manager は、レイテンシ予測の修正を即座に開始しますが、完了までに 15 日間ほどかかります。その間も Unified Manager の使用は継続できますが、Unified Manager はレイテンシ予測を使用して動的イベントを検出するため、一部のイベントは正確でなくなる可能性があります。時間の変更前に検出されたイベントは影響を受けません。

レイテンシ予測とパフォーマンス分析

Unified Manager は、レイテンシ予測を使用して監視対象のワークロードの一般的な I/O レイテンシ（応答時間）を表します。ワークロードの実際のレイテンシがレイテンシ予測の上限を上回るとアラートが生成されて動的なパフォーマンスイベントがトリガーされるため、パフォーマンス問題を分析して解決することができます。

レイテンシ予測は、ワークロードのパフォーマンスベースラインです。Unified Manager は過去のパフォーマンス測定値から学習して、ワークロードの想定されるパフォーマンスとアクティビティレベルを予測します。想定範囲の上限が動的なパフォーマンスしきい値となります。Unified Manager では、このベースラインを使用して、実際のレイテンシがしきい値を上回る、下回る、あるいは想定範囲外になったかどうかを判断します。実測値と想定値の比較を基に、ワークロードのパフォーマンスプロファイルが作成されます。

あるワークロードの実際のレイテンシがクラスタコンポーネントの競合が原因で動的なパフォーマンスしきい値を超えると、レイテンシが高くなり、ワークロードのパフォーマンスは想定よりも遅くなります。同じクラスタコンポーネントを共有する他のワークロードのパフォーマンスも想定より遅くなる可能性があります。

Unified Manager は、しきい値を超えるイベントを分析して、そのアクティビティがパフォーマンスイベントに該当するかどうかを判断します。高ワークロードアクティビティが数時間などの長い期間継続している場合、Unified Manager はそのアクティビティが正常であるとみなし、レイテンシ予測を動的な新しいパフォーマンスしきい値に動的に調整します。

ワークロードによっては、レイテンシ予測が時間が経過しても大きく変化することがない、アクティビティが一貫して低いワークロードもあります。このような低アクティビティのボリュームについては、イベントの数を最小限に抑えるために、パフォーマンスイベントの分析中、Unified Manager は処理数およびレイテンシが想定よりもはるかに高いイベントのみをトリガーします。



この例のボリュームのレイテンシ予測（グレーで表示）は、3.5~5.5ms/op です。青で表示された実際のレイテンシが、ネットワークトラフィックの断続的な急増またはクラスタコンポーネントの競合が原因で 10 ミリ秒 / 処理に突然上昇した場合、レイテンシ予測を超え、動的なパフォーマンスしきい値を超えています。

ネットワークトラフィックが減少するか、クラスタコンポーネントの競合が解消されると、レイテンシはレイテンシ予測の範囲内に戻ります。レイテンシが長期間にわたって 10ms/op 以上のままの場合、イベントを解決するための対処が必要となることがあります。

Unified Manager がワークロードのレイテンシを使用してパフォーマンスの問題を特定する仕組み

ワークロードのレイテンシ（応答時間）は、クラスタ上のボリュームがクライアントアプリケーションからの I/O 要求に応答するまでの時間です。Unified Manager は、レイテンシを使用してパフォーマンスイベントを検出し、アラートを生成します。

高レイテンシは、アプリケーションからクラスタ上のボリュームへの要求に通常よりも時間がかかっていることを意味します。高レイテンシの原因は、1 つ以上のクラスタコンポーネントの競合が原因で、クラスタ自体に存在する場合があります。高レイテンシは、ネットワークのボトルネック、アプリケーションをホストしているクライアントの問題、アプリケーション自体の問題など、クラスタ外の問題が原因で発生することもあります。

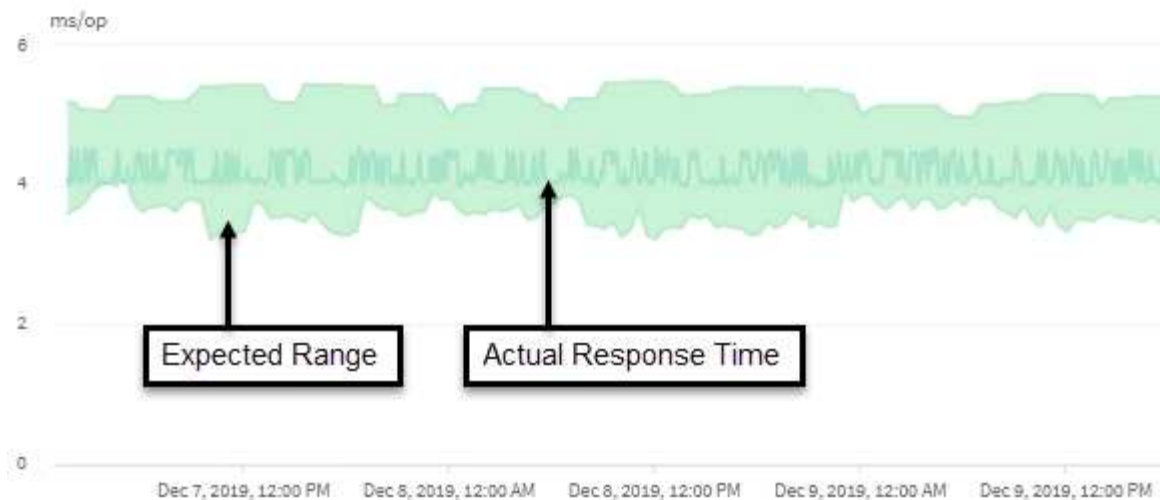


Unified Manager は、クラスタ内のワークロードだけを監視します。アプリケーション、クライアント、またはアプリケーションとクラスタ間のパスは監視しません。

バックアップの作成や重複排除の実行など、クラスタで他のワークロードが共有するクラスタコンポーネントに対する要求が増加すると、レイテンシが高くなる場合があります。実際のレイテンシが想定範囲（レイテンシ予測）の動的パフォーマンスしきい値を超えると、Unified Manager はイベントを分析して、解決が必要なパフォーマンスイベントであるかどうかを判断します。レイテンシは処理あたりのミリ秒（ms/op）単位で測定されます。

ワークロード分析ページのレイテンシ合計グラフでは、レイテンシ統計の分析を表示して、読み取り要求や書き込み要求などの個々のプロセスのアクティビティと全体的なレイテンシ統計を比較することができます。この比較により、最もアクティビティが高い処理を特定したり、ボリュームのレイテンシに影響を及ぼしている異常なアクティビティがある特定の処理がないかを判断できます。パフォーマンスイベントを分析するにあたっては、レイテンシの統計値を使用してイベントの原因がクラスタ上の問題であるかどうかを判断できます。また、イベントに関連するワークロードのアクティビティまたはクラスタコンポーネントを特定することもで

きます。



この例は、レイテンシグラフを示しています。実際の応答時間（レイテンシ）アクティビティは青い線、レイテンシ予測（想定範囲）は緑で表されています。

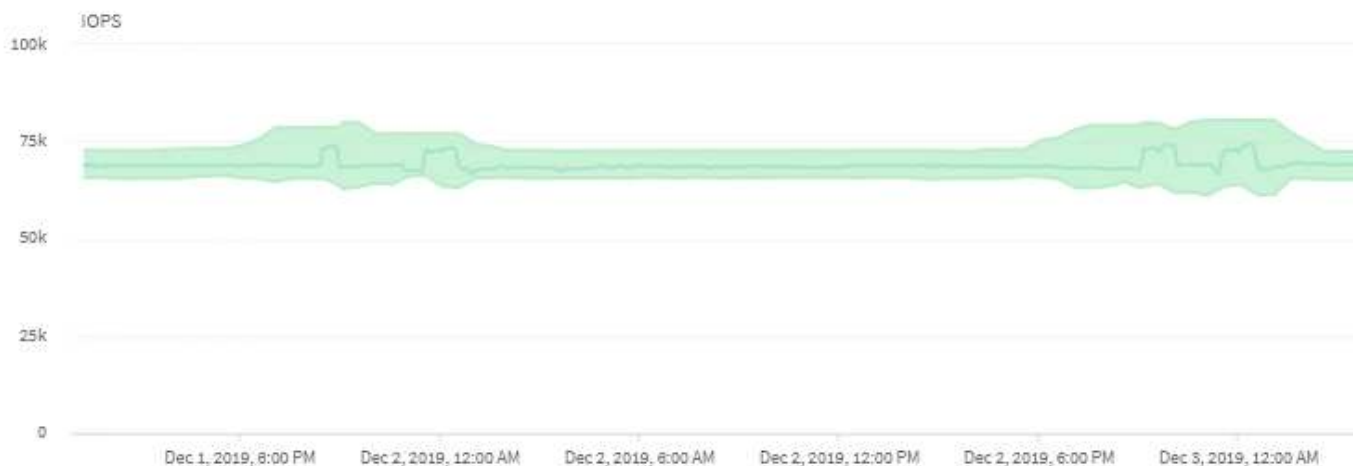


Unified Manager でデータを収集できなかった期間は、青い線が途切れています。これは、クラスタまたはボリュームと通信できなかったか、Unified Manager がその時間にオフになっていたか、データの収集に 5 分以上かかった場合に起こります。

クラスタでの処理がワークロードのレイテンシに与える影響

処理（IOPS）には、クラスタで実行されるユーザ定義とシステム定義のすべてのワークロードのアクティビティが含まれます。IOPS の統計は、クラスタでの処理（バックアップの作成や重複排除の実行など）がワークロードのレイテンシ（応答時間）に影響を及ぼしていないかどうかやパフォーマンスイベントの原因となっていないかどうかを確認するのに役立ちます。

パフォーマンスイベントを分析するにあたっては、IOPS の統計を使用して、クラスタの問題がパフォーマンスイベントの原因となっていないかどうかを確認できます。パフォーマンスイベントの原因となった可能性がある具体的なワークロードアクティビティを特定することができます。IOPS は 1 秒あたりの処理数（処理数 / 秒）として測定されます。



次の例は、IOPS チャートを示しています。実際の処理の統計が青い線で、処理の IOPS 予測が緑で表示されています。



Unified Managerでは、クラスタが過負荷状態の場合、というメッセージが表示されることがあります `Data collection is taking too long on Cluster cluster_name`。これは、Unified Manager で分析に使用する統計が十分に収集されていないことを意味します。クラスタで使用しているリソースを減らして統計を収集できるようにする必要があります。

MetroCluster 構成のパフォーマンス監視

Unified Manager では、MetroCluster 構成のクラスタ間の書き込みスループットを監視して、大量の書き込みスループットを生成しているワークロードを特定できます。

このような負荷の高いワークロードが原因でローカルクラスタの他のボリュームの I/O 応答時間が長くなると、Unified Manager はパフォーマンスイベントをトリガーしてユーザに通知します。



Unified Manager では、MetroCluster 構成のクラスタを個別のクラスタとして扱います。クラスタがパートナーかどうかは区別されず、各クラスタからの書き込みスループットが関連付けられることはありません。

MetroCluster 構成のローカルクラスタがデータをパートナークラスタにミラーリングすると、データは NVRAM に書き込まれてからインタースイッチリンク (ISL) 経由でリモートアグリゲートに転送されます。Unified Manager は NVRAM を分析し、大量の書き込みスループットが NVRAM を過剰に使用して NVRAM を競合状態にしているワークロードを特定します。

応答時間の偏差がパフォーマンスしきい値を超えたワークロードは `_Victim` と呼ばれ、NVRAM への書き込みスループットの偏差が通常より高く、競合を引き起こしているワークロードは `_Bully` と呼ばれます。パートナークラスタには書き込み要求のみがミラーされるため、Unified Manager は読み取りスループットを分析しません。

MetroCluster 構成内のいずれかのクラスタのスループットを表示するには、次の画面で対応する LUN およびボリュームのワークロードを分析します。クラスタで結果をフィルタリングできます。左側のナビゲーションペインで、次の操作を実行します

- * [ストレージ] > [クラスタ] > [パフォーマンス] : [すべてのクラスタ] 表示を参照してください
- * [ストレージ] > [ボリューム] > [パフォーマンス] : [すべてのボリューム] *ビュー
- * [ストレージ] > [LUN] > [パフォーマンス] : すべての LUN*ビュー
- ワークロード分析>すべてのワークロード
- 関連情報 *

["パフォーマンスイベントの分析と通知"](#)

["MetroCluster 構成のパフォーマンスイベント分析"](#)

["パフォーマンスイベントに関連したワークロードの役割"](#)

["パフォーマンスイベントに関連した Victim ワークロードの特定"](#)

["パフォーマンスイベントに関連した Bully ワークロードの特定"](#)

パフォーマンスイベントとアラートの概要

パフォーマンスイベントとは、クラスタでのワークロードパフォーマンスに関連するインシデントです。応答時間が長いワークロードを特定するのに役立ちます。同時に発生した健全性イベントと一緒に確認することで、応答時間が長くなった原因と考えられる関連する問題を特定することができます。

Unified Manager では、同じクラスタコンポーネントに対する同じ状況についての一連のイベントを検出すると、それらのすべてのイベントを個別のイベントではなく 1 つのイベントとして扱います。

特定の重大度タイプのパフォーマンスイベントが発生したときに自動的に E メール通知を送信するアラートを設定できます。

パフォーマンスイベントのソース

パフォーマンスイベントとは、クラスタでのワークロードパフォーマンスに関連する問題です。応答時間が長いストレージオブジェクト（高レイテンシとも呼ばれます）を特定するのに役立ちます。同時に発生したその他の健全性イベントと一緒に確認することで、応答時間が長くなった原因と考えられる関連する問題を特定することができます。

Unified Manager は、次のソースからパフォーマンスイベントを受け取ります。

- * ユーザ定義のパフォーマンスしきい値ポリシーイベント *

独自に設定したしきい値に基づいたパフォーマンスの問題。アグリゲートやボリュームなどのストレージオブジェクトに対してパフォーマンスしきい値ポリシーを設定して、パフォーマンスカウンタのしきい値を超えたときにイベントが生成されるようにします。

これらのイベントを受け取るためには、パフォーマンスしきい値ポリシーを定義してストレージオブジェクトに割り当てる必要があります。

- * システム定義のパフォーマンスしきい値ポリシーイベント *

システム定義のしきい値に基づいたパフォーマンスの問題。このしきい値ポリシーは Unified Manager にあらかじめ含まれており、一般的なパフォーマンスの問題に対処します。

このしきい値はデフォルトで有効化されており、クラスタの追加後すぐにイベントが生成される場合があります。

- * 動的なパフォーマンスしきい値イベント *

IT インフラストラクチャの障害やエラー、またはクラスタリソースの使用率が高いワークロードによるパフォーマンスの問題。これらのイベントの原因は、時間がたてば修復する、または修理や設定変更によって解決可能な単純な問題です。動的しきい値イベントは、他のワークロードが共有のクラスタコンポーネントを利用していることが原因で、ONTAP システムのワークロードの処理速度が低下した場合に生成されます。

このしきい値はデフォルトで有効になっており、新しいクラスタからデータを収集してから 3 日後にイベ

ントが表示されることがあります。

パフォーマンスイベントの重大度タイプ

パフォーマンスイベントには、対処する際の優先度を判別できるように、それぞれ重大度タイプが関連付けられています。

- * 重要 *

パフォーマンスイベントが発生しており、すぐに対処しないとサービスが停止する可能性があります。

重大イベントは、ユーザ定義のしきい値からのみ生成されます。

- * 警告 *

クラスタオブジェクトのパフォーマンスカウンタが正常な範囲から外れており、重大な問題にならないように監視が必要です。この重大度のイベントでは原因サービスは停止しません。早急な対処も不要です。

警告イベントは、システムまたはユーザ定義のしきい値、あるいは動的なしきい値から生成されます。

- * 情報 *

新しいオブジェクトが検出されたときやユーザ操作が実行されたときに発生します。たとえば、ストレージオブジェクトが削除された場合や設定に変更があった場合は、情報タイプの重大度のイベントが生成されます。

情報イベントは、設定の変更が検出されたときに ONTAP から直接送信されます。

詳細については、次のリンクを参照してください。

- ["イベント受信時の動作"](#)
- ["アラート E メールに含まれる情報"](#)
- ["アラートの追加"](#)
- ["パフォーマンスイベントのアラートを追加しています"](#)

Unified Manager によって設定の変更が検出されました

Unified Manager では、クラスタの構成の変更が監視され、それが原因で発生したパフォーマンスイベントがないかどうかを判断できます。パフォーマンスエクスプローラのページには、変更イベントアイコン (●) をクリックして、変更が検出された日時を示します。

パフォーマンスエクスプローラのページおよびワークロード分析ページでパフォーマンスチャートを確認して、変更イベントが選択したクラスタオブジェクトのパフォーマンスに影響したかどうかを確認できます。パフォーマンスイベントとほぼ同時に変更が検出された場合、その変更が問題にもたらした可能性があります。イベントのアラートがトリガーされた可能性があります。

Unified Manager では次の変更イベントを検出できます。これらは情報イベントに分類されます。

- ボリュームがアグリゲート間で移動されたとき。

移動が開始されたとき、完了したとき、または失敗したときに Unified Manager で検出されます。ボリュームの移動中に Unified Manager が停止していた場合は、稼働状態に戻ったあとにボリュームの移動が検出され、対応する変更イベントが表示されます。

- 1 つ以上の監視対象ワークロードを含む QoS ポリシーグループのスループット（MBps または IOPS）の制限が変更されたとき。

ポリシーグループ制限を変更原因すると、レイテンシ（応答時間）が一時的に長くなることがあり、ポリシーグループのイベントがトリガーされる可能性もあります。レイテンシは徐々に正常に戻り、発生したイベントは廃止状態になります。

- HA ペアのノードのストレージがパートナーノードにテイクオーバーまたはギブバックされたとき。

テイクオーバー、部分的なテイクオーバー、またはギブバックの処理が完了したときに Unified Manager で検出されます。ノードのパニック状態が原因で発生したテイクオーバーは Unified Manager では検出されません。

- ONTAP のアップグレード処理またはリバート処理が完了しました。

以前のバージョンと新しいバージョンが表示されます。

システム定義のパフォーマンスしきい値ポリシーのタイプ

Unified Manager には、クラスタのパフォーマンスを監視し、イベントを自動生成する標準のしきい値ポリシーがいくつか用意されています。これらのポリシーはデフォルトで有効になっており、監視対象のパフォーマンスしきい値を超えたときに警告イベントまたは情報イベントを生成します。



システム定義のパフォーマンスしきい値ポリシーは、Cloud Volumes ONTAP、ONTAP Edge、ONTAP Select の各システムでは無効です。

システム定義のパフォーマンスしきい値ポリシーから不要なイベントが送られてくる場合は、Event Setup ページで個々のポリシーのイベントを無効にすることができます。

クラスタのしきい値ポリシー

システム定義のクラスタパフォーマンスしきい値ポリシーは、Unified Manager で監視されている各クラスタにデフォルトで割り当てられます。

- * クラスタ負荷の不均衡 *

クラスタ内の 1 つのノードの負荷が他のノードよりもはるかに高く、ワークロードのレイテンシに影響を及ぼす可能性がある状況を特定します。

クラスタ内のすべてのノードの使用済みパフォーマンス容量の値が比較され、いずれかのノードがしきい値の30%を超えて24時間以上経過していないかどうかを確認されます。これは警告イベントです。

- * クラスタ容量の不均衡 *

クラスタ内の 1 つのアグリゲートの使用済み容量が他のアグリゲートよりもはるかに多く、その結果、処理に必要なスペースに影響を及ぼす可能性がある状況を特定します。

クラスタ内のすべてのアグリゲートの使用済み容量の値が比較され、いずれかのアグリゲート間で 70% の差があるかどうかを確認されます。これは警告イベントです。

ノードのしきい値ポリシー

システム定義のノードパフォーマンスしきい値ポリシーは、Unified Manager で監視されているクラスタ内の各ノードにデフォルトで割り当てられます。

• * 使用済みパフォーマンス容量しきい値を超過 *

1 つのノードが運用効率の上限を超えて稼働していて、ワークロードのレイテンシに影響を及ぼしている可能性がある状況を特定します。

100% 以上のパフォーマンス容量を 12 時間以上使用しているノードが特定されます。これは警告イベントです。

• * 利用率の高いノード HA ペア *

HA ペアのノードが HA ペアの運用効率の上限を超えて稼働している状況を特定します。

HA ペアの 2 つのノードの使用済みパフォーマンス容量の値が確認されます。2 つのノードの使用済みパフォーマンス容量の合計が 12 時間以上にわたって 200% を超えている場合は、コントローラフェイルオーバーがワークロードのレイテンシに影響を及ぼします。これは情報イベントです。

• * ノードディスクの断片化 *

アグリゲート内の 1 つまたは複数のディスクが断片化されていて、主要なシステムサービスの速度が低下し、ノード上のワークロードのレイテンシに影響を及ぼしている可能性がある状況を特定します。

ノード上のすべてのアグリゲートで特定の読み取り / 書き込み処理の比率が確認されます。このポリシーは、SyncMirror の再同期中、またはディスクスクラビング処理中にエラーが検出されたときにもトリガーされることがあります。これは警告イベントです。



「ノードディスクの断片化」ポリシーは、HDD のみのアグリゲートを分析します。Flash Pool、SSD、および FabricPool の各アグリゲートは分析しません。

アグリゲートのしきい値ポリシー

システム定義のアグリゲートパフォーマンスしきい値ポリシーは、Unified Manager で監視されているクラスタ内の各アグリゲートにデフォルトで割り当てられます。

• * 利用率の高いアグリゲートディスク *

アグリゲートが運用効率の上限を超えて稼働していて、ワークロードのレイテンシに影響を及ぼしている可能性がある状況を特定します。そのために、アグリゲート内のディスクの利用率が 30 分以上にわたって 95% を超えているアグリゲートが特定されます。この複数条件のポリシーでは、次に示す分析を実行して、問題の原因を特定します。

- アグリゲート内のディスクがバックグラウンドでメンテナンス作業を実行中かどうか。

ディスクに対してバックグラウンドで実行されるメンテナンス作業には、ディスク再構築、ディスクスクラビング、 SyncMirror の再同期、再パリティ化などがあります。

- ディスクシェルフの Fibre Channel インターコネクに通信のボトルネックはあるか。
- アグリゲートの空きスペースが不足しているか。3 つの下位ポリシーのうちの 1 つ（または複数）にも違反しているとみなされた場合にのみ、このポリシーに対して警告イベントが発行されます。アグリゲート内のディスクの利用率が 95% を超えているだけであれば、パフォーマンスイベントはトリガーされません。



「利用率の高いディスクを集約」ポリシーは、HDD のみのアグリゲートと Flash Pool（ハイブリッド）アグリゲートを分析します。SSD アグリゲートと FabricPool アグリゲートは分析しません。

ワークロードレイテンシのしきい値ポリシー

システム定義のワークロード遅延しきい値ポリシーは、「想定レイテンシ」の値が定義されたパフォーマンスサービスレベルポリシーが設定されているワークロードに割り当てられます。

- * パフォーマンスサービスレベル * に定義されたワークロードのボリューム / LUN レイテンシしきい値を超過

ボリューム（ファイル共有）と LUN のうち、「想定レイテンシ」の制限を超えていて、ワークロードのパフォーマンスに影響を及ぼしているものを特定します。これは警告イベントです。

想定レイテンシの値を超えた時間が過去 1 時間に 30% を超えるワークロードがないかどうかを確認されます。

QoS のしきい値ポリシー

システム定義の QoS パフォーマンスしきい値ポリシーは、ONTAP の QoS 最大スループットポリシー（IOPS、IOPS/TB、または MBps）が設定されているワークロードに割り当てられます。ワークロードのスループットの値が設定された QoS 値を 15% 下回ると、Unified Manager はイベントをトリガーします。

- * QoS 最大 IOPS または MBps しきい値 *

IOPS または MBps が QoS 最大スループット制限を超えていて、ワークロードのレイテンシに影響を及ぼしているボリュームおよび LUN を特定します。これは警告イベントです。

ポリシーグループにワークロードが 1 つしか割り当てられていない場合、割り当てられている QoS ポリシーグループで定義された最大スループットしきい値を超えているワークロードが過去 1 時間の各収集期間にないかどうかを確認されます。

複数のワークロードで同じ QoS ポリシーを使用している場合は、ポリシーに割り当てられたすべてのワークロードの IOPS または MBps の合計が求められ、その合計がしきい値を超えていないかどうかを確認されます。

- * QoS ピーク IOPS/TB またはブロックサイズしきい値 *

IOPS/TB がアダプティブ QoS ピークスループット制限（またはブロックサイズ指定の IOPS/TB 制限）を

超えていて、ワークロードのレイテンシに影響を及ぼしているボリュームを特定します。これは警告イベントです。

このポリシーでは、アダプティブ QoS ポリシーで定義された IOPS/TB のピークしきい値を各ボリュームのサイズに基づいて QoS 最大 IOPS の値に変換し、過去 1 時間の各パフォーマンス収集期間に QoS 最大 IOPS を超えているボリュームを探します。



このポリシーは、クラスタに ONTAP 9.3 以降のソフトウェアがインストールされている場合にのみボリュームに適用されます。

アダプティブ QoS ポリシーに「block size」要素が定義されている場合、しきい値は各ボリュームのサイズに基づいて QoS の最大 MBps の値に変換されます。過去 1 時間の各パフォーマンス収集期間にこの値を超えているボリュームがないかどうかを確認されます。



このポリシーは、クラスタに ONTAP 9.5 以降のソフトウェアがインストールされている場合にのみボリュームに適用されます。

パフォーマンスイベントの分析と通知

パフォーマンスイベントは、クラスタコンポーネントの競合に起因するワークロードの I/O パフォーマンスの問題を管理者に通知します。Unified Manager はイベントを分析して、関連するすべてのワークロード、競合状態のコンポーネント、および解決する必要のある問題かどうかを特定します。

Unified Manager は、クラスタ上のボリュームの I/O レイテンシ（応答時間）と IOPS（処理数）を監視します。たとえば、他のワークロードがクラスタコンポーネントを過剰に使用している場合、そのコンポーネントは競合状態にあり、ワークロードの要件を満たす最適なパフォーマンスレベルを提供できません。同じコンポーネントを使用している他のワークロードのパフォーマンスに影響し、レイテンシが増加する可能性があります。レイテンシが動的なパフォーマンスしきい値を超えると、Unified Manager はパフォーマンスイベントをトリガーしてユーザに通知します。

イベント分析

Unified Manager は、過去 15 日間のパフォーマンス統計を使用して次の分析を実行し、Victim ワークロード、Bully ワークロード、およびイベントに関連するクラスタコンポーネントを特定します。

- レイテンシがレイテンシ予測の上限である動的なパフォーマンスしきい値を超えた Victim ワークロードを特定します。
 - HDD または Flash Pool のハイブリッドアグリゲート（ローカル階層）のボリュームの場合、レイテンシが 5 ミリ秒を超え、かつ IOPS が 1 秒あたり 10 件（ops/sec）を超えた場合にのみイベントがトリガーされます。
 - オール SSD アグリゲートまたは FabricPool アグリゲート（クラウド階層）のボリュームの場合、レイテンシが 1 ミリ秒を超え、かつ IOPS が 100ops/ 秒を超えた場合にのみイベントがトリガーされます。
- 競合状態のクラスタコンポーネントを特定します。



クラスタインターコネクトで Victim ワークロードのレイテンシが 1 ミリ秒を超えた場合、Unified Manager はこれを重大な状況とみなしてクラスタインターコネクトのイベントをトリガーします。

- クラスタコンポーネントを過剰に消費して競合状態を引き起こしている Bully ワークロードを特定します。
- クラスタコンポーネントの利用率またはアクティビティの偏差に基づいて関連するワークロードをランク付けし、クラスタコンポーネントの使用量の変化が最も大きい Bully ワークロードと最も影響を受けた Victim ワークロードを特定します。

ごく短時間しか発生せず、コンポーネントの競合状態が解消した時点で自己修復されるイベントもあります。継続的なイベントとは、5 分以内に同じクラスタコンポーネントについて再発し、アクティブな状態のままのイベントのことです。Unified Manager は、連続する 2 つの分析期間に同じイベントを検出するとアラートをトリガーします。

解決されたイベントは、ボリュームの過去のパフォーマンス問題の記録として Unified Manager で引き続き参照できます。各イベントには、イベントタイプとボリューム、クラスタ、および関連するクラスタコンポーネントを識別する一意の ID が割り当てられます。



1 つのボリュームが複数のイベントに同時に関連している場合があります。

イベントの状態

イベントは次のいずれかの状態になります。

• * アクティブ *

現在アクティブなパフォーマンスイベント（新規または確認済みのイベント）を示します。自己修復または解決されていないイベントを引き起こしている問題。ストレージオブジェクトのパフォーマンスカウンタがパフォーマンスしきい値を超えたままになっているものです。

• * 廃止 *

アクティブではなくなったイベントを示します。自己修復または解決されたイベントである問題。ストレージオブジェクトのパフォーマンスカウンタがパフォーマンスしきい値を上回らなくなったものです。

イベント通知

イベントはダッシュボードページやユーザインターフェイスのその他の多くのページに表示され、指定した E メールアドレスに送信されます。イベントに関する詳細な分析情報を表示し、推奨される解決方法をイベントの詳細ページおよびワークロードの分析ページで確認できます。

イベントの対話

イベントの詳細ページおよびワークロード分析ページでは、次の方法でイベントを操作できます。

- イベントの上にマウスを移動すると、イベントが検出された日時を示すメッセージが表示されます。

同じ期間にイベントが複数ある場合は、イベントの数が表示されます。

- 1 つのイベントをクリックすると、関連するクラスタコンポーネントを含むイベントの詳細情報を表示す

るダイアログボックスが表示されます。

競合状態のコンポーネントは赤い丸で囲んで表示されます。[完全な解析を表示 (View full analysis)] をクリックすると、[イベントの詳細 (Event details)] ページに完全な解析を表示できます。同じ期間にイベントが複数ある場合は、最新の 3 つのイベントの詳細がダイアログボックスに表示されます。イベントをクリックすると、イベントの詳細ページでイベント分析を確認できます。

Unified Manager がイベントによるパフォーマンスへの影響を判定する仕組み

Unified Manager は、ワークロードについてそのアクティビティ、利用率、書き込みスループット、クラスタコンポーネントの使用量、または I/O レイテンシ（応答時間）の偏差を使用して、ワークロードパフォーマンスへの影響のレベルを判定します。この情報によって、イベントにおける各ワークロードの役割とイベントの詳細ページでのランク付けが決まります。

Unified Manager は、ワークロードの最新の分析値を値の想定範囲（レイテンシ予測）と比較します。最新の分析値と値の想定範囲の差が最も大きいワークロードが、イベントによってパフォーマンスに最も影響を受けたワークロードです。

たとえば、クラスタにワークロードが 2 つあるとします。ワークロード A とワークロード B です。ワークロード A のレイテンシ予測は 5~10ms/op で、実際のレイテンシは通常で約 7ms/op です。ワークロード B のレイテンシ予測は 10~20ms/op です。実際のレイテンシは通常で約 15ms/op です。どちらのワークロードも、レイテンシ予測の範囲内に収まっています。クラスタでの競合が原因で両方のワークロードのレイテンシが 40ms/op に上昇し、レイテンシ予測の上限である動的なパフォーマンスしきい値を超えた結果イベントがトリガーされたとします。レイテンシの偏差は、想定値からパフォーマンスしきい値を超える値までの値で、ワークロード A の約 33ms/op です。ワークロード B の偏差は約 25ms/op です。両方のワークロードのレイテンシは 40ms/op に上昇しましたが、ワークロード A のパフォーマンスへの影響は大きな値でした。これは、レイテンシ偏差が 33ms/op 以上であったためです。

イベントの詳細ページのシステム診断セクションでは、クラスタコンポーネントのアクティビティ、利用率、またはスループットの偏差でワークロードをソートできます。また、レイテンシでソートすることもできます。ソートオプションを選択すると、Unified Manager は、アクティビティ、利用率、スループット、またはレイテンシについて、想定される値とイベント検出後の値の差を分析して、ワークロードのソート順序を決定します。レイテンシの赤のドット (●) は、Victim ワークロードがパフォーマンスしきい値を超えたこと、および以降のレイテンシへの影響を示しています。ドットが多いほどレイテンシの偏差が大きいことを示しており、イベントによってレイテンシが最も影響を受けた Victim ワークロードを特定するのに役立ちます。

クラスタコンポーネントとその競合要因

クラスタコンポーネントの競合の原因となるクラスタのパフォーマンスの問題を特定することができます。コンポーネントを使用するワークロードのパフォーマンスが低下し、クライアント要求に対する応答時間（レイテンシ）が長くなると、Unified Manager でイベントがトリガーされます。

競合状態のコンポーネントは、最適なレベルのパフォーマンスを提供できません。パフォーマンスが低下し、_Victim_ と呼ばれる他のクラスタコンポーネントやワークロードのパフォーマンスによってレイテンシが増大する可能性があります。コンポーネントの競合状態を解消するには、ワークロードを減らすか処理能力を高めることでパフォーマンスを通常レベルに戻す必要があります。Unified Manager では、ワークロードのパフォーマンスの収集と分析が 5 分間隔で行われるため、クラスタコンポーネントの利用率が高い状態が長時間続いたときにのみ検出されます。利用率が高い状態が 5 分インターバルの間に短時間しか続かないような一時的な利用率の急増は検出されません。

ストレージアグリゲートが競合状態になる原因としては、たとえば、1 つ以上のワークロードがそれぞれの I/O 要求に対応するために競合する場合などがあります。アグリゲートの他のワークロードに影響し、それらのワークロードのパフォーマンスが低下する可能性があります。アグリゲートのアクティビティを減らす方法はいくつかありますが、たとえば、1 つ以上のワークロードを負荷の低いアグリゲートまたはノードに移動し、現在のアグリゲートに対する全体的なワークロードの負荷を低くするなどの方法が効果的です。QoS ポリシーグループの場合は、スループット制限を調整したりワークロードを別のポリシーグループに移動したりすることで、ワークロードが抑制されないようにすることができます。

Unified Manager では、次のクラスタコンポーネントを監視して、これらのコンポーネントが競合状態になるとアラートを生成します。

- * ネットワーク *

クラスタの外部ネットワークプロトコルによる I/O 要求の待機時間を表します。待機時間とは、クラスタが I/O 要求に応答できるようになるまで「transfer ready」トランザクションが完了するのを待機する時間です。ネットワークコンポーネントが競合状態にある場合、プロトコルレイヤでの長い待機時間は、1 つ以上のワークロードのレイテンシに影響していることを意味します。

- * ネットワーク処理 *

プロトコルレイヤとクラスタ間の I/O 処理に関与する、クラスタ内のソフトウェアコンポーネントを表します。ネットワーク処理を実行するノードがイベント検出後に変更された可能性があります。ネットワーク処理コンポーネントが競合状態にある場合、ネットワーク処理ノードでの高利用率は、1 つ以上のワークロードのレイテンシに影響していることを意味します。

アクティブ / アクティブ構成でオール SAN アレイクラスタを使用している場合は、両方のノードのネットワーク処理のレイテンシの値が表示され、ノードが負荷を均等に共有していることを確認できます。

- * 最大 QoS

ワークロードに割り当てられたストレージ QoS ポリシーグループの最大スループット（ピーク）設定を表します。ポリシーグループコンポーネントが競合状態にある場合、ポリシーグループ内のすべてのワークロードに、スループットの制限によってスロットルが適用され、1 つ以上のワークロードのレイテンシに影響していることを意味します。

- * 最小 QoS

他のワークロードに割り当てられた QoS スループットの下限（想定）設定によって引き起こされている、ワークロードへのレイテンシを表します。設定されている QoS の下限に応じて特定のワークロードが保証されたスループットを確保するために帯域幅の大部分を使用すると、他のワークロードは調整されてレイテンシが増大します。

- * クラスタインターコネクト *

クラスタノードを物理的に接続するケーブルとアダプタを表します。クラスタインターコネクトコンポーネントが競合状態にある場合は、クラスタインターコネクトでの I/O 要求の長い待機時間がワークロードのレイテンシに影響していることを意味します。

- * データ処理 *

クラスタとストレージアグリゲート間でワークロードを含む I/O 処理に関与する、クラスタ内のソフトウェアコンポーネントを表します。データ処理を実行するノードがイベント検出後に変更された可能性があります。データ処理コンポーネントが競合状態にある場合、データ処理ノードでの高利用率は、1 つ以上のワークロードのレイテンシに影響していることを意味します。

- * ボリュームアクティベーション *

すべてのアクティブボリュームの使用状況を追跡するプロセスです。1000 を超えるアクティブボリュームを擁する大規模な環境で、ノード経由で同時にリソースにアクセスする必要がある重要なボリュームの数を追跡します。同時アクティブボリュームの数が推奨される最大しきい値を超えると、重要でない一部のボリュームでレイテンシが発生します。

- * MetroCluster リソース *

NVRAM とインタースイッチリンク（ISL）を含む MetroCluster リソースを表します。MetroCluster 構成のクラスタ間でデータをミラーリングするのに使用します。MetroCluster コンポーネントが競合状態問題にある場合は、ローカルクラスタのワークロードによる大量の書き込みスループットまたはリンクの不具合が、ローカルクラスタの 1 つ以上のワークロードのレイテンシに影響していることを意味します。クラスタが MetroCluster 構成に含まれていない場合は、このアイコンは表示されません。

- * アグリゲートまたは SSD アグリゲートの処理 *

ワークロードが実行されているストレージアグリゲートを表します。アグリゲートコンポーネントが競合状態にある場合、アグリゲートの高利用率が 1 つ以上のワークロードのレイテンシに影響していることを意味します。アグリゲートには、HDD のみで構成されるものと、HDD と SSD が混在するもの（Flash Pool アグリゲート）と、HDD とクラウド階層が混在するもの（FabricPool アグリゲート）があります。「SD アグリゲート」は、すべての SSD（オールフラッシュアグリゲート）、または SSD とクラウド階層（FabricPool アグリゲート）が混在しています。

- * クラウドレイテンシ *

クラスタとユーザデータ格納先のクラウド階層の間の I/O 処理に関与する、クラスタ内のソフトウェアコンポーネントを表します。クラウドレイテンシコンポーネントが競合状態にある場合、クラウド階層でホストされたボリュームからの大量の読み取りが 1 つ以上のワークロードのレイテンシに影響していることを意味します。

- * 同期 SnapMirror *

SnapMirror 同期関係でのプライマリボリュームからセカンダリボリュームへのユーザデータのレプリケーションに関係する、クラスタ内のソフトウェアコンポーネントを表します。同期 SnapMirror コンポーネントが競合状態にある場合、SnapMirror Synchronous 処理のアクティビティが 1 つ以上のワークロードのレイテンシに影響していることを意味します。

パフォーマンスイベントに関連したワークロードの役割

Unified Manager では、ロールを使用して、パフォーマンスイベントにワークロードがどのように関連しているかを特定します。役割には Victim、Bully、Shark があります。ユーザ定義のワークロードは同時に Victim、Bully、Shark となることがあります。

ルール	説明
被害者	クラスタコンポーネントを過剰に使用している、他のワークロード（Bully）によってパフォーマンスが低下したユーザ定義のワークロード。Victim とみなされるのはユーザ定義のワークロードのみです。Unified Manager はレイテンシの偏差に基づいて、イベント中のレイテンシの実測値がレイテンシ予測（想定範囲）から大幅に増加しているワークロードを Victim ワークロードとして特定します。
影響源	ユーザ定義またはシステム定義のワークロードで、クラスタコンポーネントが過剰に使用されていると、「Victim」と呼ばれる他のワークロードのパフォーマンスが低下した場合。Unified Manager はクラスタコンポーネントの使用量の偏差に基づいて、イベント中の使用量の実測値が想定範囲から大幅に増加しているワークロードを Bully ワークロードとして特定します。
シャーク	イベントに関連するすべてのワークロードの中でクラスタコンポーネントの使用量が最も多いユーザ定義のワークロード。Unified Manager はイベント中のクラスタコンポーネントの使用量に基づいて Shark ワークロードを特定します。

クラスタのワークロードは、アグリゲートや CPU などのクラスタコンポーネントの多くを共有し、ネットワークやデータの処理に使用できます。ボリュームなどのワークロードがあると、クラスタコンポーネントの使用量が増えて、コンポーネントがワークロードの要求を効率的に満たすことができない状態になると、コンポーネントは競合状態になります。この、クラスタコンポーネントを過剰に消費しているワークロードが「Bully」で、これらのコンポーネントを共有しており、Bully によってパフォーマンスに影響が出ているワークロードが「Victim」です。重複排除や Snapshot コピーなど、システム定義のワークロードのアクティビティも、「いじめ」にエスカレーションできます。

Unified Manager はイベントを検出すると、関連するすべてのワークロードとクラスタコンポーネントを特定します。これには、イベントの原因となった Bully ワークロード、競合状態のクラスタコンポーネント、および Bully ワークロードのアクティビティが増加したためにパフォーマンスが低下した Victim ワークロードが含まれます。



Unified Manager が Bully ワークロードを特定できない場合は、Victim ワークロードと関連するクラスタコンポーネントに関するアラートだけが生成されます。

Unified Manager は Bully ワークロードの Victim ワークロードを特定でき、同じワークロードが Bully ワークロードになった場合にも特定できます。ワークロードは自身に対して Bully ワークロードになることがあります。たとえば、負荷の高いワークロードがポリシーグループの制限によって調整される場合、そのワークロードが含まれるポリシーグループ内のすべてのワークロードが調整されます。継続的なパフォーマンスイベントでは、Bully ワークロードまたは Victim ワークロードは役割が変わったり、あるいはイベントに関連しなくなったりすることがあります。

パフォーマンスしきい値の管理

パフォーマンスしきい値ポリシーを使用して、Unified Manager がイベントを生成し、ワークロードパフォーマンスに影響している可能性のある問題についてシステム管理者に通知するレベルを決定できます。このしきい値ポリシーは、`_user_defined_performance` しきい値と呼ばれます。

このリリースでは、ユーザ定義、システム定義、および動的なパフォーマンスしきい値がサポートされます。動的およびシステム定義のパフォーマンスしきい値の場合、Unified Manager がワークロードのアクティビティを分析して、適切なしきい値を決定します。ユーザ定義のしきい値の場合、多くのパフォーマンスカウンタおよびストレージオブジェクトに対してパフォーマンスの上限を定義できます。



システム定義のパフォーマンスしきい値と動的なパフォーマンスしきい値は Unified Manager によって設定され、ユーザが設定することはできません。システム定義のパフォーマンスしきい値ポリシーから不要なイベントが送られてくる場合は、Event Setup ページで個々のポリシーを無効にすることができます。

ユーザ定義のパフォーマンスしきい値ポリシーの仕組み

ストレージオブジェクト（アグリゲートやボリュームなど）に対してパフォーマンスしきい値ポリシーを設定して、クラスタでパフォーマンス問題が発生していることを通知するイベントをストレージ管理者に送信できるようにします。

ストレージオブジェクトのパフォーマンスしきい値ポリシーを作成する手順は次のとおりです。

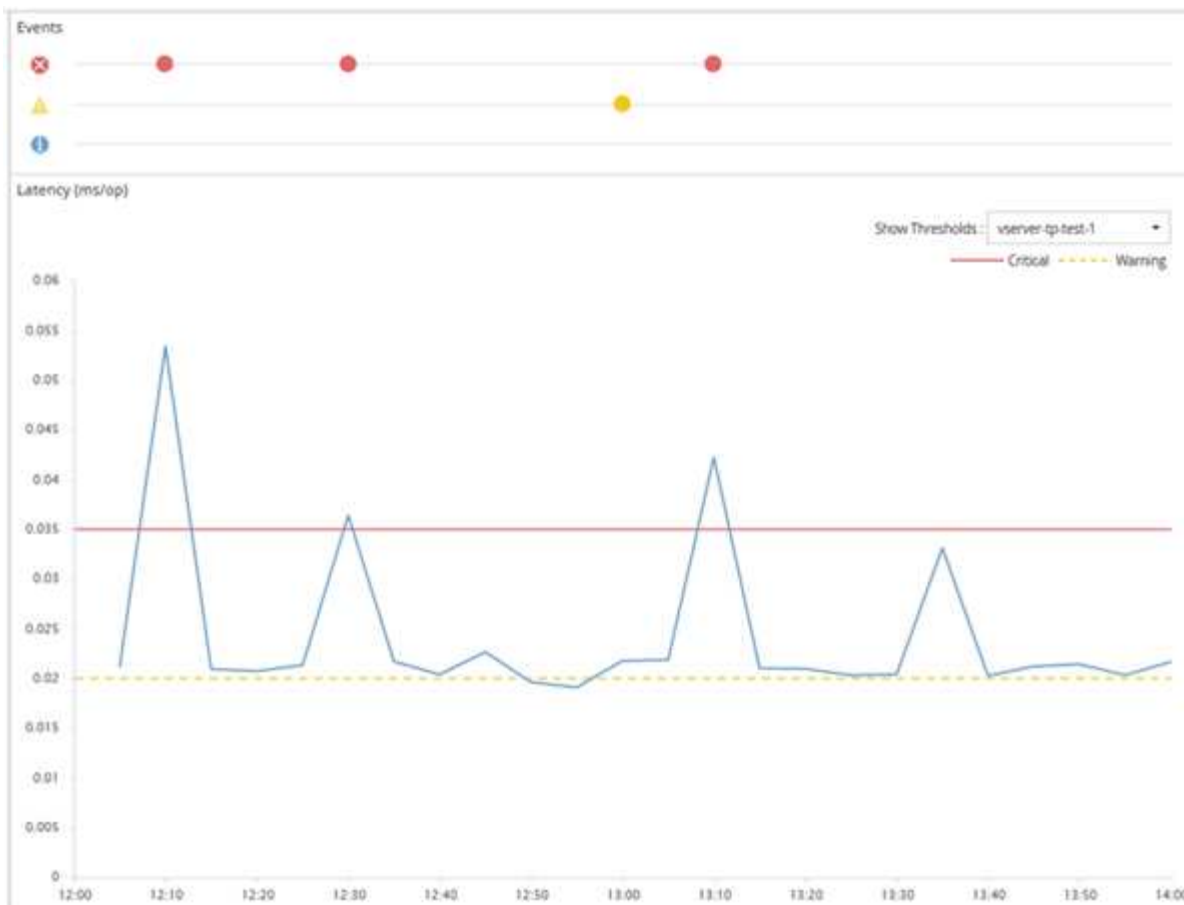
- ストレージオブジェクトを選択する
- オブジェクトに関連付けられているパフォーマンスカウンタを選択しています
- 警告および重大な状況とみなされるパフォーマンスカウンタの上限値を指定します
- カウンタが上限値を超える必要がある期間を指定します

たとえば、ボリュームの IOPS が 10 分間連続して 1 秒あたり 750 件の処理数を超えるたびに重大イベントの通知を受け取るように、ボリュームに対してパフォーマンスしきい値ポリシーを設定できます。同じしきい値ポリシーで、IOPS が 10 分間にわたって 1 秒あたり 500 件の処理数を超えたときに警告イベントを送信するように指定することもできます。



現在のリリースでは、カウンタの値が設定値を超えたときにイベントを送信するしきい値を設定できます。カウンタの値が設定値を下回ったときにイベントを送信するしきい値は設定できません。

次のカウンタグラフの例では、1 : 00 に警告のしきい値（黄色のアイコン）に違反し、12 : 10、12 : 30、1 : 10 に重大のしきい値（赤のアイコン）に違反していることがわかります。



しきい値の違反は、指定した期間、継続的に発生する必要があります。何らかの理由でしきい値を下回った場合は、以降の違反が新しい期間の開始とみなされます。

一部のクラスタオブジェクトとパフォーマンスカウンタでは、2つのパフォーマンスカウンタが上限を超えた場合にイベントが生成されるしきい値ポリシーを作成できます。たとえば、次の条件を使用してしきい値ポリシーを作成できます。

クラスタオブジェクト	パフォーマンスカウンタ	警告しきい値	重大のしきい値	期間
ボリューム	レイテンシ	10 ミリ秒	20 ミリ秒	15 分
アグリゲート	利用率	65%	85%	

2つのクラスタオブジェクトを使用するしきい値ポリシー原因両方の条件に違反した場合にのみイベントが生成されます。たとえば、次の表に定義されているしきい値ポリシーを使用します。

ボリュームレイテンシの平均	アグリゲートのディスク利用率	作業
15 ミリ秒	50%	イベントは報告されません。
15 ミリ秒	75%	警告イベントが報告されます。

ボリュームレイテンシの平均	アグリゲートのディスク利用率	作業
25 ミリ秒	75%	警告イベントが報告されます。
25 ミリ秒	90%	重大イベントが報告されます。

パフォーマンスしきい値ポリシーを超えた場合の動作

カウンタの値が定義されているパフォーマンスしきい値を超えて指定された期間が経過すると、しきい値違反としてイベントが報告されます。

イベントにより、次の処理が開始されます。

- ・ イベントは、ダッシュボード、パフォーマンスクラスタの概要ページ、イベントページ、およびオブジェクト固有のパフォーマンスインベントリページに表示されます。
- ・ (オプション) イベントに関する E メールアラートを 1 つ以上の受信者に送信したり、SNMP トラップをトラップレシーバに送信したりできます。
- ・ (オプション) ストレージオブジェクトを自動的に変更または更新するスクリプトを実行できます。

最初のアクションは常に実行されます。オプションのアクションを実行するかどうかは、Alert Setup ページで設定します。警告と重大のしきい値ポリシーについて、違反した場合の処理をそれぞれ定義することができます。

ストレージオブジェクトでパフォーマンスしきい値ポリシー違反が発生した場合、カウンタの値がしきい値を下回り、その制限の期間がリセットされるまでは、そのポリシーに対する以降のイベントは生成されません。しきい値を超えたままイベントが継続していることを示すために、イベントの終了時刻が更新されます。

しきい値イベントには重大度やポリシー定義に関する情報がキャプチャされるため、以降にしきい値ポリシーが変更された場合でもそのイベントに対して表示されるしきい値情報は変化しません。

しきい値を使用して追跡可能なパフォーマンスカウンタ

IOPS や MBps など、一部の共通のパフォーマンスカウンタでは、すべてのストレージオブジェクトを対象にしきい値を設定できます。それ以外のカウンタでは、特定のストレージオブジェクトに対してのみしきい値を設定できます。

使用可能なパフォーマンスカウンタ

ストレージオブジェクト	パフォーマンスカウンタ	説明
クラスタ	IOPS	クラスタで処理される 1 秒あたりの平均入出力処理数
MB/s	このクラスタとの間で転送されたデータの 1 秒あたりの平均メガバイト数。	ノード

ストレージオブジェクト	パフォーマンスカウンタ	説明
IOPS	ノードで処理される 1 秒あたりの平均入出力処理数	MB/s
このノードとの間で転送された 1 秒あたりの平均データ量 (MB)。	レイテンシ	ノードがアプリケーションの要求に応答するまでの平均時間 (ミリ秒)。
利用率	ノードの CPU と RAM の平均使用率	使用済みパフォーマンス容量
ノードによるパフォーマンス容量の平均消費率	使用済みパフォーマンス容量 - テイクオーバー	ノードによるパフォーマンス容量の平均消費率とパートナーノードのパフォーマンス容量
アグリゲート	IOPS	アグリゲートで処理される 1 秒あたりの平均入出力処理数
MB/s	このアグリゲートとの間で転送された 1 秒あたりの平均データ量 (MB)。	レイテンシ
アグリゲートがアプリケーションの要求に応答するまでの平均時間 (ミリ秒)。	利用率	アグリゲートのディスクの平均使用率
使用済みパフォーマンス容量	アグリゲートによるパフォーマンス容量の平均消費率	Storage VM
IOPS	SVM で処理される 1 秒あたりの平均入出力処理数	MB/s
この SVM との間で転送されたデータの平均メガバイト数 / 秒	レイテンシ	SVM がアプリケーションの要求に応答するまでの平均時間 (ミリ秒)。
ボリューム	IOPS	ボリュームで処理される 1 秒あたりの平均入出力処理数
MB/s	このボリュームとの間で転送された 1 秒あたりの平均データ量	レイテンシ
ボリュームがアプリケーションの要求に応答するまでの平均時間 (ミリ秒)。	キャッシュミス率	クライアントアプリケーションからの読み取り要求に対してキャッシュからではなくボリュームからデータが返される割合の平均値

ストレージオブジェクト	パフォーマンスカウンタ	説明
LUN	IOPS	LUN で処理される 1 秒あたりの平均入出力処理数
MB/s	この LUN との間で転送されたデータの平均メガバイト数 / 秒	レイテンシ
LUN がアプリケーションの要求に応答するまでの平均時間（ミリ秒）。	ネームスペース	IOPS
ネームスペースで処理される 1 秒あたりの平均入出力処理数	MB/s	このネームスペースとの間で転送された 1 秒あたりの平均データ量（MB）。
レイテンシ	ネームスペースがアプリケーションの要求に応答するまでの平均時間（ミリ秒）。	ポート
帯域幅使用率	ポートの使用可能な帯域幅の平均使用率	MB/s
このポートとの間で転送された 1 秒あたりの平均データ量（MB）。	ネットワークインターフェイス（LIF）	MB/s

組み合わせしきい値ポリシーで使用できるオブジェクトとカウンタ

組み合わせポリシーと一緒に使用できるパフォーマンスカウンタには種類に制限があります。プライマリとセカンダリのパフォーマンスカウンタを指定した場合、両方のパフォーマンスカウンタが上限を超えたときにイベントが生成されます。

プライマリストレージのオブジェクトとカウンタ	セカンダリストレージのオブジェクトとカウンタ
ボリュームレイテンシ	Volume IOPS の略
Volume MB/s の略	アグリゲート利用率
アグリゲート - 使用済みパフォーマンス容量	ノード利用率
ノード使用済みパフォーマンス容量	ノード使用済みパフォーマンス容量 - テイクオーバー
LUN レイテンシ	LUN の IOPS
LUN MBps	アグリゲート利用率

プライマリストレージのオブジェクトとカウンタ	セカンダリストレージのオブジェクトとカウンタ
アグリゲート - 使用済みパフォーマンス容量	ノード利用率
ノード使用済みパフォーマンス容量	ノード使用済みパフォーマンス容量 - テイクオーバー



ボリュームの組み合わせポリシーが FlexVol ボリュームではなく FlexGroup ボリュームに適用される場合、セカンダリ・カウンタとして選択できる属性は「ボリューム IOPS」と「ボリューム MBps」のみです。しきい値ポリシーにノードまたはアグリゲートの属性が1つでも含まれていると、そのポリシーは FlexGroup ボリュームには適用されず、エラーメッセージが表示されます。これは、FlexGroup ボリュームは複数のノードまたはアグリゲートに存在できるためです。

ユーザ定義のパフォーマンスしきい値ポリシーを作成する

ストレージオブジェクトに対するパフォーマンスしきい値ポリシーを作成して、パフォーマンスカウンタが特定の値を超えたときに通知が送信されるように設定します。イベント通知により、クラスタでパフォーマンス問題が発生していることを確認できます。

- 必要なもの *

アプリケーション管理者のロールが必要です。

パフォーマンスしきい値ポリシーを作成するには、Create Performance Threshold Policy ページでしきい値を入力します。このページでポリシーのすべての値を定義して新しいポリシーを作成できるほか、既存のポリシーのコピー（cloning）を作成して値を変更することもできます。

しきい値の有効な値は、数値については 0.001~10、000、000、割合については 0.001~100、使用済みパフォーマンス容量の割合については 0.001~200 です。



現在のリリースでは、カウンタの値が設定値を超えたときにイベントを送信するしきい値を設定できます。カウンタの値が設定値を下回ったときにイベントを送信するしきい値は設定できません。

手順

1. 左側のナビゲーションペインで、* イベントしきい値 * > * パフォーマンス * を選択します。

Performance Thresholds ページが表示されます。

2. 新しいポリシーを作成するか、類似のポリシーのクローンを作成して変更するかに応じて、該当するボタンをクリックします。

目的	をクリックします
新しいポリシーを作成します。	• 作成 *。
既存のポリシーのクローンを作成します	既存のポリシーを選択し、* Clone * をクリックします

Create Performance Threshold Policy ページまたは Clone Performance Threshold Policy ページが表示されます。

3. 特定のストレージオブジェクトに対して設定するパフォーマンスカウンタのしきい値を指定して、しきい値ポリシーを定義します。

- a. ストレージオブジェクトのタイプを選択し、ポリシーの名前と概要を指定します。
- b. 追跡するパフォーマンスカウンタを選択し、警告イベントと重大イベントの制限値を指定します。

警告または重大のいずれかの制限を少なくとも 1 つ定義する必要があります。両方のタイプの制限を定義する必要はありません。

- c. 必要に応じて、セカンダリパフォーマンスカウンタを選択し、警告イベントと重大イベントの制限値を指定します。

セカンダリカウンタを使用する場合は、両方のカウンタが制限値を超えた場合にしきい値違反としてイベントが報告される必要があります。組み合わせポリシーを使用して設定できるオブジェクトとカウンタには制限があります。

- d. 制限値に違反した状態がどれくらい続いたらイベントを送信するかを選択します。

既存のポリシーをクローニングする場合は、ポリシーの新しい名前を入力する必要があります。

4. [保存 (Save)] をクリックして、ポリシーを保存します。

Performance Thresholds ページに戻ります。しきい値ポリシーが作成されたことを示すメッセージがページの上部に表示されます。新しいポリシーをストレージオブジェクトにすぐに適用できるように、該当するオブジェクトタイプのインベントリページへのリンクも表示されます。

この時点で新しいしきい値ポリシーをストレージオブジェクトに適用する場合は、 * Go to object_type Now * リンクをクリックしてインベントリページに移動できます。

ストレージオブジェクトにパフォーマンスしきい値ポリシーを割り当てます

パフォーマンスカウンタの値がポリシーの設定を超えたときに Unified Manager からイベントが報告されるように、ストレージオブジェクトにユーザ定義のパフォーマンスしきい値ポリシーを割り当てます。

- 必要なもの *

アプリケーション管理者のロールが必要です。

オブジェクトに適用するパフォーマンスしきい値ポリシーを用意しておく必要があります。

パフォーマンスポリシーは、オブジェクトまたはオブジェクトのグループに一度に 1 つずつ適用できます。

各ストレージオブジェクトに最大 3 つのしきい値ポリシーを割り当てることができます。複数のオブジェクトにポリシーを割り当てる際に、ポリシーがすでに上限まで割り当てられたオブジェクトが含まれていると、Unified Manager では次のように処理されます。

- 選択したオブジェクトのうち、ポリシーの数が上限に達していないすべてのオブジェクトにポリシーを適用します

- ポリシーの数が上限に達しているオブジェクトは無視されます
- すべてのオブジェクトにポリシーが割り当てられなかったことを示すメッセージが表示されます

手順

1. いずれかのストレージオブジェクトのパフォーマンスインベントリページで、しきい値ポリシーを割り当てるオブジェクトを選択します。

しきい値を割り当てる対象	をクリックします
単一のオブジェクト	そのオブジェクトの左側にあるチェックボックスをオンにします。
複数のオブジェクト	各オブジェクトの左側にあるチェックボックスをオンにします。
ページ上のすべてのオブジェクト	。 <input type="checkbox"/> ドロップダウンボックスで、「* このページのすべてのオブジェクトを選択 *」を選択します。
同じタイプのすべてのオブジェクト	。 <input type="checkbox"/> ドロップダウンボックスで、「* すべてのオブジェクトを選択 *」を選択します。

ソートやフィルタの機能を使用してインベントリページに表示されるオブジェクトのリストを絞り込むと、複数のオブジェクトにしきい値ポリシーを簡単に適用できます。

2. 選択してから、* パフォーマンスしきい値ポリシーの割り当て * をクリックします。

パフォーマンスしきい値ポリシーの割り当てページが表示され、そのタイプのストレージオブジェクトに対応するしきい値ポリシーのリストが表示されます。

3. 各ポリシーをクリックしてパフォーマンスしきい値設定の詳細を表示し、正しいしきい値ポリシーが選択されていることを確認します。
4. 適切なしきい値ポリシーを選択したら、[* ポリシーの割り当て *] をクリックします。

しきい値ポリシーがオブジェクトに割り当てられたことを示すメッセージがページの上部に表示され、このオブジェクトとポリシーのアラート設定を行えるようにアラートページへのリンクも表示されます。

特定のパフォーマンスイベントが生成されたことを通知するために、アラートを E メールまたは SNMP トラップで送信する場合は、Alert Setup ページでアラートを設定する必要があります。

パフォーマンスしきい値ポリシーを表示します

現在定義されているパフォーマンスしきい値ポリシーはすべて、パフォーマンスしきい値ページで確認できます。

しきい値ポリシーのリストは、ポリシー名のアルファベット順にソートされます。このリストには、すべてのタイプのストレージオブジェクトのポリシーが含まれています。列ヘッダーをクリックすると、その列でポリシーをソートできます。特定のポリシーを検索する場合は、フィルタと検索を使用して、インベントリリスト

に表示するしきい値ポリシーを絞り込むことができます。

ポリシー名と条件名にカーソルを合わせると、ポリシーの設定の詳細を確認できます。また、ユーザ定義のしきい値ポリシーを作成、クローニング、編集、削除するためのボタンもあります。

ステップ

1. 左側のナビゲーションペインで、* イベントしきい値 * > * パフォーマンス * を選択します。

Performance Thresholds ページが表示されます。

ユーザ定義のパフォーマンスしきい値ポリシーを編集する

既存のパフォーマンスしきい値ポリシーのしきい値の設定を編集することができます。これは、特定のしきい値条件に対するアラートが多すぎたり少なすぎたりする場合に便利です。

- 必要なもの *

アプリケーション管理者のロールが必要です。

ポリシーの名前や既存のしきい値ポリシーで監視しているストレージオブジェクトのタイプは変更できません。

手順

1. 左側のナビゲーションペインで、* イベントしきい値 * > * パフォーマンス * を選択します。

Performance Thresholds ページが表示されます。

2. 変更するしきい値ポリシーを選択し、* Edit * をクリックします。

パフォーマンスしきい値ポリシーの編集ページが表示されます。

3. しきい値ポリシーを変更して、* Save * をクリックします。

Performance Thresholds ページに戻ります。

変更を保存すると、そのポリシーを使用するすべてのストレージオブジェクトにすぐに反映されます。

ポリシーに加えた変更の種類に応じて、[Alert Setup] ページでポリシーを使用するオブジェクトに設定されているアラート設定を確認することができます。

ストレージオブジェクトからパフォーマンスしきい値ポリシーを削除する

Unified Manager でパフォーマンスカウンタの値を監視する必要がなくなった場合は、ストレージオブジェクトからユーザ定義のパフォーマンスしきい値ポリシーを削除できます。

- 必要なもの *

アプリケーション管理者のロールが必要です。

選択したオブジェクトから一度に削除できるポリシーは 1 つだけです。

リストから複数のオブジェクトを選択すると、複数のストレージオブジェクトからしきい値ポリシーを削除できます。

手順

1. いずれかのストレージオブジェクトの * インベントリ * ページで、パフォーマンスしきい値ポリシーが少なくとも 1 つ適用されているオブジェクトを選択します。

しきい値を消去する対象	手順
単一のオブジェクト	そのオブジェクトの左側にあるチェックボックスをオンにします。
複数のオブジェクト	各オブジェクトの左側にあるチェックボックスをオンにします。
ページ上のすべてのオブジェクト	をクリックします  をクリックします。

2. パフォーマンスしきい値ポリシーのクリア * をクリックします。

しきい値ポリシーのクリアページが表示され、ストレージオブジェクトに現在割り当てられているしきい値ポリシーのリストが表示されます。

3. オブジェクトから削除するしきい値ポリシーを選択し、 * ポリシーのクリア * をクリックします。

しきい値ポリシーを選択するとそのポリシーの詳細が表示され、適切なポリシーを選択したことを確認できます。

パフォーマンスしきい値ポリシーが変更された場合の動作

既存のパフォーマンスしきい値ポリシーのカウンタの値や期間を調整した場合、そのポリシーを使用するすべてのストレージオブジェクトに変更が反映されます。新しい設定はすぐに有効になり、 Unified Manager で新たに収集されるすべてのパフォーマンスデータについて、パフォーマンスカウンタの値が新しいしきい値の設定と比較されるようになります。

変更されたしきい値ポリシーを使用しているオブジェクトに対してのアクティブなイベントがある場合、それらのイベントは廃止とマークされ、新たに定義されたしきい値ポリシーとしてカウンタの監視が開始されます。

カウンタグラフ詳細ビューでしきい値が適用されているカウンタを表示した場合、重大および警告のしきい値行には現在のしきい値の設定が反映されます。古いしきい値の設定が有効になっていた期間の履歴データを表示しても、このページに元のしきい値の設定は表示されません。



古いしきい値の設定はカウンタグラフ詳細ビューに表示されないため、現在のしきい値線より下に表示される過去のイベントが確認されることがあります。

オブジェクトの移動によるパフォーマンスしきい値ポリシーへの影響

パフォーマンスしきい値ポリシーはストレージオブジェクトに割り当てられているため、オブジェクトを移動した場合、割り当てられているすべてのしきい値ポリシーが移動の完了後もオブジェクトに関連付けられたままになります。たとえば、ボリュームまたは LUN を別のアグリゲートに移動した場合、しきい値ポリシーは新しいアグリゲートのボリュームまたは LUN で引き続きアクティブになります。

アグリゲートやノードに追加の条件が割り当てられているなど、セカンダリカウンタ条件があるしきい値ポリシー（組み合わせポリシー）の場合、セカンダリカウンタ条件は、ボリュームまたは LUN が移動された新しいアグリゲートやノードに適用されます。

変更されたしきい値ポリシーを使用しているオブジェクトに対して新しいアクティブイベントが存在する場合、それらのイベントは廃止とマークされ、新たに定義されたしきい値ポリシーとしてカウンタの監視が開始されます。

ボリューム移動処理が実行されると、ONTAP から情報変更イベントが送信されます。パフォーマンスエクスペローページのイベントタイムラインとワークロード分析ページに、移動処理が完了した時刻を示す変更イベントアイコンが表示されます。



オブジェクトを別のクラスタに移動した場合、ユーザ定義のしきい値ポリシーはオブジェクトから削除されます。必要に応じて、移動処理の完了後にしきい値ポリシーをオブジェクトに割り当てする必要があります。ただし、動的なしきい値ポリシーとシステム定義のしきい値ポリシーは、新しいクラスタへの移動後にオブジェクトに自動的に適用されます。

HA のテイクオーバーおよびギブバック時のしきい値ポリシーの機能

ハイアベイラビリティ（HA）構成でテイクオーバー処理またはギブバック処理が発生した場合、1つのノードから別のノードに移動されたオブジェクトのしきい値ポリシーは手動による移動処理の場合と同じように保持されます。Unified Manager ではクラスタの構成に変更がないかどうかを 15 分間隔でチェックするため、スイッチオーバーによる新しいノードへの影響は、クラスタの構成のポーリングが次に行われるときまで特定されません。



15 分間の構成の変更の収集期間内にテイクオーバー処理とギブバック処理の両方が発生した場合、一方のノードからもう一方のノードへのパフォーマンス統計の移動が表示されないことがあります。

アグリゲートの再配置時のしきい値ポリシーの機能

を使用して、ノード間でアグリゲートを移動する場合 `aggregate relocation start` コマンドでは、単一のしきい値ポリシーと組み合わせしきい値ポリシーの両方がすべてのオブジェクトで保持され、しきい値ポリシーのノードの部分が新しいノードに適用されます。

MetroCluster スイッチオーバー中のしきい値ポリシー機能

MetroCluster 構成で 1 つのクラスタから別のクラスタにオブジェクトが移動された場合、ユーザ定義のしきい値ポリシーの設定は保持されません。それらのしきい値ポリシーが必要な場合は、パートナークラスタに移動されたボリュームおよび LUN に適用できます。オブジェクトが元のクラスタに戻ると、それらのユーザ定義のしきい値ポリシーが自動的に再適用されます。

詳細については、を参照してください ["スイッチオーバーおよびスイッチバックの発生時のボリュームの動作](#)

"。

パフォーマンスイベントを分析しています

パフォーマンスイベントを分析して、イベントが検出されたタイミング、アクティブなイベント（新規または確認済みのイベント）が廃止されたイベントか、関連するワークロードとクラスタコンポーネント、およびイベントを解決するためのオプションを特定できます。

パフォーマンスイベントに関する情報を表示する

イベント管理インベントリページを使用して、Unified Manager で監視されているクラスタ上のすべてのパフォーマンスイベントのリストを表示できます。この情報を表示することで、最も重大なイベントを特定し、詳細情報にドリルダウンしてイベントの原因を確認できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

イベントのリストは検出時刻でソートされ、最新のイベントが最初に表示されます。列ヘッダーをクリックすると、その列でイベントをソートできます。たとえば、Status 列でソートして、重大度別にイベントを表示できます。特定のイベントまたは特定のタイプのイベントを検索する場合は、フィルタと検索を使用して、リストに表示するイベントを絞り込むことができます。

このページにはすべてのソースのイベントが表示されます。

- ユーザ定義のパフォーマンスしきい値ポリシー
- システム定義のパフォーマンスしきい値ポリシー
- 動的なパフォーマンスしきい値

[イベントタイプ] 列には、イベントのソースが一覧表示されます。イベントを選択すると、そのイベントに関する詳細をイベントの詳細ページで確認できます。

手順

1. 左側のナビゲーションペインで、* イベント管理 * をクリックします。
2. [表示] メニューから、[アクティブなパフォーマンスイベント *] を選択します。

このページには、過去 7 日間に生成された「新規」と「確認済み」のすべてのパフォーマンスイベントが表示されます。

3. 分析するイベントを特定し、イベント名をクリックします。

イベントの詳細ページが表示されます。



また、パフォーマンスエクスプローラのページでイベント名のリンクをクリックし、アラート E メールでイベントの詳細ページを表示することもできます。

ユーザ定義のパフォーマンスしきい値で生成されたイベントを分析します

ユーザ定義のしきい値で生成されたイベントは、アグリゲートやボリュームなどの特定のストレージオブジェクトのパフォーマンスカウンタがポリシーで定義されたしきい値を超えたことを示しています。これは、クラスタオブジェクトでパフォーマンス問題が発生していることを示しています。

イベントの詳細ページを使用してパフォーマンスイベントを分析し、必要に応じてイベントに対処してパフォーマンスを正常な状態に戻します。

ユーザ定義のパフォーマンスしきい値イベントへの対処

Unified Manager を使用して、パフォーマンスカウンタがユーザ定義の警告または重大のしきい値を超えたことに起因するパフォーマンスイベントを調査できます。また、Unified Manager を使用してクラスタコンポーネントの健全性を確認し、コンポーネントで検出された最近の健全性イベントがパフォーマンスイベントに関与しているかどうかを判断できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 新規または廃止状態のパフォーマンスイベントがある必要があります。

手順

1. イベントの詳細情報を表示するには、イベントの詳細 * ページを表示します。
2. イベントの原因となったしきい値違反の説明が記載された * 概要 * を確認します。

たとえば、「レイテンシ値 456 ms/op has triggered a WARNING event based on threshold setting of 400 ms/op」というメッセージは、オブジェクトに対してレイテンシ警告イベントが発生したことを示しています。

3. ポリシー名にカーソルを合わせると、イベントをトリガーしたしきい値ポリシーの詳細が表示されます。

これには、ポリシー名、評価されるパフォーマンスカウンタ、超過した場合に重大または警告イベントが生成されるカウンタ値、およびカウンタが値を超える必要がある期間が含まれます。

4. イベントトリガー時間 * をメモしておき、このイベントの原因となった可能性のある他のイベントが同時に発生したかどうかを調べることができます。
5. 次のいずれかのオプションを使用してイベントをさらに詳しく調査し、パフォーマンスの問題を解決するための操作を実行する必要があるかどうかを判断します。

オプション	調査方法
ソースオブジェクト名をクリックすると、そのオブジェクトのエクスプローラページが表示されます	このページでは、オブジェクトの詳細を表示して他の同様のストレージオブジェクトと比較し、他のストレージオブジェクトに同じタイミングでパフォーマンス問題が設定されているかどうかを確認できます。たとえば、同じアグリゲート上の他のボリュームにもパフォーマンス問題があるかどうかを確認できます。
クラスタ名をクリックして、クラスタの概要ページを表示します。	このページでは、オブジェクトが配置されているクラスタの詳細を表示して、他のパフォーマンスの問題が同時に発生していないかどうかを確認できます。

システム定義のパフォーマンスしきい値で生成されたイベントを分析します

システム定義のパフォーマンスしきい値で生成されたイベントは、特定のストレージオブジェクトの1つまたは複数のパフォーマンスカウンタがシステム定義ポリシーのしきい値を超えたことを示しています。これは、アグリゲートやノードなどのストレージオブジェクトでパフォーマンス問題が発生していることを示しています。

イベントの詳細ページを使用してパフォーマンスイベントを分析し、必要に応じてイベントに対処してパフォーマンスを正常な状態に戻します。



システム定義のしきい値ポリシーは、Cloud Volumes ONTAP、ONTAP Edge、ONTAP Select の各システムでは無効です。

システム定義のパフォーマンスしきい値のイベントへの対処

Unified Manager を使用して、パフォーマンスカウンタがシステム定義の警告しきい値を超えたことに起因するパフォーマンスイベントを調査できます。また、Unified Manager を使用してクラスタコンポーネントの健全性を確認し、コンポーネントで検出された最近のイベントがパフォーマンスイベントに関与しているかどうかを判断できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 新規または廃止状態のパフォーマンスイベントがある必要があります。

手順

1. イベントの詳細情報を表示するには、イベントの詳細 * ページを表示します。
2. イベントの原因となったしきい値違反の説明が記載された * 概要 * を確認します。

たとえば、「Node utilization value of 90 % has triggered a WARNING event based on threshold setting of 85 %」というメッセージは、クラスタオブジェクトに対してノード使用率警告イベントが発生したことを示しています。

3. イベントトリガー時間 * をメモしておき、このイベントの原因となった可能性のある他のイベントが同時に発生したかどうかを調べることができます。
4. システム診断 * で、クラスタオブジェクトに対してシステム定義のポリシーで実行されている分析タイプの簡易概要を確認します。

一部のイベントについては、診断の横に、その診断で問題が見つかったかどうかを示す緑または赤のアイコンが表示されます。システム定義のその他のタイプのイベントのカウンタグラフには、オブジェクトのパフォーマンスが表示されます。

5. [推奨される操作] で、[ヘルプ][この操作を実行する] リンクをクリックして、自分でパフォーマンスイベントを解決するために実行できる推奨される操作を表示します。

QoS ポリシーグループパフォーマンスイベントへの対処

ワークロードのスループット（IOPS、IOPS/TB、または MBps）が定義されている ONTAP QoS ポリシーの設定を超え、ワークロードのレイテンシに影響を及ぼしている場合、Unified Manager で QoS ポリシー警告イベントが生成されます。これらのシステム定義のイベントにより、多くのワークロードにレイテンシの影響が及ぶ前に潜在的なパフォーマンスの問題を修正することができます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 新規、確認済み、または廃止状態のパフォーマンスイベントが存在する必要があります。

Unified Manager では、定義されている QoS ポリシーの設定を超えるワークロードが過去 1 時間の各パフォーマンス収集期間で見つかった場合に、QoS ポリシーの違反とみなして警告イベントを生成します。ワークロードのスループットが各収集期間に短時間だけ QoS のしきい値を超えることがありますが、Unified Manager のグラフには収集期間中の「平均」のスループットしか表示されません。そのため、QoS のイベントを受け取った場合でも、グラフではワークロードのスループットがポリシーのしきい値を超えていないように見えることがあります。

System Manager または ONTAP コマンドを使用してポリシーグループを管理できます。これには次のタスクが含まれます。

- ワークロード用の新しいポリシーグループを作成します
- ポリシーグループ内のワークロードの追加または削除
- ポリシーグループ間でワークロードを移動する
- ポリシーグループのスループット制限を変更する
- 別のアグリゲートまたはノードにワークロードを移動する

手順

1. イベントの詳細情報を表示するには、イベントの詳細 * ページを表示します。
2. イベントの原因となったしきい値違反の説明が記載された * 概要 * を確認します。

たとえば、「vol1_NFS1 の IOPS 値が 1、352 IOPS のため、警告イベントがトリガーされました。ワークロードに潜在的なパフォーマンスの問題があります」というメッセージは、ボリューム vol1_NFS1 で QoS 最大 IOPS イベントが発生したことを示しています。

3. イベントが発生した日時とイベントがアクティブになっている期間の詳細については、「イベント情報」セクションを参照してください。

また、QoS ポリシーのスループットを共有しているボリュームまたは LUN については、IOPS または MBps が高い上位 3 つのワークロードの名前を確認できます。

4. システム診断 * セクションで、合計平均 IOPS または MBps（イベントに応じて）とレイテンシの 2 つのグラフを確認します。これらのグラフを見ると、ワークロードが QoS の上限に達したときに、どのクラスタコンポーネントがレイテンシに最も影響しているかを確認できます。

共有 QoS ポリシーのイベントの場合、スループットグラフに上位 3 つのワークロードが表示されます。3 つ以上のワークロードが QoS ポリシーを共有している場合、「other workloads」カテゴリに追加されたワークロードが表示されます。また、レイテンシグラフには、QoS ポリシーに含まれるすべてのワークロードの平均レイテンシが表示されます。

アダプティブ QoS ポリシーのイベントの場合、IOPS および MBps のグラフには、ボリュームのサイズに基づいて、ONTAP が割り当てられた IOPS/TB しきい値ポリシーから変換した IOPS または MBps の値が表示されます。

5. 「推奨される対処方法」セクションで、推奨される対処方法を確認し、ワークロードのレイテンシ増加を回避するために実行する必要がある対処方法を決定します。

必要に応じて、ヘルプ * ボタンをクリックして、パフォーマンスイベントの解決方法に関する推奨される操作の詳細を確認します。

ブロックサイズの定義を含むアダプティブ QoS ポリシーによるイベントの概要

アダプティブ QoS ポリシーグループでは、ボリュームサイズに基づいてスループットの上限と下限が自動的に調整され、TB または GB あたりの IOPS が一定に維持されます。ONTAP 9.5 以降では、QoS ポリシーにブロックサイズを指定することで MB/s のしきい値も同時に適用できます。

アダプティブ QoS ポリシーに IOPS のしきい値を割り当てると、各ワークロードで発生する処理数にのみ制限のみが適用されます。ワークロードを生成するクライアントに設定されているブロックサイズによっては、一部の IOPS にはるかに多くのデータが含まれ、処理を実行するノードの負荷はるかに大きくなることがあります。

ワークロードの MB/s は次の式を使用して算出されます。

$$\text{MB/s} = (\text{IOPS} * \text{Block Size}) / 1000$$

平均 IOPS が 3、000 のワークロードについて、クライアントのブロックサイズが 32KB に設定されている場合、このワークロードの実効 MB/s は 96 です。平均 IOPS が 3、000 の同じワークロードについて、クライアントのブロックサイズが 48KB に設定されている場合は、このワークロードの実効 MB/s は 144 になります。この場合、ブロックサイズが大きい方がノードでの処理データが 50% 多くなることがわかります。

次に、アダプティブ QoS ポリシーにブロックサイズが定義されている場合について、クライアントで設定されているブロックサイズに基づいてどのようにイベントがトリガーされるかを見てみましょう。

ポリシーを作成し、ピークスループットを 2、500IOPS/TB、ブロックサイズを 32KB に設定します。この

場合、使用容量が 1TB のボリュームに対する MB/s のしきい値は 80MB/s ($(2500 \text{ IOPS} * 32\text{KB}) / 1000$) に設定されます。Unified Manager では、スループットの値が定義されたしきい値を 10% 下回ると警告イベントが生成されます。イベントは次の状況で生成されます。

使用済み容量	イベントが生成されるスループットのしきい値	
	IOPS	MB/s
1 TB	2、250 IOPS	72 MB/s
2TB	4、500 IOPS	144 MB/s
5 TB	11、250 IOPS	360 MB/s

ボリュームの使用可能なスペースが 2TB、IOPS が 4、000、クライアントで設定されている QoS ブロックサイズが 32KB である場合、スループットは 128MB/s ($(4,000 \text{ IOPS} * 32\text{KB}) / 1000$) になります。この場合、4、000 IOPS と 128MB/s のどちらについても、ボリュームで 2TB のスペースを使用する場合のしきい値を超えていないため、イベントは生成されません。

ボリュームの使用可能なスペースが 2TB、IOPS が 4、000、クライアントで設定されている QoS ブロックサイズが 64KB である場合、スループットは 256MB/s ($(4,000 \text{ IOPS} * 64\text{KB}) / 1000$) になります。この場合、4、000 IOPS についてはイベントは生成されませんが、MB/s の値については 256MB/s でしきい値の 144MB/s を超えているためイベントが生成されます。

そのため、アダプティブ QoS ポリシーにブロックサイズを含む MBps の違反が発生してイベントがトリガーされると、イベントの詳細ページのシステム診断セクションに MBps のグラフが表示されます。アダプティブ QoS ポリシーに対する IOPS の違反に基づいてイベントがトリガーされると、システム診断セクションに IOPS チャートが表示されます。IOPS と MBps の両方に違反がある場合は、2 つのイベントが表示されます。

QoS設定の調整の詳細については、を参照してください ["パフォーマンス管理の概要"](#)。

ノードリソース過剰使用パフォーマンスイベントへの対処

1 つのノードが運用効率の上限を超えて稼働していて、ワークロードのレイテンシに影響を及ぼしている可能性がある場合、Unified Manager でノードリソース過剰使用警告イベントが生成されます。これらのシステム定義のイベントにより、多くのワークロードにレイテンシの影響が及ぶ前に潜在的なパフォーマンスの問題を修正することができます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 新規または廃止状態のパフォーマンスイベントがある必要があります。

Unified Manager では、パフォーマンス容量の使用率が 30 分以上にわたって 100% を超えているノードが見つかったと、ノードリソース過剰使用ポリシーの違反とみなして警告イベントを生成します。

System Manager または ONTAP コマンドを使用して、このタイプのパフォーマンス問題を修正できます。これには次の作業が含まれます。

- QoS ポリシーを作成してシステムリソースを過剰に消費しているボリュームや LUN に適用する
- ワークロードが適用されているポリシーグループの QoS の最大スループット制限を小さくします
- 別のアグリゲートまたはノードにワークロードを移動する
- ノードにディスクを追加するか、高速 CPU とより多くの RAM を搭載したノードにアップグレードして、容量を増やす

手順

1. イベントの詳細情報を表示するには、イベントの詳細 * ページを表示します。
2. イベントの原因となったしきい値違反の説明が記載された * 概要 * を確認します。

たとえば、「Perf」というメッセージが表示されます。simplicity-02 の使用済み容量が 139% のため、警告イベントがトリガーされました。データ処理装置に潜在的なパフォーマンスの問題があります。」は、ノード simplicity-02 のパフォーマンス容量の使用率が高く、ノードのパフォーマンスに影響を及ぼしていることを示しています。

3. システム診断 * セクションで、3 つのグラフを確認します。1 つはノードで使用されているパフォーマンス容量、1 つは上位のワークロードで使用されている平均ストレージ IOPS、もう 1 つは上位のワークロードで使用されているレイテンシです。これらのグラフを参考に、ノード上のレイテンシの原因であるワークロードを確認できます。

QoS ポリシーが適用されているワークロードと適用されていないワークロードを表示するには、IOPS グラフにカーソルを合わせます。

4. 「推奨される対処方法」セクションで、推奨される対処方法を確認し、ワークロードのレイテンシ増加を回避するために実行する必要がある対処方法を決定します。

必要に応じて、ヘルプ * ボタンをクリックして、パフォーマンスイベントの解決方法に関する推奨される操作の詳細を確認します。

クラスタ不均衡パフォーマンスイベントに対処する

Unified Manager は、クラスタ内の 1 つのノードの負荷が他のノードよりもはるかに高く、ワークロードのレイテンシに影響を及ぼしている可能性がある場合、クラスタ不均衡警告イベントを生成します。これらのシステム定義のイベントにより、多くのワークロードにレイテンシの影響が及ぶ前に潜在的なパフォーマンスの問題を修正することができます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

Unified Manager では、クラスタ内のすべてのノードの使用済みパフォーマンス容量の値を比較し、負荷の差が 30% を超えるノードがないかどうかを確認することで、クラスタ不均衡しきい値ポリシーの違反とみなして警告イベントを生成します。

負荷の高いワークロードを利用率の低いノードに移動するには、以下に示す手順で次のリソースを特定します。

- 同じクラスタ上の利用率の低いノード

- この別のノードで最も利用率の低いアグリゲート
- 現在のノードで最も負荷の高いボリューム

手順

1. イベントの詳細ページを表示して、イベントに関する情報を確認します。
2. イベントの原因となったしきい値違反の説明が記載された * 概要 * を確認します。

たとえば、「使用済みパフォーマンス容量カウンタは、クラスタ Dallas-1-8 のノード間で負荷に 62% の差があることを示しており、システムしきい値 30% に基づいて警告イベントをトリガーしました」というメッセージは、いずれかのノードのパフォーマンス容量の使用率が高く、ノードのパフォーマンスに影響を及ぼしていることを示しています。

3. 使用済みパフォーマンス容量の値が高いノードから使用済みパフォーマンス容量の値が最も低いノードに負荷の高いボリュームを移動するには、「Suggested Actions」のテキストを確認します。
4. 使用済みパフォーマンス容量の値が最も高いノードと最も低いノードを特定します。
 - a. 「* イベント情報」セクションで、ソースクラスタの名前をクリックします。
 - b. [Cluster/Performance Summary] ページの [Managed Objects] 領域で [Nodes] をクリックします。
 - c. ノード * インベントリページで、ノードを * Performance Capacity Used * 列でソートします。
 - d. 使用済みパフォーマンス容量の値が最も高いノードと最も低いノードを特定し、名前をメモします。
5. 使用済みパフォーマンス容量の値が最も高いノードで IOPS が最も高いボリュームを特定します。
 - a. 使用済みパフォーマンス容量の値が最も高いノードをクリックします。
 - b. ノード / パフォーマンスエクスプローラ * ページで、* 表示と比較 * メニューからこのノード上のアグリゲートを選択します。
 - c. 使用済みパフォーマンス容量の値が最も高いアグリゲートをクリックします。
 - d. アグリゲート / パフォーマンスエクスプローラ * ページで、* 表示と比較 * メニューから * このアグリゲート上のボリュームを選択します。
 - e. ボリュームを * IOPS * 列でソートし、IOPS が最も高いボリュームの名前と、ボリュームが配置されているアグリゲートの名前をメモします。
6. 使用済みパフォーマンス容量の値が最も低いノードの利用率が最も低いアグリゲートを特定します。
 - a. Storage * > * Aggregates * をクリックして、* Aggregates * インベントリページを表示します。
 - b. パフォーマンス：すべてのアグリゲート * ビューを選択します。
 - c. [Filter] ボタンをクリックして 'フィルタを追加しますここで 'Node' は '手順 4 で書き留めたパフォーマンス容量の使用済みの最小値を持つノードの名前です
 - d. 使用済みパフォーマンス容量の値が最も低いアグリゲートの名前を書き留めます。
7. 新しいノードの利用率が低いアグリゲートに過負荷のノードからボリュームを移動します。

移動処理は、ONTAP の System Manager、OnCommand Workflow Automation、ONTAP コマンド、またはこれらのツールを組み合わせ使用して実行できます。

数日後に、このクラスタから同じクラスタ不均衡イベントを受け取っていないかを確認します。

動的なパフォーマンスしきい値で生成されたイベントを分析する

動的なしきい値で生成されたイベントは、ワークロードの実際の応答時間（レイテンシ）が想定範囲と比較して高すぎたり低すぎたりしたことを示します。イベントの詳細ページを使用してパフォーマンスイベントを分析し、必要に応じてイベントに対処してパフォーマンスを正常な状態に戻します。



動的なパフォーマンスしきい値は、Cloud Volumes ONTAP、ONTAP Edge、ONTAP Select の各システムでは無効です。

動的なパフォーマンスイベントに関連した **Victim** ワークロードの特定

Unified Manager では、競合状態のストレージコンポーネントが原因の応答時間（レイテンシ）の偏差が最も高いボリュームワークロードを特定できます。このようなワークロードを特定すると、そのワークロードにアクセスするクライアントアプリケーションのパフォーマンスが通常よりも遅い理由を把握できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 新規、確認済み、または廃止された動的パフォーマンスイベントが存在する必要があります。

イベントの詳細ページには、コンポーネントのアクティビティまたは使用量の偏差が大きい順、またはイベントの影響が最も大きい順に、ユーザ定義およびシステム定義のワークロードのリストが表示されます。値は、Unified Manager がイベントを検出および最後に分析した際に特定したピーク値に基づいています。

手順

1. イベントの詳細情報を表示するには、イベントの詳細 * ページを表示します。
2. ワークロードレイテンシ / ワークロードアクティビティのグラフで、「* Victim workloads *」を選択します。
3. グラフにカーソルを合わせると、コンポーネントに影響を与えている上位のユーザ定義ワークロード、および Victim ワークロードの名前が表示されます。

動的なパフォーマンスイベントに関連した **Bully** ワークロードの特定

Unified Manager では、競合しているクラスタコンポーネントを集中的に使用しているワークロードを特定できます。このようなワークロードを特定すると、クラスタ上の特定のボリュームの応答時間（レイテンシ）が長くなっている理由を把握できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 新規、確認済み、または廃止された動的パフォーマンスイベントが存在する必要があります。

イベントの詳細ページには、コンポーネントの使用量が多い順、またはイベントの影響が最も大きい順に、ユーザ定義およびシステム定義のワークロードのリストが表示されます。値は、Unified Manager がイベントを検出および最後に分析した際に特定したピーク値に基づいています。

手順

1. イベントの詳細ページを表示してイベントに関する情報を確認します。
2. ワークロードレイテンシ / ワークロードアクティビティのグラフで、「* Bully workloads *」を選択します。
3. グラフにカーソルを合わせると、コンポーネントに影響を与えている上位のユーザ定義 Bully ワークロードが表示されます。

動的なパフォーマンスイベントに関連した **Shark** ワークロードの特定

Unified Manager では、競合しているストレージコンポーネントを集中的に使用しているワークロードを特定できます。このようなワークロードを特定すると、利用率が低いクラスタにこれらのワークロードを移動する必要があるかどうかを判断できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 新規、確認済み、または廃止されたパフォーマンス動的イベントがあります。

イベントの詳細ページには、コンポーネントの使用量が多い順、またはイベントの影響が最も大きい順に、ユーザ定義およびシステム定義のワークロードのリストが表示されます。値は、Unified Manager がイベントを検出および最後に分析した際に特定したピーク値に基づいています。

手順

1. イベントの詳細情報を表示するには、イベントの詳細 * ページを表示します。
2. ワークロードレイテンシ / ワークロードアクティビティグラフで、「* Shark workloads *」を選択します。
3. グラフにカーソルを合わせると、コンポーネントに影響を与えている上位のユーザ定義ワークロードと Shark ワークロードの名前が表示されます。

MetroCluster 構成のパフォーマンスイベント分析

Unified Manager を使用して、MetroCluster 構成のパフォーマンスイベントを分析できます。イベントに関連するワークロードを特定し、推奨される解決方法を確認できます。

MetroCluster のパフォーマンスイベントは、クラスタ間のインタースイッチリンク（ISL）を過剰に使用している Bully ワークロード、またはリンクの健全性の問題が原因である可能性があります。Unified Manager は、パートナークラスタのパフォーマンスイベントを考慮せずに、MetroCluster 構成内の各クラスタを個別に監視します。

MetroCluster 構成内の両方のクラスタのパフォーマンスイベントは、Unified Manager のダッシュボードページにも表示されます。Unified Manager の健全性のページでは、各クラスタの健全性を確認したり、クラスタとの関係を表示したりすることもできます。

MetroCluster 構成のクラスタの動的なパフォーマンスイベントを分析する

Unified Manager を使用して、パフォーマンスイベントが検出された MetroCluster 構成のクラスタについて分析することができます。クラスタの名前、イベントの検出時間、および関連する _OBully と _Victim のワークロードを特定できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- MetroCluster 構成に対する新規、確認済み、または廃止状態のパフォーマンスイベントがある必要があります。
- MetroCluster 構成の両方のクラスタを Unified Manager の同じインスタンスで監視している必要があります。

手順

1. イベントの詳細情報を表示するには、イベントの詳細 * ページを表示します。
2. イベント概要を参照して、関連するワークロードの名前と数を確認します。

この例では、MetroCluster リソースのアイコンが赤になっています。これは、MetroCluster リソースが競合状態にあることを示しています。アイコンにカーソルを合わせると、アイコンの概要が表示されます。

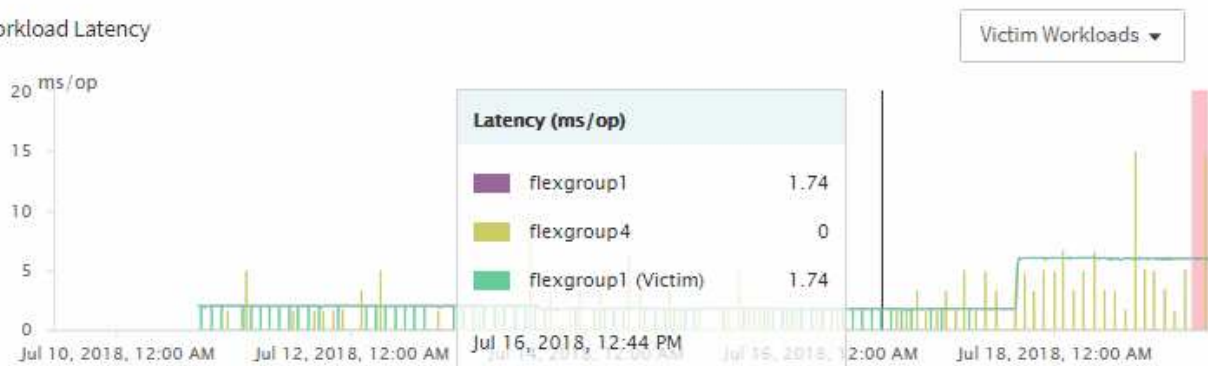


3. クラスタの名前とイベントの検出時刻を書き留めます。この情報は、パートナークラスタのパフォーマンスイベントを分析するときに使用します。
4. グラフで、_Victim ワークロードの応答時間がパフォーマンスしきい値を超えていることを確認します。

この例では、マウスオーバーで表示される情報に Victim ワークロードが表示されています。レイテンシグラフには、関連する Victim ワークロードの全体的なレイテンシのパターンは一貫していることが表示されます。Victim ワークロードの異常なレイテンシによってイベントがトリガーされた場合でも、レイテンシのパターンが一貫していれば、ワークロードのパフォーマンスは想定範囲内に収まっており、I/O の一時的な上昇によってレイテンシが増加したことでイベントがトリガーされた可能性が考えられます。

System Diagnosis (Jul 9, 2018, 11:09 AM - Jul 19, 2018, 7:39 AM) ?

Workload Latency



これらのボリュームのワークロードにアクセスするアプリケーションをクライアントに最近インストールした場合は、そのアプリケーションから大量の I/O が送信されたことが原因でレイテンシが増加した可能性があります。ワークロードのレイテンシが想定範囲内に戻ってイベントの状態が廃止に変わり、その状態が 30 分以上続くようであれば、このイベントは無視しても問題がないと考えられます。イベントがの

状態のまま継続する場合は、イベントの原因となった問題がほかにはないかどうかをさらに詳しく調査できます。

5. ワークロードスループットグラフで、「* Bully workloads *」を選択して Bully ワークロードを表示します。

Bully ワークロードがある場合は、ローカルクラスタの 1 つ以上のワークロードが MetroCluster リソースを過剰に消費しているためにイベントが発生した可能性が考えられます。Bully ワークロードの書き込みスループット（MBps）の偏差が大きくなっています。

このグラフは、ワークロードの書き込みスループット（MBps）の全体的なパターンを示しています。書き込み MBps のパターンからスループットの異常が認められるため、ワークロードが MetroCluster リソースを過剰に消費している可能性があります。

イベントに関連する Bully ワークロードがない場合は、クラスタ間のリンクが付いた健全性問題またはパートナークラスタのパフォーマンス問題が原因でイベントが発生した可能性があります。Unified Manager を使用して MetroCluster 構成の両方のクラスタの健全性を確認できます。また、パートナークラスタのパフォーマンスイベントの確認と分析も Unified Manager で実行できます。

MetroCluster 構成のリモートクラスタの動的なパフォーマンスイベントを分析する

Unified Manager を使用して、MetroCluster 構成のリモートクラスタの動的なパフォーマンスイベントを分析できます。この分析によって、リモートクラスタのイベントがそのパートナークラスタのイベントの原因となったかどうかを判断できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- MetroCluster 構成内のローカルクラスタのパフォーマンスイベントを分析し、イベント検出時刻を確認しておく必要があります。
- パフォーマンスイベントに関連したローカルクラスタとそのパートナークラスタの健全性を確認し、パートナークラスタの名前を確認しておく必要があります。

手順

1. パートナークラスタを監視している Unified Manager インスタンスにログインします。
2. 左側のナビゲーションペインで、* Events * をクリックしてイベントリストを表示します。
3. * 時間範囲 * セレクタから * 過去 1 時間 * を選択し、* 範囲の適用 * をクリックします。
4. [Filtering*selector] で、左ドロップダウンメニューから [*Cluster] を選択し、テキストフィールドにパートナークラスタの名前を入力して、[Apply Filter] をクリックします。

選択したクラスタのイベントが過去 1 時間ない場合は、パートナーでイベントが検出されたときにこのクラスタではパフォーマンスの問題は発生していません。

5. 選択したクラスタで過去 1 時間にイベントが検出された場合は、イベントの検出時刻をローカルクラスタのイベントの検出時刻と比較します。

これらのイベントにデータ処理コンポーネントの競合を引き起こしている Bully ワークロードが関係している場合は、これらの Bully ワークロードが原因でローカルクラスタのイベントが発生した可能性があります。イベントをクリックして分析し、推奨される解決方法をイベントの詳細ページで確認できます。

これらのイベントに Bully ワークロードが関係していない場合、ローカルクラスタのパフォーマンスイベントの原因を作成していません。

QoS ポリシーグループの調整が原因の動的なパフォーマンスイベントへの対処

Unified Manager を使用して、ワークロードのスループット（MBps）を調整しているサービス品質（QoS）ポリシーグループが原因のパフォーマンスイベントを調査できます。この調整によって、ポリシーグループ内のボリュームワークロードの応答時間（レイテンシ）が増加します。イベント情報を使用して、ポリシーグループに新しい制限値を設定して調整を停止する必要があるかどうかを判断できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 新規、確認済み、または廃止状態のパフォーマンスイベントが存在する必要があります。

手順

1. イベントの詳細情報を表示するには、イベントの詳細 * ページを表示します。
2. 概要 * を確認します。スロットルの影響を受けるワークロードの名前が表示されます。



調整の結果、あるワークロードは自身の Victim になるため、概要には Victim と Bully に同じワークロードが表示されることがあります。

3. テキストエディタなどのアプリケーションを使用して、ボリュームの名前を記録します。

あとでボリューム名で検索できます。

4. ワークロードレイテンシ / ワークロード利用率のグラフで、「* Bully workloads *」を選択します。
5. グラフにカーソルを合わせると、ポリシーグループに影響を与えている上位のユーザ定義ワークロードが表示されます。

偏差が最も大きく、調整の原因となったワークロードがリストの最上位に表示されます。アクティビティは、ポリシーグループ制限に対して各ワークロードが使用している割合です。

6. Suggested Actions * 領域で、上位のワークロードの * Analyze Workload * ボタンをクリックします。
7. ワークロードの分析ページで、レイテンシグラフにすべてのクラスタコンポーネントを表示し、スループットグラフに内訳を表示するように設定します。

内訳グラフは、レイテンシグラフと IOPS グラフの下に表示されます。

8. 「* Latency *」グラフの QoS 制限を比較して、調整した量がイベント発生時にレイテンシに影響した状況を確認します。

QoS ポリシーグループの最大スループットが 1 秒あたり 1、000op/sec の場合、ポリシーグループ内のワークロードの合計がこの値を超えることはできません。イベント発生時、ポリシーグループ内のワークロードの合計スループットが 1、200op/sec を超えたため、ポリシーグループのアクティビティが 1、000op/sec に調整されました

9. 読み取り / 書き込みレイテンシ * の値と、読み取り / 書き込み / その他 * の値を比較します。

どちらのグラフでも、レイテンシが高い読み取り要求が多数ある一方で、書き込み要求の数は少なくレイテンシも低くなっています。これらの値から、レイテンシを増加させた大量のスループットまたは処理の有無を判断できます。これらの値は、スループットまたは処理数にポリシーグループの制限を設定するかどうかを決定する際に使用できます。

10. ONTAP システムマネージャを使用して、ポリシーグループの現在の制限値を 1、300op/sec に増やします
11. 1 日後、手順 3 でメモしたワークロードを「ワークロードの分析 *」ページに入力します。
12. スループット内訳グラフを選択します。

読み取り / 書き込み / その他のグラフが表示されます。

13. ページの上部で、変更イベントのアイコン (●) をクリックします。
14. 読み取り / 書き込み / その他 * のグラフを * Latency * のグラフと比較します。

読み取り要求と書き込み要求は同じですが、調整は停止し、レイテンシは低下しています。

ディスク障害が原因の動的なパフォーマンスイベントへの対処

Unified Manager を使用して、アグリゲートを過剰に消費しているワークロードが原因のパフォーマンスイベントを調査できます。また、Unified Manager を使用してアグリゲートの健全性を確認し、アグリゲートで検出された最近の健全性イベントがパフォーマンスイベントに関与しているかどうかを判断できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 新規、確認済み、または廃止状態のパフォーマンスイベントが存在する必要があります。

手順

1. イベントの詳細情報を表示するには、イベントの詳細 * ページを表示します。
2. イベントに関連するワークロードおよび競合状態のクラスタコンポーネントを示す * 概要 * を確認します。

競合状態のクラスタコンポーネントによってレイテンシが影響を受けた Victim ボリュームが複数あります。障害ディスクをスペアディスクと交換するために RAID の再構築を実行中のアグリゲートが、競合状態のクラスタコンポーネントです。競合状態のコンポーネントの下にあるアグリゲートアイコンが赤で強調表示され、かっこ内にアグリゲートの名前が表示されます。

3. ワークロード利用率グラフで、「* Bully workloads *」を選択します。
4. グラフにカーソルを合わせると、コンポーネントに影響を与えている上位の Bully ワークロードが表示されます。

イベントの検出以降、最大利用率が最も高い上位のワークロードがグラフの最上位に表示されます。上位のワークロードの 1 つはシステム定義のワークロード「Disk Health」です。これは RAID の再構築を示しています。再構築は、スペアディスクを使用してアグリゲートを再構築する内部プロセスです。Disk Health ワークロードとアグリゲートの他のワークロードが原因で、アグリゲートの競合および関連するイベントが発生した可能性があります。

5. Disk Health ワークロードのアクティビティがイベントの原因であることを確認したら、再構築が完了し、Unified Manager がイベントを分析してアグリゲートが引き続き競合状態にあるかどうかを検出するまで約 30 分待ちます。
6. イベントの詳細を更新します。 *

RAID の再構築が完了したら、状態が「廃止」になっていることを確認します。これは、イベントが解決したことを示します。

7. ワークロード利用率チャートで「* Bully workloads *」を選択して、アグリゲートのワークロードを最大利用率で表示します。
8. Suggested Actions * 領域で、上位のワークロードの * Analyze Workload * ボタンをクリックします。
9. [ワークロード分析 *] ページで、選択したボリュームの過去 24 時間（1 日）のデータを表示する時間範囲を設定します。

イベントタイムラインで、赤い点（●）ディスク障害イベントが発生したタイミングを示します。

10. ノードとアグリゲートの利用率チャートで、ノードの統計の線を非表示にして、アグリゲートの線だけを表示します。
11. このグラフのデータを、イベント発生時の * レイテンシ * グラフのデータと比較します。

イベントが発生すると、アグリゲート利用率には、RAID の再構築プロセスが原因の読み取りおよび書き込みアクティビティの量が多く表示されます。これにより、選択したボリュームのレイテンシが増加します。イベント発生の数時間後には、読み取り / 書き込みとレイテンシの両方が減少し、アグリゲートの競合状態は解消しました。

HA テイクオーバーが原因の動的なパフォーマンスイベントへの対処

Unified Manager を使用して、ハイアベイラビリティ（HA）ペアを構成するクラスタノードでの大量のデータ処理が原因のパフォーマンスイベントを調査できます。また、Unified Manager を使用してノードの健全性を確認し、ノードで検出された最近の健全性イベントがパフォーマンスイベントに関与しているかどうかを判断できます。


- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 新規、確認済み、または廃止状態のパフォーマンスイベントが存在する必要があります。

手順

1. イベントの詳細情報を表示するには、イベントの詳細 * ページを表示します。
2. イベントに関連するワークロードおよび競合状態のクラスタコンポーネントを示す * 概要 * を確認します。

競合状態のクラスタコンポーネントによってレイテンシが影響を受けた Victim ボリュームが 1 つあります。パートナーノードからすべてのワークロードをテイクオーバーしてデータを処理中のノードが、競合状態のクラスタコンポーネントです。競合状態のコンポーネントの下にあるデータ処理アイコンが赤で強調表示され、イベント発生時にデータ処理を行っていたノードの名前がカッコ内に表示されます。

3. 概要 * で、ボリュームの名前をクリックします。

ボリュームパフォーマンスエクスプローラページが表示されます。ページ上部のイベントタイムラインで、変更イベントアイコン () Unified Manager が HA テイクオーバーの開始を検出した時間。

4. HA テイクオーバーの変更イベントアイコンにカーソルを合わせます。HA テイクオーバーの詳細がホバーテキストで表示されます。

レイテンシグラフに表示されたイベントから、HA テイクオーバーと同じタイミングで発生した高レイテンシが原因で、選択したボリュームでパフォーマンスしきい値を超えたことがわかります。

5. 新しいページにレイテンシグラフを表示するには、* Zoom View * をクリックします。
6. 表示メニューでクラスタコンポーネント * を選択し、クラスタコンポーネント別の合計レイテンシを表示します。
7. HA テイクオーバーの開始を示す変更イベントアイコンにマウスカーソルを合わせ、データ処理のレイテンシを合計レイテンシと比較します。

HA テイクオーバーの実行時に、データ処理ノードでワークロード需要が増加したためにデータ処理の急増が発生しています。CPU 利用率の増加によってレイテンシが増加し、イベントがトリガーされました。

8. 障害が発生したノードを修正したら、ONTAP System Manager を使用して HA ギブバックを実行します。ワークロードはパートナーノードから修復されたノードに移動します。
9. HA ギブバックが完了したら、Unified Manager での次回の構成の検出のあと (約 15 分後) に、HA テイクオーバーによってトリガーされたイベントとワークロードを「* Event Management *」インベントリページで確認します。

HA テイクオーバーによってトリガーされたイベントの状態が廃止となり、イベントが解決されたことを確認できるようになりました。データ処理コンポーネントでのレイテンシが低下し、その結果合計レイテンシも低下しています。選択したボリュームが現在データ処理に使用しているノードでイベントが解決されました。

パフォーマンスイベントを解決しています

推奨される対処方法を使用して、パフォーマンスイベントを解決することができます。最初の 3 つの推奨策は常に表示され、表示されたイベントに固有の推奨策が 4 つ目以降に表示されます。

[ヘルプ][この操作を実行する] リンクには、特定の操作の実行手順を含む、推奨される各操作の追加情報が表示されます。一部の対処方法では、Unified Manager、ONTAP System Manager、OnCommand Workflow Automation、ONTAP CLI コマンド、またはこれらのツールの組み合わせを使用する場合があります。

レイテンシが想定範囲内であることを確認します

クラスタコンポーネントが競合状態にある場合は、そのコンポーネントを使用するボリュームワークロードの応答時間 (レイテンシ) が増加した可能性があります。競合状態のコンポーネントの各 Victim ワークロードのレイテンシを参照して、実際のレイテンシが想定範囲内に収まっていることを確認できます。ボリューム名をクリックして、ボリュームの履歴データを表示することもできます。

パフォーマンスイベントが廃止状態の場合は、イベントに関連する各 Victim のレイテンシが想定範囲内に戻った可能性があります。

構成の変更がワークロードのパフォーマンスに与える影響を確認します

ディスク障害、HA フェイルオーバー、ボリューム移動などのクラスタの構成変更が、ボリュームのパフォーマンスの低下や原因レイテンシの増加につながる可能性があります。

Unified Manager のワークロード分析ページでは、最新の構成変更がいつ行われたかを確認し、処理やレイテンシ（応答時間）を比較して、選択したボリュームのワークロードでのアクティビティに変化が生じたかどうかを確認できます。

Unified Manager のパフォーマンスページで検出できる変更イベントの数は限られています。健全性のページには、構成の変更に起因する他のイベントに関するアラートが表示されます。Unified Manager でボリュームを検索すると、イベント履歴を確認できます。

クライアント側からワークロードパフォーマンスを改善するためのオプション

パフォーマンスイベントに関連したボリュームに I/O を送信しているアプリケーションやデータベースなどのクライアントワークロードを確認して、クライアント側の変更にによってイベントが修正される可能性があるかどうかを判断できます。

クラスタ上のボリュームに接続されたクライアントの I/O 要求が増加すると、その要求に対応するためにクラスタの負荷が増大します。クラスタの特定のボリュームに大量の I/O 要求を送信しているクライアントがわかれば、そのボリュームにアクセスするクライアントの数を調整するか、またはボリュームに送信される I/O の量を減らすことで、クラスタのパフォーマンスを向上させることができます。また、ボリュームがメンバーになっている QoS ポリシーグループに制限を適用または拡張することもできます。

クライアントとそのアプリケーションを調査して、クライアントが通常よりも多くの I/O を送信していることがクラスタコンポーネントでの競合の原因となっていないかを確認できます。イベントの詳細ページのシステム診断セクションに、競合状態にあるコンポーネントを使用する上位のボリュームワークロードが表示されます。特定のボリュームにアクセスしているクライアントがわかった場合は、そのクライアントに移動して、クライアントのハードウェアまたはアプリケーションが正常に動作しているか、あるいは通常より負荷が増えているかを確認できます。

MetroCluster 構成では、ローカルクラスタ上のボリュームへの書き込み要求が、リモートクラスタ上のボリュームにミラーされます。ローカルクラスタ上のソースボリュームとリモートクラスタ上のデスティネーションボリュームの同期を維持することで、MetroCluster 構成での両クラスタの要求が増加する可能性もあります。このようなミラーボリュームへの書き込み要求を減らすことで、クラスタが実行する同期処理が減り、他のワークロードのパフォーマンスに与える影響を軽減できます。

クライアントまたはネットワークに問題がないかどうかを確認します

クラスタ上のボリュームに接続されたクライアントの I/O 要求が増加すると、その要求に対応するためにクラスタの負荷が増大します。クラスタの需要が増加することで、コンポーネントが競合状態になり、そのコンポーネントを使用するワークロードのレイテンシが増加し、Unified Manager でイベントがトリガーされる可能性があります。

イベントの詳細ページのシステム診断セクションに、競合状態にあるコンポーネントを使用する上位のボリューム

ームワークロードが表示されます。特定のボリュームにアクセスしているクライアントがわかった場合は、そのクライアントに移動して、クライアントのハードウェアまたはアプリケーションが正常に動作しているか、あるいは通常より負荷が増えていないかを確認できます。クライアント管理者またはアプリケーションベンダーにサポートを依頼しなければならない場合があります。

ネットワークインフラを確認することで、クラスタと接続されているクライアントとの間の I/O 要求の実行速度が想定よりも遅くなる原因となるハードウェアの問題、ボトルネック、またはワークロードの競合が発生していないかどうかを判断できます。ネットワーク管理者にサポートを依頼しなければならない場合があります。

QoS ポリシーグループ内の他のボリュームのアクティビティが非常に高くなっていないかを確認してください

アクティビティの変化が最も大きい QoS ポリシーグループ内のワークロードを確認すると、複数のワークロードがイベントの原因となったかどうかを判断できます。また、他のワークロードがスループット制限を超えているかどうか、またはアクティビティの想定範囲内に戻ったかどうかを確認することもできます。

イベントの詳細ページのシステム診断セクションで、ワークロードをアクティビティのピーク偏差でソートして、アクティビティの変化が最も大きいワークロードをテーブルの先頭に表示できます。これらのワークロードは、アクティビティが設定された制限を超え、イベントの原因となった「いじめ」である可能性があります。

各ボリュームワークロードのワークロードの分析ページに移動して、その IOPS アクティビティを確認できます。処理のアクティビティが非常に高い期間が存在するワークロードは、イベントの原因となった可能性があります。ワークロードのポリシーグループの設定を変更したり、ワークロードを別のポリシーグループに移動したりできます。

ONTAP System Manager または ONTAP CLI コマンドを使用して、ポリシーグループを次のように管理できます。

- ポリシーグループを作成する。
- ポリシーグループ内のワークロードを追加または削除します。
- ポリシーグループ間でワークロードを移動します。
- ポリシーグループのスループット制限を変更します。

論理インターフェイス（LIF）の移動

論理インターフェイス（LIF）を負荷の低いポートに移動すると、負荷分散を改善し、メンテナンス処理やパフォーマンスの調整、間接アクセスの軽減に役立ちます。

間接アクセスはシステムの効率を低下させる可能性があります。ボリュームワークロードでネットワーク処理とデータ処理に別々のノードが使用されている場合に発生します。間接アクセスを軽減するには LIF を再配置します。つまり、ネットワーク処理とデータ処理に同じノードが使用されるように LIF を移動します。負荷の高い LIF が ONTAP によって自動的に別のポートに移動されるようにロードバランシングを設定することも、LIF を手動で移動することもできます。

* 利点 *	* 考慮事項 *
<ul style="list-style-type: none"> • 負荷分散を改善します。 • 間接アクセスが軽減されます。 	<div style="display: flex; align-items: center;">  <div> <p>CIFS 共有に接続されている LIF を移動すると、CIFS 共有にアクセスするクライアントが切断されます。CIFS 共有に対する読み取り要求や書き込み要求はすべて中断されます。</p> </div> </div>

ロードバランシングを設定するには、ONTAP コマンドを使用します。詳細については、ONTAP のネットワークに関するドキュメントを参照してください。

LIF を手動で移動する場合は、ONTAP System Manager と ONTAP CLI コマンドを使用します。

負荷の低い時間帯で **Storage Efficiency** 処理を実行

Storage Efficiency 処理に適用されるポリシーやスケジュールを変更して、影響を受けるボリュームワークロードの負荷が低いときに Storage Efficiency 処理を実行するように設定できます。

Storage Efficiency 処理では、大量のクラスタ CPU リソースが使用されて、処理を実行するボリュームの負荷が高くなることがあります。Storage Efficiency 処理の実行中に、影響を受けるボリュームでアクティビティレベルが上がると、レイテンシが高くなってイベントがトリガーされる可能性があります。

イベントの詳細ページのシステム診断セクションに、QoS ポリシーグループ内のワークロードがアクティビティのピーク偏差で表示され、Bully ワークロードが特定されます。表の上部に「storage efficiency」と表示された場合は、この処理が当該ワークロードの負荷を高めています。これらのワークロードの負荷が低いときに実行されるように効率化ポリシーまたはスケジュールを変更すれば、Storage Efficiency 処理を原因とするクラスタの競合を回避できます。

ONTAP System Manager を使用して効率化ポリシーを管理できます。効率化ポリシーとスケジュールの管理には、ONTAP コマンドを使用します。

Storage Efficiency とは

Storage Efficiency を使用すると、低コストで最大限のデータを格納し、スペースを節約しながら急増するデータに対応することができます。ネットアップのストレージ効率化戦略は、コアオペレーティングシステムである ONTAP と Write Anywhere File Layout (WAFL) ファイルシステムが提供するストレージ仮想化とユニファイドストレージに基づいています。

Storage Efficiency では、シンプロビジョニング、Snapshot コピー、重複排除、データ圧縮、FlexClone、SnapVault および Volume SnapMirror、RAID-DP、Flash Cache、Flash Pool アグリゲート、および FabricPool 対応アグリゲートを使用したシンレプリケーション。ストレージ利用率の向上とストレージコストの削減に役立ちます。

ユニファイドストレージアーキテクチャでは、Storage Area Network (SAN ; ストレージエリアネットワーク)、Network-Attached Storage (NAS ; ネットワーク接続型ストレージ)、および単一プラットフォーム上のセカンダリストレージを効率的に統合できます。

Serial Advanced Technology Attachment (SATA) ドライブなどの高密度ディスクドライブを、Flash Pool アグリゲート内で、または Flash Cache や RAID-DP テクノロジーを使用して構成すると、パフォーマンスと耐障害性を低下させることなく効率性を向上させることができます。

FabricPool 対応アグリゲートには、ローカルのパフォーマンス階層としてのオール SSD アグリゲートまたは HDD アグリゲート (ONTAP 9.8 以降) と、クラウド階層として指定するオブジェクトストアが含まれます。FabricPool を設定すると、アクセス頻度に基づいてデータを格納するストレージ階層 (ローカル階層またはクラウド階層) を管理する際に役立ちます。

シンプロビジョニング、Snapshot コピー、重複排除、データ圧縮、SnapVault と Volume SnapMirror を使用したシンレプリケーション、FlexClone などのテクノロジーは、さらに削減効果を高めます。これらのテクノロジーを個別に、または組み合わせて使用することで、ストレージ効率を最大限に高めることができます。

ディスクを追加してデータを再配置

アグリゲートにディスクを追加することで、ストレージ容量を増やし、そのアグリゲートのパフォーマンスを高めることができます。ディスクを追加したあと、追加したディスクにデータを再配置するまでは読み取りパフォーマンスは向上しません。

この手順は、Unified Manager で動的しきい値またはシステム定義のパフォーマンスしきい値に基づいてトリガーされたアグリゲートイベントを受信したときに使用できます。

- 動的しきい値のイベントを受信した場合、イベントの詳細ページで、競合状態にあるアグリゲートを表すクラスタコンポーネントのアイコンが赤で強調表示されます。

このアイコンの下には、ディスクを追加できるアグリゲートの名前がカッコ内に表示されます。

- システム定義のしきい値のイベントを受信した場合、イベントの詳細ページのイベント概要に、問題があるアグリゲートの名前が表示されます。

このアグリゲートにディスクを追加してデータを再配置できます。

アグリゲートに追加できるのは、クラスタにすでに存在しているディスクだけです。クラスタに使用可能なディスクが残っていない場合は、必要に応じて管理者に問い合わせるか追加のディスクを購入してください。ONTAP System Manager または ONTAP コマンドを使用して、アグリゲートにディスクを追加できます。



データの再配置を行うのは、HDD アグリゲートおよび Flash Pool アグリゲートを使用している場合だけです。SSD アグリゲートまたは FabricPool アグリゲートにはデータを再割り当てしないでください。

ノードで **Flash Cache** を有効にしてワークロードパフォーマンスを改善する仕組み

クラスタ内の各ノードで Flash Cache ™ インテリジェントデータキャッシングを有効にすることで、ワークロードパフォーマンスを向上させることができます。

Flash Cache モジュールまたは Performance Acceleration Module PCIe ベースのメモリモジュールは、インテリジェントな外部読み取りキャッシュとして機能することで、ランダムリード中心のワークロードのパフォーマンスを最適化します。このハードウェアは、ONTAP の WAFL 外部キャッシュソフトウェアコンポーネントと連携して機能します。

Unified Manager のイベントの詳細ページで、競合状態にあるアグリゲートを表すクラスタコンポーネントアイコンが赤で強調表示されます。このアイコンの下には、アグリゲートを特定するアグリゲートの名前がカッコ内に表示されます。アグリゲートが配置されているノードで Flash Cache を有効にすることができます。

ONTAP System Manager または ONTAP コマンドを使用して、Flash Cache がインストールされて有効になっているかを確認し、有効になっていない場合は有効にすることができます。次のコマンドは、Flash Cache が特定のノードで有効になっているかどうかを示します。 **cluster::> run local options flexscale.enable**

Flash Cache とその使用要件については、次のテクニカルレポートを参照してください。

"[テクニカルレポート 3832](#) : 『Flash Cache Best Practices Guide』"

ストレージアグリゲートで **Flash Pool** を有効にしてワークロードパフォーマンスを改善する方法

アグリゲートで Flash Pool 機能を有効にすることで、ワークロードパフォーマンスを改善できます。Flash Pool は、HDD と SSD の両方が組み込まれているアグリゲートです。プライマリストレージには HDD を使用し、SSD を使用して読み取りと書き込みの高性能なキャッシュを実現することで、アグリゲートのパフォーマンスを向上させることができます。

Unified Manager のイベントの詳細ページには、競合状態にあるアグリゲートの名前が表示されます。ONTAP System Manager または ONTAP コマンドを使用して、アグリゲートで Flash Pool が有効になっているかどうかを確認できます。SSD を搭載している場合は、コマンドラインインターフェイスを使用して有効にすることができます。SSD を搭載している場合は、アグリゲートで次のコマンドを実行して Flash Pool が有効になっているかどうかを確認できます。 **cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled**

このコマンドでは、*aggr_name* は、競合状態にあるアグリゲートなどのアグリゲートの名前です。

Flash Pool とその使用要件の詳細については、『clustered Data ONTAP 物理ストレージ管理ガイド』を参照してください。

MetroCluster 構成の健全性チェック

Unified Manager を使用して、MetroCluster 構成内の IP または FC 経由のクラスタの健全性を確認できます。健全性のステータスとイベントから、ワークロードのパフォーマンスに影響するハードウェアやソフトウェアの問題がないかを判断できます。

Unified Manager で E メールアラートの送信を設定した場合は、E メールを調べて、ローカルクラスタやリモートクラスタで発生した健全性の問題がパフォーマンスイベントの原因となっていないかを確認できます。Unified Manager の GUI では、「* イベント管理 *」を選択して現在のイベントのリストを表示し、フィルタを使用して MetroCluster 構成のイベントのみを表示できます。

詳細については、を参照してください "[MetroCluster 構成のクラスタの健全性を確認しています](#)"

MetroCluster 構成の検証

MetroCluster over FCおよびIP構成でミラーされたワークロードにパフォーマンスの問題が発生しないようにするには、MetroCluster 構成が正しく設定されていることを確認します。また、構成を変更するか、ソフトウェアまたはハードウェアコンポーネントをアップグレードすることで、ワークロードのパフォーマンスを向上させることもできます。

を参照してください ["MetroCluster のドキュメント"](#) Fibre Channel (FC) スイッチ、ケーブル、スイッチ間リンク (ISL) など、MetroCluster 構成のクラスタのセットアップ手順について説明します。また、ローカルクラスタとリモートクラスタがミラーボリュームデータと通信できるように MetroCluster ソフトウェアを設定する際にも役立ちます。MetroCluster over IPの設定に固有の情報については、を参照してください ["MetroCluster IP 構成をインストール"](#)。

MetroCluster 構成との要件をで比較できます ["MetroCluster のドキュメント"](#) MetroCluster 構成のコンポーネントを変更またはアップグレードすることでワークロードのパフォーマンスが向上するかどうかを判断する。この比較は、次の点について回答を行う場合に役立ちます。

- コントローラはワークロードに適していますか？
- スループットの処理能力を高めるために、ISL バンドルをより大きな帯域幅にアップグレードする必要があるか。
- 帯域幅を増やすためにスイッチ上でバッファ間クレジット (BBC) を調整できるか。
- ワークロードに SSD ストレージへの大量の書き込みスループットがある場合、そのスループットに対応するために FC-to-SAS ブリッジをアップグレードする必要があるか。
- 関連情報 *
- MetroCluster コンポーネントの交換またはアップグレードについては、を参照してください ["MetroCluster のドキュメント"](#)。
- コントローラのアップグレードについては、を参照してください ["スイッチオーバーとスイッチバックを使用して MetroCluster FC 構成のコントローラをアップグレードする"](#) および ["スイッチオーバーとスイッチバックを使用したMetroCluster IP構成のコントローラのアップグレード"](#)

ワークロードを別のアグリゲートに移動しています

ワークロードが現在配置されているアグリゲートよりも負荷の低いアグリゲートを Unified Manager で特定し、選択したボリュームまたは LUN をそのアグリゲートに移動できます。負荷の高いワークロードを負荷の低いアグリゲートまたはフラッシュストレージが有効なアグリゲートに移動すると、ワークロードの効率が向上します。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 現在パフォーマンス問題があるアグリゲートの名前を記録しておく必要があります。
- アグリゲートがイベントを受け取った日時を記録しておく必要があります。
- Unified Manager で 1 カ月分以上のパフォーマンスデータの収集と分析が行われている必要があります。

負荷の高いワークロードを利用率の低いアグリゲートに移動するには、以下に示す手順で次のリソースを特定

します。

- 同じクラスタ上の利用率の低いアグリゲート
- 現在のアグリゲートで最も負荷の高いボリューム

手順

1. クラスタ内で最も利用率の低いアグリゲートを特定します。

- a. イベント * の詳細ページで、アグリゲートが配置されているクラスタの名前をクリックします。

パフォーマンス / クラスタランディングページにクラスタの詳細が表示されます。

- b. [* 概要] ページで、[管理対象オブジェクト *] ペインの [* アグリゲート] をクリックします。

このクラスタ上のアグリゲートのリストが表示されます。

- c. 利用率 * 列をクリックして、アグリゲートを利用率が低い順にソートします。

空き容量が最も多いアグリゲートを特定することもできます。これにより、ワークロードの移動先にするアグリゲートの候補が一覧表示されます。

- d. ワークロードの移動先にするアグリゲートの名前を書き留めます。

2. イベントを受け取ったアグリゲートで負荷の高いボリュームを特定します。

- a. パフォーマンス問題があるアグリゲートをクリックします。

アグリゲートの詳細は、Performance/AggregateExplorer ヘエシに表示されます。

- b. * 時間範囲 * セレクタから「* 過去 30 日間 *」を選択し、* 範囲の適用 * をクリックします。

これにより、デフォルトの 72 時間よりも長い期間のパフォーマンス履歴を表示できます。過去 72 時間だけでなく一貫した数のリソースを使用しているボリュームを移動したい。

- c. View and Compare * コントロールから、* このアグリゲートのボリュームを選択します。

このアグリゲート上の FlexVol ボリュームおよび FlexGroup コンスティチュエントボリュームのリストが表示されます。

- d. ボリュームを MBps の高い順に並べ替えたあとに IOPS の高い順に並べ替えることで、最も負荷の高いボリュームがわかります。

- e. 別のアグリゲートに移動するボリュームの名前を書き留めます。

3. 事前に特定した利用率の低いアグリゲートに負荷の高いボリュームを移動します。

移動処理は、ONTAP の System Manager、OnCommand Workflow Automation、ONTAP コマンド、またはこれらのツールを組み合わせを使用して実行できます。

数日後に、このノードまたはアグリゲートから同じタイプのイベントを受け取っていないかどうかを確認します。

ワークロードを別のノードに移動する

ワークロードが現在実行されているノードよりも負荷の低い別のノード上のアグリゲートを Unified Manager で特定し、選択したボリュームをそのアグリゲートに移動できます。負荷の低いノード上のアグリゲートに負荷の高いワークロードを移動すれば、両ノードでのワークロードの効率が向上します。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 現在パフォーマンス問題があるノードの名前を記録しておく必要があります。
- ノードがパフォーマンスイベントを受け取った日付と時刻を記録しておく必要があります。
- Unified Manager で 1 カ月分以上のパフォーマンスデータの収集と分析が行われている必要があります。

この手順で次のリソースを特定すると、負荷の高いワークロードを利用率の低いノードに移動できるようになります。

- 同じクラスタで最も空きパフォーマンス容量が大きいノード
- 別のノードで最も空きパフォーマンス容量が大きいアグリゲート
- 現在のノードで最も負荷の高いボリューム

手順

1. クラスタで最も空きパフォーマンス容量が大きいノードを特定します。

- a. [* Event Details *] ページで、ノードが配置されているクラスタの名前をクリックします。

パフォーマンス / クラスタランディングページにクラスタの詳細が表示されます。

- b. [* 概要 *] タブの [* 管理対象オブジェクト *] ペインで [* ノード *] をクリックします。

このクラスタ上のノードのリストが表示されます。

- c. 使用済みパフォーマンス容量 * 列をクリックして、ノードを使用率が最も低い順にソートします。

これにより、ワークロードの移動先にするノードの候補が一覧表示されます。

- d. ワークロードの移動先にするノードの名前を書き留めます。

2. この別のノード上の最も利用率の低いアグリゲートを特定します。

- a. 左側のナビゲーションペインで、 * Storage * > * Aggregates * をクリックし、View メニューから * Performance * > * All Aggregates * を選択します。

Performance : All Aggregates ビューが表示されます。

- b. [Filtering] をクリックし、左側のドロップダウンメニューから [Node] を選択して、テキストフィールドにノード名を入力し、 [Apply Filter] をクリックします。

Performance : All aggregates ビューが再表示され、このノードで使用可能なアグリゲートのリストが表示されます。

- c. 使用済みパフォーマンス容量 * 列をクリックして、アグリゲートを使用量が最も少ない順にソートします。

これにより、ワークロードの移動先にするアグリゲートの候補が一覧表示されます。

- d. ワークロードの移動先にするアグリゲートの名前を書き留めます。
3. イベントを受け取ったノードで負荷の高いワークロードを特定します。
 - a. イベントの * Event Details * ページに戻ります。
 - b. [* 影響を受けるボリューム *] フィールドで、ボリューム数のリンクをクリックします。

Performance : All Volumes ビューには、そのノード上のボリュームがフィルタリングされて表示されます。

- c. 合計容量 * 列をクリックして、ボリュームを最大割り当てスペースでソートします。

これにより、移動するボリュームの候補が一覧表示されます。

- d. 移動するボリュームの名前と、そのボリュームが現在配置されているアグリゲートの名前を書き留めます。
4. 事前に特定した別のノードで最も空きパフォーマンス容量が大きいアグリゲートにボリュームを移動します。

移動処理は、ONTAP の System Manager 、 OnCommand Workflow Automation 、 ONTAP コマンド、またはこれらのツールを組み合わせを使用して実行できます。

数日後に、このノードまたはアグリゲートから同じタイプのイベントを受け取っていないかどうかを確認します。

別のノード上のアグリゲートへのワークロードの移動

ワークロードが現在実行されているノードよりも負荷の低い別のノード上のアグリゲートを Unified Manager で特定し、選択したボリュームをそのアグリゲートに移動できます。負荷の低いノード上のアグリゲートに負荷の高いワークロードを移動すれば、両ノードでのワークロードの効率が向上します。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- 現在パフォーマンス問題があるノードの名前を記録しておく必要があります。
- ノードがパフォーマンスイベントを受け取った日付と時刻を記録しておく必要があります。
- Unified Manager で 1 カ月分以上のパフォーマンスデータの収集と分析が行われている必要があります。

負荷の高いワークロードを利用率の低いノードに移動するには、以下に示す手順で次のリソースを特定します。

- 同じクラスタ上の利用率の低いノード
- この別のノードで最も利用率の低いアグリゲート

- 現在のノードで最も負荷の高いボリューム

手順

1. クラスタ内で最も利用率の低いノードを特定します。

- a. イベント * の詳細ページで、ノードが配置されているクラスタの名前をクリックします。

パフォーマンス / クラスタランディングページにクラスタの詳細が表示されます。

- b. [* 概要 *] ページの [* 管理対象オブジェクト *] ペインで [* ノード *] をクリックします。

このクラスタ上のノードのリストが表示されます。

- c. ノードを利用率が低い順にソートするには、* Utilization * 列をクリックします。

また、最大の * 空き容量 * を持つノードを特定することもできます。これにより、ワークロードの移動先にするノードの候補が一覧表示されます。

- d. ワークロードの移動先にするノードの名前を書き留めます。

2. この別のノード上の最も利用率の低いアグリゲートを特定します。

- a. 左側のナビゲーションペインで、* Storage * > * Aggregates * をクリックし、View メニューから * Performance * > * All Aggregates * を選択します。

Performance : All Aggregates ビューが表示されます。

- b. **[Filtering]** をクリックし、左側のドロップダウンメニューから **[Node]** を選択して、テキストフィールドにノード名を入力し、**[*Apply Filter]** をクリックします。

Performance : All aggregates ビューが再表示され、このノードで使用可能なアグリゲートのリストが表示されます。

- c. 利用率 * 列をクリックして、アグリゲートを利用率が低い順にソートします。

空き容量が最も多いアグリゲートを特定することもできます。これにより、ワークロードの移動先にするアグリゲートの候補が一覧表示されます。

- d. ワークロードの移動先にするアグリゲートの名前を書き留めます。

3. イベントを受け取ったノードで負荷の高いワークロードを特定します。

- a. イベントの * Event * 詳細ページに戻ります。

- b. [* 影響を受けるボリューム *] フィールドで、ボリューム数のリンクをクリックします。

Performance : All Volumes ビューには、そのノード上のボリュームがフィルタリングされて表示されます。

- c. 合計容量 * 列をクリックして、ボリュームを最大割り当てスペースでソートします。

これにより、移動するボリュームの候補が一覧表示されます。

- d. 移動するボリュームの名前と、そのボリュームが現在配置されているアグリゲートの名前を書き留めます。

4. 事前に特定した別のノードで最も利用率の低いアグリゲートにボリュームを移動します。

移動処理は、ONTAP の System Manager 、 OnCommand Workflow Automation 、 ONTAP コマンド、またはこれらのツールを組み合わせ使用して実行できます。

数日後に、このノードまたはアグリゲートから同じタイプのイベントを受け取っていないかどうかを確認します。

別の HA ペアのノードへのワークロードの移動

現在ワークロードが実行されている HA ペアよりも空きパフォーマンス容量が大きい別のハイアベイラビリティ（HA）ペアのノード上のアグリゲートを Unified Manager で特定し、その後、選択したボリュームを新しい HA ペア上のアグリゲートに移動できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- クラスタが 2 つ以上の HA ペアで構成されている必要があります

クラスタに HA ペアが 1 つしかない場合は、この改善策を実施できません。

- 現在パフォーマンス問題がある HA ペアの 2 つのノードの名前を記録しておく必要があります。
- ノードがパフォーマンスイベントを受け取った日付と時刻を記録しておく必要があります。
- Unified Manager で 1 カ月分以上のパフォーマンスデータの収集と分析が行われている必要があります。

空きパフォーマンス容量が大きいノード上のアグリゲートに負荷の高いワークロードを移動すれば、両ノードでのワークロードの効率が向上します。この手順で次のリソースを特定すると、負荷の高いワークロードを別の HA ペアの空きパフォーマンス容量の大きいノードに移動できます。

- 同じクラスタ上の別の HA ペアで最も空きパフォーマンス容量が大きいノード
- 別のノードで最も空きパフォーマンス容量が大きいアグリゲート
- 現在のノードで最も負荷の高いボリューム

手順

1. 同じクラスタ上の別の HA ペアを構成するノードを特定します。
 - a. [* Event Details *] ページで、ノードが存在するクラスタの名前をクリックします。

パフォーマンス / クラスタランディングページにクラスタの詳細が表示されます。
 - b. [* 概要 *] ページの [* 管理対象オブジェクト *] ペインで [* ノード *] をクリックします。

このクラスタ上のノードのリストは、Performance : All Nodes ビューに表示されます。
 - c. 現在パフォーマンス問題がある HA ペアとは別の HA ペアのノードの名前を書き留めます。
2. 別の HA ペアで最も空きパフォーマンス容量が大きいノードを特定します。
 - a. [パフォーマンス：すべてのノード *] ビューで、[使用済みパフォーマンス容量 *] 列をクリックし

て、使用率が最も低いノードをソートします。

これにより、ワークロードの移動先にするノードの候補が一覧表示されます。

b. ワークロードの移動先にする別の HA ペアのノードの名前を書き留めます。

3. 別のノードで最も空きパフォーマンス容量が大きいアグリゲートを特定します。

a. [* パフォーマンス：すべてのノード * (* Performance : All Nodes *)] ビューで、ノードをクリックします。

ノードの詳細が Performance/NodeExplorer ヘエシに表示されます。

b. View and Compare * メニューで、このノードのアグリゲートを選択します。

このノード上のアグリゲートがグリッドに表示されます。

c. 使用済みパフォーマンス容量 * 列をクリックして、アグリゲートを使用量が最も少ない順にソートします。

これにより、ワークロードの移動先にするアグリゲートの候補が一覧表示されます。

d. ワークロードの移動先にするアグリゲートの名前を書き留めます。

4. イベントを受け取ったノードで負荷の高いワークロードを特定します。

a. イベントの * Event * 詳細ページに戻ります。

b. 影響を受けるボリューム * フィールドで、最初のノードのボリューム数のリンクをクリックします。

Performance : All Volumes ビューには、そのノード上のボリュームがフィルタリングされて表示されます。

c. 合計容量 * 列をクリックして、ボリュームを最大割り当てスペースでソートします。

これにより、移動するボリュームの候補が一覧表示されます。

d. 移動するボリュームの名前と、そのボリュームが現在配置されているアグリゲートの名前を書き留めます。

e. このイベントに関係した 2 つ目のノードに対して手順 4c と 4d を実行して、そのノードから移動するボリュームの候補を特定します。

5. 事前に特定した別のノードで最も空きパフォーマンス容量が大きいアグリゲートにボリュームを移動します。

移動処理は、ONTAP の System Manager 、 OnCommand Workflow Automation 、 ONTAP コマンド、またはこれらのツールを組み合わせを使用して実行できます。

数日後に、このノードまたはアグリゲートから同じタイプのイベントを受け取っていないかどうかを確認します。

別の HA ペアのもう一方のノードへのワークロードの移動

現在ワークロードが実行されている HA ペアよりも負荷の低い別の HA ペアのノード上

のアグリゲートを Unified Manager で特定し、その後、選択したボリュームを新しい HA ペア上のアグリゲートに移動できます。負荷の低いノード上のアグリゲートに負荷の高いワークロードを移動すれば、両ノードでのワークロードの効率が向上します。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- クラスタが 2 つ以上の HA ペアで構成されている必要があります。クラスタに HA ペアが 1 つしかない場合は、この改善策を実施できません。
- 現在パフォーマンス問題を備えている HA ペアの 2 つのノードの名前を記録しておく必要があります。
- ノードがパフォーマンスイベントを受け取った日付と時刻を記録しておく必要があります。
- Unified Manager で 1 カ月分以上のパフォーマンスデータの収集と分析が行われている必要があります。

負荷の高いワークロードを別の HA ペアの利用率の低いノードに移動するには、以下に示す手順で次のリソースを特定します。

- 同じクラスタで別の HA ペアを構成する利用率の低いノード
- この別のノードで最も利用率の低いアグリゲート
- 現在のノードで最も負荷の高いボリューム

手順

1. 同じクラスタ上の別の HA ペアを構成するノードを特定します。

- a. 左側のナビゲーションペインで、* Storage * > * Clusters * をクリックし、表示メニューから * Performance * > * All Clusters * を選択します。

Performance : All Clusters ビューが表示されます。

- b. 現在のクラスタのノード数 * フィールドの数値をクリックします。

Performance : All Nodes ビューが表示されます。

- c. 現在パフォーマンス問題がある HA ペアとは別の HA ペアのノードの名前を書き留めます。

2. この別の HA ペアで最も利用率の低いノードを特定します。

- a. ノードを利用率が低い順にソートするには、* Utilization * 列をクリックします。

また、最大の * 空き容量 * を持つノードを特定することもできます。これにより、ワークロードの移動先にするノードの候補が一覧表示されます。

- b. ワークロードの移動先にするノードの名前を書き留めます。

3. この別のノード上の最も利用率の低いアグリゲートを特定します。

- a. 左側のナビゲーションペインで、* Storage * > * Aggregates * をクリックし、View メニューから * Performance * > * All Aggregates * を選択します。

Performance : All Aggregates ビューが表示されます。

- b. **[Filtering]** をクリックし、左側のドロップダウンメニューから **[Node]** を選択して、テキストフィールドにノード名を入力し、**[*Apply Filter]** をクリックします。

Performance : All aggregates ビューが再表示され、このノードで使用可能なアグリゲートのリストが表示されます。

- c. 利用率 * 列をクリックして、アグリゲートを利用率が低い順にソートします。

空き容量が最も多いアグリゲートを特定することもできます。これにより、ワークロードの移動先にするアグリゲートの候補が一覧表示されます。

- d. ワークロードの移動先にするアグリゲートの名前を書き留めます。

4. イベントを受け取ったノードで負荷の高いワークロードを特定します。

- a. イベントの * Event * 詳細ページに戻ります。

- b. 影響を受けるボリューム * フィールドで、最初のノードのボリューム数のリンクをクリックします。

Performance : All Volumes ビューには、そのノード上のボリュームがフィルタリングされて表示されます。

- c. 合計容量 * 列をクリックして、ボリュームを最大割り当てスペースでソートします。

これにより、移動するボリュームの候補が一覧表示されます。

- d. 移動するボリュームの名前と、そのボリュームが現在配置されているアグリゲートの名前を書き留めます。

- e. このイベントに関係した 2 つ目のノードに対して手順 4c と 4d を実行して、そのノードから移動するボリュームの候補を特定します。

5. 事前に特定した別のノードで最も利用率の低いアグリゲートにボリュームを移動します。

移動処理は、ONTAP の System Manager 、 OnCommand Workflow Automation 、 ONTAP コマンド、またはこれらのツールを組み合わせ使用して実行できます。

数日後に、このノードまたはアグリゲートから同じタイプのイベントを受け取っていないかどうかを確認します。

QoS ポリシーの設定を使用して、このノードでの作業に優先順位を付けます

QoS ポリシーグループに上限を設定して、ポリシーグループに含まれるワークロードの 1 秒あたりの I/O 処理数 (IOPS) やスループット (MBps) の上限を制御できます。デフォルトポリシーグループなどの制限が設定されていないポリシーグループにワークロードが含まれている場合や、設定された制限値が設定されていない場合は、設定された制限値を増やすか、必要な制限値が設定された新規または既存のポリシーグループにワークロードを移動できます。

ノードのパフォーマンスイベントの原因がノードリソースを過剰に消費しているワークロードにある場合、イベントの詳細ページのイベント概要に関連するボリュームのリストへのリンクが表示されます。パフォーマンス / ボリュームページで、影響を受けたボリュームを IOPS と MBps でソートすると、イベントの原因となった可能性がある使用率が最も高いワークロードを確認できます。

ノードリソースを過剰に消費しているボリュームは、より制限の厳しいポリシーグループに割り当てます。これにより、ポリシーグループによる調整でワークロードのアクティビティが制限されて、そのノードでのリソ

ースの使用が削減されます。

ONTAP System Manager または ONTAP コマンドを使用してポリシーグループを管理できます。これには次のタスクが含まれます。

- ポリシーグループを作成する
- ポリシーグループ内のワークロードの追加または削除
- ポリシーグループ間でワークロードを移動する
- ポリシーグループのスループット制限を変更する

非アクティブなボリュームと LUN を削除します

アグリゲートの空きスペースが問題として識別されている場合は、使用されていないボリュームと LUN を検索してアグリゲートから削除できます。これにより、ディスクスペース不足の問題を軽減できます。

アグリゲートでのパフォーマンスイベントの原因がディスクスペースの不足である場合は、使用されなくなったボリュームと LUN をいくつかの方法で特定できます。

使用されていないボリュームを特定する方法

- イベントの詳細ページの * 影響を受けるオブジェクト数 * フィールドには、影響を受けるボリュームのリストを示すリンクが表示されます。

リンクをクリックすると、Performance : All Volumes ビューにボリュームが表示されます。このページで関連するボリュームを * IOPS * でソートすると、アクティブでないボリュームがわかります。

使用されていない LUN を特定する方法

1. イベントの詳細ページで、イベントが発生したアグリゲートの名前を書き留めます。
2. 左側のナビゲーションペインで、* Storage * > * LUNs * をクリックし、表示メニューから * Performance * > * All LUNs * を選択します。
3. **[Filtering]** をクリックし、左側のドロップダウンメニューから **[Aggregate]** を選択して、テキストフィールドにアグリゲートの名前を入力し、**[Apply Filter]** をクリックします。
4. 表示された影響を受ける LUN のリストを * IOPS * でソートして、アクティブでない LUN を確認します。

使用されていないボリュームと LUN を特定したら、ONTAP System Manager または ONTAP コマンドを使用して、それらのオブジェクトを削除できます。

ディスクを追加してアグリゲートレイアウトを再構築する

アグリゲートにディスクを追加することで、ストレージ容量を増やし、そのアグリゲートのパフォーマンスを高めることができます。ディスクの追加後は、アグリゲートを再構築したあとのパフォーマンスの改善だけを確認できます。

イベントの詳細ページにシステム定義のしきい値イベントが表示された場合、問題があるアグリゲートの名前がイベント概要のテキストに表示されます。このアグリゲートに対して、ディスクを追加してデータを再構築

できます。

アグリゲートに追加できるのは、クラスタにすでに存在しているディスクだけです。クラスタに使用可能なディスクが残っていない場合は、必要に応じて管理者に問い合わせるか追加のディスクを購入してください。ONTAP System Manager または ONTAP コマンドを使用して、アグリゲートにディスクを追加できます。

"テクニカルレポート 3838 : 『Storage Subsystem Configuration Guide』"

Unified Manager サーバと外部データプロバイダ間の接続の設定

Unified Manager サーバと外部データプロバイダを接続すると、クラスタのパフォーマンスデータを外部サーバに送信できるので、ストレージ管理者は他社製ソフトウェアを使用してパフォーマンス指標をグラフ化できるようになります。

Unified Manager サーバと外部データプロバイダの間の接続は、メンテナンスコンソールの「External Data Provider」というメニューオプションを使用して確立されます。

外部サーバに送信可能なパフォーマンスデータ

Unified Manager は、監視対象のすべてのクラスタからさまざまなパフォーマンスデータを収集します。特定のデータグループを外部サーバに送信できます。

グラフ化するパフォーマンスデータに応じて、次のいずれかの統計グループを選択して送信できます。

統計グループ	データが含まれます	詳細
Performance Monitor の略	以下のオブジェクトのパフォーマンス統計の概要： <ul style="list-style-type: none">• LUN• 個のボリューム	このグループは、監視対象のすべてのクラスタ内のすべての LUN とボリュームの合計 IOPS / レイテンシを提供します。 提供する統計データが最も少ないグループです。
リソース利用率	次のオブジェクトのリソース利用率の統計情報： <ul style="list-style-type: none">• ノード• アグリゲート	このグループは、監視対象のすべてのクラスタ内のノードおよびアグリゲートの物理リソースの利用率に関する統計情報を提供します。 また、Performance Monitor グループで収集された統計も表示されます。

統計グループ	データが含まれます	詳細
ドリルダウンします	<p>すべての追跡対象オブジェクトの読み取り / 書き込み、およびプロトコルごとの低レベルの統計情報：</p> <ul style="list-style-type: none"> • ノード • アグリゲート • LUN • 個のボリューム • ディスク • LIF • ポート /NIC 	<p>このグループは、監視対象のすべてのクラスタで追跡される 7 つのオブジェクトタイプのすべてについて、読み取り / 書き込みおよびプロトコルごとの内訳データを提供します。</p> <p>また、Performance Monitor グループおよび Resource Utilization グループで収集された統計情報も表示されます。</p> <p>提供する統計データが最も多いグループです。</p>



ストレージシステム上でクラスタまたはクラスタオブジェクトの名前が変更された場合、古いオブジェクトと新しいオブジェクトの両方に外部サーバ上のパフォーマンスデータが含まれます（「両パス」）。2 つのオブジェクトが同じオブジェクトとして関連付けられることはありません。たとえば、ボリュームの名前を「volume1_acct」から「acct_vol1」に変更した場合は、古いボリュームの古いパフォーマンスデータと、新しいボリュームの新しいパフォーマンスデータが表示されます。

外部データプロバイダに送信可能なすべてのパフォーマンスカウンタの一覧については、ナレッジベースの記事 30096 を参照してください。

["外部データプロバイダにエクスポート可能な Unified Manager のパフォーマンスカウンタ"](#)

Unified Manager からパフォーマンスデータを受信するための Graphite の設定

Graphite は、コンピュータシステムからパフォーマンスデータを収集してグラフ化するオープンソフトウェアツールです。Unified Manager から統計データを受信するには、Graphite サーバとソフトウェアを適切に設定する必要があります。

ネットアップが、特定のバージョンの Graphite またはその他の他社製ツールをテストまたは検証することはありません。

インストール手順に従って Graphite をインストールしたら、Unified Manager から統計データを受信できるようにするために、次の変更を加える必要があります。

- を参照してください /opt/graphite/conf/carbon.conf ファイル。Graphiteサーバで1分間に作成できるファイルの最大数は、_200_に設定する必要があります (**MAX_CREATES_PER_MINUTE = 200**)。

構成内のクラスタ数や送信することを選択した統計オブジェクトによっては、最初に何千もの新しいファイルを作成する必要があります。1 分間に 200 個のファイルが生成されると、最初にすべての指標ファイルが作成されるまで 15 分以上かかることがあります。指標ファイルがすべて作成されると、このパラメータの値は不要になります。

- 導入したサーバでIPv6アドレスを使用してGraphiteを実行している場合は、のLINE_receiver_interfaceに

値を指定します /opt/graphite/conf/carbon.conf ファイルは「0.0.0.0」から「:」に変更する必要があります。(LINE_RECEIVER_INTERFACE = ::)

- を参照してください /opt/graphite/conf/storage-schemas.conf ファイル、retentions 頻度を5分、保持期間を環境に適した日数に設定するには、パラメータを使用する必要があります。

保持期間は環境で許容される範囲であればいくらでも長く設定できますが、頻度は最低 1 つの保持設定で 5 分に設定する必要があります。次の例では、を使用して Unified Manager 用のセクションを定義しています pattern パラメータを指定し、の値を指定して初期の頻度を5分、保持期間を100日に設定します。

[OPM]

```
pattern = ^netapp-performance\..
```

```
retentions = 5m:100d
```



デフォルトのベンダー・タグが「netapp-performance」から別のものに変更された場合は、その変更をに反映する必要があります pattern パラメータも指定します。



Unified Manager サーバがパフォーマンスデータを送信する際に Graphite サーバが使用できないとデータは送信されず、その間のデータは収集されません。

Unified Manager サーバから外部データプロバイダへの接続の設定

Unified Manager から外部サーバにクラスタのパフォーマンスデータを送信できます。送信する統計データの種類およびデータの送信間隔を指定できます。

- 必要なもの *
- Unified Manager サーバのメンテナンスコンソールへのログインが許可されているユーザ ID が必要です。
- 外部データプロバイダに関する次の情報が必要です。
 - サーバの名前または IP アドレス（IPv4 または IPv6）
 - サーバのデフォルトポート（デフォルトポート 2003 を使用していない場合）
- Unified Manager サーバから統計データを受信できるようにリモートサーバと他社製ソフトウェアを設定しておく必要があります。
- 送信する統計情報のグループを確認しておく必要があります。
 - performion_indicator : パフォーマンスモニタの統計情報
 - RESOURCE_UTILIZATION : リソース利用率とパフォーマンスモニタの統計データ
 - DRILL_DOWN : すべての統計データ
- 統計情報を送信する間隔を 5 分、10 分、または 15 分で指定する必要があります

デフォルトでは、Unified Manager は 5 分間隔で統計データを収集します。送信間隔を 10 分（または 15 分）に設定すると、各送信中に送信されるデータ量は、デフォルトの 5 分間隔を使用する場合の 2 倍（または 3 倍）になります。



Unified Manager のパフォーマンス収集間隔を 10 分または 15 分に変更した場合は、送信間隔も Unified Manager の収集間隔以上に変更する必要があります。

1 台の Unified Manager サーバと 1 台の外部データプロバイダサーバの間に接続を設定できます。

手順

1. Unified Manager サーバのメンテナンスコンソールにメンテナンスユーザとしてログインします。

Unified Manager メンテナンスコンソールのプロンプトが表示されます。

2. メンテナンスコンソールで、* 外部データプロバイダ * メニューオプションの番号を入力します。

External Server Connection (外部サーバ接続) メニューが表示されます。

3. [サーバー接続の追加 / 変更 *] メニューオプションの番号を入力します。

現在のサーバ接続情報が表示されます。

4. プロンプトが表示されたら、と入力します **y** 続行します。

5. プロンプトが表示されたら、宛先サーバの IP アドレスまたは名前、およびサーバポート情報を入力します (デフォルトポート 2003 と異なる場合)。

6. プロンプトが表示されたら、と入力します **y** 入力した情報が正しいことを確認します。

7. 任意のキーを押して、[External Server Connection] メニューに戻ります。

8. [サーバー構成の変更 *] メニューオプションの番号を入力します。

現在のサーバ設定情報が表示されます。

9. プロンプトが表示されたら、と入力します **y** 続行します。

10. プロンプトが表示されたら、送信する統計のタイプ、統計情報の送信間隔、および統計情報の送信を今すぐ有効にするかどうかを入力します。

用途	入力するコマンド
統計グループ ID	0 - performion_indicator (デフォルト) 1 - resource_utilizationを指定します 2 -ドリルダウン
ベンダータグ	統計情報を外部サーバに保存するフォルダのわかりやすい名前。デフォルト名は「netapp-performance」ですが、別の値を入力できます。 点線表記を使用すると、階層フォルダ構造を定義できます。たとえば、と入力します stats.performance.netapp 統計は、* stats > performance > NetApp *に保存されます。
送信間隔	5 (デフォルト)、 10 、または 15 分

用途	入力するコマンド
有効化 / 無効化	0 -無効 1 -有効（デフォルト）

11. プロンプトが表示されたら、と入力します **y** 入力した情報が正しいことを確認します。
12. 任意のキーを押して、[External Server Connection] メニューに戻ります。
13. を入力します **x** をクリックしてメンテナンスコンソールを終了します。

接続の設定が完了すると、選択したパフォーマンスデータが指定したサーバに指定した送信間隔で送信されます。指標が外部ツールに表示されるまでに数分かかります。新しい指標を表示するには、ブラウザの表示の更新が必要になる場合があります。

クラスタヘルスを監視および管理する

Active IQ Unified Manager の健全性監視の概要

Active IQ Unified Manager（旧 OnCommand Unified Manager）では、ONTAP ソフトウェアを実行する多数のシステムを一元化されたユーザインターフェイスで監視できます。Unified Manager サーバインフラは拡張性とサポート性に優れ、高度な監視機能と通知機能を備えています。

Unified Manager の主な機能には、クラスタの可用性と容量の監視 / 通知 / 管理、保護機能の管理、診断データの収集とテクニカルサポートへの送信などがあります。

Unified Manager を使用してクラスタを監視できます。クラスタで問題が発生すると、Unified Manager のイベントを通じて問題の詳細が通知されます。一部のイベントでは、問題を解決するための対応策も提示されます。問題が発生したときに E メールや SNMP トラップで通知されるように、イベントにアラートを設定することができます。

Unified Manager では、アノテーションを関連付けることで環境内のストレージオブジェクトを管理できます。カスタムアノテーションを作成し、ルールに基づいて動的にクラスタ、Storage Virtual Machine（SVM）、およびボリュームを関連付けることができます。

また、それぞれのクラスタオブジェクトについて、容量や健全性のグラフに表示される情報を使用してストレージ要件を計画することもできます。

物理容量と論理容量

Unified Manager は、ONTAP ストレージオブジェクトに使用される物理スペースと論理スペースの概念を利用します。

- 物理容量：物理スペースは、ボリュームで使用されているストレージの物理ブロックを表します。「物理使用容量」は、通常、ストレージ効率化機能（重複排除や圧縮など）からのデータ削減のため、使用済み論理容量よりも小さくなります。
- 論理容量：論理スペースは、ボリューム内の使用可能なスペース（論理ブロック）を表します。論理スペースとは、重複排除や圧縮の結果を考慮せずに、理論上のスペースをどのように使用できるかを指します。「Logical space used」は、使用済みの物理スペースに加えて、設定済みの Storage Efficiency 機能（重複排除や圧縮など）による削減量を示します。Snapshot コピー、クローン、その他のコンポーネントが含まれ、データ圧縮やその他の物理スペースの削減が反映されていないため、この測定値は、多くの場合、物理使用容量よりも大きく表示されます。したがって、合計論理容量は、プロビジョニング済みスペースよりも多くなる可能性があります。

容量の単位

Unified Manager は、1024（ 2^{10} ）バイトのバイナリ単位に基づいてストレージ容量を計算します。ONTAP 9.10.0 以前では、これらの単位は KB、MB、GB、TB、PB として表示されていました。ONTAP 9.10.1 以降、Unified Manager では KiB、MiB、GiB、TiB、および PiB として表示されます。



スループットに使用される単位は、すべてのリリースのONTAPについて、1秒あたりのキロバイト数（Kbps）、1秒あたりのメガバイト数（Mbps）、1秒あたりのギガバイト数（Gbps）、1秒あたりのテラバイト数（Tbps）などとなります。

Unified Manager for ONTAP 9.10.0 以前の容量ユニットが表示 されます	Unified Manager for ONTAP 9.10.1 で表示される容量の単位	計算	バイト単位の値
KB	KiB	1024	1024 バイト
MB	MiB	1024 * 1024	1、048、576 バイト
GB	GiB	1024 * 1024 * 1024	1,073,741,824 バイト
容量	TiB	1024 * 1024 * 1024 * 1024	1、099、511、627、 776 バイト

Unified Manager の健全性監視機能

Unified Manager のサービインフラは拡張性とサポート性に優れ、高度な監視機能と通知機能を備えています。Unified Manager では、ONTAP ソフトウェアを実行しているシステムの監視をサポートします。

Unified Manager には次の機能があります。

- ONTAP ソフトウェアがインストールされたシステムの検出、監視、通知
 - 物理オブジェクト：ノード、ディスク、ディスクシェルフ、SFO ペア、ポート、」を参照してください
 - 論理オブジェクト：クラスタ、Storage Virtual Machine（SVM）、アグリゲート、ボリューム、LUN、ネームスペース、qtree、LIF、Snapshot コピー、ジャンクションパス、NFS 共有、SMB 共有、ユーザクォータとグループクォータ、QoS ポリシーグループ、イニシエータグループ
 - プロトコル：CIFS、NFS、FC、iSCSI、NVMe および fcoe です
 - ストレージ効率化：SSD アグリゲート、Flash Pool アグリゲート、FabricPool アグリゲート、重複排除、圧縮
 - 保護：SnapMirror 関係（同期および非同期）および SnapVault 関係
- クラスタの検出と監視のステータスを表示します
- MetroCluster over FCおよびIP構成：クラスタコンポーネントの設定、問題、接続ステータスを表示および監視します。MetroCluster over FC構成用のMetroCluster スイッチおよびブリッジ
- アラート、イベント、およびしきい値インフラが強化されています
- LDAP、LDAPS、SAML 認証、およびローカルユーザのサポート
- RBAC（事前定義された一連のロール）
- AutoSupport とサポートバンドル
- ダッシュボードが強化され、環境の容量、可用性、保護、パフォーマンスなどの健全性が表示されるようになりました
- ボリューム移動の相互運用性、ボリューム移動の履歴、およびジャンクションパスの変更履歴

- 影響範囲：障害が発生したディスク、MetroCluster アグリゲートのミラーリングがデグレード状態、MetroCluster のスペアディスクなど、イベントの影響を受けるリソースがグラフィカルに表示されます
- MetroCluster イベントの影響を表示する有効範囲
- Suggested Corrective Actions area : Some Failed Disks 、 MetroCluster Aggregate Mirroring Degraded 、 MetroCluster Spare Disks Left Behind イベントなどのイベントに対処するために実行できる対処方法を表示します
- 「影響を受ける可能性があるリソース」領域には、「ボリュームがオフライン」イベント、「ボリュームが制限状態」イベント、「シンプロビジョニングボリュームにスペースリスクあり」イベントなどのイベントの影響を受ける可能性があるリソースが表示されます
- FlexVol または FlexGroup を備えた SVM がサポートされます
- ノードのルートボリュームの監視がサポートされます
- 再利用可能なスペースの計算や Snapshot コピーの削除など、Snapshot コピーの監視機能が強化されました
- ストレージオブジェクトのアノテーション
- 物理容量と論理容量、利用率、スペース削減率、パフォーマンス、関連イベントなど、ストレージオブジェクトの情報の作成と管理に関するレポート
- OnCommand Workflow Automation と統合してワークフローを実行

Storage Automation Store で、OnCommand Workflow Automation（WFA）用に開発されたネットアップ認定のストレージワークフロー自動化パックを提供しています。パックをダウンロードし、WFA にインポートして実行できます。自動化されたワークフローは、次の場所で入手でき

["Storage Automation Store の略"](#)

ストレージシステムの健全性を管理するために使用される **Unified Manager** のインターフェイス

ここでは、Active IQ Unified Manager でデータストレージの容量、可用性、保護に関する問題をトラブルシューティングするための2つのユーザインターフェイスについて説明します。2種類のUIとは、Unified Manager Web UI とメンテナンスコンソールです。

Unified Manager の保護機能を使用する場合は、OnCommand Workflow Automation（WFA）もインストールして設定する必要があります。

Unified Manager Web UI

Unified Manager Web UI では、管理者がデータストレージの容量、可用性、保護に関連するクラスタの問題を監視してトラブルシューティングすることができます。

これらのセクションでは、管理者がUnified Manager Web UIに表示されるストレージ容量、データの可用性、または保護に関する問題をトラブルシューティングする際に従う共通のワークフローについて説明します。

メンテナンスコンソール

Unified Manager のメンテナンスコンソールでは、管理者が Unified Manager サーバ自体に関連するオペレーティングシステムの問題、バージョンアップグレードの問題、ユーザアクセスの問題、およびネットワークの問題を監視し、診断し、対処することができます。Unified Manager Web UI を使用できない場合は、メンテ

ナンスコンソールが Unified Manager にアクセスする唯一の手段となります。

この情報は、メンテナンスコンソールにアクセスして Unified Manager サーバの機能に関連する問題を解決するために使用します。

クラスタおよびクラスタオブジェクトの健全性を管理および監視する

Unified Manager では、定期的な API クエリとデータ収集エンジンを使用してクラスタからデータが収集されます。Unified Manager データベースにクラスタを追加することで、そのクラスタの可用性と容量のリスクを監視して管理できるようになります。

クラスタの監視の概要

Unified Manager データベースにクラスタを追加して、クラスタの可用性や容量などの詳細を監視できます。CPU 使用率、インターフェイスの統計、空きディスクスペース、qtree 使用率、シャーシの環境などが監視されます。

ステータスが異常な場合や事前定義されたしきい値を超えた場合は、イベントが生成されます。イベントによってアラートがトリガーされたときに指定した受信者に通知を送信するように Unified Manager を設定することもできます。

ノードルートボリュームの概要

Unified Manager を使用して、ノードのルートボリュームを監視できます。ノードの停止を防ぐための十分な容量をノードのルートボリュームに確保しておくことを推奨します。

ノードのルートボリュームの使用容量がノードのルートボリュームの合計容量の 80% を超えると、「Node Root Volume Space Nearly Full」イベントが生成されます。通知を受け取るようにイベントのアラートを設定できます。ONTAP System Manager または ONTAP CLI を使用して、ノードの停止を防ぐための適切な処置を行うことができます。

ノードのルートアグリゲートのイベントとしきい値の概要

Unified Manager を使用して、ノードのルートアグリゲートを監視できます。ルートアグリゲート内のルートボリュームをシックプロビジョニングしてノードの停止を防ぐことを推奨します。

デフォルトでは、ルートアグリゲートについては容量とパフォーマンスのイベントは生成されません。また、Unified Manager で使用されるしきい値はノードのルートアグリゲートには適用されません。これらのイベントが生成されるように設定を変更できるのは、テクニカルサポート担当者だけです。テクニカルサポート担当者が設定を変更すると、容量のしきい値がノードのルートアグリゲートにも適用されるようになります。

ONTAP System Manager または ONTAP CLI を使用して、ノードの停止を防ぐための適切な処置を行うことができます。

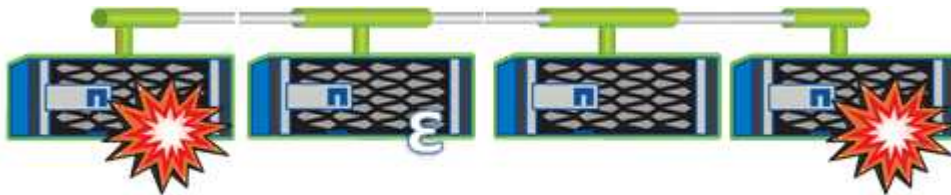
クォーラムとイプシロンについて

クォーラムとイプシロンは、クラスタの健全性と機能を判断するための重要な基準で、通信および接続に関する潜在的な問題へのクラスタの対応を決定します。

Quorum は、クラスタが完全に機能するための前提条件です。クラスタがクォーラムを構成している場合は、過半数のノードが正常で、相互に通信可能です。クォーラムが失われると、クラスタは通常のクラスタ処理を実行できなくなります。すべてのノードが1つのまとまりとしてデータの単一のビューを共有するため、任意の時点において1つのノードの集まりだけがクォーラムを構成することができます。したがって、通信が確立されていない2つのノードで、異なる方法でデータを変更することが許可されている場合には、データを1つのデータビューに表示できなくなります。

クラスタ内の各ノードはノードマスターを選出する投票プロトコルに属しており、マスター以外の各ノードはセカンダリとなります。マスターノードは、クラスタ内に情報を同期する役割を担います。形成されたクォーラムは継続的な投票によって維持されます。マスターノードがオフラインになった場合、クラスタでクォーラムが維持されていれば、オンラインのノードの投票によって新しいマスターが選出されます。

ノード数が偶数のクラスタの場合は同票となる可能性があるため、1つのノードにイプシロンと呼ばれる追加の投票荷重が設定されます。大規模なクラスタの同じ数のノード間で接続障害が発生した場合、すべてのノードが正常であることを条件に、イプシロンが設定されたノードのグループがクォーラムを維持します。たとえば、次の図では、4ノードクラスタの2つのノードで障害が発生しています。ただし、残りのノードの1つにイプシロンが設定されているため、正常なノードが過半数に満たなくてもクォーラムが維持されます。



クラスタが作成されると、自動的に最初のノードにイプシロンが割り当てられます。イプシロンを保持しているノードで障害が発生したり、ハイアベイラビリティパートナーをテイクオーバーしたり、ハイアベイラビリティパートナーにテイクオーバーされた場合、イプシロンは別の HA ペアの正常なノードに自動的に再割り当てされます。

ノードをオフラインにすると、クラスタがクォーラムを維持できるかどうかに影響することがあります。そのため ONTAP、クラスタのクォーラムが失われたり、あと1つのノード障害によってクォーラムが失われるような処理を実行しようとすると、警告メッセージが表示されます。クォーラムに関する警告メッセージを無効にするには、advanced 権限レベルで `cluster quorum-service options modify` コマンドを使用します。

一般に、クラスタのノード間に信頼性の高い接続が確立されている場合、小規模のクラスタよりも大規模のクラスタの方が安定します。ノードの半数にイプシロンを加えた過半数のクォーラムの要件は、2ノードのクラスタよりも24ノードのクラスタの方が簡単に維持できます。

2ノードクラスタでは、クォーラムの維持に独特な課題が存在します。2ノードクラスタでは、どちらのノードにもイプシロンが設定されていないクラスタ HA を使用します。代わりに、両方のノードを継続的にポーリングすることで、一方のノードで障害が発生した場合に、もう一方のノードでデータに対する読み取り / 書き込みのフルアクセスが許可されるとともに、論理インターフェイスと管理機能にアクセス

クラスタリストおよび詳細の表示

Health : All Clusters ビューを使用すると、クラスタのインベントリを表示できま

す。Capacity：All Clusters ビューでは、すべてのクラスタのストレージ容量と使用状況についてまとめた情報を表示できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

個々のクラスタの健全性、容量、構成、LIF、ノードなどの詳細を表示することもできます。クラスタのディスクや健全性の詳細ページで確認できます。

健全性：すべてのクラスタビュー、容量：すべてのクラスタビュー、およびクラスタ / 健全性の詳細ページで、ストレージを計画する際に役立ちます。たとえば、新しいアグリゲートをプロビジョニングする前に、特定のクラスタを Health：All Clusters ビューで選択し、容量の詳細を取得して必要なスペースがクラスタにあるかどうかを確認できます。

手順

1. 左側のナビゲーションペインで、* Storage * > * Clusters * をクリックします。
2. [表示] メニューで、[* 健全性：すべてのクラスタ * 表示] を選択して健全性情報を表示するか、[* 容量：すべてのクラスタ * 表示] を選択してすべてのクラスタのストレージ容量と使用率に関する詳細を表示します。
3. クラスタの名前をクリックし、クラスタ / 健全性 * の詳細ページにクラスタのすべての詳細を表示します。
 - 関連情報 *
 - ["クラスタ / 健全性の詳細ページ"](#)
 - ["パフォーマンス：すべてのクラスタビュー"](#)
 - ["MetroCluster 構成を監視しています"](#)
 - ["クラスタとStorage VMのセキュリティステータスの表示"](#)
 - ["評価されるセキュリティ条件"](#)

MetroCluster 構成のクラスタの健全性を確認しています

Active IQ Unified Manager（Unified Manager）を使用して、MetroCluster over FCおよびMetroCluster over IP構成のクラスタとそのコンポーネントの運用の健全性を確認できます。Unified Manager によって検出されたパフォーマンスイベントにクラスタが関連している場合は、健全性ステータスを確認することで、ハードウェアまたはソフトウェアの問題がイベントの一因となったかどうかを判断できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- MetroCluster 構成のパフォーマンスイベントを分析し、関連するクラスタの名前を取得しておく必要があります。
- MetroCluster 構成の両方のクラスタをFC経由で、IPアドレスがUnified Managerの同じインスタンスで監視する必要があります。

MetroCluster over FC構成でのクラスタの健全性を確認しています

MetroCluster over FC構成でのクラスタの健全性を確認するには、次の手順を実行します。

手順

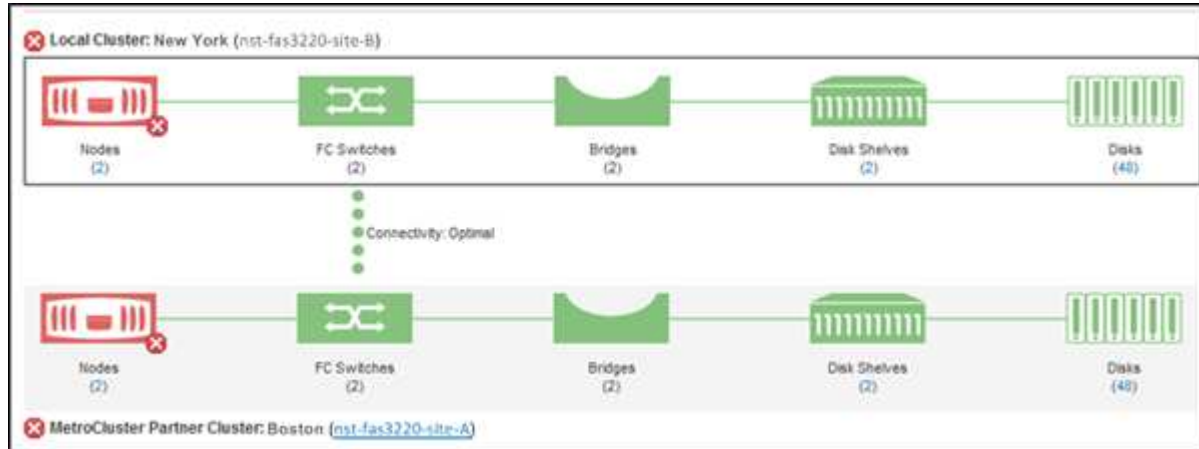
1. 左側のナビゲーションペインで、* イベント管理 * をクリックしてイベントリストを表示します。
2. フィルタパネルで、「* ソースタイプ *」カテゴリの下の「すべての MetroCluster」フィルタを選択します。すべてのMetroCluster 構成について、環境で生成されたすべてのイベントが表示されます。
3. MetroCluster イベントの横にあるクラスタの名前をクリックします。



MetroCluster イベントが表示されない場合は、検索バーを使用して、MetroCluster over FC の構成に関連するイベントに関連するクラスタの名前を検索できます。

Health : All Clusters ビューにイベントに関する詳細情報が表示されます。

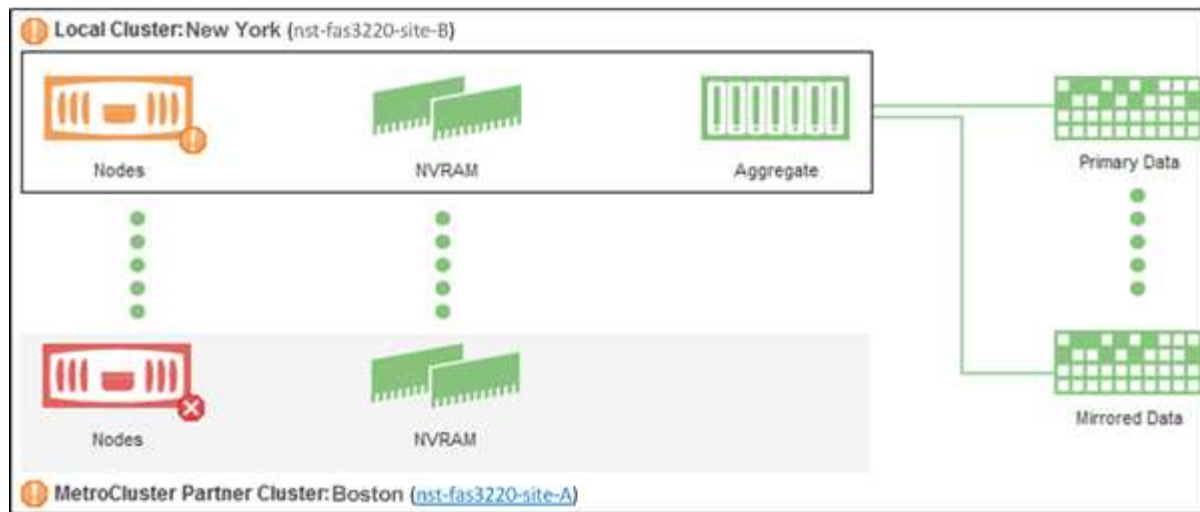
4. MetroCluster Connectivity * タブを選択して、選択したクラスタとそのパートナークラスタ間の接続のヘルスを表示します。



この例では、ローカルクラスタとそのパートナークラスタの名前とコンポーネントが表示されています。黄色または赤のアイコンは、強調表示されているコンポーネントの健全性イベントを示しています。接続アイコンは、クラスタ間のリンクを表します。アイコンにマウスカーソルを合わせると、イベント情報を表示できます。アイコンをクリックすると、イベントを表示できます。どちらかのクラスタの健全性問題がパフォーマンスイベントの一因である可能性があります。

Unified Manager は、クラスタ間のリンクの NVRAM コンポーネントを監視します。ローカルクラスタまたはパートナークラスタの FC スイッチアイコンまたは接続アイコンが赤の場合は、問題がパフォーマンスイベントの原因となっている可能性があります。

5. MetroCluster レプリケーション * タブを選択します。



この例では、ローカルクラスタまたはパートナークラスタの NVRAM アイコンが黄色または赤の場合、NVRAM を搭載したヘルス問題がパフォーマンスイベントの原因となった可能性があります。ページ上に赤または黄色のアイコンがない場合は、パートナークラスタ上のパフォーマンス問題がパフォーマンスイベントの原因である可能性があります。

MetroCluster over IP構成でのクラスタの健全性を確認しています

MetroCluster over IP構成でクラスタの健全性を確認するには、次の手順を実行します。

手順

1. 左側のナビゲーションペインで、* イベント管理 * をクリックしてイベントリストを表示します。
2. フィルターパネルの*ソースタイプ*カテゴリーで、を選択します MetroCluster Relationship フィルタ：すべてのMetroCluster 構成について、環境で生成されたすべてのイベントが表示されます。



レポートされたMetroCluster イベントが表示されない場合は、検索バーを使用して、MetroCluster over IPの設定に関連するイベントに関連するクラスタの名前で検索できます。

3. 関連するMetroCluster イベントの横にあるクラスタの名前をクリックします。クラスタページが開き、そのクラスタの詳細が表示されます。正常性の問題の判別については、を参照してください "[MetroCluster over IP構成で接続の問題を監視します](#)"。

オール SAN アレイクラスタの健全性と容量のステータスの表示

クラスタインベントリページでは、オール SAN アレイクラスタの健全性と容量のステータスを表示できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

すべての SAN アレイクラスタについて、「健全性：すべてのクラスタ」ビューと「容量：すべてのクラスタ」ビューで概要情報を確認できます。また、クラスタ / 健全性の詳細ページで詳細を確認できます。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Clusters * をクリックします。
2. 「パーソナリティ」列が * 正常性：すべてのクラスタ * ビューに表示されていることを確認するか、 * 表示 / 非表示 * コントロールを使用して追加します。

この列には 'すべての SAN アレイクラスタのすべての SAN アレイが表示されます

3. 情報を確認します。
4. これらのクラスタのストレージ容量に関する情報を表示するには、 Capacity : All Clusters ビューを選択します。
5. これらのクラスタの健全性とストレージ容量に関する詳細情報を表示するには、オール SAN アレイクラスタの名前をクリックします。

クラスタ / 健全性の詳細ページの健全性、容量、およびノードタブで詳細を確認します

ノードリストおよび詳細の表示

Health : All Nodes ビューを使用すると、クラスタ内のノードのリストを表示できます。クラスタ / 健全性の詳細ページを使用して、監視対象のクラスタに含まれるノードに関する詳細情報を表示できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ノードの状態、ノードを含むクラスタ、アグリゲートの容量の詳細（使用容量と合計容量）、物理容量の詳細（使用可能な容量、スペア容量、合計容量）などの詳細情報を参照できます。HA ペア、ディスクシェルフ、およびポートに関する情報を取得することもできます。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Nodes * をクリックします。
2. [* 正常性：すべてのノード *] ビューで、詳細を表示するノードをクリックします。

選択したノードの詳細情報がクラスタ / 健全性の詳細ページに表示されます。左側のペインには、HA ペアのリストが表示されます。デフォルトでは、HA の詳細が表示され、選択した HA ペアに関連する HA 状態の詳細とイベントが表示されます。

3. ノードに関するその他の詳細を表示するには、該当する操作を実行します。

表示する内容	をクリックします
ディスクシェルフの詳細	• ディスクシェルフ * :
ポート関連の情報	• ポート * :

詳細については、を参照してください

- ["Performance : All Nodesビュー"](#)

- "ノードとアグリゲートの使用可能な IOPS の値の表示"
- "ノードとアグリゲートの使用済みパフォーマンス容量の値の表示"

契約更新用のハードウェアインベントリレポートの生成

ハードウェアのモデル番号とシリアル番号、ディスクのタイプと数、インストールされているライセンスなど、クラスターとノードのすべての情報を含むレポートを生成できます。このレポートは、NetAppActive IQ プラットフォームに接続されていないセキュアなサイト（「ディレクトリ」）で契約更新を行う際に役立ちます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、*** Storage * > * Nodes *** をクリックします。
2. 「*** Health : All Nodes * view**」または「*** Performance : All Nodes * view**」に移動します。
3. **Reports * >> Hardware Inventory Report*** を選択します。

ハードウェアインベントリレポートは、.csv ファイルとしてダウンロードされ、現在の日付以降の完全な情報が表示されます。

4. この情報をネットアップのサポート担当者に提供して契約更新を申請します。

Storage VM リストおよび詳細を表示しています

Health : All Storage VM ビューで、Storage Virtual Machine（SVM）のインベントリを監視できます。Storage VM / 健全性の詳細ページを使用して、監視対象の SVM に関する詳細情報を表示できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

SVM の容量、効率、構成など、SVM の詳細を表示できます。また、その SVM に関連するデバイスやアラートに関する情報も参照できます。

手順

1. 左側のナビゲーションペインで、*** Storage * > * Storage VM*** をクリックします。
2. 次のいずれかの方法を選択して SVM の詳細を表示します。
 - すべてのクラスターのすべての SVM の健全性に関する情報を表示するには、表示メニューで健全性：すべての Storage VM ビューを選択します。
 - すべての詳細を表示するには、Storage VM 名をクリックします。

詳細を表示するには、[最小詳細] ダイアログボックスの [詳細の表示] をクリックします。

3. 最小限の詳細ダイアログボックスで * 関連項目の表示 * をクリックすると、SVM に関連するオブジェクトが表示されます。
 - 関連情報 *
 - ["Storage VM：健全性の詳細ページ"](#)
 - ["Performance：All Storage VMビュー"](#)
 - ["セキュリティ：ランサムウェア対策ビュー"](#)
 - ["クラスタとStorage VMのセキュリティステータスの表示"](#)
 - ["関係：すべての関係ビュー"](#)

アグリゲートリストおよび詳細を表示する

Health：All aggregates ビューでは、アグリゲートのインベントリを監視できます。Capacity：All Aggregates ビューでは、すべてのクラスタのアグリゲートの容量と使用状況に関する情報を確認できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

アグリゲートの容量と構成、ディスク情報などの詳細をアグリゲート / 健全性の詳細ページで確認できます。必要に応じて、しきい値を設定する前にこれらの詳細を使用できます。

手順

1. 左側のナビゲーションペインで、* Storage * > * Aggregates * をクリックします。
2. 次のいずれかの方法を選択してアグリゲートの詳細を表示します。
 - すべてのクラスタ内のすべてのアグリゲートの健全性に関する情報を表示するには、表示メニューで健全性：すべてのアグリゲート表示を選択します。
 - すべてのクラスタ内のすべてのアグリゲートの容量と使用状況に関する情報を表示するには、表示メニューで容量：すべてのアグリゲートビューを選択します。
 - すべての詳細を表示するには、アグリゲート名をクリックします。

詳細を表示するには、[最小詳細] ダイアログボックスの [詳細の表示] をクリックします。

3. 最小限の詳細ダイアログボックスで * 関連項目の表示 * をクリックして、アグリゲートに関連するオブジェクトを表示します。
 - 関連情報 *
 - ["アグリゲート / 健全性の詳細ページ"](#)
 - ["パフォーマンス：すべてのアグリゲートが表示されます"](#)
 - ["アグリゲート容量レポートのカスタマイズ"](#)

FabricPool の容量情報を表示しています

クラスタ、アグリゲート、およびボリュームの FabricPool 容量情報は、容量とパフォー

マンスのインベントリページおよびこれらのオブジェクトの詳細ページで確認できます。これらのページには、ミラー階層が構成されている場合の FabricPool ミラー情報も表示されます。

これらのページには、ローカルの高パフォーマンス階層とクラウド階層の使用可能容量、両方の階層で使用されている容量、クラウド階層に接続されているアグリゲート、 また、特定の情報をクラウド階層に移動することで FabricPool 機能を実装しているボリュームもあります。

クラウド階層が別のクラウドプロバイダ（「ミラー階層」）にミラーリングされている場合、両方のクラウド階層がアグリゲート / 健全性の詳細ページに表示されます。

手順

- 1. 次のいずれかを実行します。

容量の情報を表示するオブジェクト	手順
クラスタ	<div>a. Capacity : All Clusters ビューで、クラスタをクリックします。</div> <div>b. クラスタ / ヘルスの詳細ページで、 * 構成 * タブをクリックします。</div> <div>このクラスタが接続されているクラウド階層の名前が表示されます。</div>
アグリゲート	<div>a. Capacity : All Aggregates ビューで、Type フィールドに「`S SD (FabricPool) `」または「HDD (FabricPool) 」と表示されているアグリゲートをクリックします。</div> <div>b. アグリゲート / 健全性の詳細ページで、 * 容量 * タブをクリックします。</div> <div>クラウド階層で使用されている合計容量が表示されます。</div> <div>c. [ディスク情報] タブをクリックします。</div> <div>クラウド階層の名前と使用済み容量が表示されます。</div> <div>d. [* 構成 *] タブをクリックします。</div> <div>クラウド階層の名前とクラウド階層に関するその他の詳細情報が表示されます。</div>

容量の情報を表示するオブジェクト	手順
個のボリューム	<p>a. Capacity : All Volumes（容量：すべてのボリューム）ビューで、「Tiering Policy」（階層化ポリシー）フィールドにポリシー名が表示されているボリュームをクリックします。</p> <p>b. [Volume/Health details] ページで、[Configuration] タブをクリックします。</p> <p>ボリュームに割り当てられている FabricPool 階層化ポリシーの名前が表示されます。</p>

2. [* ワークロード分析 *] ページで、[容量の傾向 *] 領域の [クラウド階層ビュー] を選択すると、前月のローカルパフォーマンス階層とクラウド階層で使用されている容量を確認できます。

FabricPool アグリゲートの詳細については、を参照してください "[ディスクとアグリゲートの概要](#)"。

ストレージプールの詳細を表示しています

ストレージプールの詳細を表示して、ストレージプールの健全性、合計キャッシュと使用可能なキャッシュ、使用済みの割り当てと使用可能な割り当てを監視できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* Storage * > * Aggregates * をクリックします。
2. アグリゲート名をクリックします。

選択したアグリゲートの詳細が表示されます。

3. [ディスク情報] タブをクリックします。

詳細なディスク情報が表示されます。



キャッシュテーブルは、選択したアグリゲートでストレージプールが使用されている場合にのみ表示されます。

4. キャッシュテーブルで、目的のストレージプールの名前にカーソルを合わせます。

ストレージプールの詳細が表示されます。

ボリュームリストおよび詳細を表示します

Health : All Volumes ビューでは、ボリュームのインベントリを監視できます。Capacity : All Volumes ビューでは、クラスタ内のボリュームの容量と使用状況に

関する情報を表示できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

また、ボリューム / 健全性の詳細ページでは、ボリュームの容量、効率、設定、保護など、監視対象のボリュームに関する詳細情報を確認することもできます。また、特定のボリュームに関連するデバイスやアラートに関する情報も参照できます。

手順

1. 左側のナビゲーションペインで、* Storage * > * Volumes * をクリックします。
2. 次のいずれかの方法を選択してボリュームの詳細を表示します。
 - クラスタ内のボリュームの健全性に関する詳細情報を表示するには、ビューメニューで健全性：すべてのボリュームビューを選択します。
 - クラスタ内のボリュームの容量と使用状況に関する詳細情報を表示するには、表示メニューで容量：すべてのボリュームビューを選択します。
 - すべての詳細を表示するには、ボリューム名をクリックします。

詳細を表示するには、[最小詳細] ダイアログボックスの [詳細の表示] をクリックします。

3. * オプション：最小限の詳細ダイアログボックスで * 関連項目を表示 * をクリックして、ボリュームに関連するオブジェクトを表示します。
 - 関連情報 *
 - ["ボリューム：健全性の詳細ページ"](#)
 - ["Performance：All Volumesビュー"](#)
 - ["セキュリティ：ランサムウェア対策ビュー"](#)
 - ["ボリュームの保護関係を表示しています"](#)
 - ["使用可能なボリューム容量グラフを表示するレポートの作成"](#)

NFS 共有に関する詳細の表示

すべての NFS 共有について、ステータス、ボリューム（FlexGroup ボリュームまたは FlexVol ボリューム）に関連付けられているパス、NFS 共有に対するクライアントのアクセスレベル、エクスポートされているボリュームに定義されているエクスポートポリシーなどの詳細情報を表示できます。すべての監視対象クラスタ上のすべての NFS 共有を表示するには、Health：All NFS Shares ビューを使用し、Storage VM/Health 詳細ページを使用して特定の Storage Virtual Machine（SVM）上のすべての NFS 共有を表示します。

- 必要なもの *
- クラスタで NFS ライセンスが有効になっている必要があります。
- NFS 共有を提供するネットワークインターフェイスが設定されている必要があります。
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ステップ

1. すべての NFS 共有を表示するか特定の SVM の NFS 共有を表示するかに応じて、左側のナビゲーションペインで次の手順を実行します。

目的	実行する手順
すべての NFS 共有を表示する	[* ストレージ > NFS 共有 *] をクリックします
単一の SVM の NFS 共有を表示する	a. Storage * > * Storage VM* をクリックします b. NFS 共有の詳細を表示する SVM をクリックします。 c. Storage VM / Health の詳細ページで、 * NFS Shares * タブをクリックします。

詳細については、を参照してください ["ファイル共有ボリュームのプロビジョニング"](#) および ["APIを使用したCIFSおよびNFSファイル共有のプロビジョニング"](#)。

SMB / CIFS 共有に関する詳細の表示

すべての SMB/CIFS 共有について、共有名、ジャンクションパス、コンテナオブジェクト、セキュリティ設定、共有に対して定義されているエクスポートポリシーなどの詳細情報を表示できます。すべての監視対象クラスタ上のすべての SMB 共有を表示するには Health : All SMB Shares ビューを使用し、Storage VM/Health 詳細ページを使用して特定の Storage Virtual Machine (SVM) 上のすべての SMB 共有を表示します。

- 必要なもの *
- クラスタで CIFS ライセンスが有効になっている必要があります。
- SMB / CIFS 共有を提供するネットワークインターフェイスが設定されている必要があります。
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。



フォルダ内の共有は表示されません。

ステップ

1. すべての SMB / CIFS 共有を表示するか特定の SVM の共有を表示するかに応じて、左側のナビゲーションペインで次の手順を実行します。

目的	実行する手順
すべての SMB/CIFS 共有を表示します	[* ストレージ > SMB 共有 *] をクリックします

目的	実行する手順
単一の SVM の SMB/CIFS 共有を表示します	a. Storage * > * Storage VM* をクリックします b. SMB / CIFS 共有の詳細を表示する SVM をクリックします。 c. Storage VM / Health の詳細ページで、 * SMB Shares * タブをクリックします。

詳細については、を参照してください ["APIを使用したCIFSおよびNFSファイル共有のプロビジョニング"](#)。

Snapshot コピーリストを表示しています

選択したボリュームの Snapshot コピーのリストを表示できます。Snapshot コピーのリストを使用すると、1 つ以上の Snapshot コピーが削除された場合に再利用可能なディスクスペースの量を計算できます。また、必要に応じて Snapshot コピーを削除できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- Snapshot コピーを含むボリュームがオンラインになっている必要があります。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Volumes * をクリックします。
2. * Health : All Volumes * ビューで、表示する Snapshot コピーが含まれているボリュームを選択します。
3. [* Volume/Health * details] ページで、 [* Capacity*] タブをクリックします。
4. [容量 *] タブの [* 詳細 *] ペインの [その他の詳細] セクションで、 [* Snapshot コピー *] の横のリンクをクリックします。

Snapshot コピーの数はリンクになっており、クリックすると Snapshot コピーのリストが表示されます。

- 関連情報 *

["ケンシヨウセイ / ホリユウムヘエシ"](#)

Snapshot コピーを削除しています

スペースを節約したりディスクスペースを解放したりする場合、または Snapshot コピーが不要になった場合、Snapshot コピーを削除できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

ボリュームはオンラインである必要があります。

使用中またはロック状態の Snapshot コピーを削除する場合は、Snapshot コピーを使用しているアプリケー

ションからそのコピーを解放しておく必要があります。

- FlexClone ボリュームが親ボリューム内のベースの Snapshot コピーを使用している場合、その Snapshot コピーは削除できません。

ベースの Snapshot コピーは、FlexClone ボリュームを作成するために使用される Snapshot コピーで、ステータスが表示されます *Busy* とアプリケーション依存関係 *Busy*, *Vclone* をクリックします。

- SnapMirror 関係で使用されているロックされた Snapshot コピーは削除できません。

この Snapshot コピーはロックされており、次の更新に必要です。

手順

1. 左側のナビゲーションペインで、** Storage ** > ** Volumes ** をクリックします。
2. ** Health : All Volumes ** ビューで、表示する Snapshot コピーが含まれているボリュームを選択します。

Snapshot コピーのリストが表示されます。

3. [** Volume/Health ** details] ページで、[** Capacity **] タブをクリックします。
4. [容量 *] タブの [** 詳細 **] ペインの [その他の詳細] セクションで、[** Snapshot コピー **] の横のリンクをクリックします。

Snapshot コピーの数はリンクになっており、クリックすると Snapshot コピーのリストが表示されます。

5. Snapshot コピー * ビューで、削除する Snapshot コピーを選択し、** 選択した削除 ** をクリックします。

Snapshot コピーの再利用可能なスペースを計算しています

1 つ以上の Snapshot コピーを削除した場合に再利用可能となるディスクスペースの量を計算できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- ボリュームはオンラインである必要があります。
- ボリュームは FlexVol ボリュームである必要があります。FlexGroup ボリュームでは、この機能はサポートされていません。

手順

1. 左側のナビゲーションペインで、** Storage ** > ** Volumes ** をクリックします。
2. ** Health : All Volumes ** ビューで、表示する Snapshot コピーが含まれているボリュームを選択します。

Snapshot コピーのリストが表示されます。

3. [** Volume/Health ** details] ページで、[** Capacity **] タブをクリックします。
4. [容量 *] タブの [** 詳細 **] ペインの [その他の詳細] セクションで、[** Snapshot コピー **] の横のリンクをクリックします。

Snapshot コピーの数はリンクになっており、クリックすると Snapshot コピーのリストが表示されます。

5. 「 * Snapshot copies * 」ビューで、再利用可能なスペースを計算する Snapshot コピーを選択します。
6. [Calculate] をクリックします。

ボリューム上の再利用可能なスペース（割合、KB、MB、GB など）が表示されます。

7. 再利用可能なスペースを再計算するには、必要な Snapshot コピーを選択し、 * 再計算 * をクリックします。

クラスタオブジェクトのウィンドウとダイアログボックスの概要

それぞれのストレージオブジェクトのページで、すべてのクラスタおよびクラスタオブジェクトを表示できます。対応するストレージオブジェクトの詳細ページで詳細を確認することもできます。インベントリの次のストレージおよび保護セクションから System Manager ユーザインターフェイスを起動できるようになりました。

- クラスタインベントリ、クラスタヘルス、およびクラスタパフォーマンスの各ページ
- アグリゲートのインベントリページ、アグリゲートの健全性ページ、およびアグリゲートのパフォーマンスページ
- ボリュームのインベントリ、ボリュームの健全性、およびボリュームのパフォーマンスの各ページ
- ノードのインベントリページとノードのパフォーマンスページ
- StorageVM Inventory、StorageVM Health、StorageVM Performance の各ページ
- 保護関係のページ

Unified Manager の一般的な健全性関連のワークフローとタスク

Unified Manager に関連する一般的な管理ワークフローと管理タスクには、監視対象のストレージクラスタの選択、データの可用性 / 容量 / 保護に悪影響を及ぼす状態の診断、消失したデータのリストア、ボリュームの設定と管理、診断データのバンドルとテクニカルサポートへの送信（必要時）などがあります。

Unified Manager では、ストレージ管理者がダッシュボードを表示して管理対象ストレージクラスタの全体的な容量、可用性、保護の状態の健全性を評価できるほか、発生の可能性のある具体的な問題を突き止めて確認し、診断を行い、解決のための割り当てを行うことができます。

管理対象ストレージオブジェクトのストレージ容量やデータ可用性に影響する、クラスタ、Storage Virtual Machine（SVM）、ボリューム、または FlexGroup ボリュームに関連した最も重要な問題が、ダッシュボードページのシステムヘルスグラフおよびイベントに表示されます。重要な問題が特定されると、このページに適切なトラブルシューティングワークフローをサポートするためのリンクが表示されます。

Unified Manager は、OnCommand Workflow Automation（WFA）などの関連管理ツールを含むワークフローにも含まれており、ストレージリソースを直接設定できます。

このドキュメントでは、次の管理タスクに関連する一般的なワークフローについて説明します。

- 可用性の問題を診断および管理する

ハードウェア障害やストレージリソース構成に問題がある場合、原因のダッシュボードページにデータ可用性イベントが表示されます。ストレージ管理者は、埋め込まれたリンクに従って、該当するストレージリソースに関する接続情報を確認し、トラブルシューティングのアドバイスを参照し、他の管理者に問題の解決を割り当てることができます。

- パフォーマンスインシデントの設定と監視

管理者は、監視対象のストレージシステムリソースのパフォーマンスを監視し、管理することができます。を参照してください ["Active IQ Unified Manager によるパフォーマンス監視の概要"](#) を参照してください。

- ボリューム容量の問題を診断および管理する

ボリュームストレージ容量の問題がダッシュボードページに表示された場合、ストレージ管理者はリンク先を参照して該当するボリュームのストレージ容量に関連する現在と過去の傾向を確認し、トラブルシューティングのアドバイスを参照して、他の管理者に問題の解決を割り当てることができます。

- 保護関係の設定、監視、問題の診断

保護関係を作成して設定したあと、ストレージ管理者は、保護関係に関連する潜在的な問題、保護関係の現在の状態、該当する関係に対して成功した現在と過去の保護ジョブの情報、およびトラブルシューティングのアドバイスを確認できます。を参照してください ["保護関係の作成、監視、およびトラブルシューティング"](#) を参照してください。

- バックアップファイルの作成とバックアップファイルからのデータのリストア
- ストレージオブジェクトへのアノテーションの関連付け

ストレージ管理者は、ストレージオブジェクトにアノテーションを関連付けることで、ストレージオブジェクトに関連するイベントをフィルタリングして表示できます。これにより、イベントに関連する問題に優先順位を付けて解決することができます。

- REST API を使用すると、Unified Manager で収集された健全性、容量、パフォーマンスの情報を確認することができます。クラスタの管理に便利です。を参照してください ["Active IQ Unified Manager REST API の使用を開始する"](#) を参照してください。
- テクニカルサポートへのサポートバンドルの送信

ストレージ管理者は、メンテナンスコンソールを使用して、サポートバンドルを取得し、テクニカルサポートに送信できます。問題で AutoSupport メッセージよりも詳しい診断とトラブルシューティングが必要な場合は、サポートバンドルをテクニカルサポートに送信する必要があります。

データの可用性の監視とトラブルシューティング

Unified Manager は、許可されたユーザが格納データにアクセスできる信頼性を監視し、アクセスのブロックや妨害をもたらしている状態をユーザに警告します。また、ユーザがその状態を診断して解決方法を決定し、追跡することができます。

このセクションで取り上げる可用性関連のワークフローのトピックでは、ストレージ管理者が Unified Manager Web UI を使用して、データの可用性に悪影響を与えるハードウェアとソフトウェアの状態を検出、診断、および解決方法の決定を行う方法の例を説明します。

ストレージフェイルオーバーインターコネクトリンクの停止状態をスキャンして解決しています


このワークフローでは、ストレージフェイルオーバーインターコネクトリンクの停止状態をスキャンし、評価して解決する方法の例を示します。このシナリオでは、管理者が、ノードで ONTAP バージョンのアップグレードを開始する前に Unified Manager を使用してストレージフェイルオーバーのリスクがないかをスキャンします。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

無停止アップグレードの実行中に HA ペアノード間のストレージフェイルオーバーインターコネクトで障害が発生すると、アップグレードは失敗します。そのため、一般的には、管理者がアップグレードの開始前にアップグレード対象のクラスタノードでストレージフェイルオーバーの信頼性を監視して確認します。

手順

1. 左側のナビゲーションペインで、* イベント管理 * をクリックします。
2. [* イベント管理 *] インベントリページで、[アクティブな可用性イベント *] を選択します。
3. [* イベント管理 * インベントリページ * 名前 *] 列の上部で、をクリックします  と入力します
*failover ストレージフェイルオーバー関連のイベントだけを表示する場合は、テキストボックスに表示されます。

ストレージフェイルオーバーの状態に関連する過去のイベントがすべて表示されます。

このシナリオでは、Unified Manager の [可用性のインシデント] セクションに「ストレージフェイルオーバーインターコネクトの 1 つ以上のリンクが停止」というイベントが表示されます。

4. イベント管理 * インベントリページにストレージフェイルオーバーに関連するイベントが 1 つ以上表示された場合は、次の手順を実行します。
 - a. イベントタイトルのリンクをクリックすると、そのイベントの詳細が表示されます。

この例では、「ストレージフェイルオーバーインターコネクト 1 つ以上のリンクがダウン」というイベントタイトルをクリックします。

そのイベントのイベントの詳細ページが表示されます。

- a. イベントの詳細ページで、次のタスクを 1 つ以上実行できます。
 - 原因フィールドのエラーメッセージを確認し、問題を評価します。
 - イベントを管理者に割り当てます。
 - イベントに応答します。
 - 関連情報 *

["イベントの詳細ページ"](#)

["Unified Manager のユーザロールと機能"](#)

ストレージフェイルオーバー関連イベントのイベントの詳細ページを表示して、ページの概要情報を確認し、イベントの緊急性、問題の原因の候補、問題への解決策を特定できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

この例では、イベントの詳細ページに表示されるイベントの概要に、ストレージフェイルオーバーインターコネクトリンクの停止状態に関する次の情報が表示されます。

```
Event: Storage Failover Interconnect One or More Links Down
```

```
Summary
```

```
Severity: Warning
```

```
State: New
```

```
Impact Level: Risk
```

```
Impact Area: Availability
```

```
Source: aardvark
```

```
Source Type: Node
```

```
Acknowledged By:
```

```
Resolved By:
```

```
Assigned To:
```

```
Cause: At least one storage failover interconnected link  
       between the nodes aardvark and bonobo is down.  
       RDMA interconnect is up (Link0 up, Link1 down)
```

このイベント情報から、HA ペアの aardvark ノードと bonobo ノードの間のストレージフェイルオーバーインターコネクトリンク Link1 が停止している一方で、Apple と Boy の間の Link0 はアクティブであることがわかります。一方のリンクがアクティブであるため、Remote Dynamic Memory Access（RDMA）は引き続き機能し、ストレージフェイルオーバージョブも正常に実行されます。

ただし、両方のリンクが停止してストレージのフェイルオーバー保護が完全に無効になる状態を防ぐために、Link1 が停止した理由を詳しく診断することにします。

手順

1. イベント * の詳細ページで、ソースフィールドで指定されたイベントへのリンクをクリックすると、ストレージフェイルオーバーインターコネクトリンクの停止状態に関連するその他のイベントの詳細を確認できます。

この例では、aardvark というノードがイベントのソースです。そのノード名をクリックすると、該当する HA ペア aardvark および bonobo の HA の詳細がクラスタ / 健全性の詳細ページのノードタブに表示され、影響を受けた HA ペアで最近発生したその他のイベントが表示されます。

2. イベントに関連する詳細情報については、HA の詳細を確認してください。

この例では、関連する情報が Events テーブルに表示されています。この表には、「ストレージフェイルオーバー接続 1 つ以上のリンク停止」イベント、イベントが生成された時刻、およびこのイベントの生成元のノードが表示されます。

HA の詳細で確認したノードの場所情報を使用して、該当する HA ペアノードでのストレージフェイルオーバー問題の物理的な調査と修復を依頼するか、または自ら実施します。

- 関連情報 *

["イベントの詳細ページ"](#)

["Unified Manager のユーザロールと機能"](#)

ボリュームのオフライン状態の問題を解決する

このワークフローでは、Unified Manager のイベント管理インベントリページに表示されるボリュームオフラインイベントを評価して解決する方法の例を示します。このシナリオでは、管理者が Unified Manager を使用してボリュームオフラインイベントをトラブルシューティングします。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ボリュームがオフライン状態と報告された場合は、いくつかの理由が考えられ

- SVM 管理者が意図的にボリュームをオフラインにした。
- ボリュームをホストしているクラスタノードが停止し、その HA ペアパートナーへのストレージフェイルオーバーも失敗した。
- ボリュームをホストしている SVM のルートボリュームをホストしているノードが停止したために、SVM が停止した。
- 2 つの RAID ディスクで同時に障害が発生したために、ボリュームをホストしているアグリゲートが停止した。

イベント管理インベントリページおよびクラスタ / 健全性、Storage VM / 健全性、およびボリューム / 健全性の詳細ページを使用して、これらの可能性を確認したり、それらを除外したりできます。

手順

1. 左側のナビゲーションペインで、* イベント管理 * をクリックします。
2. [* イベント管理 *] インベントリページで、[アクティブな可用性イベント *] を選択します。
3. 「ボリュームはオフライン」イベントのハイパーテキストリンクをクリックします。

可用性インシデントのイベント詳細ページが表示されます。

4. このページで、SVM 管理者が対象のボリュームをオフラインにしたことを示すメモがないか確認します。
5. イベント * の詳細ページで、次のタスクの 1 つ以上に関する情報を確認できます。
 - 原因（診断）フィールドに表示された情報を確認して、考えられる診断ガイダンスを確認します。

この例では、原因フィールドの情報から、ボリュームがオフラインであることのみがわかります。

- Notes and Updates 領域で、SVM 管理者が該当のボリュームを意図的にオフラインにしたかどうかを確認します。
- イベントのソースをクリックすると、オフラインとして報告されるボリュームをクリックすると、そのボリュームに関する詳細情報が表示されます。
- イベントを管理者に割り当てます。
- イベントに応答するか、必要に応じて解決済みとしてマークします。

ボリュームがオフライン状態になった場合の診断処置の実施

オフラインと報告されたボリュームのボリューム / 健全性の詳細ページに移動したら、ボリュームのオフライン状態を診断するのに役立つ追加情報を検索できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

オフラインと報告されたボリュームが、意図的にオフラインにされたのではない場合は、いくつかの理由が考えられます。

オフラインボリュームのボリューム / 健全性の詳細ページから他のページやペインに移動して、考えられる原因を確認するかどうかを確認することができます。

- ボリューム / 健全性 * の詳細ページのリンクをクリックして、ボリュームのオフライン状態の原因が、ホストノードの停止およびその HA ペアパートナーへのストレージフェイルオーバーの失敗であるかどうかを確認します。

を参照してください ["ボリュームのオフライン状態の原因がノードの停止であるかどうかを判別します"](#)。

- ボリューム / 健全性 * の詳細ページのリンクをクリックして、ボリュームがオフラインで、その SVM のルートボリュームをホストしているノードが停止したためにホストしている Storage Virtual Machine (SVM) が停止していないかを確認します。

を参照してください ["ボリュームのオフライン状態と SVM の停止の原因がノードの停止であるかどうかの判別"](#)。

- ボリューム / 健全性 * の詳細ページのリンクをクリックして、ボリュームがオフラインになっている原因がホストアグリゲート内の破損ディスクであるかどうかを確認します。

を参照してください ["ボリュームのオフライン状態の原因がアグリゲート内の破損ディスクであるかどうかを判別しています"](#)。

- 関連情報 *

["Unified Manager のユーザロールと機能"](#)

ボリュームのオフライン状態の原因がホストノードの停止であるかどうかを判別します

Unified Manager Web UI を使用して、ボリュームがオフラインになっている原因が、ボ

リユームのホストノードの停止およびその HA ペアパートナーへのストレージフェイルオーバーの失敗であるかどうかを確認することができます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ボリュームのオフライン状態の原因が、ホストノードの障害とその後のストレージフェイルオーバーの失敗であるかどうかを判別するには、次の手順を実行します。


手順

1. オフラインボリュームの「 * Volume/Health * details 」ページの「 * Related Devices * 」ペインに表示されたハイパーテキストリンクを探してクリックします。


Storage VM / Health の詳細ページには、オフラインボリュームのホスト Storage Virtual Machine （ SVM ）に関する情報が表示されます。

2. Storage VM/Health * の詳細ページの * Related Devices * ペインで、 Volumes の下に表示されるハイパーテキストリンクを探してクリックします。

Health ： All Volumes ビューには、 SVM でホストされているすべてのボリュームに関する情報が表形式で表示されます。

3. [* 正常性：すべてのボリューム * 表示状態] 列ヘッダーで、フィルタシンボルをクリックします  をクリックし、オプション * Offline * を選択します。

オフライン状態の SVM ボリュームのみが表示されます。

4. Health ： All Volumes ビューで、グリッド記号をクリックします  をクリックし、オプション * Cluster Nodes * を選択します。

グリッド選択ボックスをスクロールして * Cluster Nodes * オプションを探します。

ボリュームインベントリに Cluster Nodes 列が追加され、各オフラインボリュームをホストするノードの名前が表示されます。

5. * Health ： All Volumes * ビューでオフラインボリュームのリストを探し、そのクラスタノード列でホストノードの名前をクリックします。

クラスタ / 健全性の詳細ページのノードタブには、ホストノードが属している HA ペアの状態が表示されます。ホストノードの状態とクラスタフェイルオーバー処理の成功を示すメッセージが表示されます。

ボリュームのオフライン状態の原因が、そのホストノードの停止および HA ペアパートナーへのストレージフェイルオーバーの失敗であることを確認したら、適切な管理者またはオペレータに連絡して、停止したノードの手動による再起動とストレージフェイルオーバーの問題の解決を依頼します。

ボリュームのオフライン状態とその **SVM** の停止の原因がノードの停止であるかどうかの判別

Unified Manager Web UI を使用して、ボリュームがオフラインになっている原因が、そのホスト Storage Virtual Machine （ SVM ）のルートボリュームをホストするノードの停止に起因して SVM が停止したためであるかどうかを確認することができます。

- 必要なもの *


オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ボリュームのオフライン状態の原因が、そのホスト SVM のルートボリュームをホストするノードの停止に起因する SVM の停止であるかどうかを判別するには、次の手順を実行します。


手順

1. オフラインボリュームの「* Volume/Health * details」ページの「* Related Devices *」ペインに表示されたハイパーテキストリンクを探してクリックします。

Storage VM/Health の詳細ページには、ホスト SVM の「Running」または「's's'」のステータスが表示されます。SVM のステータスが「実行中」である場合は、ボリュームのオフライン状態の原因が、その SVM のルートボリュームをホストするノードの停止ではないことがわかります。

2. SVM のステータスが stopped になっていることを確認するには、* SVM の表示 * をクリックして、停止しているホスト SVM の原因を特定します。
3. [* Health: All Storage VMs] ビューの [SVM] 列ヘッダーで、フィルタ記号をクリックします  停止している SVM の名前を入力します。

その SVM の情報が表形式で表示されます。

4. [* Health: All Storage VMs] ビューで、 をクリックします。次に、オプション * Root Volume * を選択します。

SVM インベントリにルートボリューム列が追加され、停止している SVM のルートボリュームの名前が表示されます。

5. Root Volume 列で、ルートボリュームの名前をクリックして、そのボリュームの * Storage VM / Health * の詳細ページを表示します。

SVM ルートボリュームのステータスが（オンライン）の場合は、元のボリュームのオフライン状態の原因が、その SVM ルートボリュームをホストするノードの停止ではないことがわかります。

6. SVM ルートボリュームのステータスが（オフライン）の場合は、SVM ルートボリュームのボリューム / 健全性の詳細ページの関連デバイスペインに表示されているハイパーテキストリンクを探してクリックします。
7. Aggregate の「* Aggregate/Health * details」ページの「* Related Devices *」ペインに表示されているハイパーテキストリンクを探してクリックします。

クラスタ / 健全性の詳細ページのノードタブには、SVM ルートボリュームのホストノードが属しているノードの HA ペアの状態が表示されます。ノードの状態が画面に示されます。

ボリュームのオフライン状態の原因が、そのボリュームのホスト SVM のオフライン状態であり、さらにその状態の原因が SVM のルートボリュームをホストするノードの停止であることを確認したら、適切な管理者またはオペレータに連絡して、停止したノードを手動で再起動するように依頼します。

ボリュームのオフライン状態の原因がアグリゲート内の破損ディスクであるかどうかを判別しています

Unified Manager Web UI を使用して、ボリュームがオフラインになっている原因が、RAID ディスクの問題によりそのホストアグリゲートがオフラインになったためである

かどうかを確認することができます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ボリュームのオフライン状態の原因が、RAID ディスクの問題によりホストアグリゲートがオフラインになったためであるかどうかを判別するには、次の手順を実行します。

手順

1. 「* Volume/Health * details」ページの「Aggregate」（アグリゲート）に表示されているハイパーテキストリンクを探してクリックします。

アグリゲート / 健全性の詳細ページに、ホストアグリゲートのオンラインまたはオフラインのステータスが表示されます。アグリゲートのステータスが「オンライン」の場合、RAID ディスクの問題は、オフラインになっているボリュームの原因ではありません。

2. アグリゲートのステータスがオフラインの場合は、* ディスク情報 * をクリックし、* ディスク情報 * タブの * イベント * リストで破損ディスクイベントを探します。
3. 破損ディスクをさらに特定するには、[**Related Devices**（関連デバイス）] ペインの [Node（ノード）] に表示されるハイパーテキストリンクをクリックします。

クラスタ / 健全性の詳細ページが表示されます。

4. [* ディスク] をクリックし、[* フィルタ *] ペインで [* 破損 *] を選択して、破損状態のすべてのディスクを一覧表示します。

破損状態のディスクが原因でホストアグリゲートがオフラインになった場合は、「Impacted Aggregate」列にアグリゲートの名前が表示されます。

ボリュームのオフライン状態の原因が、RAID ディスクの破損とそれによるホストアグリゲートのオフライン状態であることを確認したら、適切な管理者またはオペレータに連絡し、手動による破損ディスクの交換とアグリゲートをオンラインに戻す処理を依頼します。

容量の問題を解決する

このワークフローでは、容量問題を解決する方法の例を示します。このシナリオでは、管理者またはオペレータが Unified Manager のダッシュボードページにアクセスして、監視対象のストレージオブジェクトに容量の問題がないかどうかを確認します。問題に対する原因の候補と解決策を特定する。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ダッシュボードページでは ' イベントのドロップダウン・リストの下にある Capacity パネルで ' Volume Space Full エラー・イベントを探します

手順

1. ダッシュボード * ページの * 容量 * パネルで、ボリュームスペースがフルエラーイベントの名前をクリッ

クします。

エラーのイベントの詳細ページが表示されます。

2. イベント * の詳細ページでは、次のタスクを 1 つ以上実行できます。

- 原因フィールドのエラーメッセージを確認し、Suggested Remedial Actions の下の提案をクリックして、考えられる修正方法の説明を確認します。
- オブジェクトの詳細を表示するには、ソースフィールドでオブジェクト名（この場合はボリューム）をクリックします。
- このイベントに関して追加されたメモを探します。
- イベントにメモを追加します。
- イベントを別のユーザに割り当てます。
- イベントに応答します。
- イベントを解決済みとマークします。
 - 関連情報 *

"イベントの詳細ページ"

ボリュームがフルになった場合の推奨修正策の実施

「ボリューム容量がいっぱいです」エラーイベントを受け取った後、イベントの詳細ページで推奨される修正策を確認し、推奨されるアクションのいずれかを実行することになります。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

Unified Manager を使用するこのワークフロー内のタスクは、どのロールのユーザでも実行できます。

この例では、Unified Manager のイベント管理インベントリページで「ボリュームスペースがフル」エラーイベントが表示されたので、そのイベントの名前をクリックしています。

ボリュームがフルになった場合に実施できる修正策には、次のものがあります。

- ボリュームに対して自動拡張、重複排除、または圧縮を有効にする
- ボリュームをサイズ変更するか、移動しています
- ボリュームからデータを削除または移動する

これらのすべての操作は ONTAP System Manager または ONTAP CLI から実行する必要がありますが、実行する操作を決定するために必要な情報は Unified Manager で確認できます。

手順

1. イベント * の詳細ページで、ソースフィールドのボリューム名をクリックすると、該当するボリュームの詳細が表示されます。
2. ボリューム / 健全性 * の詳細ページで * Configuration * をクリックすると、ボリュームで重複排除と圧縮

がすでに有効になっていることがわかります。

ボリュームのサイズを変更することにします。

3. **Related Devices *** ペインで、ホスティングアグリゲートの名前をクリックすると、アグリゲートがボリュームの拡張に対応できるかどうかわかります。
4. **アグリゲート / 健全性 *** の詳細ページには、フルボリュームをホストしているアグリゲートにコミットされていない容量が十分にあることが表示されます。そのため、ONTAP システムマネージャを使用してボリュームのサイズを変更し、容量を拡大します。
 - **関連情報 ***

"イベントの詳細ページ"

健全性しきい値の管理

すべてのアグリゲート、ボリューム、および qtree に適用されるグローバル健全性しきい値を設定して、健全性しきい値の違反を追跡することができます。

ストレージ容量の健全性しきい値とは

ストレージ容量の健全性しきい値は、ストレージオブジェクトに関する容量の問題を報告するために Unified Manager サーバがイベントを生成するポイントです。そのようなイベントが発生するたびに通知を送信するようにアラートを設定できます。

すべてのアグリゲート、ボリューム、および qtree のストレージ容量の健全性しきい値がデフォルト値に設定されます。設定は、オブジェクトまたはオブジェクトのグループに対して必要に応じて変更できます。

グローバル健全性しきい値を設定します

アグリゲート、ボリューム、および qtree のサイズを効果的に監視できるように、容量、増加率、Snapshot リザーブ、クォータ、および inode について、グローバル健全性しきい値の条件を設定することができます。また、遅延しきい値を超えた場合にイベントを生成する設定を編集することもできます。

グローバル健全性しきい値の設定は、アグリゲートやボリュームなど、関連付けられているすべてのオブジェクトに適用されます。しきい値を超えるとイベントが生成され、アラートが設定されている場合はアラート通知も送信されます。しきい値はデフォルトで推奨値に設定されていますが、それらの値を変更することでイベントが生成される間隔をニーズに合わせて調整することができます。しきい値を変更した場合、次の監視サイクルから反映され、その値に基づいてイベントが生成または廃止されます。

グローバル健全性しきい値の設定には、左側のナビゲーションメニューの「イベントしきい値」セクションからアクセスできます。また、個々のオブジェクトのインベントリページまたは詳細ページから、そのオブジェクトのしきい値の設定を変更することもできます。

- 詳細については、を参照してください ["アグリゲートのグローバル健全性しきい値を設定します"](#)。

すべてのアグリゲートに対する容量、増加率、および Snapshot コピーの健全性しきい値を設定して、しきい値の違反を追跡することができます。

- 詳細については、を参照してください ["ボリュームのグローバル健全性しきい値を設定しています"](#)。

容量、Snapshot コピー、qtree クォータ、ボリューム増加率、オーバーライトリザーブスペースの健全性しきい値の設定を編集することができます。しきい値の違反を追跡するには、すべてのボリュームの inode を使用します。

- 詳細については、を参照してください ["qtree のグローバル健全性しきい値を設定しています"](#)。

すべての qtree に対する容量の健全性しきい値の設定を編集して、しきい値の違反を追跡することができます。

- 詳細については、を参照してください ["管理対象外の保護関係の遅延健全性しきい値の編集"](#)。

警告やエラーの遅延時間の割合を増やしたり減らしたりすることで、イベントが生成される間隔をニーズに合わせて調整することができます。

アグリゲートのグローバル健全性しきい値を設定します

すべてのアグリゲートに対するグローバル健全性しきい値を設定して、しきい値の違反を追跡することができます。しきい値の違反が発生すると該当するイベントが生成されるため、それらのイベントに基づいて予防策を講じることが可能です。監視対象のすべてのアグリゲートに適用されるしきい値について、ベストプラクティスの設定に基づいてグローバルな値を設定することができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

オプションをグローバルレベルで設定すると、オブジェクトのデフォルト値が変更されます。ただし、オブジェクトレベルでデフォルト値が変更されている場合、グローバルな値は変更されません。

しきい値のオプションは、効果的に監視できるようにデフォルトで値が設定されています。ただし、それぞれの環境の要件に合わせて値を変更することができます。

アグリゲートに配置されているボリュームで自動拡張が有効になっている場合は、元のボリュームサイズではなく、自動拡張で設定された最大ボリュームサイズに基づいて、アグリゲートの容量のしきい値を超えているかどうか判定されます。



ノードのルートアグリゲートには健全性しきい値の値は適用されません。

手順

1. 左側のナビゲーションペインで、* イベントしきい値 * > * 集計 * をクリックします。
2. 容量、増加率、および Snapshot コピーのしきい値を必要に応じて設定します。
3. [保存 (Save)] をクリックします。

◦ 関連情報 *

["ユーザを追加する"](#)

ボリュームのグローバル健全性しきい値を設定しています

すべてのボリュームに対するグローバル健全性しきい値を設定して、しきい値の違反を追跡することができます。健全性しきい値の違反が発生すると該当するイベントが生成されるため、それらのイベントに基づいて予防策を講じることが可能です。監視対象のすべてのボリュームに適用されるしきい値について、ベストプラクティスの設定に基づいてグローバルな値を設定することができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

ほとんどのしきい値のオプションは、効果的に監視できるようにデフォルト値が設定されていますただし、それぞれの環境の要件に合わせて値を変更することができます。

ボリュームで自動拡張が有効になっている場合は、元のボリュームサイズではなく、自動拡張で設定された最大ボリュームサイズに基づいて、容量のしきい値を超えているかどうか判定されることに注意してください。



デフォルト値の 1000 は、ONTAP のバージョンが 9.4 以降である FlexVol ボリューム、および ONTAP のバージョンが 9.8 以降である FlexGroup ボリュームにのみ適用されます。古いバージョンの ONTAP ソフトウェアがインストールされたクラスタの場合、ボリュームあたりの Snapshot コピーの最大数は 250 です。このような古いバージョンでは、Unified Manager はこの数 1000（および 1000 ~ 250 の任意の数）を 250 と解釈します。つまり、Snapshot コピーの数が 250 に達してもイベントは引き続き受信します。これらの古いバージョンでこのしきい値を 250 未満に設定する場合は、しきい値を 250 以下に設定するか、Health : All Volumes ビューまたは Volume/Health details ページで設定する必要があります。

手順

1. 左側のナビゲーションペインで、* イベントしきい値 * > * 音量 * をクリックします。
2. 容量、Snapshot コピー、qtree クォータ、ボリューム増加率、および inode について、適切なしきい値を設定します。
3. [保存 (Save)] をクリックします。
 - 関連情報 *

"ユーザを追加する"

qtree のグローバル健全性しきい値を設定しています

すべての qtree に対するグローバル健全性しきい値を設定して、しきい値の違反を追跡することができます。健全性しきい値の違反が発生すると該当するイベントが生成されるため、それらのイベントに基づいて予防策を講じることが可能です。監視対象のすべての qtree に適用されるしきい値について、ベストプラクティスの設定に基づいてグローバルな値を設定することができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

しきい値のオプションは、効果的に監視できるようにデフォルトで値が設定されています。ただし、それぞれの環境の要件に合わせて値を変更することができます。

qtree についてのイベントが生成されるのは、qtree に対して qtree クォータまたはデフォルトクォータが設定されている場合だけです。ユーザクォータまたはグループクォータで定義されているスペースがしきい値を超えてもイベントは生成されません。

手順

1. 左側のナビゲーションペインで、* イベントしきい値 * > * qtree * をクリックします。
2. 容量のしきい値を必要に応じて設定します。
3. [保存 (Save)] をクリックします。

管理対象外の保護関係の遅延しきい値を設定しています

管理対象外の保護関係のデフォルトの遅延警告しきい値と遅延エラー健全性しきい値のグローバルな設定を編集して、それぞれのニーズに適した間隔でイベントを生成することができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

遅延時間は定義されている転送スケジュールの間隔よりも短い必要があります。たとえば、転送スケジュールが 1 時間ごとの場合、遅延時間は 1 時間未満でなければなりません。遅延しきい値では、遅延時間が超えてはならない割合を指定します。たとえば、1 時間の例で遅延しきい値が 150% と定義されている場合、遅延時間が 1.5 時間を超えるとイベントが生成されます。

このタスクで説明する設定は、管理対象外のすべての保護関係にグローバルに適用されます。管理対象外の 1 つの保護関係に対して、設定を個別に指定して適用することはできません。

手順

1. 左側のナビゲーションペインで、* イベントしきい値 * > * 関係 * をクリックします。
2. 警告またはエラーの遅延時間を増減して、デフォルトのグローバル設定を変更します。
3. 遅延しきい値の値を超えて警告またはエラーイベントがトリガーされないようにするには、「* enabled *」の横のボックスをオフにします。
4. [保存 (Save)] をクリックします。
 - 関連情報 *

"ユーザを追加する"

個々のアグリゲートの健全性しきい値の設定を編集

1 つ以上のアグリゲートの容量、増加率、および Snapshot コピーについての健全性しきい値の設定を編集することができます。しきい値を超えるとアラートが生成され、通知が送信されます。これらの通知は、生成されたイベントに基づいて予防策を講じるのに役立ちます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

しきい値の値を変更すると、次の監視サイクルから、その値に基づいてイベントが生成または廃止されます。

アグリゲートに配置されているボリュームで自動拡張が有効になっている場合は、元のボリュームサイズではなく、自動拡張で設定された最大ボリュームサイズに基づいて、アグリゲートの容量のしきい値を超えているかどうか判定されます。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Aggregates * をクリックします。
2. * Health : All Aggregates * ビューで 1 つ以上のアグリゲートを選択し、 * Edit Thresholds * をクリックします。
3. アグリゲートのしきい値の編集 * ダイアログボックスで、該当するチェックボックスを選択して値を変更し、容量、増加率、または Snapshot コピーのしきい値の設定を編集します。
4. [保存 (Save)] をクリックします。

- 関連情報 *

"ユーザを追加する"

個々のボリュームの健全性しきい値の設定を編集し

1 つ以上のボリュームの容量、増加率、クォータ、およびスペースリザーベーションについての健全性しきい値の設定を編集することができます。しきい値を超えるとアラートが生成され、通知が送信されます。これらの通知は、生成されたイベントに基づいて予防策を講じるのに役立ちます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

しきい値の値を変更すると、次の監視サイクルから、その値に基づいてイベントが生成または廃止されます。

ボリュームで自動拡張が有効になっている場合は、元のボリュームサイズではなく、自動拡張で設定された最大ボリュームサイズに基づいて、容量のしきい値を超えているかどうか判定されることに注意してください。



デフォルト値の 1000 は、ONTAP のバージョンが 9.4 以降である FlexVol ボリューム、および ONTAP のバージョンが 9.8 以降である FlexGroup ボリュームにのみ適用されます。古いバージョンの ONTAP ソフトウェアがインストールされたクラスタの場合、ボリュームあたりの Snapshot コピーの最大数は 250 です。このような古いバージョンでは、Unified Manager はこの数 1000（および 1000 ~ 250 の任意の数）を 250 と解釈します。つまり、Snapshot コピーの数が 250 に達してもイベントは引き続き受信します。これらの古いバージョンでこのしきい値を 250 未満に設定する場合は、しきい値を 250 以下に設定するか、Health : All Volumes ビューまたは Volume/Health details ページで設定する必要があります。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Volumes * をクリックします。
2. * 健全性：すべてのボリューム * 表示で、1 つ以上のボリュームを選択し、* しきい値の編集 * をクリックします。
3. ボリュームしきい値の編集 * ダイアログボックスで、該当するチェックボックスを選択して値を変更し、容量、Snapshot コピー、qtree クォータ、増加率、または inode についてのしきい値の設定を編集します。
4. [保存 (Save)] をクリックします。
 - 関連情報 *

"ユーザを追加する"

個々の **qtree** の健全性しきい値の設定を編集する

1 つ以上の qtree の容量についての健全性しきい値の設定を編集することができます。しきい値を超えるとアラートが生成され、通知が送信されます。これらの通知は、生成されたイベントに基づいて予防策を講じるのに役立ちます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

しきい値の値を変更すると、次の監視サイクルから、その値に基づいてイベントが生成または廃止されます。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Qtrees * をクリックします。
2. 容量：すべての qtree * ビューで 1 つ以上の qtree を選択し、しきい値の編集 * をクリックします。
3. Edit Qtree Thresholds * ダイアログボックスで、選択した qtree または qtree の容量しきい値を変更し、* Save * をクリックします。



また、Storage VM / Health の詳細ページの qtree タブで個々の qtree しきい値を設定することもできます。

クラスタのセキュリティ目標の管理

Unified Manager には、『ONTAP 9_NetApp Security Hardening Guide for ONTAP』に定義されている推奨事項を基に、クラスタ、Storage Virtual Machine (SVM)、およびボリュームがどの程度セキュアであるかを示すダッシュボードが用意されています。

セキュリティダッシュボードの目的は、ONTAP クラスタがネットアップ推奨のガイドラインに従っていない領域を提示して、潜在的な問題を修正できるようにすることです。ほとんどの場合、問題は ONTAP System Manager または ONTAP CLI を使用して解決します。組織がすべての推奨事項に従うとは限らないため、場合によっては変更を加える必要がありません。

を参照してください ["ONTAP 9 セキュリティ設定ガイド"](#) 詳細な推奨事項と解決策については、TR-4569 を参照してください。

Unified Manager は、セキュリティステータスを報告するだけでなく、セキュリティ違反があるクラスタまたは SVM に対してセキュリティイベントを生成します。これらの問題はイベント管理インベントリページで追跡できます。また、イベントにアラートを設定して、新たなセキュリティイベントが発生したときにストレージ管理者が通知を受け取るようにすることができます。

詳細については、を参照してください ["評価されるセキュリティ条件"](#)。

評価されるセキュリティ条件

一般に、ONTAP クラスタ、Storage Virtual Machine（SVM）、およびボリュームのセキュリティ条件は、『ONTAP 9 ネットアップセキュリティ設定ガイド』に定義されている推奨事項に照らして評価されます。

セキュリティチェックには、次のようなものがあります。

- クラスタが SAML などのセキュアな認証方式を使用しているかどうか
- ピアクラスタの通信が暗号化されているかどうか
- Storage VM の監査ログが有効になっているかどうか
- ボリュームでソフトウェアまたはハードウェアの暗号化が有効になっているかどうか

コンプライアンスのカテゴリおよびのトピックを参照してください ["ONTAP 9 セキュリティ設定ガイド"](#) を参照してください。



Active IQ プラットフォームから報告されるアップグレードイベントもセキュリティイベントとみなされます。これらのイベントは、ONTAP ソフトウェア、ノードファームウェア、またはオペレーティングシステムソフトウェア（セキュリティアドバイザリ用）のアップグレードが必要な問題を示します。これらのイベントは[セキュリティ]パネルには表示されませんが、[イベント管理]インベントリページから確認できます。

詳細については、を参照してください ["クラスタのセキュリティ目標の管理"](#)。

クラスタコンプライアンスのカテゴリ

次の表に、Unified Manager で評価されるクラスタセキュリティコンプライアンスのパラメータ、ネットアップの推奨事項、およびクラスタが準拠か非準拠かの総合的な判断にパラメータが影響するかどうかを示します。

クラスタに非準拠の SVM があると、クラスタのコンプライアンスに影響します。そのため、クラスタのセキュリティが準拠とみなされるためには、事前に SVM のセキュリティ問題の修正が必要となる場合があります。

以下のパラメータは、すべてのインストール環境で表示されるわけではありません。たとえば、ピアクラスタがない場合やクラスタで AutoSupport を無効にしている場合、「クラスタピアリング」や「AutoSupport HTTPS 転送」の項目は表示されません。

パラメータ	説明	推奨事項	クラスタコンプライアンスに影響します
グローバル FIPS	グローバル FIPS（連邦情報処理標準）140-2 準拠モードが有効になっているかどうかを示します。FIPS を有効にすると、TLSv1 と SSLv3 は無効になり、TLSv1.1 と TLSv1.2 のみが許可されます。	有効	はい。
Telnet	システムへの Telnet アクセスが有効になっているかどうかを示します。ネットアップでは、セキュアなリモートアクセスのために Secure Shell（SSH）を推奨しています。	無効	はい。
セキュアでない SSH 設定	SSH でセキュアでない暗号を使用しているかどうかを示します。たとえば、CBC で始まる暗号などです。	いいえ	はい。
ログインバナー	システムにアクセスするユーザに対してログインバナーが有効になっているかどうかを示します。	有効	はい。
クラスタピアリング	ピアクラスタ間の通信が暗号化されているかどうかを示します。このパラメータが準拠とみなされるためには、ソースとデスティネーションの両方のクラスタで暗号化が設定されている必要があります。	暗号化	はい。

パラメータ	説明	推奨事項	クラスタコンプライアンスに影響します
Network Time Protocol の略	クラスタに NTP サーバが 1 つ以上設定されているかどうかを示します。ネットアップでは、冗長性と最適なサービスを実現するために最低 3 台の NTP サーバをクラスタに関連付けることを推奨しています。	を設定します	はい。
OCSP	ONTAP に OCSP (Online Certificate Status Protocol) が設定されていないアプリケーションがないか、そのため通信が暗号化されていないかどうかを示します。非標準のアプリケーションが一覧表示されます。	有効	いいえ
リモート監査ログ	ログ転送 (syslog) が暗号化されているかどうかを示します。	暗号化	はい。
AutoSupport HTTPS 転送	ネットアップサポートに AutoSupport メッセージを送信するためのデフォルトの転送プロトコルとして HTTPS が使用されているかどうかを示します。	有効	はい。
デフォルトの管理ユーザ	デフォルトの管理ユーザ (組み込み) が有効になっているかどうかを示します。ネットアップでは、不要な組み込みアカウントはすべてロック (無効化) することを推奨しています。	無効	はい。
SAML ユーザ	SAML が設定されているかどうかを示します。SAML を使用すると、シングルサインオンのログイン方法として多要素認証 (MFA) を設定できます。	いいえ	いいえ

パラメータ	説明	推奨事項	クラスタコンプライアンスに影響します
Active Directory ユーザ	Active Directory が設定されているかどうかを示します。Active Directory と LDAP は、クラスタにアクセスするユーザに対して推奨される認証メカニズムです。	いいえ	いいえ
LDAP ユーザ	LDAP が設定されているかどうかを示します。Active Directory と LDAP は、ローカルユーザよりもクラスタを管理するユーザに対して推奨される認証メカニズムです。	いいえ	いいえ
証明書ユーザ	証明書ユーザがクラスタにログインするように設定されているかどうかを示します。	いいえ	いいえ
ローカルユーザ	ローカルユーザがクラスタにログインするように設定されているかどうかを示します。	いいえ	いいえ
リモートシェル (Remote Shell)	RSH が有効になっているかどうかを示します。セキュリティ上の理由から、RSH は無効にする必要があります。セキュアなリモートアクセスを実現するために、Secure Shell (SSH) が推奨されます。	無効	はい。
MD5 使用中です	ONTAP ユーザアカウントでセキュアでない MD5 ハッシュ関数を使用しているかどうかを示します。MD5 ハッシュ化されたユーザアカウントは、SHA-512 などのより安全な暗号化ハッシュ関数への移行が推奨されます。	いいえ	はい。

パラメータ	説明	推奨事項	クラスタコンプライアンスに影響します
証明書発行者タイプ	使用されているデジタル証明書のタイプを示します。	CA 署名	いいえ

Storage VM コンプライアンスのカテゴリ

次の表に、 Unified Manager で評価される Storage Virtual Machine （ SVM ）セキュリティコンプライアンスの条件、ネットアップの推奨事項、および SVM が準拠か非準拠かの総合的な判断にパラメータが影響するかどうかを示します。

パラメータ	説明	推奨事項	SVM コンプライアンスに影響します
監査ログ	監査ロギングが有効になっているかどうかを示します。	有効	はい。
セキュアでない SSH 設定	SSHでセキュアでない暗号（で始まる暗号など）を使用しているかどうかを示します cbc*。	いいえ	はい。
ログインバナー	システムで SVM にアクセスするユーザに対してログインバナーが有効になっているかどうかを示します。	有効	はい。
LDAP 暗号化	LDAP 暗号化が有効になっているかどうかを示します。	有効	いいえ
NTLM 認証	NTLM 認証が有効になっているかどうかを示します。	有効	いいえ
LDAP ペイロードの署名	LDAP ペイロードの署名が有効になっているかどうかを示します。	有効	いいえ
CHAP 設定	CHAP が有効になっているかどうかを示します。	有効	いいえ

パラメータ	説明	推奨事項	SVM コンプライアンスに影響 します
Kerberos V5	Kerberos v5 認証が有効か無効かを示します。	有効	いいえ
NIS 認証	NIS 認証の使用が設定されているかどうかを示します。	無効	いいえ
FPolicy ステータスがアクティブです	FPolicy が作成されているかどうかを示します。	はい。	いいえ
SMB 暗号化が有効です	SMB 署名と封印が有効になっていないかどうかを示します。	はい。	いいえ
SMB 署名が有効になりました	SMB 署名が有効になっていないかどうかを示します。	はい。	いいえ

ボリュームコンプライアンスのカテゴリ

Unified Manager は、次の表に示すボリューム暗号化パラメータを評価して、ボリューム上のデータが権限のないユーザによるアクセスから適切に保護されているかどうかを判断します。




ボリューム暗号化パラメータは、クラスタまたは Storage VM が準拠しているとみなされるかどうかには影響しません。

パラメータ	説明
暗号化されたソフトウェア	NetApp Volume Encryption （ NVE ） または NetApp Aggregate Encryption （ NAE ） ソフトウェア暗号化ソリューションを使用して保護されているボリュームの数が表示されます。
ハードウェア暗号化	NetApp Storage Encryption （ NSE ） ハードウェア暗号化を使用して保護されているボリュームの数が表示されます。
ソフトウェアとハードウェアを暗号化	ソフトウェア暗号化とハードウェア暗号化の両方で保護されているボリュームの数が表示されます。
暗号化なし	暗号化されていないボリュームの数が表示されます。

非準拠の条件

『ONTAP 9 セキュリティ設定ガイド』に定義されている推奨事項に照らして評価されるセキュリティ条件が1つでも満たされていない場合、クラスタと Storage Virtual Machine (SVM) は非準拠とみなされます。また、非準拠と判断された SVM が1つでもある場合も、クラスタは非準拠とみなされます。

セキュリティカード内の各ステータスアイコンとその意味は次のとおりです。

-  - パラメータは推奨事項に従って設定されています。
-  - パラメータは推奨事項に従って設定されていません。
-  - クラスタで機能が有効になっていないか、パラメータが推奨事項に従って設定されていませんが、このパラメータはオブジェクトのコンプライアンスには影響しません。

ボリューム暗号化ステータスは、クラスタまたは SVM が準拠とみなされるかどうかには影響しません。

クラスタと Storage VM のセキュリティステータスの表示

Active IQ Unified Manager を使用すると、環境内のストレージオブジェクトのセキュリティステータスを、インターフェイスのさまざまなポイントから確認できます。定義されたパラメータに基づいて情報とレポートを収集および分析し、監視対象のクラスタおよび Storage VM について、疑わしい動作や不正なシステム変更を検出できます。

セキュリティに関する推奨事項については、を参照してください ["ONTAP 9 セキュリティ設定ガイド"](#)

セキュリティページでオブジェクトレベルのセキュリティステータスを表示します

システム管理者は、セキュリティ*ページを使用して、データセンターレベルとサイトレベルのONTAP クラスタと Storage VM のセキュリティ強度を可視化できます。サポートされるオブジェクトは、クラスタ、Storage VM、およびボリュームです。次の手順を実行します。

手順

1. 左側のナビゲーションペインで、* ダッシュボード * をクリックします。
2. すべての監視対象クラスタのセキュリティステータスを表示するか、1つのクラスタのセキュリティステータスを表示するかに応じて、* すべてのクラスタ * を選択するか、ドロップダウンメニューから1つのクラスタを選択します。
3. セキュリティ * パネルの右矢印をクリックします。[セキュリティ]ページが表示されます。

棒グラフ、カウント、およびをクリックします View Reports リンクをクリックすると、ボリューム、クラスタ、または Storage VM のページが表示され、必要に応じて対応する詳細を確認したりレポートを生成したりできます。

セキュリティページには、次のパネルが表示されます。

- クラスタコンプライアンス：データセンター内のすべてのクラスタのセキュリティステータス（準拠または非準拠のクラスタ数）
- * Storage VM Compliance *：データセンター内のすべての Storage VM のセキュリティステータス（準拠または非準拠の Storage VM 数）

- * Volume Encryption *：環境内のすべてのボリュームの暗号化ステータス（暗号化されているボリュームまたは暗号化されていないボリュームの数）
- * Volume Anti-Ransomware Status *：環境内のすべてのボリュームのセキュリティステータス（ランサムウェア対策が有効または無効になっているボリュームの数）
- クラスタ認証および証明書：SAML、Active Directory、証明書およびローカル認証など、各タイプの認証方法を使用するクラスタの数。このパネルには、証明書の有効期限が切れているか、60日以内に期限切れになる予定のクラスタの数も表示されます。


クラスタページで、すべてのクラスタのセキュリティの詳細を表示します

[*クラスタ/セキュリティ*の詳細]ページでは、セキュリティコンプライアンスのステータスをクラスタレベルで表示できます。

手順

1. 左側のナビゲーションペインで、* Storage > Clusters *の順にクリックします。
2. [表示]>[セキュリティ]>[すべてのクラスタ]を選択します。

グローバルFIPS、Telnet、セキュアでないSSH設定、ログインバナー、ネットワークタイムプロトコル、AutoSupport HTTPS転送プロトコルと、クラスタ証明書の有効期限のステータスが表示されます。

をクリックできます  オプションボタンをクリックし、Unified ManagerまたはSystem Managerの* Security *ページでセキュリティの詳細を表示します。System Managerで詳細を表示するには、有効なクレデンシャルが必要です。



クラスタの証明書の有効期限が切れている場合は、をクリックします expired 「*クラスタ証明書の有効性」の下にあるSystem Manager（9.10.1以降）から更新してください。をクリックすることはできません expired System Managerインスタンスが9.10.1より前のリリースの場合。


すべてのクラスタのセキュリティの詳細を**Storage VM**ページで表示する

Storage VMs/Security *の詳細ページでは、Storage VMレベルでセキュリティ準拠ステータスを確認できます。

手順

1. 左側のナビゲーションペインで、* Storage > Storage VM*をクリックします。
2. [表示]>[セキュリティ]>[すべてのStorage VMs]を選択します。*セキュリティパラメータが設定されたクラスタのリストが表示されます。

Storage VMのセキュリティコンプライアンスのデフォルトビューを使用するには、Storage VM、クラスタ、ログインバナー、監査ログ、安全でないSSH設定などのセキュリティパラメータを確認します。

をクリックできます  オプションボタンをクリックし、Unified ManagerまたはSystem Managerの* Security *ページでセキュリティの詳細を表示します。System Managerで詳細を表示するには、有効なクレデンシャルが必要です。

ボリュームやStorage VMのランサムウェア対策セキュリティの詳細については、を参照してください ["すべてのボリュームおよびStorage VMのランサムウェア対策ステータスを表示する"](#)。

ソフトウェアまたはファームウェアの更新が必要なセキュリティイベントの表示

「アップグレード」の影響領域を持つセキュリティイベントがあります。これらのイベントは Active IQ プラットフォームから報告され、ONTAP ソフトウェア、ノードファームウェア、またはオペレーティングシステムソフトウェア（セキュリティアドバイザリ用）のアップグレードが必要な問題を特定します。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

これらの問題については、すぐに対処が必要なものもあれば、スケジュールされた次のメンテナンスまで待てるものもあります。これらのイベントをすべて表示し、問題を解決できるユーザに割り当てることができます。また、通知が不要なセキュリティアップグレードイベントがある場合は、このリストを利用して無効にするイベントを特定できます。

手順

1. 左側のナビゲーションペインで、* イベント管理 * をクリックします。

デフォルトでは、すべてのアクティブな（新規および確認済みの）イベントがイベント管理インベントリページに表示されます。

2. [表示] メニューから [* アップグレードイベント *] を選択します。

アクティブなすべてのアップグレードセキュリティイベントが表示されます。

すべてのクラスタでのユーザ認証の管理状況の表示

Security ページには、各クラスタでユーザの認証に使用されている認証の種類と、各タイプを使用してクラスタにアクセスしているユーザの数が表示されます。これにより、ユーザ認証が組織の定義に従って安全に実行されていることを確認できます。

手順

1. 左側のナビゲーションペインで、* ダッシュボード * をクリックします。
2. ダッシュボードの上部で、ドロップダウンメニューから「* すべてのクラスタ *」を選択します。
3. セキュリティ * パネルの右矢印をクリックすると、セキュリティ * ページが表示されます。
4. クラスタ認証 * カードを表示して、各認証タイプを使用してシステムにアクセスしているユーザの数を確認します。
5. クラスタセキュリティ * カードを表示して、各クラスタのユーザ認証に使用される認証メカニズムを確認します。

安全でない方法またはネットアップが推奨していない方法でシステムにアクセスしているユーザがいる場合は、その方法を無効にできます。

すべてのボリュームの暗号化ステータスを表示します

すべてのボリュームとその現在の暗号化ステータスのリストを表示して、ボリューム上のデータが権限のないユーザによるアクセスから適切に保護されているかどうかを確認

できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ボリュームに適用できる暗号化のタイプは次のとおりです。

- ソフトウェア - NetApp Volume Encryption (NVE) または NetApp Aggregate Encryption (NAE) ソフトウェア暗号化ソリューションを使用して保護されているボリューム。
- ハードウェア - NetApp Storage Encryption (NSE) ハードウェア暗号化を使用して保護されているボリューム。
- ソフトウェアとハードウェア - ソフトウェア暗号化とハードウェア暗号化の両方で保護されているボリューム。
- なし - 暗号化されていないボリューム。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Volumes * をクリックします。
2. [表示]メニューで、[* 正常性 * > * ボリューム暗号化 *]を選択します
3. [* Health:Volumes Encryption*]ビューで、[* Encryption Type*]フィールドをソートするか、[Filter]を使用して、特定の暗号化タイプを持つボリューム、または暗号化されていないボリュームを表示します ([Encryption Type] は [None])。

すべてのボリュームおよび**Storage VM**のランサムウェア対策ステータスを表示する

すべてのボリュームとStorage VM (SVM) およびその最新のランサムウェア対策ステータスのリストを表示して、ボリュームやSVM上のデータがランサムウェア攻撃から適切に保護されているかどうかを確認できます。

- 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ランサムウェア対策のさまざまなステータスの詳細については、を参照してください ["ONTAP：ランサムウェア対策を有効化"](#)。

ランサムウェア対策の検出機能で、すべてのボリュームのセキュリティの詳細を表示できます

手順

1. 左側のナビゲーションペインで、 * Storage * > * Volumes * をクリックします。
2. [表示]メニューで、[* Health > Security > Anti-Ransomware *]を選択します
3. セキュリティ：アンチランサムウェア*表示では、さまざまなフィールドでソートしたり、フィルタを使用したりできます。



ランサムウェア対策は、オフラインボリューム、制限付きボリューム、SnapLock ボリューム、FlexGroup ボリューム、FlexCache ボリュームではサポートされていません。SAN専用ボリューム、停止しているStorage VMのボリューム、Storage VMのルートボリューム、またはデータ保護ボリューム。

ランサムウェア対策検出で、すべての**Storage VM**のセキュリティの詳細を確認できます

手順

1. 左側のナビゲーションペインで、* Storage > Storage VM*をクリックします。
2. [表示] > [セキュリティ] > [ランサムウェア対策] の順に選択します。ランサムウェア対策のステータスが設定されたSVMのリストが表示されます。



NASプロトコルが有効になっていないStorage VMでは、ランサムウェア対策監視はサポートされていません。

アクティブなすべてのセキュリティイベントを表示します

アクティブなセキュリティイベントをすべて表示し、問題を解決できるユーザに各イベントを割り当てることができます。また、受信不要なセキュリティイベントがある場合は、このリストを利用して無効にするイベントを特定できます。

• 必要なもの *

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* イベント管理 * をクリックします。

デフォルトでは、新規と確認済みのイベントがイベント管理のインベントリページに表示されます。

2. [表示] メニューから、[アクティブセキュリティイベント *] を選択します。

このページには、過去 7 日間に生成された「新規」と「確認済み」のすべてのセキュリティイベントが表示されます。

セキュリティイベントのアラートを追加する

セキュリティイベントのアラートは、Unified Manager で受信する他のイベントと同様に、イベントごとに個別に設定することができます。また、すべてのセキュリティイベントを同じように扱い、同じユーザに E メールを送信する場合は、セキュリティイベントがトリガーされたときに通知する共通のアラートを作成することもできます。

• 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

次に 'Telnet Protocol enabled' セキュリティ・イベントのアラートを作成する例を示します。クラスタへのリモート管理アクセス用に Telnet アクセスが設定されると、アラートが送信されます。同じ方法で、すべてのセ

セキュリティイベントに対してアラートを作成できます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Alert Setup * をクリックします。
2. [* Alert Setup*] ページで、 [* Add] をクリックします。
3. [* アラートの追加 *] ダイアログボックスで、 [* 名前 *] をクリックし、アラートの名前と概要を入力します。
4. リソースをクリックし、このアラートを有効にするクラスタを選択します。
5. [* Events （イベント）] をクリックして、次の操作を実行します。
 - a. イベントの重大度リストで、 * 警告 * を選択します。
 - b. [Matching Events] リストで、 [Telnet Protocol Enabled*] を選択します。
6. [* アクション *] をクリックし、 [これらのユーザーに警告] フィールドで警告メールを受信するユーザーの名前を選択します。
7. 通知頻度、SNMP トラップの発行、スクリプトの実行など、このページの他のオプションを設定します。
8. [保存 （ Save ）] をクリックします。

特定のセキュリティイベントを無効にする

デフォルトでは、すべてのイベントが有効になっています。環境で重要でないイベントは、無効にして通知が生成されないようにすることができます。無効にしたイベントの通知を再開するには、該当するイベントを有効にします。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

イベントを無効にすると、システムで以前に生成されたイベントは「廃止」とマークされ、それらのイベントに設定されたアラートはトリガーされなくなります。無効にしたイベントを有効にすると、それらのイベントの通知の生成が次の監視サイクルから開始されます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Event Setup * をクリックします。
2. イベント * 設定ページで、次のいずれかのオプションを選択してイベントを無効または有効にします。

状況	操作
イベントを無効にします	<ul style="list-style-type: none"> a. [Disable] をクリックします。 b. [イベントの無効化] ダイアログボックスで、[警告] の重大度を選択します。これは、すべてのセキュリティイベントのカテゴリです。 c. [Matching Events] カラムで、ディセーブルにするセキュリティイベントを選択し、右矢印をクリックして [Disable Events] カラムに移動します。 d. [保存して閉じる] をクリックします。 e. 無効にしたイベントが Event Setup ページのリストビューに表示されることを確認します。
イベントを有効にします	<ul style="list-style-type: none"> a. 無効になっているイベントのリストから、再度有効にするイベントのチェックボックスを選択します。 b. [Enable] をクリックします。

セキュリティイベント

セキュリティイベントは、『ONTAP 9_NetApp Security Hardening Guide』に定義されているパラメータに基づいて、ONTAP クラスタ、Storage Virtual Machine（SVM）、およびボリュームのセキュリティステータスに関する情報を提供します。これらのイベントは潜在的な問題を通知するもので、問題の重大度を評価し、必要に応じて問題を修正することができます。

セキュリティイベントはソースタイプ別にグループ化され、イベント名とトラップ名、影響レベル、および重大度が表示されます。これらのイベントは、クラスタおよび Storage VM のイベントカテゴリに表示されます。

バックアップとリストアの処理の管理

Active IQ Unified Manager のバックアップを作成し、リストア機能を使用して、システム障害やデータ損失が発生した場合に、同じ（ローカル）システムまたは新しい（リモート）システムにバックアップをリストアできます。

Unified Manager をインストールしたオペレーティングシステム、および管理対象のクラスタとノードの数に応じて、バックアップとリストアの方法は 3 種類あります。

オペレーティングシステム	展開のサイズ	推奨されるバックアップ方法
VMware vSphere の場合	任意	Unified Manager 仮想アプライアンスの VMware スナップショット

オペレーティングシステム	展開のサイズ	推奨されるバックアップ方法
Red Hat Enterprise Linux または CentOS Linux	小規模	Unified Manager の MySQL データベースダンプ
	大規模	Unified Manager データベースの NetApp Snapshot
Microsoft Windows の場合	小規模	Unified Manager の MySQL データベースダンプ
	大規模	NetApp Snapshot of Unified Manager database with iSCSI protocol

これらのさまざまな方法については、以降のセクションで説明します。

仮想アプライアンスでの **Unified Manager** のバックアップとリストア

仮想アプライアンスにインストールされた Unified Manager のバックアップとリストアのモデルでは、仮想アプリケーション全体のイメージをキャプチャしてリストアします。

次のタスクを実行することで、仮想アプライアンスのバックアップを完了できます。

1. VM の電源をオフにして、Unified Manager 仮想アプライアンスの VMware スナップショットを作成します。
2. データストアで NetApp Snapshot コピーを作成して VMware スナップショットをキャプチャします。

ONTAP ソフトウェアを実行しているシステム以外でデータストアをホストしている場合は、ストレージベンダーのガイドラインに従って VMware スナップショットを作成します。

3. NetApp Snapshot コピーまたはそれに相当するスナップショットを別のストレージにレプリケートします。
4. VMware スナップショットを削除します。

問題が発生した場合に Unified Manager 仮想アプライアンスが保護されるようにするには、これらのタスクを使用してバックアップスケジュールを実装します。

VM をリストアする際は、作成した VMware スナップショットを使用して、VM をバックアップの作成時点の状態にリストアします。

MySQL データベースダンプを使用したバックアップとリストア

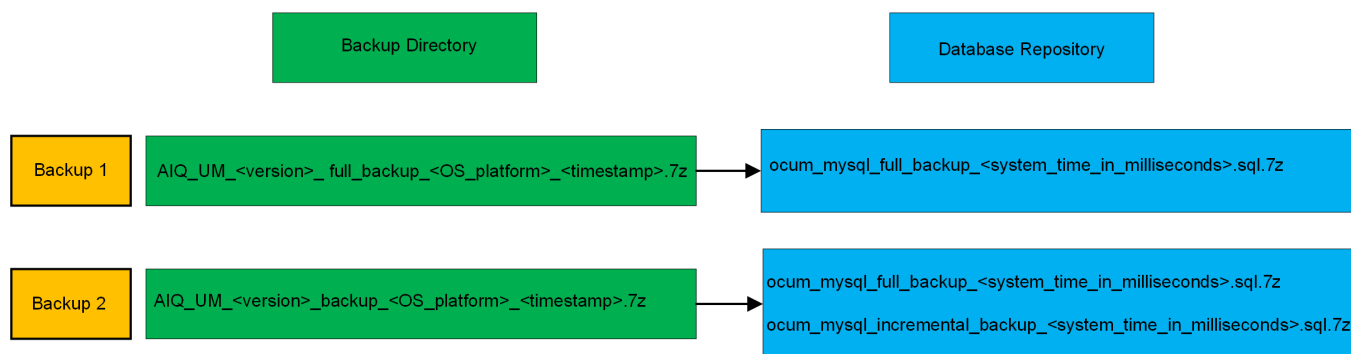
MySQL データベースダンプバックアップは、システム障害やデータ損失が発生した場合に使用できる Active IQ Unified Manager データベースと構成ファイルのコピーです。バックアップはローカルにもリモートにも保存できますが、Active IQ Unified Manager ホストシステムとは別のリモートの場所を定義することを強く推奨します。



Linux サーバと Windows サーバに Unified Manager をインストールした場合のデフォルトのバックアップメカニズムは MySQL データベースダンプです。ただし、Unified Manager で管理しているクラスタやノードの数が多い場合や、MySQL バックアップの完了に数時間かかる場合は、Snapshot コピーを使用してバックアップを実行できます。この機能は、Red Hat Enterprise Linux、CentOS Linux システム、および Windows で使用できます。

データベースダンプバックアップは、バックアップディレクトリ内の 1 つのファイルとデータベースリポジトリディレクトリ内の 1 つ以上のファイルで構成されます。バックアップディレクトリ内のファイルは非常に小さく、バックアップを再作成するために必要なデータベースリポジトリディレクトリ内のファイルへのポインタのみが含まれます。

データベースバックアップの初回生成時は、1 つのファイルがバックアップディレクトリに作成され、フルバックアップファイルがデータベースリポジトリディレクトリに作成されます。次にバックアップを生成するときは、1 つのファイルがバックアップディレクトリに作成され、フルバックアップファイルとの差分を含む増分バックアップファイルがデータベースリポジトリディレクトリに作成されます。追加のバックアップを作成すると、次の図に示すように、最大保持設定までこのプロセスが繰り返されます。



これらの 2 つのディレクトリ内のバックアップファイルは、名前を変更したり削除したりしないでください。それらの処理を行うと、以降のリストア処理が失敗します。

バックアップファイルをローカルシステムに書き込む場合、完全なリストアを必要とするシステム問題があるときに使用できるように、バックアップファイルをリモートの場所にコピーするプロセスを開始する必要があります。

バックアップ処理を開始する前に、Active IQ Unified Manager で整合性チェックが実行され、必要なすべてのバックアップファイルとバックアップディレクトリが存在し、書き込み可能であることが確認されます。また、バックアップファイルを作成できるだけの十分なスペースがシステムにあるかどうかも確認されます。

データベースダンプバックアップのデスティネーションの設定とスケジュール設定

Unified Manager のデータベースダンプバックアップ設定で、データベースのバックアップパス、保持数、およびバックアップスケジュールを設定できます。日単位または週単位のスケジュールされたバックアップを有効にすることができます。デフォルトでは、スケジュールされたバックアップは無効になっていますが、バックアップスケジュールを設定する必要があります。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

- バックアップパスとして定義する場所に 150GB 以上の利用可能なスペースが必要です。

Unified Manager ホストシステムとは別のリモートの場所を使用することを推奨します。

- Unified Manager を Linux システムにインストールし、MySQL バックアップを使用する場合は、バックアップディレクトリに対して次の権限と所有権が設定されていることを確認してください。

権限：0750、所有権：jboss:maintenance

- Unified Manager を Windows システムにインストールし、MySQL バックアップを使用する場合は、バックアップディレクトリにアクセスできるのが管理者だけであることを確認してください。

初回のバックアップではフルバックアップが実行されるため、2 回目以降のバックアップよりも時間がかかります。フルバックアップは 1GB を超えることもあり、3~4 時間かかる場合があります。2 回目以降のバックアップは増分バックアップとなり、所要時間は短くなります。



- 増分バックアップファイルがバックアップ用に割り当てたスペースに対して大きすぎる場合は、定期的にフルバックアップを実行して、古いバックアップとその増分ファイルを置き換えることができます。別の方法として、Snapshotコピーを使用してバックアップを作成することもできます。
- 新しいクラスタに追加してから最初の 15 日間に作成されたバックアップは、過去のパフォーマンスデータを取得するのに十分な精度がない可能性があります。

手順

1. 左側のナビゲーションペインで、* General * > * Database Backup * をクリックします。
2. [* データベース・バックアップ *] ページで、[* バックアップ設定 *] をクリックします。
3. バックアップパス、保持数、およびスケジュールの値を設定します。

保持数のデフォルト値は 10 です。バックアップを無制限に作成する場合は 0 に設定します。

4. 「毎日スケジュール」または「毎週スケジュール」* ボタンを選択し、スケジュールの詳細を指定します。
5. [適用 (Apply)] をクリックします。

スケジュールに基づいてデータベースダンプバックアップファイルが作成されます。使用可能なバックアップファイルは、[データベースバックアップ] ページに表示されます。

データベースリストアとは何ですか

MySQL データベースのリストアとは、既存の Unified Manager バックアップファイルと同じまたは別の Unified Manager サーバにリストアする処理です。リストア処理は Unified Manager メンテナンスコンソールから実行します。

同じ（ローカル）システムでリストア処理を実行する場合、バックアップファイルがすべてローカルに保存されていれば、デフォルトの場所を使用してリストアオプションを実行できます。別の Unified Manager システム（リモートシステム）でリストア処理を実行する場合は、リストアオプションを実行する前に、バックアップファイルをセカンダリストレージからローカルディスクにコピーする必要があります。

リストアプロセス中は Unified Manager からログアウトされます。リストアプロセスが完了したら、システムにログインできます。

バックアップイメージを新しいサーバにリストアする場合は、リストア処理の完了後に新しい HTTPS セキュリティ証明書を生成して Unified Manager サーバを再起動する必要があります。また、バックアップイメージを新しいサーバにリストアするときに、必要に応じて SAML 認証の設定を再設定する必要があります。



Unified Manager ソフトウェアを新しいバージョンにアップグレードしたあとに、古いバックアップファイルを使用してイメージをリストアすることはできません。スペースを節約するために、Unified Manager をアップグレードすると、最新のファイルを除く古いバックアップファイルがすべて自動的に削除されます。

• 関連情報 *

["HTTPS セキュリティ証明書の生成"](#)

["SAML 認証の有効化"](#)

["Active Directory または OpenLDAP による認証"](#)

Linux システムでの MySQL データベースバックアップのリストア

データ損失やデータ破損が発生した場合、Unified Manager を以前の安定した状態にリストアすることでデータ損失を最小限に抑えることができます。Unified Manager データベースは、Unified Manager メンテナンスコンソールを使用してローカルとリモートのどちらの Red Hat Enterprise Linux または CentOS システムにもリストアできます。

- 必要なもの *
- Unified Manager がインストールされている Linux ホストの root ユーザのクレデンシャルが必要です。
- Unified Manager サーバのメンテナンスコンソールへのログインが許可されているユーザ ID とパスワードが必要です。
- リストア処理を実行するシステムに Unified Manager のバックアップファイルとデータベースリポジトリディレクトリの内容をコピーしておく必要があります。

バックアップファイルはデフォルトのディレクトリにコピーすることを推奨します /data/ocum-バックアップ。データベースリポジトリのファイルは、にコピーする必要があります /database-dumps-repo のサブディレクトリ /ocum-backup ディレクトリ。

- バックアップファイルはにする必要があります .7z を入力します。

リストア機能は、プラットフォームおよびバージョンに固有の機能です。Unified Manager のバックアップは、同じバージョンの Unified Manager にのみリストアできます。Red Hat Enterprise Linux または CentOS システムにリストアできるのは、Linux のバックアップファイルと仮想アプライアンスのバックアップファイルです。



バックアップフォルダ名にスペースが含まれている場合は、絶対パスまたは相対パスを二重引用符で囲む必要があります。

手順

1. 新しいサーバへのリストアを実行する場合は、Unified Manager のインストールの完了後に、UI を起動したり、クラスタ、ユーザ、または認証設定を設定したりしないでください。この情報は、リストアプロセスでバックアップファイルに取り込まれます。

- Secure Shell を使用して、Unified Manager システムの IP アドレスまたは完全修飾ドメイン名に接続します。
- メンテナンスユーザ（umadmin）の名前とパスワードでシステムにログインします。
- 入力するコマンド maintenance_console を押します。
- メンテナンスコンソール * メインメニュー * で、* バックアップリストア * オプションの番号を入力します。
- 「MySQL バックアップのリストア」 * の番号を入力します。
- プロンプトが表示されたら、バックアップファイルの絶対パスを入力します。

```
Bundle to restore from: /data/ocum-  
backup/UM_9.8.N151113.1348_backup_rhel_02-20-2020-04-45.7z
```

リストア処理が完了したら、Unified Manager にログインできます。

バックアップをリストアしたあとに OnCommand Workflow Automation サーバが動作しない場合は、次の手順を実行します。

- Workflow Automation サーバで、Unified Manager サーバの IP アドレスを最新のマシンを参照するように変更します。
- 手順 1 で取得に失敗した場合は、Unified Manager サーバでデータベースパスワードをリセットします。

Windows での MySQL データベースバックアップのリストア

データ損失やデータ破損が発生した場合、リストア機能を使用して Unified Manager を以前の安定した状態にリストアすることで損失を最小限に抑えることができます。Unified Manager の MySQL データベースは、Unified Manager メンテナンスコンソールを使用してローカルとリモートのどちらの Windows システムにもリストアできます。

- 必要なもの *
- Windows の管理者権限が必要です。
- リストア処理を実行するシステムに Unified Manager のバックアップファイルとデータベースリポジトリディレクトリの内容をコピーしておく必要があります。

バックアップファイルはデフォルトのディレクトリにコピーすることを推奨します

\ProgramData\NetApp\OnCommandAppData\ocum\backup。データベースリポジトリのファイルは、にコピーする必要があります \database_dumps_repo のサブディレクトリ \backup ディレクトリ。

- バックアップファイルはにする必要があります .7z を入力します。

リストア機能は、プラットフォームおよびバージョンに固有の機能です。Unified Manager の MySQL バックアップは、同じバージョンの Unified Manager にのみリストアできます。また、Windows のバックアップは、Windows プラットフォームにのみリストアできます。



フォルダ名にスペースが含まれている場合は、バックアップファイルの絶対パスまたは相対パスを二重引用符で囲む必要があります。

手順

1. 新しいサーバへのリストアを実行する場合は、Unified Manager のインストールの完了後に、UI を起動したり、クラスタ、ユーザ、または認証設定を設定したりしないでください。この情報は、リストアプロセスでバックアップファイルに取り込まれます。
2. 管理者のクレデンシャルで Unified Manager システムにログインします。
3. Windows 管理者として PowerShell または コマンドプロンプト を起動します。
4. 入力するコマンド `maintenance_console` を押します。
5. メンテナンスコンソール * メインメニュー * で、* バックアップリストア * オプションの番号を入力します。
6. 「MySQL バックアップのリストア」 * の番号を入力します。
7. プロンプトが表示されたら、バックアップファイルの絶対パスを入力します。

```
Bundle to restore from:  
\\ProgramData\\NetApp\\OnCommandAppData\\ocum\\backup\\UM_9.8.N151118.2300_backup_windows_02-20-2020-02-51.7z
```

リストア処理が完了したら、Unified Manager にログインできます。

バックアップをリストアしたあとに OnCommand Workflow Automation サーバが動作しない場合は、次の手順を実行します。

1. Workflow Automation サーバで、Unified Manager サーバの IP アドレスを最新のマシンを参照するように変更します。
2. 手順 1 で取得に失敗した場合は、Unified Manager サーバでデータベースパスワードをリセットします。

NetApp Snapshot を使用したバックアップとリストア

NetApp Snapshot コピーは、システム障害やデータ損失が発生した場合にリストアに使用できる Unified Manager データベースと構成ファイルのポイントインタイムイメージを作成します。Snapshot コピーをいずれかの ONTAP クラスタ上のボリュームに定期的に書き込まれるようにスケジュールして、常に最新のコピーを保持します。



この機能は、仮想アプライアンスにインストールされている Active IQ Unified Manager では使用できません。

Linux でバックアップを設定しています

Active IQ Unified Manager が Linux マシンにインストールされている場合は、NetApp Snapshot を使用してバックアップとリストアを設定できます。

Snapshot コピーにかかる時間はごくわずかで、通常は数分です。Unified Manager データベースが非常に短時

間ロックされるため、インストールの中断はほとんどありません。イメージには Snapshot コピーが最後に作成されたあとに発生したファイルへの変更だけが記録されるため、ストレージスペースは最小限しか消費せず、パフォーマンスのオーバーヘッドもわずかです。この Snapshot は ONTAP クラスタ上に作成されるため、必要に応じて、SnapMirror などのネットアップの他の機能を利用してセカンダリ保護を作成できます。

バックアップ処理を開始する前に、Unified Manager で整合性チェックが実行され、デスティネーションシステムが使用可能であることが確認されます。



- Snapshot コピーは、同じバージョンの Active IQ Unified Manager にのみリストアできます。

たとえば、Unified Manager 9.12 でバックアップを作成した場合、そのバックアップは Unified Manager 9.12 システムにのみリストアできます。

- Snapshot 設定に変更原因があると、Snapshot が無効である可能性があります。

Snapshot コピーの場所を設定しています

ONTAP System Manager または ONTAP CLI を使用して、ONTAP クラスタのいずれかに Snapshot コピーを格納するボリュームを設定できます。

- 必要なもの *

クラスタ、Storage VM、およびボリュームが次の要件を満たしている必要があります。

- クラスタの要件：

- ONTAP 9.3 以降がインストールされている必要があります
- Unified Manager サーバに地理的に近い場所に配置する必要があります
- Unified Manager で監視できますが、必須ではありません

- Storage VM の要件：

- ネームスイッチとネームマッピングは「files」を使用するように設定する必要があります。
- クライアント側ユーザに対応するように作成されたローカルユーザ
- すべての読み取り / 書き込みアクセスが選択されていることを確認します
- エクスポートポリシーで Superuser Access が「any」に設定されていることを確認します
- Linux 用 NetApp Snapshot 用の NFS
- NFS サーバと、クライアントおよび Storage VM で指定された NFSv4 ID ドメインで NFSv4 が有効になっている必要があります
- ボリュームのサイズは、Unified Manager /opt/NetApp/data ディレクトリのサイズの少なくとも 2 倍にする必要があります

コマンド `du -sh /opt/NetApp/data/` を使用して、現在のサイズを確認します。

- ボリューム要件：

- ボリュームのサイズは、Unified Manager /opt/NetApp/data ディレクトリのサイズの少なくとも 2 倍にする必要があります

- セキュリティ形式は UNIX に設定する必要があります
- ローカル Snapshot ポリシーを無効にする必要があります
- ボリュームのオートサイズを有効にする必要があります
- パフォーマンス・サービス・レベルは 'Extreme など' 高い IOPS と低い遅延を持つポリシーに設定する必要があります

NFS ボリュームの作成手順の詳細については、を参照してください ["ONTAP 9 で NFSv4 を設定する方法"](#) および ["ONTAP 9 NFS 構成エクスペンスガイド"](#)。

Snapshotコピーのデスティネーションの指定

いずれかのONTAP クラスタですでに設定してあるボリューム上のActive IQ Unified Manager Snapshotコピーのデスティネーションの場所を設定する必要があります。メンテナンスコンソールを使用して場所を定義する必要があります。

- Active IQ Unified Manager がインストールされている Linux ホストの root ユーザのクレデンシャルが必要です。
- Unified Manager サーバのメンテナンスコンソールへのログインが許可されているユーザ ID とパスワードが必要です。
- クラスタ管理 IP アドレス、Storage VM の名前、ボリュームの名前、およびストレージシステムのユーザ名とパスワードが必要です。
- Active IQ Unified Manager ホストにボリュームをマウントし、マウントパスを確認しておく必要があります。

手順

1. Secure Shell を使用して、Active IQ Unified Manager システムの IP アドレスまたは FQDN に接続します。
2. メンテナンスユーザ（umadmin）の名前とパスワードでシステムにログインします。
3. 入力するコマンド `maintenance_console` を押します。
4. メンテナンスコンソール * メインメニュー * で、* バックアップリストア * オプションの番号を入力します。
5. Configure NetApp Snapshot Backup * の番号を入力します。
6. NFS を設定する番号を入力します。
7. 指定する必要がある情報を確認し、「バックアップ設定の詳細を入力」* の番号を入力します。
8. Snapshot を書き込むボリュームを特定するには、クラスタ管理インターフェイスの IP アドレス、Storage VM の名前、ボリュームの名前、LUN 名、ストレージシステムのユーザ名とパスワード、およびマウントパスを入力します。
9. この情報を確認してと入力します `y`。

システムは次のタスクを実行します。

- クラスタへの接続を確立します
- すべてのサービスを停止します

- ボリュームに新しいディレクトリを作成し、Active IQ Unified Manager データベース構成ファイルをコピーします
 - Active IQ Unified Manager からファイルを削除し、新しいデータベースディレクトリへのシンボリックリンクを作成します
 - すべてのサービスを再起動します
10. メンテナンスコンソールを終了し、Active IQ Unified Manager インターフェイスを起動してSnapshotコピーのスケジュールを作成します（まだ作成していない場合）。

Windows でバックアップを設定しています

Active IQ Unified Manager では、Windows オペレーティングシステムでの NetApp Snapshot を使用したバックアップとリストアがサポートされています。LUN では iSCSI プロトコルを使用します。

Snapshotベースのバックアップは、Unified Managerのすべてのサービスの実行中に作成できます。データベースの整合性が取れた状態はスナップショットの一部としてキャプチャされます。バックアップによってデータベース全体にグローバルな読み取りロックが適用され、同時に書き込みを行うことができなくなります。Unified Manager システムを Windows OS 上にインストールし、NetApp Snapshot を使用してバックアップとリストアを実行する場合は、まずメンテナンスコンソールを使用して、Unified Manager のバックアップを Snapshot に設定します。

Unified ManagerでSnapshotコピーを作成するように設定する前に、次の設定タスクを実行する必要があります。

- ONTAP クラスタを設定する
- Windows ホスト・マシンを設定します

Windows のバックアップの場所を設定しています

WindowsでのUnified Managerのバックアップ後、Snapshotコピーを格納するようにボリュームを設定する必要があります。

- 必要なもの *

クラスタ、Storage VM、およびボリュームが次の要件を満たしている必要があります。

- クラスタの要件：
 - ONTAP 9.3 以降がインストールされている必要があります
 - Unified Manager サーバに地理的に近い場所に配置する必要があります
 - Unified Manager によって監視されます
- Storage VM の要件：
 - ONTAP クラスタでの iSCSI 接続
 - 構成されたマシンで iSCSI プロトコルが有効になっている必要があります
 - バックアップ構成用に専用のボリュームと LUN を用意します。選択したボリュームには LUN が 1 つしか含まれていない必要があります。

- LUN のサイズは、9.9 Active IQ Unified Manager で処理されると想定されるデータサイズの 2 倍以上にする必要があります。

これにより、ボリュームにも同じサイズ要件が設定されます。

- すべての読み取り / 書き込みアクセスが選択されていることを確認します
- エクスポートポリシーで Superuser Access が「any」に設定されていることを確認します

• ボリュームと LUN の要件：

- ボリュームのサイズは、Unified Manager の MySQL データディレクトリの 2 倍以上にする必要があります。
- セキュリティ形式は Windows に設定する必要があります
- ローカル Snapshot ポリシーを無効にする必要があります
- ボリュームのオートサイズを有効にする必要があります
- パフォーマンス・サービス・レベルは 'Extreme など' 高い IOPS と低い遅延を持つポリシーに設定する必要があります

ONTAP クラスタを設定しています

Windows システムで Snapshot コピーを使用して Active IQ Unified Manager をバックアップおよびリストアするには、ONTAP クラスタでいくつかの事前設定手順を実行する必要があります。

ONTAP クラスタは、コマンドプロンプトまたは System Manager ユーザインターフェイスを使用して設定できます。ONTAP クラスタの設定では、データ LIF を設定して、iSCSI LIF として Storage VM に割り当てることができます。次の手順は、System Manager ユーザインターフェイスを使用して、iSCSI 対応の Storage VM を設定することです。この Storage VM には、LIF が発信トラフィックをネットワークでどのように取り扱うかを制御するための静的なネットワークルートを設定する必要があります。



バックアップ構成用に専用のボリュームと LUN を用意します。選択したボリュームに含まれる LUN は 1 つだけです。LUN のサイズは、Active IQ Unified Manager で処理されると予想されるデータサイズの 2 倍以上にする必要があります。

次の設定を行う必要があります。

手順

1. iSCSI 対応の Storage VM を設定するか、設定が同じ既存の Storage VM を使用してください。
2. 設定された Storage VM のネットワークルートを設定
3. ボリュームがこの LUN 専用になるように、適切な容量と単一の LUN を内部で設定します。



System Manager で LUN を作成した場合、LUN のマッピングを解除すると igroup が削除されてリストアが失敗することがあります。この状況を回避するには、LUN の作成時に、LUN がマッピング解除されても明示的に作成され、削除されないようにします。

4. Storage VM にイニシエータグループを設定します。
5. ポートセットを設定します。

6. igroup をポートセットに統合します。
7. LUN を igroup にマッピングします。

Windows ホスト・マシンを設定しています

NetApp Snapshotを使用してActive IQ Unified Manager をバックアップおよびリストアするには、Windowsホストマシンを設定する必要があります。Windows ホスト・マシン上で Microsoft iSCSI イニシエータを起動するには、検索バーに「iscsi」と入力し「[* iSCSI Initiator *]」をクリックします

- 必要なもの *

ホストマシン上の以前の設定をすべてクリーンアップする必要があります。

Windows の新規インストール時に iSCSI イニシエータを起動しようとする、確認のプロンプトが表示され、確認のために [iSCSI Properties] ダイアログボックスが表示されます。既存の Windows インストールの場合は、非アクティブまたは接続しようとしているターゲットとともに iSCSI Properties (iSCSI プロパティ) ダイアログボックスが表示されます。そのため、Windows ホストで以前の設定をすべて削除する必要があります。

手順

1. ホストマシン上の以前の設定をクリーンアップします。
2. ターゲットポータルを検出する。
3. ターゲットポータルに接続します。
4. マルチパスを使用してターゲットポータルに接続します。
5. 両方の LIF を検出します。
6. Windows マシンでデバイスとして設定されている LUN を検出します。
7. Windows で、検出された LUN を新しいボリュームドライブとして設定します。

WindowsでのSnapshotコピーのデスティネーションの指定

いずれかのONTAP クラスタですでに設定してあるボリューム上のActive IQ Unified Manager Snapshotコピーのデスティネーションの場所を設定する必要があります。メンテナンスコンソールを使用して場所を定義する必要があります。

- Active IQ Unified Manager がインストールされている Windows ホストに対する管理者権限が必要です。
- Unified Manager サーバのメンテナンスコンソールへのログインが許可されているユーザ ID とパスワードが必要です。
- クラスタ管理 IP アドレス、Storage VM の名前、ボリュームの名前、LUN 名、およびストレージシステムのユーザ名とパスワードが必要です。
- ボリュームをネットワークドライブとして Active IQ Unified Manager ホストにマウントし、マウントドライブを用意しておく必要があります。

手順

1. パワーシェルを使用して、Active IQ Unified Manager システムの IP アドレスまたは完全修飾ドメイン名

に接続します。

2. メンテナンスユーザ（umadmin）の名前とパスワードでシステムにログインします。
3. 入力するコマンド `maintenance_console` を押します。
4. メンテナンスコンソール * メインメニュー * で、* バックアップリストア * オプションの番号を入力します。
5. Configure NetApp Snapshot Backup * の番号を入力します。
6. iSCSI を設定する番号を入力します。
7. 指定する必要がある情報を確認し、「バックアップ設定の詳細を入力」* の番号を入力します。
8. Snapshot を書き込むボリュームを特定するには、クラスタ管理インターフェイスの IP アドレス、Storage VM の名前、ボリュームの名前、LUN 名、ストレージシステムのユーザ名とパスワード、およびマウントドライブを入力します。
9. この情報を確認してと入力します `y`。

システムは次のタスクを実行します。

- Storage VM が検証されました
 - ボリュームが検証されています
 - マウントドライブとステータスが検証されます
 - LUN の有無とステータス
 - ネットワークドライブの存在
 - マウントされたボリュームに推奨されるスペース（MySQL データディレクトリの 2 倍以上）があるかどうか検証されます
 - ボリューム内の専用 LUN に対応する LUN パス
 - igroup 名
 - ネットワークドライブがマウントされているボリュームの GUID
 - ONTAP との通信に使用する iSCSI イニシエータ
10. メンテナンスコンソールを終了し、Active IQ Unified Manager インターフェイスを起動してSnapshotコピーのスケジュールを作成します。

メンテナンスコンソールから**Snapshot**コピーを使用してバックアップを設定する

Snapshotコピーを使用してActive IQ Unified Manager バックアップを作成するには、メンテナンスコンソールからいくつかの設定手順を実行する必要があります。

- 必要なもの *

システムに関する次の詳細を確認しておく必要があります。

- クラスタの IP アドレス
- Storage VM 名
- ボリューム名

- LUN 名
- マウントパス
- ストレージシステムのクレデンシャル

手順

1. Unified Manager のメンテナンスコンソールにアクセスします。
2. 「4」と入力して、「* Backup Restore *」を選択します。
3. 「2」と入力して、「NetApp Snapshot を使用したバックアップとリストア」を選択します。



バックアップ設定を変更する場合は、「* NetApp Snapshotバックアップ設定を更新*」を選択するために「3」と入力します。更新できるのはパスワードのみです。

4. メニューから「1」と入力して、「NetApp Snapshot バックアップの設定」を選択します。
5. 必要な情報を入力するには、1を入力します。
6. メンテナンスコンソールのユーザ名とパスワードを入力し、LUN がホストにマウントされたことを確認します。

次に、このプロセスでは、データディレクトリ、LUN パス、Storage VM、ボリューム、スペースの可用性、ドライブなど、お客様から提供されたものは正しいものです。バックグラウンドで実行される処理は次のとおりです。

- サービスが停止されました
- データベースディレクトリがマウントされたストレージに移動されます
- データベースディレクトリが削除され、シンボリックリンクが確立されます
- サービスは Active IQ Unified Manager インターフェイスでの設定の完了後に再開されます。バックアップタイプはネットアップの Snapshot に変更され、ユーザインターフェイスにはデータベースバックアップ（Snapshot ベース）として反映されます。

バックアップ処理原因を開始する前に、Snapshot 設定に変更がないかどうかを確認する必要があります。これは、Snapshot が無効である可能性があるためです。G ドライブにバックアップを設定し、Snapshot を作成したとします。後でバックアップを E ドライブに再構成し、データは新しい設定に従って E ドライブに保存されます。G ドライブ内で作成されたスナップショットをリストアしようとする、G ドライブが存在しないというエラーで失敗します。

Linux と Windows のバックアップスケジュールの定義

Unified ManagerのUIを使用して、Unified Manager Snapshotコピーを作成するスケジュールを設定できます。

- 必要なもの *
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- メンテナンスコンソールからSnapshotコピーを作成するための設定を行って、Snapshotを作成するデスティネーションを特定しておく必要があります。

数分でSnapshotコピーが作成され、Unified Managerデータベースがロックされるのは数秒だけです。



新しいクラスタに追加してから最初の 15 日間に作成されたバックアップは、過去のパフォーマンスデータを取得するのに十分な精度がない可能性があります。

手順

1. 左側のナビゲーションペインで、* General * > * Database Backup * をクリックします。
2. [* データベース・バックアップ *] ページで、[* バックアップ設定 *] をクリックします。
3. 保持する Snapshot コピーの最大数を「* Retention Count *」フィールドに入力します。

保持数のデフォルト値は 10 です。Snapshot コピーの最大数は、クラスタ上の ONTAP ソフトウェアのバージョンによって決まります。このフィールドを空白のままにすると、ONTAP のバージョンに関係なく最大値を実装できます。

4. 「毎日スケジュール」または「毎週スケジュール」* ボタンを選択し、スケジュールの詳細を指定します。
5. [適用 (Apply)] をクリックします。

Snapshot コピーはスケジュールに基づいて作成されます。使用可能なバックアップファイルは、[データベースバックアップ] ページに表示されます。

このボリュームと Snapshot の重要性により、次のいずれかの場合に通知を受けるために、このボリュームに対して 1 つまたは 2 つのアラートを作成することができます。

- ボリュームスペースが 90% フルの場合。イベント「* Volume Space Full」を使用してアラートを設定します。

ONTAP System Manager または ONTAP CLI を使用してボリュームに容量を追加し、Unified Manager データベースのスペースが不足しないようにすることができます。

- Snapshot が最大数に近づいています。イベント * Snapshot コピー数が多すぎる * を使用してアラートを設定してください。

ONTAP System Manager または ONTAP CLI を使用して古い Snapshot を削除して、新しい Snapshot コピー用の空きスペースを常に確保することができます。

アラートの設定は、Alert Setup ページで行います。

Snapshot コピーを使用した Unified Manager のリストア

データ損失やデータ破損が発生した場合、Unified Manager を以前の安定した状態にリストアすることでデータ損失を最小限に抑えることができます。Unified Manager の Snapshot データベースは、Unified Manager メンテナンスコンソールを使用してローカルとリモートのどちらのオペレーティングシステムにもリストアできます。

- 必要なもの *
- Unified Manager がインストールされている Windows ホストマシンに対する Linux ホストの root ユーザのクレデンシャルと管理者権限が必要です。
- Unified Manager サーバのメンテナンスコンソールへのログインが許可されているユーザ ID とパスワードが必要です。

リストア機能は、プラットフォームおよびバージョンに固有の機能です。Unified Manager のバックアップは、同じバージョンの Unified Manager にのみリストアできます。

手順

1. Unified Manager システムの IP アドレスまたは完全修飾ドメイン名に接続します。
 - Linux : Secure Shellの略
 - Windows : PowerShell
2. root ユーザのクレデンシャルでシステムにログインします。
3. 入力するコマンド `maintenance_console` を押します。
4. メンテナンスコンソール*メインメニュー*で、*バックアップリストア*オプションに4を入力します。
5. 「* NetApp Snapshotを使用したバックアップとリストア」を選択するには、2を入力します。

新しいサーバへのリストアを実行する場合は、Unified Manager のインストールの完了後に、UI を起動したり、クラスタ、ユーザ、または認証設定を設定したりしないでください。Configure NetApp Snapshot Backup*を選択するには1を入力し、元のシステムと同様にSnapshotコピーの設定を行います。

6. 「3」と入力して、「NetApp Snapshotを使用してリストア」を選択します。
7. Unified Managerのリストアに使用するSnapshotコピーを選択します。Enter キーを押します。
8. リストアプロセスが完了したら、Unified Manager ユーザインターフェイスにログインします。

バックアップをリストアしたあとに Workflow Automation サーバが動作しなくなった場合は、次の手順を実行します。

1. Workflow Automation サーバで、Unified Manager サーバの IP アドレスを最新のマシンを参照するように変更します。
2. 手順 1 で取得に失敗した場合は、Unified Manager サーバでデータベースパスワードをリセットします。

バックアップタイプを変更しています

Active IQ Unified Manager システムのバックアップタイプを変更する場合は、メンテナンスコンソールのオプションを使用できます。Unconfigure NetApp Snapshot Backup * オプションを使用すると、MySQLベースのバックアップにフォールバックできます。

- 必要なもの *

Unified Manager サーバのメンテナンスコンソールへのログインが許可されているユーザ ID とパスワードが必要です。

手順

1. メンテナンスコンソールにアクセスします
2. バックアップとリストアを実行するには、*メインメニュー*から4を選択します。
3. [バックアップと復元] メニューから 2 を選択します。
4. 「NetApp Snapshot バックアップの設定を解除」で 4 を選択します。

実行される操作が表示され、サービスの停止、シンボリックリンクの解除、ストレージからディレクトリ

へのデータの移動、サービスの再開が可能になります。

バックアップ方法を変更すると、バックアップメカニズムがSnapshotコピーからデフォルトのMySQLバックアップに変更されます。この変更は、[一般]設定の[データベースバックアップ]セクションに表示されます。

Unified Manager のオンデマンドバックアップ

Active IQ Unified Manager のユーザインターフェイスを使用して、必要に応じてオンデマンドバックアップを生成することができます。オンデマンドバックアップを使用すると、既存のバックアップ方式で瞬時にバックアップを作成できます。オンデマンドバックアップでは、MySQL や NetApp Snapshot ベースのバックアップが区別されません。

[データベース・バックアップ] ページの [今すぐバックアップ] ボタンを使用して、オンデマンド・バックアップを実行できます。オンデマンドバックアップは、Active IQ Unified Manager 用に設定したスケジュールに依存しません。

Linux システムへの Unified Manager 仮想アプライアンスの移行

Unified Manager を実行するホストオペレーティングシステムを変更する場合は、Unified Manager の MySQL データベースダンプバックアップを仮想アプライアンスから Red Hat Enterprise Linux システムまたは CentOS Linux システムにリストアすることができます。

- 必要なもの *
- 仮想アプライアンス：
 - オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
 - リストア処理用に、Unified Manager のメンテナンスユーザの名前を確認しておく必要があります。
- Linux システム：
 - の手順に従って、LinuxサーバにUnified Managerがインストールされている必要があります "[Linux システムへの Unified Manager のインストール](#)"。
 - このサーバの Unified Manager のバージョンは、バックアップファイルを使用する仮想アプライアンスのバージョンと同じである必要があります。
 - インストールが完了しても、UI を起動したり、クラスタ、ユーザ、または認証設定を設定したりしないでください。この情報は、リストアプロセスでバックアップファイルに取り込まれます。
 - Linux ホストの root ユーザのクレデンシャルが必要です。

ここでは、仮想アプライアンスにバックアップファイルを作成し、そのバックアップファイルを Red Hat Enterprise Linux または CentOS のシステムにコピーして、新しいシステムにデータベースバックアップをリストアする方法について説明します。

手順

1. 仮想アプライアンスで、* Management * > * Database Backup * をクリックします。
2. [* データベース・バックアップ *] ページで、[* バックアップ設定 *] をクリックします。
3. バックアップパスを /jail / サポートに変更します。

4. Schedule（スケジュール）セクションで、Scheduled Daily（毎日のスケジュール）を選択し、バックアップがすぐに作成されるように、現在の時刻から数分経過した時刻を入力します。
5. [適用（Apply）] をクリックします。
6. バックアップが生成されるまで数時間待ちます。

フルバックアップは 1GB を超えることもあり、完了までに 3~4 時間かかる場合があります。

7. Unified ManagerがインストールされているLinuxホストにrootユーザとしてログインし、仮想アプライアンスでSCPを使用してバックアップファイルを/サポートからコピーします.
root@<rhel_server>:/#
scp -r admin@<vapp_server_ip_address>:/support/* .

```
root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
```

/database-dumps-repo サブディレクトリに .7z バックアップファイルとすべての .7z リポジトリファイルがコピーされたことを確認してください。

8. コマンドプロンプトで、バックアップをリストアします。um backup restore -f
/<backup_file_path>/<backup_file_name>

```
um backup restore -f /UM_9.7.N151113.1348_backup_unix_02-12-2019-04-16.7z
```

9. リストア処理が完了したら、Unified Manager Web UI にログインします。

次のタスクを実行する必要があります。

- 新しい HTTPS セキュリティ証明書を生成し、Unified Manager サーバを再起動します。
- Linux システムに jail / サポートパスがないため、バックアップパスを Linux システムのデフォルト設定（/data/ocum-backup）または任意の新しいパスに変更します。
- WFA を使用している場合は、Workflow Automation の接続の両側を再設定します。
- SAML を使用している場合は、SAML 認証の設定を再設定します。

Linux システムですべてが想定どおりに動作していることを確認したら、Unified Manager 仮想アプライアンスをシャットダウンして削除できます。

スクリプトの管理

Unified Manager で複数のストレージオブジェクトを自動的に変更または更新するスクリプトを作成することができます。スクリプトはアラートに関連付けられます。イベントによってアラートがトリガーされるとスクリプトが実行されます。カスタムスクリプトをアップロードし、アラートが生成されたときの動作をテストすることができます。

スクリプトを Unified Manager にアップロードして実行する機能は、デフォルトで有効になっています。セキュリティ上の理由からこの機能を許可しない場合は、* ストレージ管理 * > * 機能設定 * からこの機能を無効にできます。

スクリプトとアラートの連携方法

Unified Manager でイベントに対するアラートが発生したときにスクリプトが実行される

ように、スクリプトにアラートを関連付けることができます。スクリプトを使用して、ストレージオブジェクトの問題を解決したり、イベントの生成元のストレージオブジェクトを特定したりできます。

Unified Manager でイベントに対するアラートが生成されると、指定した受信者にアラート E メールが送信されます。アラートがスクリプトに関連付けられている場合は、そのスクリプトが実行されます。スクリプトに渡された引数の詳細をアラート E メールから取得できます。



カスタムスクリプトを作成し、そのスクリプトを特定のイベントタイプのアラートに関連付けた場合、そのイベントタイプのカスタムスクリプトに基づいて操作が実行されます。* Fix it * アクションは、デフォルトでは管理アクションページまたは Unified Manager ダッシュボードで使用できません。

スクリプトの実行には次の引数が使用されます。

- -eventID
- -eventName
- -eventSeverity
- -eventSourceID
- -eventSourceName
- -eventSourceType
- -eventState
- -eventArgs

これらの引数をスクリプトで使用して、関連するイベントの情報を収集したり、ストレージオブジェクトを変更したりできます。

スクリプトから引数を取得する例

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

アラートが生成されると、このスクリプトが実行され、次の出力が表示されます。

```
-eventID : 290
-eventSourceID : 4138
```

スクリプトの追加

Unified Manager でスクリプトを追加し、アラートに関連付けることができます。アラートが生成されるとこれらのスクリプトが自動的に実行されるため、イベントが生成されたストレージオブジェクトに関する情報を取得できます。

- 必要なもの *
- Unified Manager サーバに追加するスクリプトを作成して保存しておく必要があります。
- サポートされるスクリプトのファイル形式は、Perl、Shell、PowerShell、Python、およびです .bat ファイル。

Unified Manager がインストールされているプラットフォーム	サポートされている言語
VMware	Perl / シェルスクリプト
Linux の場合	Perl、Python、シェルの各スクリプト
Windows の場合	PowerShell、Perl、Python、.bat スクリプト

- Perl スクリプトを使用するには、Perl が Unified Manager サーバにインストールされている必要があります。VMware 環境には Perl 5 がデフォルトでインストールされ、Perl 5 のサポート対象のみがスクリプトでサポートされます。Unified Manager のあとに Perl をインストールした場合は、Unified Manager サーバを再起動する必要があります。
- PowerShell スクリプトを使用するには、スクリプトを実行するための適切な PowerShell 実行ポリシーが Windows サーバで設定されている必要があります。



スクリプトでログファイルを作成してアラートスクリプトの進捗を追跡する場合は、ログファイルが Unified Manager のインストールフォルダ内に作成されないようにする必要があります。

- アプリケーション管理者またはストレージ管理者のロールが必要です。

カスタムスクリプトをアップロードし、アラートに関するイベントの詳細を収集できます。



この機能がユーザインターフェイスに表示されない場合は、管理者によって無効にされています。この機能は、必要に応じて、* Storage Management * > * Feature Settings * から有効にできます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Scripts * をクリックします。
2. [* スクリプト *] ページで、[* 追加] をクリックします。
3. [スクリプトの追加 *] ダイアログボックスで、[* 参照 *] をクリックしてスクリプトファイルを選択します。
4. 選択したスクリプトの概要を入力します。
5. [追加 (Add)] をクリックします。

スクリプトの削除

不要または無効になったスクリプトは、Unified Manager から削除できます。

- 必要なもの *

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- スクリプトがアラートに関連付けられていないことを確認する必要があります。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Scripts * をクリックします。
2. [* スクリプト *] ページで、削除するスクリプトを選択し、[* 削除] をクリックします。
3. [警告 *] ダイアログボックスで、[はい] をクリックして削除を確認します。

スクリプトの実行テスト

ストレージオブジェクトに対してアラートが生成されたときにスクリプトが正しく実行されるかどうかを確認することができます。

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- サポートされるファイル形式のスクリプトを Unified Manager にアップロードしておく必要があります。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Scripts * をクリックします。
2. [スクリプト] ページで、テストスクリプトを追加します。
3. 左側のナビゲーションペインで、 * Storage Management * > * Alert Setup * をクリックします。
4. [* Alert Setup*] ページで、次のいずれかの操作を実行します。

目的	手順
アラートを追加します	<ol style="list-style-type: none"> a. [追加 (Add)] をクリックします。 b. [アクション] セクションで、アラートをテストスクリプトに関連付けます。
アラートを編集する	<ol style="list-style-type: none"> a. アラートを選択し、* 編集 * をクリックします。 b. [アクション] セクションで、アラートをテストスクリプトに関連付けます。

5. [保存 (Save)] をクリックします。
6. [* アラート設定 *] ページで、追加または変更したアラートを選択し、[* テスト *] をクリックします。

スクリプトは「-test」引数を使用して実行され、アラートの作成時に指定された電子メールアドレスに通知アラートが送信されます。

グループの管理と監視

Unified Manager でグループを作成してストレージオブジェクトを管理できます。

グループの概要

Unified Manager でグループを作成してストレージオブジェクトを管理できます。グループの概念とグループルールを使用してストレージオブジェクトをグループに追加する方法を理解しておくと、環境内のストレージオブジェクトを管理するのに役立ちます。

グループとは

グループとは、種類の異なるストレージオブジェクト（クラスタ、SVM、またはボリューム）の動的な集まりです。Unified Manager でグループを作成することで、一連のストレージオブジェクトを簡単に管理できます。グループのメンバーは、その時点で Unified Manager が監視しているストレージオブジェクトに応じて変更される場合があります。

- 各グループには一意の名前が付けられます。
- グループごとに少なくとも 1 つのグループルールを設定する必要があります。
- 1 つのグループを複数のグループルールに関連付けることができます。
- 各グループには、クラスタ、SVM、ボリュームなど、複数のタイプのストレージオブジェクトを含めることができます。
- ストレージオブジェクトは、グループルールが作成されたタイミング、または Unified Manager による監視サイクルが完了したタイミングに基づいて、動的にグループに追加されます。
- ボリュームのしきい値の設定など、グループ内のすべてのストレージオブジェクトに対する処理を同時に適用できます。

グループでのグループルールの仕組み

グループルールとは、ストレージオブジェクト（ボリューム、クラスタ、または SVM）を特定のグループに追加する基準を定義したものです。グループのグループルールは、条件グループまたは条件を使用して定義できます。

- グループにはグループルールを関連付ける必要があります。
- グループルールにはオブジェクトタイプを関連付ける必要があります。関連付けることができるオブジェクトタイプは 1 つだけです。
- グループに対してストレージオブジェクトが追加または削除されるのは、各監視サイクルの完了後、またはルールの作成、編集、削除時です。
- グループルールには 1 つ以上の条件グループを、各条件グループには 1 つ以上の条件を含めることができます。
- ストレージオブジェクトは、作成したグループルールに基づいて複数のグループに属することができます。

条件：

複数の条件グループを作成し、各条件グループに 1 つ以上の条件を含めることができます。グループのグループルールに定義されたすべての条件グループを適用して、グループに含めるストレージオブジェクトを指定することができます。

条件グループ内の条件は論理 AND を使用して実行されます。条件グループのすべての条件が満たされている必要があります。条件はグループルールを作成または変更すると作成され、条件グループのすべての条件を満たすストレージオブジェクトのみが適用、選択、およびグループの対象となります。グループに含めるストレージオブジェクトの範囲を限定するには、条件グループで複数の条件を使用します。

次のオペランドと演算子を使用して必要な値を指定することで、ストレージオブジェクトの条件を作成できます。

ストレージオブジェクトのタイプ	適用可能なオペランド
ボリューム	<ul style="list-style-type: none">• オブジェクト名• 所有クラスタ名• 所有 SVM 名• 注釈
SVM	<ul style="list-style-type: none">• オブジェクト名• 所有クラスタ名• 注釈
クラスタ	<ul style="list-style-type: none">• オブジェクト名• 注釈

ストレージ・オブジェクトのオペランドとしてアノテーションを選択すると 'is' 演算子を使用できますそれ以外のオペランドについては ' 演算子として Is または Contains を選択できます

- オペランド

Unified Manager では、選択したオブジェクトタイプによってリストに表示されるオペランドが変わります。リストには、オブジェクト名、所有クラスタ名、所有 SVM 名、および Unified Manager で定義したアノテーションが含まれます。

- 演算子

演算子のリストは、条件に対して選択したオペランドによって変わります。Unified Manager でサポートされる演算子は「Is」で、「contains」です。

「Is」演算子を選択すると、選択したオペランドの値が指定した値と完全に一致する場合に条件が評価されます。

"contains" 演算子を選択すると、条件は次のいずれかの条件を満たすように評価されます。

- 選択したオペランドの値が指定した値と完全に一致する
- 選択したオペランドの値に指定した値が含まれる

- 価値

値のフィールドは、選択したオペランドによって変わります。

条件を使用したグループルールの例

ボリュームに対する条件グループで、次の 2 つの条件が定義されているとします。

- 名前に「vol」を含む
- SVM 名は「data_svm」です。

この条件グループでは、名前に「vol」を含み、「data_svm」という名前の SVM でホストされているすべてのボリュームが選択されます。

条件グループ

条件グループは論理 OR を使用して実行され、ストレージオブジェクトに適用されます。ストレージオブジェクトがグループに追加されるためには、いずれかの条件グループを満たす必要があります。すべての条件グループのストレージオブジェクトがまとめられます。条件グループを使用して、グループに含めるストレージオブジェクトの範囲を広げることができます。

条件グループを使用したグループルールの例

ボリュームに対する 2 つの条件グループで、各グループにそれぞれ次の 2 つの条件が定義されているとします。

- 条件グループ 1
 - 名前に「vol」を含む
 - SVM 名が「data_svm」の場合、条件グループ 1 では、名前に「vol」を含み、名前が「data_svm」の SVM でホストされているすべてのボリュームが選択されます。
- 条件グループ 2.
 - 名前に「vol」を含む
 - data-priority のアノテーション値は「critical」条件グループ 2 では、名前に「vol」を含み、data-priority アノテーションの値「critical」とアノテートされているすべてのボリュームが選択されます。

これらの 2 つの条件グループを含むグループルールをストレージオブジェクトに適用した場合、選択したグループに次のストレージオブジェクトが追加されます。

- 名前に「vol」を含み、「data_svm」という名前の SVM でホストされているすべてのボリューム
- 名前に「vol」を含み、data-priority アノテーションの値「critical」でアノテートされているすべてのボリューム

ストレージオブジェクトでのグループ操作の仕組み

グループアクションは、グループ内のすべてのストレージオブジェクトに対して実行される処理です。たとえば、ボリュームしきい値のグループアクションを設定して、グループ内のすべてのボリュームのしきい値を同時に変更できます。

グループは、一意のグループアクションタイプをサポートします。ボリューム健全性しきい値タイプのグループアクションは 1 つのグループに 1 つしか設定できません。ただし、同じグループに別のタイプのグループアクションがある場合は、それを設定できます。グループアクションがストレージオブジェクトに適用される順序はアクションのランクで決まります。ストレージオブジェクトに適用されるグループアクションの情報は、ストレージオブジェクトの詳細ページで確認できます。

一意なグループアクションの例

ボリューム A がグループ G1 と G2 に属しており、これらのグループに次のボリューム健全性しきい値グループアクションが設定されているとします。

- `Change_capacity_threshold` ボリュームの容量を設定するためのランク1のグループ操作
- `Change_snapshot_copies` グループ操作のランク2。ボリュームのSnapshotコピーを設定します

。 `Change_capacity_threshold` グループ操作は、よりも常に優先されます `Change_snapshot_copies` グループ操作でボリュームAに適用されます Unified Managerによる監視サイクルが1回完了すると、ボリュームAの健全性しきい値関連イベントがごとに再評価されます `Change_capacity_threshold` グループ操作 G1 または G2 のどちらのグループにも、ボリュームしきい値タイプの別のグループアクションを設定することはできません。

グループの追加

クラスタ、ボリューム、および Storage Virtual Machine （ SVM ） を管理しやすいように、グループを作成して 1 つにまとめることができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

グループルールを定義して、グループのメンバーを追加または削除したり、グループに対するグループ操作を変更したりできます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Groups * をクリックします。
2. [* グループ *] タブで、[* 追加] をクリックします。
3. [グループの追加 *] ダイアログボックスで、グループの名前と概要を入力します。
4. [追加（Add）] をクリックします。

グループの編集

Unified Manager で作成したグループの名前と概要を編集できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

グループを編集して名前を更新する場合は、一意の名前を指定する必要があります。既存のグループ名は使用できません。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Groups * をクリックします。
2. [* グループ *] タブで、編集するグループを選択し、[* 編集 *] をクリックします。
3. [グループの編集 *] ダイアログボックスで、グループの名前、概要、またはその両方を変更します。

4. [保存 (Save)] をクリックします。

グループの削除

不要になったグループは、 Unified Manager から削除できます。

- 必要なもの *
- 削除するグループのグループルールに関連付けられたストレージオブジェクト（クラスタ、 SVM 、またはボリューム）がないことを確認する必要があります。
- アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Groups * をクリックします。
2. [* グループ *] タブで、削除するグループを選択し、 [* 削除 *] をクリックします。
3. [警告 *] ダイアログボックスで、 [はい] をクリックして削除を確認します。

グループを削除しても、そのグループに関連付けられているグループ操作は削除されません。ただし、グループを削除すると、これらのグループ操作のマッピングは解除されます。

グループルールを追加しています

グループのグループルールを作成して、ボリューム、クラスタ、 Storage Virtual Machine （ SVM ）などのストレージオブジェクトを動的にグループに追加できます。グループルールを作成するには、少なくとも 1 つの条件を含む条件グループを少なくとも 1 つ設定する必要があります。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

監視中のストレージオブジェクトは、グループルールを作成後すぐに追加されます。新しいオブジェクトは、監視サイクルの完了後に追加されます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Groups * をクリックします。
2. [* グループルール *] タブで、 [* 追加] をクリックします。
3. [グループルールの追加 *] ダイアログボックスで、グループルールの名前を指定します。
4. [ターゲットオブジェクトタイプ *] フィールドで、グループ化するストレージオブジェクトのタイプを選択します。
5. [* グループ *] フィールドで、グループルールを作成する必要があるグループを選択します。
6. [条件 *] セクションで、次の手順を実行して条件、条件グループ、またはその両方を作成します。

を作成します	手順
条件	<ul style="list-style-type: none"> a. オペランドのリストからオペランドを選択します。 b. 演算子として「* Contains *」または「* is *」を選択します。 c. 値を入力するか、使用可能な値のリストから値を選択します。
条件グループ	<ul style="list-style-type: none"> a. [条件グループの追加（ Add Condition Group ）] をクリックする b. オペランドのリストからオペランドを選択します。 c. 演算子として「* Contains *」または「* is *」を選択します。 d. 値を入力するか、使用可能な値のリストから値を選択します。 e. 必要に応じて、[条件の追加（ Add Condition ）] をクリックして条件をさらに作成し、条件ごとに手順 a ~ d を繰り返します。

7. [追加（ Add ）] をクリックします。

グループルールの作成例

[Add Group Rule] ダイアログボックスで次の手順を実行して、条件の設定および条件グループの追加を含むグループルールを作成します。

手順

1. グループルールの名前を指定します。
2. オブジェクトタイプとして Storage Virtual Machine （ SVM ）を選択します。
3. グループのリストからグループを選択します。
4. 条件セクションで、オペランドとして * オブジェクト名 * を選択します。
5. 演算子として * Contains * を選択します。
6. 値をと入力します `svm_data`。
7. [* 条件グループの追加 *] をクリックします。
8. オペランドとして * オブジェクト名 * を選択します。
9. 演算子として * Contains * を選択します。
10. 値をと入力します `vol`。
11. [条件の追加（ Add Condition ）] をクリックする。
12. ステップ 8 のオペランドとして * data-priority * を選択し、ステップ 9 の演算子として * is * を、ステップ 10 の値として * critical * を選択して、ステップ 8 から 10 を繰り返します。

13. * Add * をクリックして、グループルールの条件を作成します。

グループルールを編集しています

グループルールを編集して条件グループおよび条件グループに含まれる条件を変更することで、特定のグループに対してまたは特定のグループからストレージオブジェクトを追加または削除できます。

• 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Groups * をクリックします。
2. [* グループルール *] タブで、編集するグループルールを選択し、[* 編集 *] をクリックします。
3. Edit Group Rule * ダイアログボックスで、グループルールの名前、関連付けられているグループ名、条件グループ、および条件を必要に応じて変更します。



グループルールのターゲットオブジェクトタイプは変更できません。

4. [保存 (Save)] をクリックします。

グループルールを削除しています

不要になったグループルールは Active IQ Unified Manager から削除できます。

• 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

グループルールを削除すると、関連付けられているストレージオブジェクトがグループから削除されます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Groups * をクリックします。
2. [* グループルール *] タブで、削除するグループルールを選択し、[* 削除 *] をクリックします。
3. [警告 *] ダイアログボックスで、[はい] をクリックして削除を確認します。

グループ操作の追加

グループ内のストレージオブジェクトに適用するグループ操作を設定できます。グループのアクションを設定すると、これらのアクションを各オブジェクトに個別に追加する必要がないため、時間を節約できます。

• 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Groups * をクリックします。
2. [* グループアクション *] タブで、[* 追加 *] をクリックします。
3. [グループアクションの追加 * (Add Group Action *)] ダイアログボックスで、アクションの名前と概要を入力します。
4. [グループ *] メニューから、アクションを設定するグループを選択します。
5. アクションタイプ * メニューからアクションタイプを選択します。

ダイアログボックスが展開され、選択したアクションタイプに必要なパラメータを設定できます。

6. 必須パラメータに適切な値を入力して、グループ操作を設定します。
7. [追加 (Add)] をクリックします。

グループ操作を編集しています

グループ操作の名前、概要、関連付けられているグループの名前、操作タイプのパラメータなど、Unified Manager で設定したグループ操作のパラメータを編集することができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Groups * をクリックします。
2. [* グループアクション *] タブで、編集するグループアクションを選択し、[* 編集 *] をクリックします。
3. [グループアクションの編集 * (* Edit Group Action *)] ダイアログボックスで、グループアクション名、概要、関連付けられたグループ名、およびアクションタイプのパラメーターを必要に応じて変更します。
4. [保存 (Save)] をクリックします。

グループに対するボリューム健全性しきい値を設定する

ボリュームの容量、Snapshot コピー、qtree クォータ、増加率、および inode について、グループレベルで健全性しきい値を設定することができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

ボリューム健全性しきい値タイプのグループ操作は、グループのボリュームにのみ適用されます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Groups * をクリックします。
2. [* グループアクション *] タブで、[* 追加 *] をクリックします。

3. グループ操作の名前と概要を入力します。
4. [* グループ*] ドロップダウンボックスから、グループアクションを設定するグループを選択します。
5. ボリュームの健全性しきい値として「* Action Type *」を選択します。
6. しきい値を設定するカテゴリを選択します。
7. 健全性しきい値の必要な値を入力します。
8. [追加 (Add)] をクリックします。

グループ操作を削除しています

不要になったグループ操作は、Unified Manager から削除できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

ボリューム健全性しきい値のグループ操作を削除すると、そのグループ内のストレージオブジェクトにグローバルしきい値が適用されます。ストレージオブジェクトに対して設定されたオブジェクトレベルの健全性しきい値には影響はありません。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Groups * をクリックします。
2. [* グループアクション*] タブで、削除するグループアクションを選択し、[* 削除*] をクリックします。
3. [警告*] ダイアログボックスで、[はい] をクリックして削除を確認します。

グループ操作の順序を変更する

グループ操作をグループ内のストレージオブジェクトに適用する順序を変更することができます。グループ操作は、ランクに基づいてストレージオブジェクトに順番に適用されます。グループ操作には、設定した時点では最も低いランクが割り当てられます。要件に応じてグループ操作のランクを変更することができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

単一の行または複数の行を選択し、ドラッグアンドドロップ操作を複数実行してグループ操作のランクを変更することができます。ただし、変更後の優先度を変更してグループ操作のグリッドに反映するには、保存する必要があります。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Groups * をクリックします。
2. [グループアクション] タブで、[*Reorder] をクリックします。
3. [グループアクションの並べ替え*] ダイアログボックスで、行をドラッグアンドドロップしてグループアクションの順序を必要に応じて並べ替えます。

4. [保存 (Save)] をクリックします。

アノテーションを使用したストレージオブジェクトイベントの優先順位の設定

アノテーションルールを作成してストレージオブジェクトに適用すると、適用されたアノテーションのタイプとその優先度に基づいてオブジェクトを特定し、フィルタリングできるようになります。

アノテーションに関する詳細情報

アノテーションの概念を理解しておく、環境内のストレージオブジェクトに関連するイベントを管理するのに役立ちます。

アノテーションとは

アノテーションは、別のテキスト文字列 (値) に割り当てられたテキスト文字列 (名前) です。アノテーションの名前と値の各ペアは、アノテーションルールを使用して動的にストレージオブジェクトに関連付けることができます。事前定義されたアノテーションにストレージオブジェクトを関連付けると、そのアノテーションに関連するイベントをフィルタリングして表示できます。アノテーションは、クラスタ、ボリューム、および Storage Virtual Machine (SVM) に適用できます。

アノテーションの名前には、それぞれ複数の値を割り当てることができます。それらの名前と値の各ペアをルールに基づいてストレージオブジェクトに関連付けることができます。

たとえば、「"ボストン"」と「カナダ」の値を持つ「`data-ccenter"」というアノテーションを作成できます。これにより、ボリューム v1 にアノテーション「`Boston」を「"ボストン"」の値で適用できるようになります。「`data-center'」でアノテートされているボリューム v1 でのイベントに対してアラートが生成されると、生成された E メールにボリュームの場所「Boston」が示されるため、問題の優先順位を設定して解決することができます。

Unified Manager でのアノテーションルールの仕組み

アノテーションルールとは、ストレージオブジェクト (ボリューム、クラスタ、または Storage Virtual Machine (SVM)) をアノテートする基準を定義したものです。アノテーションルールは、条件グループまたは条件のいずれかを使用して定義できます。

- アノテーションには必ずアノテーションルールを関連付ける必要があります。
- アノテーションルールにはオブジェクトタイプを関連付ける必要があります。関連付けることができるオブジェクトタイプは 1 つだけです。
- Unified Manager でストレージオブジェクトに対してアノテーションが追加または削除されるのは、各監視サイクルの完了後、およびルールの作成、編集、削除、順序変更時です。
- アノテーションルールには 1 つ以上の条件グループを、各条件グループには 1 つ以上の条件を含めることができます。
- ストレージオブジェクトには複数のアノテーションを適用できます。特定のアノテーションに対するアノテーションルールの条件で別のアノテーションを使用して、すでにアノテートされているオブジェクトに別のアノテーションを追加することもできます。

条件：

複数の条件グループを作成し、各条件グループに 1 つ以上の条件を含めることができます。アノテーションのアノテーションルールに定義されたすべての条件グループを適用して、ストレージオブジェクトをアノテートすることができます。

条件グループ内の条件は論理 AND を使用して実行されます。条件グループのすべての条件が満たされている必要があります。条件はアノテーションルールを作成または変更すると作成され、条件グループのすべての条件を満たすストレージオブジェクトのみが適用、選択、およびアノテートの対象となります。アノテートするストレージオブジェクトの範囲を限定するには、条件グループで複数の条件を使用します。

次のオペランドと演算子を使用して必要な値を指定することで、ストレージオブジェクトの条件を作成できます。

ストレージオブジェクトのタイプ	適用可能なオペランド
ボリューム	<ul style="list-style-type: none">• オブジェクト名• 所有クラスタ名• 所有 SVM 名• 注釈
SVM	<ul style="list-style-type: none">• オブジェクト名• 所有クラスタ名• 注釈
クラスタ	<ul style="list-style-type: none">• オブジェクト名• 注釈

ストレージ・オブジェクトのオペランドとしてアノテーションを選択すると 'is' 演算子を使用できますそれ以外のオペランドについては ' 演算子として Is または Contains を選択できます「Is」演算子を選択した場合は、選択したオペランドの値が指定した値と完全に一致する場合に条件が評価されます。"contains" 演算子を選択すると、条件は次のいずれかの条件を満たすように評価されます。

- 選択したオペランドの値が指定した値と完全に一致する。
- 選択したオペランドの値に指定した値が含まれる。

条件を使用したアノテーションルールの例

ボリュームに対して条件グループが 1 つ設定されたアノテーションルールで、次の 2 つの条件が定義されているとします。

- 名前に「vol」を含む
- SVM 名は「data_svm」です。

このアノテーションルールでは、名前に「vol」を含み、「data_svm」という名前の SVMs でホストされているすべてのボリュームが、選択したアノテーションとアノテーションタイプでアノテートされます。

条件グループ

条件グループは論理 OR を使用して実行され、ストレージオブジェクトに適用されます。ストレージオブジェクトがアノテートされるためには、いずれかの条件グループの要件を満たす必要があります。すべての条件グループの条件を満たすすべてのストレージオブジェクトがアノテートされます。条件グループを使用して、アノテートするストレージオブジェクトの範囲を広げることができます。

条件グループを使用したアノテーションルールの例

ボリュームに対する条件グループが 2 つ設定されたアノテーションルールで、各グループにそれぞれ次の 2 つの条件が定義されているとします。

- 条件グループ 1
 - 名前に「vol」を含む
 - SVM 名が「d ATA_SVM」である場合、この条件グループでは、名前に「vol」を含み、「d ATA_SVM」という名前の SVM でホストされているすべてのボリュームがアノテートされます。
- 条件グループ 2.
 - 名前に「vol」を含む
 - data-priority のアノテーション値は「critical」ですこの条件グループは '名前に「vol」を含み 'data-priority アノテーションの値「critical」でアノテートされているすべてのボリュームをアノテートします

これらの 2 つの条件グループを含むアノテーションルールをストレージオブジェクトに適用した場合、次のストレージオブジェクトがアノテートされます。

- 名前に「vol」を含み、「d ata_SVM」という名前の SVM でホストされているすべてのボリューム
- 名前に「vol」を含み、data-priority アノテーションの値「critical」でアノテートされているすべてのボリューム

事前定義されたアノテーション値の概要

- Data-priority * は、Mission critical、High、および Low という値を持つ事前定義されたアノテーションです。これらの値を使用して、格納されているデータの優先度に基づいて、ストレージオブジェクトをアノテートできます。事前定義されたアノテーションの値を編集または削除することはできません。

- * データ優先度：ミッションクリティカル *

このアノテーションは、ミッションクリティカルなデータが格納されたストレージオブジェクトに適用されます。たとえば、本番用アプリケーションを含むオブジェクトなどが考えられます。

- * データ優先度：高 *

このアノテーションは、優先度の高いデータが格納されたストレージオブジェクトに適用されます。たとえば、ビジネスアプリケーションをホストしているオブジェクトなどが考えられます。

- * データ優先度：低 *

このアノテーションは、優先度の低いデータが格納されたストレージオブジェクトに適用されます。たとえば、バックアップやミラーのデスティネーションなど、セカンダリストレージにあるオブジェクトなどが考えられます。

アノテーションの動的な追加

Unified Manager でカスタムアノテーションを作成すると、クラスタ、Storage Virtual Machine（SVM）、およびボリュームがルールに基づいてアノテーションに動的に関連付けられます。ルールにより、ストレージオブジェクトにアノテーションが自動的に割り当てられます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Annotations * をクリックします。
2. [* 注釈 *] ページで、[* 注釈の追加 *] をクリックします。
3. [注釈の追加 * (* Add Annotation *)] ダイアログボックスで、注釈の名前と概要を入力します。
4. オプション：アノテーション値 * セクションで、* 追加 * をクリックしてアノテーションに値を追加します。
5. [保存 (Save)] をクリックします。

アノテーションへの値の追加

アノテーションに値を追加し、アノテーションの名前と値の特定のペアにストレージオブジェクトを関連付けることができます。アノテーションに値を追加することで、より効率的にストレージオブジェクトを管理できるようになります。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

定義済みのアノテーションに値を追加することはできません。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Annotations * をクリックします。
2. [* 注釈 * (* Annotations *)] ページで、値を追加する注釈を選択し、[* 値 * (* Values *)] セクションで [* 追加 (* Add *)] をクリックする。
3. アノテーション値の追加 * (* Add Annotation Value *) ダイアログボックスで、アノテーションの値を指定します。

指定する値は、選択したアノテーションで一意である必要があります。

4. [追加 (Add)] をクリックします。

アノテーションを削除する

不要になったカスタムアノテーションとその値を削除できます。

- 必要なもの *

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- アノテーションの値が他のアノテーションやグループルールで使用されていないことを確認する必要があります。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Annotations * をクリックします。
2. [* 注釈 * (* Annotations *)] タブで、削除する注釈を選択する。

選択したアノテーションの詳細が表示されます。

3. 選択したアノテーションとその値を削除するには、 * Actions * > * Delete * をクリックします。
4. 警告ダイアログボックスで、「 * はい * 」をクリックして削除を確認します。

アノテーションリストおよび詳細の表示

クラスタ、ボリューム、および Storage Virtual Machine (SVM) に動的に関連付けられるアノテーションのリストを確認することができます。また、概要、 Created By 、 Created Date 、 Values 、 rules などの詳細も参照できます。 およびアノテーションに関連付けられているオブジェクト。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Annotations * をクリックします。
2. アノテーション * タブでアノテーション名をクリックすると、関連付けられている詳細が表示されます。

アノテーションから値を削除する

カスタムアノテーションに関連付けられている値がアノテーションの環境でなくなった場合は、その値を削除できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- アノテーションの値がアノテーションルールやグループルールに関連付けられていないことを確認する必要があります。

定義済みのアノテーションから値を削除することはできません。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Annotations * をクリックします。
2. アノテーション * タブのアノテーションリストで、値を削除するアノテーションを選択します。
3. [注釈 *] タブの [値 *] 領域で、削除する値を選択し、 [* 削除 *] をクリックします。
4. 警告 * (Warning *) ダイアログボックスで、 * はい * (* Yes) をクリックします。

値が削除され、選択したアノテーションの値のリストに表示されなくなります。

アノテーションルールの作成

Unified Manager がボリューム、クラスタ、Storage Virtual Machine（SVM）などのストレージオブジェクトを動的にアノテートするために使用するアノテーションルールを作成できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

監視中のストレージオブジェクトは、アノテーションルールの作成後すぐにアノテートされます。新しいオブジェクトは、監視サイクルの完了後にアノテートされます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Annotations * をクリックします。
2. [* 注釈ルール *（* Annotation Rules *）] タブで、[* 追加（* Add *）] をクリックする
3. アノテーションルールの追加 * ダイアログボックスで、アノテーションルールの名前を指定します。
4. [* ターゲットオブジェクトタイプ *] フィールドで、アノテーションを適用するストレージオブジェクトのタイプを選択します。
5. [* アノテーションの適用 *] フィールドで、使用するアノテーションとアノテーションの値を選択します。
6. [条件] セクションで、条件、条件グループ、またはその両方を作成するための適切なアクションを実行します。

作成対象	手順
条件	<ol style="list-style-type: none">a. オペランドのリストからオペランドを選択します。b. 演算子として「* Contains *」または「* is *」を選択します。c. 値を入力するか、使用可能な値のリストから値を選択します。
条件グループ	<ol style="list-style-type: none">a. [条件グループの追加（Add Condition Group）] をクリックする。b. オペランドのリストからオペランドを選択します。c. 演算子として「* Contains *」または「* is *」を選択します。d. 値を入力するか、使用可能な値のリストから値を選択します。e. 必要に応じて、[条件の追加（Add Condition）] をクリックして条件をさらに作成し、条件ごとに手順 a ~ d を繰り返します。

7. [追加（Add）] をクリックします。

アノテーションルールの作成例

アノテーションルールを作成し、条件の設定と条件グループの追加を行うには、アノテーションルールの追加ダイアログで次の手順を実行します。

手順

1. アノテーションルールの名前を指定します。
2. ターゲットオブジェクトタイプとして Storage Virtual Machine（SVM）を選択します。
3. アノテーションのリストからアノテーションを選択し、値を指定します。
4. 条件セクションで、オペランドとして * オブジェクト名 * を選択します。
5. 演算子として * Contains * を選択します。
6. 値をと入力します svm_data。
7. [* 条件グループの追加 *] をクリックします。
8. オペランドとして * オブジェクト名 * を選択します。
9. 演算子として * Contains * を選択します。
10. 値をと入力します vol。
11. [条件の追加（Add Condition）] をクリックする。
12. 手順 8 から 10 を繰り返し、手順 8 のオペランドとして「* data-priority *」を選択し、手順 9 の演算子として「* is *」を、手順 10 の値として「* mission-critical」を選択します。
13. [追加（Add）] をクリックします。

個々のストレージオブジェクトへの手動でのアノテーションの追加

アノテーションルールを使用せずに、選択したボリューム、クラスタ、SVMs を手動でアノテートできます。単一のストレージオブジェクトまたは複数のストレージオブジェクトをアノテートし、必要なアノテーションの名前と値のペアを指定できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. アノテートするストレージオブジェクトに移動します。

アノテーションの追加先	手順
クラスタ	a. [* ストレージ * > * クラスタ *] をクリックします。 b. 1 つ以上のクラスタを選択します。

アノテーションの追加先	手順
個のボリューム	a. [* ストレージ > ボリューム *] をクリックします。 b. 1 つ以上のボリュームを選択します。
SVM	a. [* ストレージ * > * SVMs *] をクリックします。 b. 1 つ以上の SVM を選択します。

2. 「* 注釈を付ける *」をクリックして、名前と値のペアを選択します。

3. [適用 (Apply)] をクリックします。

アノテーションルールの編集

アノテーションルールを編集して条件グループおよび条件グループに含まれる条件を変更することで、ストレージオブジェクトに対してアノテーションを追加または削除できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

関連するアノテーションルールを編集すると、ストレージオブジェクトへのアノテーションの関連付けが解除されます。

手順

1. 左側のナビゲーションペインで、* Storage Management * > * Annotations * をクリックします。
2. [* アノテーションルール *] タブで、編集するアノテーションルールを選択し、[* アクション *]、[* 編集 *] の順にクリックします。
3. アノテーションルールの編集 * ダイアログボックスで、ルールの名前、アノテーションの名前と値、条件グループ、および条件を必要に応じて変更します。

アノテーションルールのターゲットオブジェクトタイプは変更できません。

4. [保存 (Save)] をクリックします。

アノテーションルールの条件の設定

1 つ以上の条件を設定して、Unified Manager がストレージオブジェクトに適用するアノテーションルールを作成できます。アノテーションルールに一致するストレージオブジェクトに、ルールで指定した値がアノテートされます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Annotations * をクリックします。
2. [* 注釈ルール * (* Annotation Rules *)] タブで、[* 追加 (* Add *)] をクリックする
3. [* アノテーションルールの追加 * (* Add Annotation Rule *)] ダイアログボックスで、ルールの名前を入力します。
4. ターゲットオブジェクトタイプリストからオブジェクトタイプを 1 つ選択し、リストからアノテーションの名前と値を選択します。
5. ダイアログボックスの * 条件 * (* Conditions *) セクションで、リストからオペランドと演算子を選択して条件値を入力するか、* 条件の追加 * (* Add Condition *) をクリックして新しい条件を作成します。
6. [保存して追加] をクリックします。

アノテーションルールの条件の設定例

オブジェクトタイプが SVM で、オブジェクト名に「'vm_data'」が含まれている場合は、条件を考慮します。

[Add Annotation Rule] ダイアログボックスで次の手順を実行して、条件を設定します。

手順

1. アノテーションルールの名前を入力します。
2. ターゲットオブジェクトタイプとして SVM を選択します。
3. アノテーションのリストからアノテーションと値を選択します。
4. [* 条件 * (* Conditions *)] フィールドで、オペランドとして [* オブジェクト名 * (* Object Name *)] を選択します。
5. 演算子として * Contains * を選択します。
6. 値をと入力します svm_data。
7. [追加 (Add)] をクリックします。

アノテーションルールを削除する

不要になったアノテーションルールは、Active IQ Unified Manager から削除できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

アノテーションルールを削除すると、アノテーションの関連付けが解除されてストレージオブジェクトから削除されます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Annotations * をクリックします。
2. [* アノテーションルール * (* Annotation Rules *)] タブで、削除するアノテーションルールを選択し、[* 削除 * (* Delete *)] をクリックします。
3. [警告 *] ダイアログボックスで、[はい *] をクリックして削除を確認します。

アノテーションルールの順序を変更する

Unified Manager で、アノテーションルールをストレージオブジェクトに適用する順序を変更することができます。アノテーションルールは、ランクに基づいてストレージオブジェクトに順番に適用されます。アノテーションルールには、設定した時点では最も低いランクが割り当てられます。ただし、要件に応じてアノテーションルールのランクを変更することができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

単一の行または複数の行を選択し、ドラッグアンドドロップ操作を繰り返し行って、アノテーションルールのランクを変更することができます。ただし 'アノテーションルールタブに再優先順位付けを表示するには' 変更を保存する必要があります

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Annotations * をクリックします。
2. [* 注釈ルール * (* Annotation Rules *)] タブで、[* リオーダー * (* Reorder *)]
3. アノテーションルールの順序を変更するには、* アノテーションルールの順序変更 * ダイアログボックスで 1 つまたは複数の行をドラッグアンドドロップします。
4. [保存 (Save)] をクリックします。

順序変更を表示するには、変更を保存する必要があります。

Web UI およびメンテナンスコンソールからのサポートバンドルの送信

サポートバンドルの送信が必要となるのは、問題メッセージよりも詳しい診断とトラブルシューティングが必要な AutoSupport です。Unified Manager Web UI およびメンテナンスコンソールを使用して、サポートバンドルをテクニカルサポートに送信できます。

Unified Manager では、最大 2 つの完全なサポートバンドルと 3 つの軽量のサポートバンドルが一度に保存されます。

- 関連情報 *

"Unified Manager のユーザロールと機能"

テクニカルサポートに **AutoSupport** メッセージとサポートバンドルを送信する

AutoSupport ページでは、事前定義されたオンデマンドの AutoSupport メッセージをテクニカルサポートチームに送信して、環境の正しい運用や環境の整合性の維持に役立てることができます。AutoSupport はデフォルトで有効になっており、NetAppActive IQ のメリットを活用するためには無効にしないでください。

Unified Manager サーバに関する診断用システムの情報と詳細なデータを必要に応じてメッセージで送信したり、メッセージを定期的に送信するようにスケジュールしたり、テクニカルサポートチームにサポートバンドルを生成して送信したりできます。



ストレージ管理者ロールを持つユーザは、AutoSupport メッセージとサポートバンドルを生成して、テクニカルサポートにオンデマンドで送信できます。ただし、定期的な AutoSupport を有効または無効にしたり、HTTP プロキシサーバの設定セクションの説明に従って HTTP 設定を設定したりできるのは、管理者またはメンテナンスユーザだけです。HTTP プロキシサーバを使用する必要がある環境では、ストレージ管理者がオンデマンドの AutoSupport メッセージとサポートバンドルをテクニカルサポートに送信する前に設定を完了しておく必要があります。

オンデマンドの **AutoSupport** メッセージの送信

テクニカルサポート、指定した E メール受信者、またはその両方に宛てたオンデマンドメッセージを生成して送信できます。

手順

1. 「* 一般 * > * AutoSupport *」に移動し、次のいずれかまたは両方の操作を実行します。
2. AutoSupport メッセージをテクニカルサポートに送信する場合は、* テクニカルサポートに送信 * チェックボックスをオンにします。
3. AutoSupport メッセージを特定の電子メール受信者に送信する場合は、[* 電子メール受信者に送信 *] チェックボックスをオンにして、受信者の電子メールアドレスを入力します。
4. [保存 (Save)] をクリックします。
5. [Generate and Send AutoSupport (生成して送信)] をクリックします。

定期的な **AutoSupport** の有効化

事前定義された特定のメッセージをテクニカルサポートに送信して、問題の診断と解決を定期的に行うことができます。この機能はデフォルトで有効になっています。無効にした場合、管理者ユーザまたはメンテナンスユーザは設定を有効にできます。

手順

1. 「* 一般 * > * AutoSupport *」に移動します。
2. [定期的なデータ (Periodic AutoSupport)] セクションで、[定期的に AutoSupport データを Active IQ に送信する (Enable Sending Data Periodically to)] チェックボックスをオン
3. 必要に応じて、HTTP プロキシサーバの名前、ポート、および認証情報を定義します。詳細については、「HTTP プロキシサーバの設定」の項を参照してください。
4. [保存 (Save)] をクリックします。

オンデマンドサポートバンドルをアップロードしています

トラブルシューティングの要件に基づいて、サポートバンドルを生成し、テクニカルサポートに送信できます。Unified Manager では、生成されたサポートバンドルのうち最新の 2 つだけが保持されます。それよりも古いサポートバンドルはシステムから削除されます。

サポートデータの種類によっては、クラスタリソースを大量に使用したり、完了までに時間がかかることがあるため、完全なサポートバンドルを選択した場合は、特定のデータタイプを追加または除外してサポートバンドルのサイズを縮小できます。また、30 日分のログと構成データベースのレコードを含む軽量のサポートバンドルを作成することもできます。パフォーマンスデータ、取得記録ファイル、サーバヒープダンプは含まれません。

手順

1. 「* 一般 * > * AutoSupport *」に移動します。
2. オンデマンドサポートバンドルセクションで、* サポートバンドルの生成と送信 * をクリックします。
3. 簡易サポートバンドルをテクニカルサポートに送信するには、サポートバンドルの生成と送信ポップアップで、簡易サポートバンドルの生成 チェックボックスをオンにします。
4. または、完全なサポートバンドルを送信するには、[Generate full support Bundle] チェックボックスをオンにします。サポートバンドルに含めるデータタイプと除外するデータタイプを選択します。



データタイプを選択しなかった場合でも、サポートバンドルは他の Unified Manager データで生成されます。

5. バンドルを生成してテクニカルサポートに送信するには、* Send the bundle to Technical Support * チェックボックスを選択します。このチェックボックスをオフにすると、バンドルが生成され、Unified Manager サーバのローカルに格納されます。生成されたサポートバンドルは、あとでVMwareシステムのサポートディレクトリにあるで使用できます /opt/netapp/data/support/ Linuxシステムの場合は、および ProgramData\NetApp\OnCommandAppData\ocum\support Windowsシステム：
6. [送信 (Send)] をクリックします。

HTTP プロキシサーバをセットアップしています

Unified Managerサーバからの直接アクセスが環境によって提供されない場合に、AutoSupport のコンテンツをサポートに送信するためのインターネットアクセスを提供するプロキシを指定できます。このセクションは、管理者およびメンテナンスユーザのみが使用できます。

- * HTTP プロキシ * を使用します

HTTP プロキシとして使用するサーバを識別するには、このチェックボックスをオンにします。

プロキシサーバのホスト名または IP アドレス、およびサーバへの接続に使用するポート番号を入力します。

- * 認証を使用 *

HTTP プロキシとして使用するサーバにアクセスするための認証情報を指定する必要がある場合は、このチェックボックスをオンにします。

HTTP プロキシでの認証に必要なユーザ名とパスワードを入力します。



ベーシック認証のみを提供する HTTP プロキシはサポートされていません。

メンテナンスコンソールへのアクセス

Unified Manager ユーザインターフェイスが動作状態でない場合、またはこのユーザインターフェイスにない機能を実行する必要がある場合は、メンテナンスコンソールにアクセスして Unified Manager システムを管理できます。

- 必要なもの *

Unified Manager をインストールして設定しておく必要があります。

15 分間操作を行わないと、メンテナンスコンソールからログアウトされます。



VMware にインストールした場合、VMware コンソールからメンテナンスユーザとしてすでにログインしているときは、Secure Shell を使用して同時にログインできません。

ステップ

1. メンテナンスコンソールにアクセスするには、次の手順を実行します。

オペレーティングシステム	実行する手順
VMware	<ol style="list-style-type: none">a. Secure Shell を使用して、Unified Manager 仮想アプライアンスの IP アドレスまたは完全修飾ドメイン名に接続します。b. メンテナンスユーザの名前とパスワードを使用してメンテナンスコンソールにログインします。
Linux の場合	<ol style="list-style-type: none">a. Secure Shell を使用して、Unified Manager システムの IP アドレスまたは完全修飾ドメイン名に接続します。b. メンテナンスユーザ（umadmin）の名前とパスワードでシステムにログインします。c. 入力するコマンド <code>maintenance_console</code> を押します。
Windows の場合	<ol style="list-style-type: none">a. 管理者のクレデンシャルで Unified Manager システムにログインします。b. Windows 管理者として PowerShell を起動します。c. 入力するコマンド <code>maintenance_console</code> を押します。

Unified Manager メンテナンスコンソールメニューが表示されます。

サポートバンドルの生成とアップロード

診断情報を含むサポートバンドルを生成して、トラブルシューティングのサポートを受けるためにテクニカルサポートに送信することができます。

Unified Manager 9.8 以降では、Unified Manager サーバがインターネットに接続されている場合に、メンテナンスコンソールからネットアップにサポートバンドルをアップロードすることもできます。

- 必要なもの *

メンテナンスコンソールにメンテナンスユーザとしてアクセスできる必要があります。

一部のタイプのサポートデータでは、クラスタリソースを大量に使用したり、完了までに時間がかかったりすることがあります。そのため、完全なサポートバンドルを選択する際には、含めるデータタイプと除外するデータタイプを指定して、サポートバンドルのサイズを縮小できます。また、30日分のログと構成データベースのレコードを含む軽量なサポートバンドルを作成することもできます。パフォーマンスデータ、取得記録ファイル、サーバヒープダンプは含まれません。

Unified Manager では、生成されたサポートバンドルのうち最新の2つだけが保持されます。それよりも古いサポートバンドルはシステムから削除されます。

手順

1. メンテナンスコンソール * メインメニュー * で、* サポート / 診断 * を選択します。
2. サポートバンドルに含める詳細のレベルに応じて、[Generate Light Support Bundle] または [*Generate Support Bundle] を選択します。
3. フルサポートバンドルを選択した場合は、次のデータタイプを選択または選択解除して、サポートバンドルに含めるか除外します。

- * データベースダンプ *

MySQL Server データベースのダンプ。

- * ヒープダンプ *

メインの Unified Manager サーバプロセスの状態の Snapshot。このオプションはデフォルトでは無効になっており、カスタマーサポートから要求された場合にのみ選択します。

- * 取得記録 *

Unified Manager と監視対象クラスタの間のすべての通信の記録。



すべてのデータタイプを選択解除しても、それ以外の Unified Manager データでサポートバンドルが生成されます。

4. を入力します `g` をクリックし、Enter キーを押してサポートバンドルを生成します。

サポートバンドルの生成ではメモリが大量に消費されるため、この時点でサポートバンドルを生成するかどうかを確認するメッセージが表示されます。

5. を入力します `y` をクリックし、Enter キーを押してサポートバンドルを生成します。

この時点でサポートバンドルを生成しない場合は、と入力します `n` をクリックし、Enter キーを押します。

6. フルサポートバンドルにデータベースダンプファイルを含めるように指定した場合は、パフォーマンス統計の対象期間を指定するように求められます。パフォーマンス統計の追加には多くの時間とスペースが必要になることがあるため、パフォーマンス統計を含めずにデータベースをダンプすることもできます。

- a. 開始日を「YYYYMMDD」の形式で入力します。

たとえば、と入力します 20210101 2021年1月1日です。入力するコマンド n パフォーマンス統計を含めない場合は、

b. 対象とする統計の日数を、午前 12 時から入力します指定した開始日の日付にある。

1 ～ 10 の数値を入力できます。

パフォーマンス統計を含める場合は、収集期間が表示されます。

7. サポートバンドルが作成されると、ネットアップにアップロードするかどうかの確認を求められます。を入力します `y` をクリックし、Enter キーを押します。

サポートケース番号の入力を求められます。

8. ケース番号がすでにある場合は、その番号を入力して Enter キーを押します。それ以外の場合は、Enter キーを押します

サポートバンドルがネットアップにアップロードされます。

Unified Manager サーバがインターネットに接続されていない場合や、何らかの理由でサポートバンドルをアップロードできない場合は、サーバを取得して手動で送信できます。このリポジトリは、SFTP クライアントを使用するか、UNIX または Linux の CLI コマンドを使用して取得できます。Windows 環境では、Remote Desktop (RDP) を使用してサポートバンドルを取得することができます。

生成されたサポートバンドルは、VMware システムの /support ディレクトリ、Linux システムの場合は /opt/NetApp/data/support/、Windows システムの場合は ProgramData\NetApp\OnCommandAppData\ocum\support にあります。

• 関連情報 *

"Unified Manager のユーザロールと機能"

Windows クライアントを使用したサポートバンドルの取得

Windows を使用している場合は、ツールをダウンロードしてインストールすることにより、Unified Manager サーバからサポートバンドルを取得することができます。サポートバンドルをテクニカルサポートに送信して、問題の詳しい診断を受けることができます。使用できるツールには、Filezilla や WinSCP などがあります。

• 必要なもの *

このタスクを実行するには、maintenance ユーザである必要があります。

SCP または SFTP をサポートするツールを使用する必要があります。

手順

1. サポートバンドルを取得するためのツールをダウンロードしてインストールします。
2. ツールを開きます。
3. Unified Manager 管理サーバに SFTP 経由で接続します。

サポートディレクトリの内容が表示され、既存のサポートバンドルをすべて確認できます。

4. サポートバンドルのコピー先となるディレクトリを選択します。

5. コピーするサポートバンドルを選択し、ツールを使用して Unified Manager サーバからローカルシステムにファイルをコピーします。

UNIX または Linux クライアントを使用したサポートバンドルの取得

UNIX または Linux を使用している場合は、Linux クライアントサーバでコマンドラインインターフェイス（CLI）を使用して、vApp からサポートバンドルを取得することができます。サポートバンドルの取得には、SCP または SFTP を使用します。

- 必要なもの *

このタスクを実行するには、maintenance ユーザである必要があります。

メンテナンスコンソールを使用してサポートバンドルを生成し、サポートバンドル名を確認しておく必要があります。

手順

1. Linux クライアントサーバを使用して、Telnet またはコンソール経由で CLI にアクセスします。
2. にアクセスします /support ディレクトリ。
3. 次のコマンドを使用して、サポートバンドルを取得してローカルディレクトリにコピーします。

使用するポート	使用するコマンド
SCP	<code>scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>
SFTP を使用する	<code>sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>

サポートバンドルの名前は、メンテナンスコンソールを使用してサポートバンドルを生成するときに自動的に付けられます。

4. メンテナンスユーザのパスワードを入力します。

例

次の例では、SCP を使用してサポートバンドルを取得します。

```
`$ scp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
support_bundle_20160216_145359.7z   100%  119MB  11.9MB/s   00:10
```

次の例では、SFTP を使用してサポートバンドルを取得します。

```
`$ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `maintenance\_user\_password`
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

テクニカルサポートへのサポートバンドルの送信

問題で AutoSupport メッセージよりも詳細な診断情報とトラブルシューティング情報が必要な場合は、テクニカルサポートにサポートバンドルを送信します。

- 必要なもの *

テクニカルサポートに送信するには、サポートバンドルへのアクセス権が必要です。

テクニカルサポートの Web サイトで生成されたケース番号が必要です。

手順

1. NetApp Support Siteにログインします。
2. ファイルをアップロードします。

["ネットアップにファイルをアップロードする方法"](#)

複数のワークフローに関連するタスクと情報

Unified Manager の多くのワークフローに、共通のタスク、およびワークフローの理解と実行に役立つ参照情報があります。たとえば、イベントに関するメモの追加と確認、イベントの割り当て、イベントへの応答と解決、ボリューム、Storage Virtual Machine (SVM)、アグリゲートに関する詳細情報、など。

クラスタコンポーネントとその競合要因

クラスタコンポーネントの競合の原因となるクラスタのパフォーマンスの問題を特定することができます。コンポーネントを使用するワークロードのパフォーマンスが低下し、クライアント要求に対する応答時間（レイテンシ）が長くなると、Unified Manager でイベントがトリガーされます。

競合状態のコンポーネントは、最適なレベルのパフォーマンスを提供できません。パフォーマンスが低下し、_Victim_ と呼ばれる他のクラスタコンポーネントやワークロードのパフォーマンスによってレイテンシが増大する可能性があります。コンポーネントの競合状態を解消するには、ワークロードを減らすか処理能力を高めることでパフォーマンスを通常レベルに戻す必要があります。Unified Manager では、ワークロードのパフォーマンスの収集と分析が 5 分間隔で行われるため、クラスタコンポーネントの利用率が高い状態が長時間続いたときにのみ検出されます。利用率が高い状態が 5 分インターバルの間に短時間しか続かないような一時的な利用率の急増は検出されません。

ストレージアグリゲートが競合状態になる原因としては、たとえば、1 つ以上のワークロードがそれぞれの I/O 要求に対応するために競合する場合などがあります。アグリゲートの他のワークロードに影響し、それらのワークロードのパフォーマンスが低下する可能性があります。アグリゲートのアクティビティを減らす方法はいくつかありますが、たとえば、1 つ以上のワークロードを負荷の低いアグリゲートまたはノードに移動し、現在のアグリゲートに対する全体的なワークロードの負荷を低くするなどの方法が効果的です。QoS ポリシーグループの場合は、スループット制限を調整したりワークロードを別のポリシーグループに移動したりすることで、ワークロードが抑制されないようにすることができます。

Unified Manager では、次のクラスタコンポーネントを監視して、これらのコンポーネントが競合状態になるとアラートを生成します。

- * ネットワーク *

クラスタの外部ネットワークプロトコルによる I/O 要求の待機時間を表します。待機時間とは、クラスタが I/O 要求に応答できるようになるまで「transfer ready」トランザクションが完了するのを待機する時間です。ネットワークコンポーネントが競合状態にある場合、プロトコルレイヤでの長い待機時間は、1 つ以上のワークロードのレイテンシに影響していることを意味します。

- * ネットワーク処理 *

プロトコルレイヤとクラスタ間の I/O 処理に関与する、クラスタ内のソフトウェアコンポーネントを表します。ネットワーク処理を実行するノードがイベント検出後に変更された可能性があります。ネットワーク処理コンポーネントが競合状態にある場合、ネットワーク処理ノードでの高利用率は、1 つ以上のワークロードのレイテンシに影響していることを意味します。

アクティブ / アクティブ構成でオール SAN アレイクラスタを使用している場合は、両方のノードのネットワーク処理のレイテンシの値が表示され、ノードが負荷を均等に共有していることを確認できます。

- * 最大 QoS

ワークロードに割り当てられたストレージ QoS ポリシーグループの最大スループット（ピーク）設定を表します。ポリシーグループコンポーネントが競合状態にある場合、ポリシーグループ内のすべてのワークロードに、スループットの制限によってスロットルが適用され、1 つ以上のワークロードのレイテンシに影響していることを意味します。

- * 最小 QoS

他のワークロードに割り当てられた QoS スループットの下限（想定）設定によって引き起こされている、ワークロードへのレイテンシを表します。設定されている QoS の下限に応じて特定のワークロードが保証されたスループットを確保するために帯域幅の大部分を使用すると、他のワークロードは調整されてレイテンシが増大します。

- * クラスタインターコネクト *

クラスタノードを物理的に接続するケーブルとアダプタを表します。クラスタインターコネクトコンポーネントが競合状態にある場合は、クラスタインターコネクトでの I/O 要求の長い待機時間がワークロードのレイテンシに影響していることを意味します。

- * データ処理 *

クラスタとストレージアグリゲート間でワークロードを含む I/O 処理に関与する、クラスタ内のソフトウェアコンポーネントを表します。データ処理を実行するノードがイベント検出後に変更された可能性があります。データ処理コンポーネントが競合状態にある場合、データ処理ノードでの高利用率は、1 つ以上のワークロードのレイテンシに影響していることを意味します。

- * ボリュームアクティベーション *

すべてのアクティブボリュームの使用状況を追跡するプロセスです。1000 を超えるアクティブボリュームを擁する大規模な環境で、ノード経由で同時にリソースにアクセスする必要がある重要なボリュームの数を追跡します。同時アクティブボリュームの数が推奨される最大しきい値を超えると、重要でない一部のボリュームでレイテンシが発生します。

- * MetroCluster リソース *

NVRAM とインタースイッチリンク（ISL）を含む MetroCluster リソースを表します。MetroCluster 構成のクラスタ間でデータをミラーリングするのに使用します。MetroCluster コンポーネントが競合状態問題にある場合は、ローカルクラスタのワークロードによる大量の書き込みスループットまたはリンクの不具合が、ローカルクラスタの 1 つ以上のワークロードのレイテンシに影響していることを意味します。クラスタが MetroCluster 構成に含まれていない場合は、このアイコンは表示されません。

- * アグリゲートまたは SSD アグリゲートの処理 *

ワークロードが実行されているストレージアグリゲートを表します。アグリゲートコンポーネントが競合状態にある場合、アグリゲートの高利用率が 1 つ以上のワークロードのレイテンシに影響していることを意味します。アグリゲートには、HDD のみで構成されるものと、HDD と SSD が混在するもの（Flash Pool アグリゲート）と、HDD とクラウド階層が混在するもの（FabricPool アグリゲート）があります。「SD アグリゲート」は、すべての SSD（オールフラッシュアグリゲート）、または SSD とクラウド階層（FabricPool アグリゲート）が混在しています。

- * クラウドレイテンシ *

クラスタとユーザデータ格納先のクラウド階層の間の I/O 処理に関与する、クラスタ内のソフトウェアコンポーネントを表します。クラウドレイテンシコンポーネントが競合状態にある場合、クラウド階層でホストされたボリュームからの大量の読み取りが 1 つ以上のワークロードのレイテンシに影響していることを意味します。

- * 同期 SnapMirror *

SnapMirror 同期関係でのプライマリボリュームからセカンダリボリュームへのユーザデータのレプリケーションに関係する、クラスタ内のソフトウェアコンポーネントを表します。同期 SnapMirror コンポーネントが競合状態にある場合、SnapMirror Synchronous 処理のアクティビティが 1 つ以上のワークロードのレイテンシに影響していることを意味します。

ボリューム / 健全性の詳細ページ

ボリューム / 健全性の詳細ページでは、選択したボリュームについて、容量、ストレージ効率、設定、保護などの詳細情報を確認できます。生成されたアノテーションおよびイベントまた、そのボリュームに関連するオブジェクトやアラートに関する情報も参照できます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

コマンドボタン

選択したボリュームについて、各コマンドボタンを使用して次のタスクを実行できます。

- * パフォーマンスビューに切り替え *

ボリューム / パフォーマンスの詳細ページに移動できます。

• * アクション *

◦ アラートを追加します

選択したボリュームにアラートを追加できます。

◦ しきい値の編集

選択したボリュームのしきい値の設定を変更できます。

◦ 注釈

選択したボリュームをアノテートできます。

◦ 保護

選択したボリュームの SnapMirror 関係または SnapVault 関係を作成できます。

◦ 関係

保護関係について次の処理を実行できます。

▪ 編集

関係の編集ダイアログボックスが開き、既存の保護関係の既存の SnapMirror ポリシー、スケジュール、および最大転送速度を変更できます。

▪ 中止

選択した関係の実行中の転送を中止します。必要に応じて、ベースライン転送以外の転送の再開チェックポイントを削除することもできます。ベースライン転送のチェックポイントは削除できません。

▪ 休止

選択した関係のスケジュールによる更新を一時的に無効にします。すでに実行中の転送は、関係を休止する前に完了しておく必要があります。

▪ 休憩

ソースボリュームとデスティネーションボリュームの間の関係を解除し、デスティネーションを読み書き可能ボリュームに変更します。

▪ 取り外します

選択したソースとデスティネーションの間の関係を完全に削除します。ボリュームが破棄されるわけではなく、ボリューム上の Snapshot コピーは削除されません。この処理を元に戻すことはできません。

▪ 再開

休止中の関係のスケジュールされた転送を有効にします。スケジュールされた次の転送時に、再開チェックポイントがある場合はそこから再開されます。

- 再同期

以前に解除した関係を再同期できます。

- 初期化 / 更新

新しい保護関係の場合は最初のベースライン転送を実行し、すでに初期化された関係の場合は手動更新を実行できます。

- リバース再同期

以前に解除した保護関係を再確立できます。この処理では、ソースとデスティネーションの機能が入れ替わり、ソースが元のデスティネーションのコピーになります。ソースのコンテンツはデスティネーションのコンテンツで上書きされ、共通の Snapshot コピーのデータよりも新しいデータはすべて削除されます。

- リストア

ボリュームのデータを別のボリュームにリストアできます。詳細については、[を参照してください "ボリューム / 健全性の詳細ページを使用したデータのリストア"](#)。



同期保護関係にあるボリュームについては、リストアボタンと関係操作ボタンは使用できません。

- * ボリュームの表示 *

Health : All Volumes ビューに移動できます。

Capacity (容量) タブ

Capacity タブには、選択したボリュームについて、物理容量、論理容量、しきい値の設定、クォータの容量、ボリューム移動処理に関する情報などの詳細が表示されます。

- * 容量物理容量 *

ボリュームの物理容量の詳細：

- Snapshot オーバーフロー

Snapshot コピーで使用されているデータスペースが表示されます。

- 使用済み

ボリュームでデータに使用されているスペースが表示されます。

- 警告

ボリュームのスペースがほぼフルであることを示します。このしきい値を超えると、「スペースがほぼフル」イベントが生成されます。

- エラー

ボリュームのスペースがフルであることを示します。このしきい値を超えると、「スペースがフル」イベントが生成されます。

- 使用不可

「シンプロビジョニングボリュームにスペースリスクあり」イベントが生成され、シンプロビジョニングボリュームのスペースがアグリゲートの容量の問題が原因で確保できないことを示します。使用不可の容量は、シンプロビジョニングボリュームの場合にのみ表示されます。

- データグラフ

ボリュームの合計データ容量と使用済みデータ容量が表示されます。

自動拡張が有効になっている場合は、アグリゲートの使用可能なスペースも表示されます。このグラフには、ボリュームのデータに使用できる実質的なストレージスペースとして、次のいずれかが表示されます。

- 次の場合は実際のデータ容量：
 - 自動拡張が無効になっている。
 - ボリュームで自動拡張が有効になっており、最大サイズに達している。
 - シックプロビジョニングボリュームで自動拡張が有効になっており、それ以上拡張できない。
- 最大ボリュームサイズを考慮したボリュームのデータ容量（シンプロビジョニングボリュームおよびシックプロビジョニングボリュームでボリュームの最大サイズに対応するスペースがアグリゲートにある場合）
- 次回の自動拡張のサイズを考慮したボリュームのデータ容量（シックプロビジョニングボリュームで自動拡張の割合のしきい値に対応できる場合）

- Snapshot コピーのグラフ

このグラフは、Snapshot 使用容量または Snapshot リザーブが 0 でない場合にのみ表示されます。

どちらのグラフにも、Snapshot 使用容量が Snapshot リザーブを超えている場合には超過分の使用容量が表示されます。

- * 容量の論理値 *

ボリュームの論理スペースが表示されます。論理スペースはディスクに格納されているデータの実際のサイズで、ONTAP の Storage Efficiency テクノロジーによる削減を適用する前のサイズです。

- 論理スペースのレポート

ボリュームで論理スペースのレポートが設定されているかどうかが表示されます。「有効」、「無効」、「該当なし」のいずれかになります。古いバージョンの ONTAP 上のボリュームまたは論理スペース・レポートをサポートしていないボリュームについては、該当しないが表示されます

- 使用済み

ボリュームでデータに使用されている論理スペースの量と合計データ容量に対する使用済みの論理スペースの割合が表示されます。

- 論理スペースの適用

シンプロビジョニングボリュームに対して論理スペースの適用が設定されているかどうかが表示されます。enabled に設定する場合、ボリュームの論理使用済みサイズを現在設定されている物理ボリュームサイズよりも大きくすることはできません。

- * 自動拡張 *

スペースが不足したときにボリュームが自動で拡張されるかどうかが表示されます。

- * スペース保証 *

FlexVol ボリュームがアグリゲートから空きブロックを削除するタイミングを制御する設定が表示されます。削除されたブロックは、ボリューム内のファイルへの書き込み用に確保されます。スペースギャランティは次のいずれかに設定できます。

- なし

ボリュームにスペースギャランティが設定されていません。

- ファイル。

データが書き込まれていないファイル（LUN など）のフルサイズが確保されます。

- ボリューム

ボリュームのフルサイズが確保されます。

- 一部有効です

FlexCache ボリュームのサイズに基づいてスペースがリザーブされます。FlexCache ボリュームのサイズが 100MB 以上の場合は、最小スペースギャランティはデフォルトで 100MB に設定されます。FlexCache ボリュームのサイズが 100MB 未満の場合は、最小スペースギャランティは FlexCache ボリュームのサイズに設定されます。FlexCache ボリュームのサイズがあとで拡張されても、最小スペースギャランティはそのままです。



ボリュームのタイプが「データキャッシュ」の場合、スペースギャランティは「一部」です。

- * 詳細（物理） *

ボリュームの物理仕様が表示されます。

- * 合計容量 *

ボリュームの合計物理容量が表示されます。

- * データ容量 *

ボリュームで使用されている物理スペース（使用済み容量）とボリュームで使用可能な残りの物理スペース（空き容量）が表示されます。それぞれについて、物理容量全体に対する割合の値も表示されます。

シンプロビジョニングボリュームについて「シンプロビジョニングボリュームにスペースリスクあり」イ

ベントが生成された場合は、ボリュームで使用されているスペース（使用済み容量）と、ボリュームで使用可能なスペースのうちアグリゲートの容量の問題が原因で使用できないスペース（使用不可の容量）が表示されます。

- * Snapshot リザーブ *

ボリュームで Snapshot コピーに使用されているスペース（使用済み容量）と Snapshot コピーに使用可能なスペース（空き容量）が表示されます。これらの値は、Snapshot リザーブ全体に対する割合としても表示されます。

シンプロビジョニングボリュームについて「シンプロビジョニングボリュームにスペースリスクあり」イベントが生成された場合は、Snapshot コピーで使用されているスペース（使用済み容量）と、ボリュームで使用可能なスペースのうち Snapshot コピーの作成に使用できないスペース（使用不可の容量）。アグリゲートの容量の問題が原因であると表示されます。

- * ボリュームしきい値 *

ボリュームの容量に関する次のしきい値が表示されます。

- ほぼフルのしきい値

ボリュームがほぼフルであるとみなす割合を示します。

- フルのしきい値

ボリュームがフルであるとみなす割合を示します。

- * その他の詳細 *

- 自動拡張時の最大サイズ

ボリュームを自動的に拡張できる最大サイズが表示されます。デフォルト値は、作成時のボリュームサイズの 120% です。このフィールドは、ボリュームで自動拡張が有効になっている場合にのみ表示されます。

- qtree クォータコミット容量

クォータでリザーブされているスペースが表示されます。

- qtree クォータオーバーコミット容量

「ボリュームの qtree クォータがオーバーコミット」イベントが生成される基準となるスペースの使用量が表示されます。

- フラクショナルリザーブ

オーバーライトリザーブのサイズを制御します。フラクショナルリザーブのデフォルト設定は 100 で、必要なリザーブスペースが 100% リザーブされ、オブジェクトの上書きが完全に保証されます。フラクショナルリザーブが 100% 未満の場合、そのボリューム内のすべてのスペースリザーブファイル用にリザーブされるスペースがその割合まで縮小されます。

- Snapshot の日次増加率

選択したボリューム内の Snapshot コピーの 24 時間ごとの変化（割合または KB、MB、GB など）が表示されます。

- Snapshot のフルまでの日数

ボリューム内の Snapshot コピー用にリザーブされたスペースが、指定のしきい値に達するまでの推定日数が表示されます。

ボリューム内の Snapshot コピーの増加率がゼロまたは負の場合、または増加率を計算するためのデータが十分でない場合は、「Snapshot Days to Full」フィールドに Not Applicable と表示されます。

- Snapshot の自動削除

アグリゲートのスペース不足が原因でボリュームへの書き込みが失敗する場合に Snapshot コピーを自動で削除するかどうかを指定します。

- Snapshot コピー

ボリューム内の Snapshot コピーに関する情報が表示されます。

ボリューム内の Snapshot コピーの数がリンクとして表示されます。リンクをクリックすると、ボリューム上の Snapshot コピーが開き、Snapshot コピーの詳細が表示されます。

Snapshot コピー数の更新は約 1 時間ごとですが、Snapshot コピーのリストはアイコンをクリックした時点で更新されます。そのため、トポロジに表示される Snapshot コピー数とアイコンをクリックしたときに表示される Snapshot コピーの数は一致しないことがあります。

- * ボリューム移動 *

ボリュームで実行された現在または前回のボリューム移動処理のステータスが表示されます。ボリューム移動処理の現在実行中のフェーズ、ソースアグリゲート、デスティネーションアグリゲート、開始時刻、終了時刻などの詳細も表示されます。と推定終了時間です。

選択したボリュームで実行されたボリューム移動処理の数も表示されます。ボリューム移動操作の詳細を表示するには、* Volume Move History * リンクをクリックします。

【構成】タブ

設定タブには、選択したボリュームについて、エクスポートポリシー、RAID タイプ、容量やストレージ効率化の関連機能に関する詳細が表示されます。

- * 概要 *

- フルネーム

ボリュームの完全な名前が表示されます。

- アグリゲート

ボリュームが配置されているアグリゲートの名前、または FlexGroup ボリュームが配置されているアグリゲートの数が表示されます。

- 階層化ポリシー

ボリュームが FabricPool 対応アグリゲートに導入されている場合に、ボリュームに対して設定されている階層化ポリシーが表示されます。「なし」、「Snapshot のみ」、「バックアップ」、「自動」、「すべて」のいずれかになります。

- Storage VM

ボリュームが含まれている SVM の名前が表示されます。

- ジャンクションパス

パスのステータスが表示されます。アクティブまたは非アクティブにできます。ボリュームのマウント先の SVM のパスも表示されます。「* History *」リンクをクリックすると、ジャンクションパスに対する最新の 5 つの変更を表示できます。

- エクスポートポリシー

ボリューム用に作成されたエクスポートポリシーの名前が表示されます。リンクをクリックすると、そのエクスポートポリシー、認証プロトコル、および SVM に属するボリュームで有効になっているアクセスに関する詳細を確認できます。

- スタイル (Style)

ボリュームの形式が表示されます。「FlexVol」または「FlexGroup」のいずれかです。

- を入力します

選択したボリュームのタイプが表示されます。「読み取り / 書き込み」、「負荷共有」、「データ保護」、「データキャッシュ」、「一時」のいずれかです。

- RAID タイプ

選択したボリュームの RAID タイプが表示されます。RAID タイプには、RAID 0、RAID 4、RAID-DP、または RAID-TEC を指定できます。



FlexGroup ボリュームの場合、コンスティチュエントボリュームを異なるタイプのアグリゲートに配置できるため、RAID タイプが複数表示されることがあります。

- SnapLock タイプ

ボリュームが含まれているアグリゲートの SnapLock タイプが表示されます。

- SnapLock の有効期限

SnapLock ボリュームの有効期限が表示されます。

- * 容量 *

- シンプロビジョニング

ボリュームにシンプロビジョニングが設定されているかどうかが表示されます。

- 自動拡張

アグリゲート内でフレキシブルボリュームが自動的に拡張されるかどうかが表示されます。

- Snapshot の自動削除

アグリゲートのスペース不足が原因でボリュームへの書き込みが失敗する場合に Snapshot コピーを自動で削除するかどうかを指定します。

- クォータ

ボリュームに対してクォータが有効になっているかどうかを示します。

- * 効率性 *

- 圧縮

圧縮が有効か無効かを示します。

- 重複排除

重複排除が有効か無効かを示します。

- 重複排除モード

ボリュームで手動、スケジュール、またはポリシーベースのいずれの重複排除処理が有効になっているかを示します。モードがスケジュールに設定されている場合は処理のスケジュールが表示され、モードがポリシーに設定されている場合はポリシーの名前が表示されます。

- 重複排除タイプ

ボリュームで実行されている重複排除処理のタイプを示します。ボリュームで SnapVault 関係が確立されている場合は、「SnapVault」と表示されます。それ以外のボリュームの場合は、「標準」と表示されます。

- ストレージ効率化ポリシー

このボリュームに対して Unified Manager から割り当てられているストレージ効率化ポリシーの名前を示します。このポリシーを使用して、圧縮と重複排除の設定を制御できます。

- * 保護 *

- Snapshot コピー

Snapshot コピーの自動作成が有効か無効かを示します。

【保護】タブ

Protection タブには、選択したボリュームの保護に関する詳細について、遅延の情報、関係のタイプ、関係のトポロジなどの情報が表示されます。

- * 概要 *

選択したボリュームの保護関係（SnapMirror、SnapVault、または Storage VM DR）のプロパティが表示されます。それ以外の関係タイプの場合は、「関係タイプ」プロパティのみが表示されます。プライマリボリュームを選択した場合は、管理対象とローカルの Snapshot コピーポリシーのみが表示されま

す。SnapMirror 関係と SnapVault 関係について表示されるプロパティは次のとおりです。

- ソースボリューム

選択したボリュームがデスティネーションの場合、選択したボリュームのソースの名前が表示されます。

- 遅延ステータス

保護関係の更新または転送の遅延ステータスが表示されます。「エラー」、「警告」、「重大」のいずれかです。

同期関係については、遅延ステータスは適用されません。

- 遅延時間

ミラーのデータがソースより遅延している時間が表示されます。

- 前回の更新成功日時

保護の更新に最後に成功した日時が表示されます。

同期関係については、前回成功した更新は適用されません。

- ストレージサービスメンバー

ボリュームがストレージサービスに属しているかどうか、およびストレージサービスによって管理されているかどうかを示す「はい」または「いいえ」が表示されます。

- バージョンに依存しないレプリケーション

[はい]、[バックアップオプションあり]、または [なし] のいずれかを表示します。「はい」の場合は、ソースボリュームとデスティネーションボリュームで異なるバージョンの ONTAP ソフトウェアを実行している場合でも SnapMirror レプリケーションが可能です。バックアップオプションを指定した場合は、デスティネーションにバックアップコピーの複数のバージョンを保持できる SnapMirror 保護が実装されます。「なし」の場合は、バージョンに依存しないレプリケーションが有効になっていません

- 関係機能

保護関係に使用できる ONTAP 機能を示します。

- 保護サービス

関係が保護パートナーアプリケーションによって管理されている場合は、保護サービスの名前が表示されます。

- 関係タイプ

非同期ミラー、非同期バックアップ、非同期ミラーバックアップ、StrictSync、同期を実行できません。

- 関係の状態

SnapMirror 関係または SnapVault 関係の状態が表示されます。「未初期化」、「SnapMirror 済み」、「切断」のいずれかです。ソースボリュームを選択した場合は、関係の状態は適用されず表示されません。

◦ 転送ステータス

保護関係の転送ステータスが表示されます。転送ステータスは、次のいずれかになります。

- 中止しています

SnapMirror 転送は有効ですが、チェックポイントの削除を含む転送の中止処理が進行中です。

- チェック中です

デスティネーションボリュームの診断チェックを実行中で、実行中の転送はありません。

- 最終処理中です

SnapMirror 転送が有効になっています。現在 SnapVault 増分転送の転送後のフェーズです。

- アイドル

転送が有効になっており、実行中の転送はありません。

- 同期中

同期関係にある 2 つのボリュームのデータが同期されています。

- 非同期

デスティネーションボリュームのデータがソースボリュームと同期されていません。

- 準備中

SnapMirror 転送が有効になっています。現在 SnapVault 増分転送の転送前のフェーズです。

- キューに登録され

SnapMirror 転送が有効になっています。実行中の転送はありません。

- 休止中です

SnapMirror 転送が無効になっています。実行中の転送はありません。

- 休止中です

SnapMirror 転送を実行中です。追加の転送は無効になります。

- 転送中です

SnapMirror 転送が有効になっており、転送を実行中です。

- 移行中

ソースボリュームからデスティネーションボリュームへの非同期のデータ転送が完了し、同期処理への移行が開始されています。

- 待機中です

SnapMirror 転送は開始されましたが、一部の関連タスクのキュー登録を待っています。

- 最大転送速度

関係の最大転送速度が表示されます。最大転送速度は、1 秒あたりのキロバイト数（Kbps）、1 秒あたりのメガバイト数（Mbps）、1 秒あたりのギガバイト数（Gbps）、1 秒あたりのテラバイト数（Tbps）のいずれかで示されます。関係間のベースライン転送に制限がない場合は「無制限」と表示されます。

- SnapMirror ポリシー

ボリュームの保護ポリシーが表示されます。「DPDefault」はデフォルトの非同期ミラー保護ポリシー、「XDPEndpoint」はデフォルトの非同期バックアップポリシー、「DPSyncDefault」はデフォルトの非同期ミラーバックアップポリシーを示します。「StrictSync」はデフォルトの厳密な同期保護ポリシー、「Sync」はデフォルトの同期ポリシーです。ポリシー名をクリックすると、そのポリシーに関連付けられた詳細について次の情報を確認できます。

- 転送の優先順位
- アクセス時間の設定を無視します
- 最大試行回数
- コメント
- SnapMirror ラベル
- 保持設定
- 実際の Snapshot コピー
- Snapshot コピーを保持
- 保持の警告のしきい値
- ソースがデータ保護（DP）ボリュームであるカスケード SnapVault 関係に保持設定がない Snapshot コピーには、「's_created」ルールのみが適用されます。

- スケジュールを更新します

関係に割り当てられている SnapMirror スケジュールが表示されます。情報アイコンにカーソルを合わせるとスケジュールの詳細が表示されます。

- ローカル Snapshot ポリシー

ボリュームの Snapshot コピーポリシーが表示されます。「デフォルト」、「なし」、またはカスタムポリシーの名前のいずれかです。

- で保護されます

選択したボリュームで使用されている保護のタイプが表示されます。たとえば、ボリュームが整合グループ関係と SnapMirror ボリューム関係で保護されている場合、このフィールドには SnapMirror と整合グループの両方が表示されます。また、このフィールドには、ユニファイド関係のステータスを

表示するための [関係] ページへのリンクも表示されます。このリンクは、コンスチチュエント関係にのみ適用されます。

- 整合グループ

SnapMirror のビジネス継続性 (SM-BC) 関係で保護されているボリュームの場合、この列にはボリュームの整合グループが表示されます。

- * ビュー *

選択したボリュームの保護トポロジが表示されます。トポロジには、選択したボリュームに関連するすべてのボリュームが図で示されます。選択したボリュームはダークグレーの線で囲んで示され、トポロジ内のボリュームをつなぐ線は保護関係のタイプを示しています。トポロジ内の関係の方向は左から右に、各関係の左側がソースで右側がデスティネーションです。

太線の二重線は非同期ミラー関係、太線の一重線は非同期バックアップ関係、細線の二重線は非同期ミラーバックアップ関係、太線と太線でない線は同期関係です。下の表に、同期関係が StrictSync であるか Sync であるかが示されます。

ボリュームを右クリックするとメニューが表示され、ボリュームの保護とデータのリストアのどちらかを選択できます。関係を右クリックすると、編集、中止、休止、解除、削除のいずれかを選択できるメニューが表示されます。関係を再開することもできます。

このメニューは、次の場合は表示されません。

- RBAC の設定で許可されていない場合：オペレータの権限しかない場合など
- ボリュームが同期保護関係にある場合
- ボリューム ID が不明な場合：クラスタ間関係が確立されているがデスティネーションクラスタが検出されていない場合、トポロジ内の別のボリュームをクリックすると、そのボリュームの情報が表示されます。疑問符 (?) をクリックします。ボリュームが見つからないか、まだ検出されていません。容量情報が見つからないことを示している場合もあります。疑問符にカーソルを合わせると、推奨される対応策などの追加情報が表示されます。

トポロジがいくつかある一般的なトポロジテンプレートのいずれかに一致している場合、ボリュームの容量、遅延、Snapshot コピー、および前回成功したデータ転送に関する情報が表示されます。いずれのテンプレートにも一致していない場合は、ボリュームの遅延と前回成功したデータ転送に関する情報がトポロジの下の関係テーブルに表示されます。その場合、選択したボリュームの行が強調表示され、トポロジビューには、選択したボリュームとそのソースボリュームの間の関係が太線と青色の点で示されます。

トポロジビューには次の情報が表示されます。

- 容量

ボリュームで使用されている合計容量が表示されます。トポロジ内のボリュームにカーソルを合わせると、そのボリュームの現在の警告および重大のしきい値設定が Current Threshold Settings ダイアログボックスに表示されます。現在のしきい値設定ダイアログボックスのしきい値編集リンクをクリックして、しきい値設定を編集することもできます。容量 * チェックボックスを選択解除すると、トポロジ内のすべてのボリュームについてのすべての容量情報が非表示になります。


- 遅延

受信保護関係の遅延時間と遅延ステータスが表示されます。* LAG * チェックボックスをオフにすると、トポロジ内のすべてのボリュームの遅延情報が非表示になります。* LAG * チェックボックスがグレー表

示になっている場合、選択したボリュームの遅延情報がトポロジの下の関係テーブルに表示され、関連するすべてのボリュームの遅延情報も表示されます。

- スナップショット

ボリュームで使用できる Snapshot コピーの数が表示されます。* Snapshot * チェック・ボックスを選択解除すると、トポロジ内のすべてのボリュームについて、すべての Snapshot コピー情報が非表示になります。

Snapshot コピーのアイコン () ボリュームの Snapshot コピーリストが表示されます。アイコンの横に表示される Snapshot コピー数の更新は約 1 時間ごとですが、Snapshot コピーのリストはアイコンをクリックした時点で更新されます。そのため、トポロジに表示される Snapshot コピー数とアイコンをクリックしたときに表示される Snapshot コピーの数は一致しないことがあります。

- 前回成功した転送

前回成功したデータ転送の量、期間、時刻、および日付が表示されます。前回成功した転送 * (Last Successful Transfer) チェックボックスがグレー表示されている場合、選択したボリュームについて成功した最後の転送情報がトポロジの下の関係テーブルに表示され、関連するすべてのボリュームについて前回成功した転送情報も表示されます。

- * 履歴 *

選択したボリュームの SnapMirror および SnapVault の受信保護関係の履歴がグラフで表示されます。この履歴グラフには、受信関係の遅延時間、受信関係の転送時間、および受信関係の転送サイズの 3 種類があります。履歴情報は、デスティネーションボリュームを選択した場合にのみ表示されます。プライマリボリュームを選択した場合、空のグラフと「データが見つかりません」というメッセージが表示されます。ボリュームが整合性グループおよび SnapMirror 同期関係で保護されている場合は、関係の転送時間と関係の転送サイズに関する情報が表示されません。

履歴ペインの上部にあるドロップダウンリストからグラフタイプを選択できます。1 週間、1 カ月、または 1 年のいずれかを選択して、特定の期間の詳細を表示することもできます。履歴グラフは傾向を確認するのに役立ちます。たとえば、毎日または毎週同じ時間に大量のデータが転送されている場合や、遅延警告または遅延エラーのしきい値を継続的に超過している場合は、適切な措置を講じることができます。また、[* エクスポート *] ボタンをクリックして、表示しているチャートの CSV 形式でレポートを作成することもできます。

保護の履歴グラフには次の情報が表示されます。

- * 関係遅延時間 *

縦軸 (y 軸) には秒、分、または時間が表示され、横軸 (x 軸) には選択した期間 (日数、月数、または年数) が表示されます。y 軸の最大値は x 軸の期間における最大遅延時間を示しています。オレンジ色の線は遅延エラーのしきい値、黄色の線は遅延警告のしきい値を示しています。これらの線にカーソルを合わせると、しきい値の設定が表示されます。青色の線は遅延時間を示しています。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。

- * 関係の転送時間 *

縦軸 (y 軸) には秒、分、または時間が表示され、横軸 (x 軸) には選択した期間 (日数、月数、または年数) が表示されます。y 軸の最大値は x 軸の期間における最大転送時間を示しています。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。



このグラフは、同期保護関係にあるボリュームについては表示されません。

- * 関係転送サイズ *

縦軸（y 軸）には転送サイズ（バイト、KB、MB）が、横軸（x 軸）には選択した期間（日数、月数、または年数）が表示されます。y 軸の最大値は x 軸の期間における最大転送サイズを示しています。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。



このグラフは、同期保護関係にあるボリュームについては表示されません。

履歴領域

履歴領域には、選択したボリュームの容量とスペースリザベーションに関する情報を示すグラフが表示されます。また、[* エクスポート *] ボタンをクリックして、表示しているチャートの CSV 形式でレポートを作成することもできます。

一定の期間にわたってデータやボリュームの状態に変化がない場合、空のグラフと「データが見つかりません」というメッセージが表示されます。

履歴ペインの上部にあるドロップダウンリストからグラフタイプを選択できます。1 週間、1 カ月、または 1 年のいずれかを選択して、特定の期間の詳細を表示することもできます。履歴グラフは傾向を確認するのに役立ちます。たとえば、ボリュームの使用量が継続的に「ほぼフル」のしきい値を超えていれば、それに応じた措置を講じることができます。

履歴グラフには次の情報が表示されます。

- * 使用容量 *

折れ線グラフの形式で、ボリュームの使用容量（バイト、KB、MB など）とボリュームの容量の使用履歴に基づく使用状況が縦軸（y 軸）に表示されます。横軸（x 軸）に期間が表示されます。期間は、1 週間、1 カ月、または 1 年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、折れ線グラフの表示と非表示を切り替えることができます。たとえば、Volume Used Capacity の凡例をクリックすると、Volume Used Capacity のグラフの線が非表示になります。

- * ボリューム - 使用容量と合計容量 *

折れ線グラフの形式で、ボリュームの容量の使用履歴に基づく使用状況と使用済み容量、合計容量、および重複排除や圧縮によるスペース削減量（バイト、KB、MB）が表示されます。垂直（y）軸など。横軸（x 軸）に期間が表示されます。期間は、1 週間、1 カ月、または 1 年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、折れ線グラフの表示と非表示を切り替えることができます。たとえば、「使用済みトレンド容量」の凡例をクリックすると、「使用済みトレンド容量」のグラフ行が非表示になります。

- * 使用容量（%） *

折れ線グラフの形式で、ボリュームの使用率とボリュームの容量の使用履歴に基づく使用状況が縦軸（y 軸）に表示されます。横軸（x 軸）に期間が表示されます。期間は、1 週間、1 カ月、または 1 年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、折れ線グラフの表示と非表示を切り替えることができます。たとえば、Volume Used Capacity の凡例をクリックすると、Volume Used Capacity のグラフの線が非表示になります。

- * Snapshot の使用容量（%） *

面積グラフの形式で、Snapshot リザーブと Snapshot の警告しきい値、および Snapshot コピーに使用されている容量の割合が縦軸（y 軸）に表示されます。Snapshot オーバーフローは別の色で示されます。横軸（x 軸）に期間が表示されます。期間は、1 週間、1 カ月、または 1 年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、折れ線グラフの表示と非表示を切り替えることができます。たとえば、Snapshot Reserve の凡例をクリックすると、Snapshot Reserve のグラフの線が非表示になります。

イベントのリスト

イベントリストには、新規イベントと確認済みイベントに関する詳細が表示されます。

- * 重大度 *

イベントの重大度が表示されます。

- * イベント *

イベント名が表示されます。

- * トリガー日時 *

イベントが生成されてからの経過時間が表示されます。1 週間を過ぎたイベントには、生成時のタイムスタンプが表示されます。

[関連注釈（Related Annotations）] パネル

関連するアノテーションペインでは、選択したボリュームに関連付けられているアノテーションの詳細を確認できます。これには、ボリュームに適用されるアノテーションの名前と値などの情報が含まれます。関連するアノテーションペインから手動アノテーションを削除することもできます。

Related Devices ペイン

Related Devices ペインでは、ボリュームに関連する SVM、アグリゲート、qtree、LUN、および Snapshot コピーを表示し、それらの場所に移動できます。

- * Storage Virtual Machine *

選択したボリュームが含まれる SVM の容量と健全性ステータスが表示されます。

- * 集計 *

選択したボリュームが含まれるアグリゲートの容量と健全性ステータスが表示されます。FlexGroup ボリュームの場合は、FlexGroup を構成するアグリゲートの数が表示されます。

- * アグリゲート内のボリューム *

選択したボリュームの親アグリゲートに属するすべてのボリュームの数と容量が表示されます。最も高い重大度レベルに基づいて、ボリュームの健全性ステータスも表示されます。たとえば、アグリゲートに 10 個のボリュームがあり、5 つのステータスが「警告」で残りの 5 つが「重大」の場合、ステータスは「重大」と表示されます。このコンポーネントは、FlexGroup ボリュームに対しては表示されません。

- * qtree *

選択したボリュームに含まれる qtree の数と、クォータが適用された qtree の容量が表示されます。クォータが適用された qtree の容量はボリュームのデータ容量に対する割合で表示されます。最も高い重大度レベルに基づいて、qtree の健全性ステータスも表示されます。たとえば、ボリュームに 10 個の qtree があり、5 つのステータスが「警告」で残りの 5 つが「重大」の場合、ステータスは「重大」と表示されます。

- * NFS 共有 *

ボリュームに関連付けられている NFS 共有の数とステータスが表示されます。

- * SMB 共有 *

SMB/CIFS 共有の数とステータスが表示されます。

- * LUN*

選択したボリューム内のすべての LUN の数と合計サイズが表示されます。最も高い重大度レベルに基づいて、LUN の健全性ステータスも表示されます。

- * ユーザー・クォータとグループ・クォータ *

ボリュームとその qtree に関連付けられているユーザおよびユーザグループクォータの数とステータスが表示されます。

- * FlexClone ボリューム *

選択したボリュームのすべてのクローンボリュームの数と容量が表示されます。選択したボリュームにクローンボリュームが含まれている場合にのみ表示されます。

- * 親ボリューム *

選択した FlexClone ボリュームの親ボリュームの名前と容量が表示されます。選択したボリュームが FlexClone ボリュームの場合にのみ表示されます。

【関連グループ】ペイン

Related Groups ペインでは、選択したボリュームに関連付けられているグループのリストを確認できます。

【関連アラート】ペイン

関連するアラートペインでは、選択したボリュームに対して作成されたアラートのリストを表示できます。また、[Add Alert] リンクをクリックしてアラートを追加したり、アラート名をクリックして既存のアラートを編集したりすることもできます。

Storage VM / 健全性の詳細ページ

Storage VM / 健全性の詳細ページでは、選択した Storage VM について、健全性、容量、構成、データポリシー、論理インターフェイス（LIF）、LUN、qtree、ユーザ、ユーザグループクォータ、および保護の詳細Storage VM に関連するオブジェクトやアラートに関する情報も確認できます。



監視できるのはデータ Storage VM だけです。

コマンドボタン

選択した Storage VM について、各コマンドボタンを使用して次のタスクを実行できます。

- * パフォーマンスビューに切り替え *

Storage VM / パフォーマンスの詳細ページに移動できます。

- * アクション *

- アラートを追加します

選択した Storage VM にアラートを追加できます。

- 注釈

選択した Storage VM をアノテートできます。

- * Storage VM* を表示します

健全性：すべての Storage VM ビューに移動できます。

正常性タブ

Health タブには、ボリューム、アグリゲート、NAS LIF、SAN LIF、LUN などのさまざまなオブジェクトのデータ可用性、データ容量、および保護の問題に関する詳細な情報が表示されます。プロトコル、サービス、NFS 共有、および CIFS 共有

オブジェクトのグラフをクリックすると、フィルタリングされたオブジェクトのリストを表示できます。たとえば、警告が表示されたボリュームの容量のグラフをクリックすると、重大度が「警告」の容量の問題があるボリュームのリストが表示されます。

- * 可用性の問題 *

可用性の問題があるオブジェクトとないオブジェクトの両方を含むオブジェクトの合計数がグラフで表示されます。グラフでは、問題の重大度レベルに応じて色が表示されます。グラフの下には、Storage VM 内のデータの可用性に影響を及ぼす可能性がある問題とすでに影響を及ぼしている問題に関する詳細が表示されます。たとえば、停止している NAS LIF および SAN LIF やオフラインになっているボリュームの情報が表示されます。

現在実行中の関連するプロトコルやサービスに関する情報のほか、NFS 共有や CIFS 共有の数とステータスも確認できます。

- * 容量の問題 *

容量の問題があるオブジェクトとないオブジェクトの両方を含むオブジェクトの合計数がグラフで表示されます。グラフでは、問題の重大度レベルに応じて色が表示されます。グラフの下には、Storage VM 内のデータの容量に影響を及ぼす可能性がある問題とすでに影響を及ぼしている問題に関する詳細が表示されます。たとえば、設定されたしきい値を超える可能性があるアグリゲートの情報が表示されます。

• * 保護の問題 *

Storage VM の保護関連の健全性に関する概要情報として、フィールドのダイアログボックスに保護の問題がある関係とない関係を含む関係の合計数が表示されます。選択した Storage VM の Storage VM DR 関係のステータスも確認できます。Storage VM DR 関係のイベントが表示されます。イベントをクリックすると、イベントの詳細ページが表示されます。保護されていないボリュームがある場合は、リンクをクリックすると Health : All Volumes ビューに移動し、Storage VM にある保護されていないボリュームのフィルタリングされたリストを確認できます。グラフでは、問題の重大度レベルに応じて色が表示されます。グラフをクリックすると、Relationship : All Relationships ビューに移動します。このビューでは、保護関係の詳細のフィルタリングされたリストを確認できます。グラフの下には、Storage VM 内のデータの保護に影響を及ぼす可能性がある問題とすでに影響を及ぼしている問題に関する詳細が表示されます。たとえば、Snapshot コピーリザーブがほぼフルのボリュームに関する情報や、SnapMirror 関係の遅延の問題に関する情報が表示されます。

Capacity（容量）タブ

容量タブには、選択した SVM のデータ容量に関する詳細情報が表示されます。

FlexVol ボリュームまたは FlexGroup ボリュームを備えた Storage VM については、次の情報が表示されます。

• * 容量 *

容量領域には、すべてのボリュームから割り当てられている使用済み容量と使用可能容量に関する詳細が表示されます。

◦ 合計容量

Storage VM の合計容量が表示されます。

◦ 使用済み

Storage VM に属するボリュームでデータに使用されているスペースが表示されます。

◦ 保証あり - 利用可能

Storage VM 内のボリュームで使用可能な保証済みのデータ用スペースが表示されます。

◦ 保証なし

Storage VM 内のシンプロビジョニングボリュームに割り当てられている、データに使用可能な残りのスペースが表示されます。

• * 容量に問題があるボリューム *

容量に問題があるボリュームのリストが、容量の問題があるボリュームに関する詳細情報が表形式で表示されます。

◦ ステータス

ボリュームに、容量関連のある問題が指定された重大度であることを示します。

ステータスにカーソルを合わせると、ボリュームに対して生成された容量関連のイベントに関する詳

細を確認できます。

ボリュームのステータスが単一のイベントに基づく場合は、イベントの名前、イベントがトリガーされた日時、イベントが割り当てられている管理者の名前、イベントの原因などの情報が表示されます。イベントの詳細情報を表示するには、* 詳細を表示 * ボタンを使用します。

ボリュームのステータスが同じ重大度の複数のイベントに基づく場合は、上位の 3 つのイベントについて、イベントの名前、イベントがトリガーされた日時、イベントが割り当てられている管理者の名前などの情報が表示されます。イベント名をクリックすると、それらの各イベントの詳細を確認できます。また、「* すべてのイベントを表示 *」リンクをクリックして、生成されたイベントのリストを表示することもできます。



ボリュームには、重大度が同じまたは異なる容量関連のイベントが複数ある場合もあります。ただし、表示されるのは最も高い重大度だけです。たとえば、重大度が「エラー」と「警告」の 2 つのイベントがボリュームにある場合、表示される重大度は「エラー」だけです。

- ボリューム

ボリュームの名前が表示されます。

- 使用済みデータ容量

ボリュームの容量の使用率に関する情報がグラフで表示されます。

- フルまでの日数

ボリュームの容量がフルに達するまでの推定日数が表示されます。

- シンプロビジョニング

選択したボリュームにスペースギャランティが設定されているかどうかが表示されます。有効な値は「はい」と「いいえ」です

- アグリゲート

FlexVol ボリュームの場合は、ボリュームが含まれているアグリゲートの名前が表示されます。FlexGroup ボリュームの場合、FlexGroup で使用されているアグリゲートの数が表示されます。

【構成】タブ

Configuration タブには、選択した Storage VM の設定に関する詳細が表示されます。これには、Storage VM に作成されたクラスタ、ルートボリューム、ボリュームのタイプ（FlexVol ボリューム）、ポリシー、保護などの情報が含まれます。

- * 概要 *

- クラスタ

Storage VM が属するクラスタの名前が表示されます。

- 使用できるボリュームタイプ

Storage VM で作成できるボリュームのタイプが表示されます。「FlexVol」または「FlexVol/FlexGroup」のいずれかです。

- ルートボリューム

Storage VM のルートボリュームの名前が表示されます。

- 許可するプロトコル

Storage VM で設定できるプロトコルのタイプが表示されます。また、プロトコルが稼働しているかどうかを示します (●)、Down (●)、またはが設定されていない (●)。

- * データ・ネットワーク・インターフェイス *

- NAS

Storage VM に関連付けられている NAS インターフェイスの数が表示されます。インターフェイスの状態 (●) または down (●)。

- SAN

Storage VM に関連付けられている SAN インターフェイスの数が表示されます。インターフェイスの状態 (●) または down (●)。

- FC-NVMe

Storage VM に関連付けられている FC-NVMe インターフェイスの数が表示されます。インターフェイスの状態 (●) または down (●)。

- * 管理ネットワーク・インターフェイス *

- 可用性

Storage VM に関連付けられている管理インターフェイスの数が表示されます。管理インターフェイスの状態 (●) または down (●)。

- * ポリシー *

- Snapshot

Storage VM に作成された Snapshot ポリシーの名前が表示されます。

- エクスポートポリシー

エクスポートポリシーが 1 つ作成されている場合はその名前が表示され、複数作成されている場合はその数が表示されます。

- * 保護 *

- Storage VM DR

選択した Storage VM が保護されているかどうか、デスティネーションが保護されていないか、および Storage VM が保護されているデスティネーションの名前が表示されます。選択した Storage VM がデスティネーションの場合、ソース Storage VM の詳細が表示されます。ファンアウトの場合、Storage VM が保護されているデスティネーション Storage VM の合計数が表示されます。ソース Storage VM でフィルタされた Storage VM 関係グリッドが表示されます。

- 保護されているボリューム

選択した Storage VM 上の保護されているボリュームのうち、合計ボリューム数から外れているボリュームの数が表示されます。デスティネーション Storage VM を表示している場合は、選択した Storage VM のデスティネーションボリュームの番号のリンクです。

- 保護されていないボリューム

選択した Storage VM の保護されていないボリュームの数が表示されます。

- * サービス *

- を入力します

Storage VM で設定されているサービスのタイプが表示されます。「Domain Name System (DNS ; ドメインネームシステム)」または「Network Information Service (NIS)」のいずれかです。

- 状態

サービスの状態が表示されます。up (●)、Down (●)、または設定されていない (●)。

- ドメイン名 (Domain Name)

DNS サービスの DNS サーバまたは NIS サービスの NIS サーバの完全修飾ドメイン名 (FQDN) が表示されます。NIS サーバが有効になっている場合は、アクティブな NIS サーバの FQDN が表示されます。NIS サーバが無効になっている場合は、すべての FQDN のリストが表示されます。

- IP アドレス

DNS サーバまたは NIS サーバの IP アドレスが表示されます。NIS サーバが有効になっている場合は、アクティブな NIS サーバの IP アドレスが表示されます。NIS サーバが無効になっている場合は、すべての IP アドレスのリストが表示されます。

Network Interfaces タブをクリックします

ネットワークインターフェイスタブには、選択した Storage VM に作成されているデータネットワークインターフェイス (LIF) に関する詳細が表示されます。

- * ネットワーク・インターフェイス *

選択した Storage VM に作成されているインターフェイスの名前が表示されます。

- * 動作ステータス *

インターフェイスの動作ステータスが表示されます。up (↑)、Down (↓)、または Unknown (?)。インターフェイスの動作ステータスは、物理ポートのステータスで決まります。

- * 管理ステータス *

インターフェイスの管理ステータスが表示されます。up (↑)、Down (↓)、または Unknown (?)。インターフェイスの管理ステータスは、設定への変更やメンテナンスを実施するために、ストレージ管理者が変更します。管理ステータスは、動作ステータスとは異なる場合があります。ただし、インターフェイスの管理ステータスが「停止」の場合、動作ステータスはデフォルトで「停止」になります。

- * IP アドレス / WWPN *

イーサネットインターフェイスの IP アドレスと FC LIF の World Wide Port Name （WWPN）が表示されます。

- * プロトコル *

CIFS、NFS、iSCSI、FC / FCoE など、インターフェイスに対して指定されているデータプロトコルのリストが表示されます。FC-NVMe、および FlexCache が必要です。

- * 役割 *

インターフェイスのロールが表示されます。「データ」または「管理」のいずれかです。

- * ホームポート *

インターフェイスが最初に関連付けられていた物理ポートが表示されます。

- * 現在のポート *

インターフェイスが現在関連付けられている物理ポートが表示されます。インターフェイスが移行された場合、現在のポートがホームポートと同じでなくなることがあります。

- * ポートセット *

インターフェイスがマッピングされているポートセットが表示されます。

- * フェイルオーバーポリシー *

インターフェイスに設定されているフェイルオーバーポリシーが表示されます。NFS インターフェイス、CIFS インターフェイス、および FlexCache インターフェイスの場合、デフォルトのフェイルオーバーポリシーは「次に使用可能」です。FC インターフェイスおよび iSCSI インターフェイスには、フェイルオーバーポリシーは適用できません。

- * ルーティンググループ *

ルーティンググループの名前が表示されます。ルーティンググループ名をクリックすると、ルートとデスティネーションゲートウェイに関する詳細を確認できます。

ルーティンググループは ONTAP 8.3 以降ではサポートされないため、それらのクラスタの列は空白になります。

- * フェイルオーバーグループ *

フェイルオーバーグループの名前が表示されます。

Qtrees （qtree）タブ

qtree タブには、qtree とそのクォータに関する詳細が表示されます。1 つ以上の qtree の容量の健全性しきい値の設定を編集するには、しきい値の編集 * ボタンをクリックします。

「* Export」ボタンを使用して、監視対象のすべての qtree の詳細を含むカンマ区切り値（.csv）ファイルを作成します。CSV ファイルにエクスポートして qtree のレポートを作成する際は、現在の Storage VM、現

在のクラスタのすべての Storage VM、またはデータセンター内のすべてのクラスタのすべての Storage VM について、のいずれかを選択できます。エクスポートした CSV ファイルには、qtree に関する追加のフィールドもいくつか表示されます。

- * ステータス *

qtree の現在のステータスが表示されます。ステータスは Critical (❌)、エラー (❗)、警告 (⚠)、または標準 (✅)。

ステータスアイコンにカーソルを合わせると、qtree に対して生成されたイベントに関する詳細を確認できます。

qtree のステータスが単一のイベントに基づく場合は、イベントの名前、イベントがトリガーされた日時、イベントが割り当てられている管理者の名前、イベントの原因などの情報が表示されます。イベントの詳細情報を表示するには、* View Details * を使用します。

qtree のステータスが同じ重大度の複数のイベントに基づく場合は、上位の 3 つのイベントについて、イベントの名前、イベントがトリガーされた日時、イベントが割り当てられている管理者の名前などの情報が表示されます。イベント名をクリックすると、それらの各イベントの詳細を確認できます。また、* すべてのイベントを表示 * を使用して、生成されたイベントのリストを表示することもできます。



qtree には、重大度が同じまたは異なる容量関連のイベントが複数ある場合もあります。ただし、表示されるのは最も高い重大度だけです。たとえば、重大度が「エラー」と「警告」の 2 つのイベントが qtree にある場合、表示される重大度は「エラー」だけです。

- * qtree *

qtree の名前が表示されます。

- * クラスタ *

qtree を含むクラスタの名前が表示されます。エクスポートした CSV ファイルにのみ表示されます。

- * Storage Virtual Machine *

qtree を含む Storage Virtual Machine (SVM) の名前が表示されます。エクスポートした CSV ファイルにのみ表示されます。

- * 音量 *

qtree が含まれているボリュームの名前が表示されます。

ボリューム名にカーソルを合わせると、ボリュームに関する詳細を確認できます。

- * クォータセット *

qtree でクォータが有効になっているかどうかを示します。

- * クォータタイプ *

ユーザ、ユーザグループ、または qtree のいずれのクォータであるかを示します。エクスポートした CSV ファイルにのみ表示されます。

- * ユーザーまたはグループ *

ユーザまたはユーザグループの名前が表示されます。ユーザおよびユーザグループごとに複数の行が表示されます。クォータのタイプが qtree の場合やクォータが設定されていない場合は空になります。エクスポートした CSV ファイルにのみ表示されます。

- * 使用ディスク %*

ディスクスペースの使用率が表示されます。ディスクのハードリミットが設定されている場合は、そのハードリミットに基づく値です。ディスクのハードリミットなしでクォータが設定されている場合は、ボリュームのデータスペースに基づきます。クォータが設定されていない場合や qtree が属するボリュームでクォータがオフになっている場合は、グリッドページに「該当なし」と表示され、CSV エクスポートデータではフィールドが空白になります。

- * ディスクハードリミット *

qtree に対するディスクスペースの最大割り当て容量が表示されます。この上限に達すると、Unified Manager で重大なイベントが生成され、ディスクへの書き込みがそれ以上許可されなくなります。ディスクのハードリミットなしでクォータが設定されている場合、クォータが設定されていない場合、または qtree が属するボリュームでクォータがオフになっている場合は、「無制限」と表示されます。

- * ディスクソフトリミット *

qtree に対するディスクスペースの割り当て容量について、警告イベントを生成する容量が表示されます。ディスクのソフトリミットなしでクォータが設定されている場合、クォータが設定されていない場合、または qtree が属するボリュームでクォータがオフになっている場合は、「無制限」と表示されます。デフォルトでは、この列は表示されません。

- * ディスクしきい値 *

ディスクスペースについて設定されているしきい値が表示されます。ディスクのしきい値の制限なしでクォータが設定されている場合、クォータが設定されていない場合、または qtree が属するボリュームでクォータがオフになっている場合は、「無制限」と表示されます。デフォルトでは、この列は表示されません。

- * 使用されているファイル数 %*

qtree で使用されているファイルの割合が表示されます。ファイルのハードリミットが設定されている場合は、そのハードリミットに基づく値です。ファイルのハードリミットなしでクォータが設定されている場合は、値は表示されません。クォータが設定されていない場合や qtree が属するボリュームでクォータがオフになっている場合は、グリッドページに「該当なし」と表示され、CSV エクスポートデータではフィールドが空白になります。

- * ファイルハードリミット *

qtree に許可されるファイル数のハードリミットが表示されます。ファイルのハードリミットなしでクォータが設定されている場合、クォータが設定されていない場合、または qtree が属するボリュームでクォータがオフになっている場合は、「無制限」と表示されます。

- * ファイルソフトリミット *

qtree に許可されるファイル数のソフトリミットが表示されます。ファイルのソフトリミットなしでクォータが設定されている場合、クォータが設定されていない場合、または qtree が属するボリュームでクォータがオフになっている場合は、「無制限」と表示されます。デフォルトでは、この列は表示されませ

ん。

【ユーザークォータ】タブと【グループクォータ】タブ

選択した Storage VM のユーザおよびユーザグループのクォータに関する詳細が表示されます。クォータのステータス、ユーザまたはユーザグループの名前、ディスクおよびファイルのソフトリミットとハードリミット、使用されているディスクスペースとファイル数、ディスクのしきい値などの情報を確認できます。ユーザまたはユーザグループに関連付けられている E メールアドレスを変更することもできます。

• * 電子メールアドレスの編集コマンドボタン *

E メールアドレスの編集ダイアログボックスが開き、選択したユーザまたはユーザグループの現在の E メールアドレスが表示されます。E メールアドレスを変更することができます。[メールアドレスの編集] フィールドが空白の場合、デフォルトルールを使用して、選択したユーザまたはユーザグループのメールアドレスが生成されます。

複数のユーザが同じクォータを使用する場合は、ユーザの名前がカンマで区切って表示されます。また、デフォルトのルールを使用して E メールアドレスが生成されることはないため、通知を送信するには E メールアドレスを指定する必要があります。

• * 電子メールルールの設定コマンドボタン *

Storage VM で設定されているユーザまたはユーザグループクォータについて、E メールアドレスを生成するルールを作成または変更できます。クォータに違反が発生すると、指定した E メールアドレスに通知が送信されます。

• * ステータス *

クォータの現在のステータスが表示されます。ステータスは Critical (❌)、警告 (⚠️)、または標準 (✅)。

ステータスアイコンにカーソルを合わせると、クォータに対して生成されたイベントに関する詳細を確認できます。

クォータのステータスが単一のイベントに基づく場合は、イベントの名前、イベントがトリガーされた日時、イベントが割り当てられている管理者の名前、イベントの原因などの情報が表示されます。イベントの詳細情報を表示するには、* View Details * を使用します。

クォータのステータスが同じ重大度の複数のイベントに基づく場合は、上位の 3 つのイベントについて、イベントの名前、イベントがトリガーされた日時、イベントが割り当てられている管理者の名前などの情報が表示されます。イベント名をクリックすると、それらの各イベントの詳細を確認できます。また、* すべてのイベントを表示 * を使用して、生成されたイベントのリストを表示することもできます。



クォータには、重大度が同じまたは異なる容量関連のイベントが複数ある場合もあります。ただし、表示されるのは最も高い重大度だけです。たとえば、重大度が「エラー」と「警告」の 2 つのイベントがクォータにある場合、表示される重大度は「エラー」だけです。

• * ユーザまたはグループ *

ユーザまたはユーザグループの名前が表示されます。複数のユーザが同じクォータを使用する場合は、ユーザの名前がカンマで区切って表示されます。

SecD のエラーによって ONTAP から有効なユーザ名が提供されない場合、値は「Unknown」と表示されます。

- * タイプ *

ユーザまたはユーザグループのどちらのクォータであるかを示します。

- * ボリュームまたは qtree *

ユーザまたはユーザグループのクォータが指定されているボリュームまたは qtree の名前が表示されます。

ボリュームまたは qtree の名前にカーソルを合わせると、そのボリュームまたは qtree に関する詳細を確認できます。

- * 使用ディスク %*

ディスクスペースの使用率が表示されます。ディスクのハードリミットなしでクォータが設定されている場合は、値は「該当なし」と表示されます。

- * ディスクハードリミット *

クォータに対するディスクスペースの最大割り当て容量が表示されます。この上限に達すると、Unified Manager で重大なイベントが生成され、ディスクへの書き込みがそれ以上許可されなくなります。ディスクのハードリミットなしでクォータが設定されている場合は、値は「無制限」と表示されます。

- * ディスクソフトリミット *

クォータに対するディスクスペースの割り当て容量について、警告イベントを生成する容量が表示されます。ディスクのソフトリミットなしでクォータが設定されている場合は、値は「無制限」と表示されます。デフォルトでは、この列は表示されません。

- * ディスクしきい値 *

ディスクスペースについて設定されているしきい値が表示されます。ディスクのしきい値制限なしでクォータが設定されている場合は「無制限」と表示されます。デフォルトでは、この列は表示されません。

- * 使用されているファイル数 %*

qtree で使用されているファイルの割合が表示されます。ファイルのハードリミットなしでクォータが設定されている場合は、値は「該当なし」と表示されます。

- * ファイルハードリミット *

クォータに許可されるファイル数のハードリミットが表示されます。ファイルのハードリミットなしでクォータが設定されている場合は、値は「無制限」と表示されます。

- * ファイルソフトリミット *

クォータに許可されるファイル数のソフトリミットが表示されます。ファイルのソフトリミットなしでクォータが設定されている場合は、値は「無制限」と表示されます。デフォルトでは、この列は表示されません。

- * 電子メールアドレス *

クォータに違反が発生した場合に通知が送信されるユーザまたはユーザグループの E メールアドレスが表示されます。

NFS Shares (NFS 共有) タブ

NFS 共有タブには、NFS 共有について、ステータス、ボリューム (FlexGroup または FlexVol ボリューム) に関連付けられたパス、NFS 共有に対するクライアントのアクセスレベル、エクスポートされているボリュームに対して定義されているエクスポートポリシーなどの情報が表示されます。NFS 共有は、ボリュームがマウントされていない場合、またはボリュームのエクスポートポリシーに関連付けられているプロトコルに NFS 共有が含まれていない場合は表示されません。

- * ステータス *

NFS 共有の現在のステータスが表示されます。ステータスは、Error (❗) または標準 (✅)。

- * ジャンクションパス *

ボリュームがマウントされているパスが表示されます。qtree に明示的な NFS エクスポートポリシーが適用されている場合、qtree にアクセスできるボリュームのパスが表示されます。

- * ジャンクションパスがアクティブ *

マウントされたボリュームにアクセスするパスがアクティブであるか非アクティブであるかが表示されます。

- * ボリュームまたは qtree *

NFS エクスポートポリシーが適用されているボリュームまたは qtree の名前が表示されます。NFS エクスポートポリシーがボリューム内の qtree に適用されている場合は、ボリュームと qtree の両方の名前が表示されます。

リンクをクリックすると、オブジェクトに関する詳細を対応する詳細ページで確認できます。オブジェクトが qtree の場合、qtree とボリュームの両方のリンクが表示されます。

- * ボリュームの状態 *

エクスポートされるボリュームの状態が表示されます。「オフライン」、「オンライン」、「制限」、「混在」のいずれかです。

- オフラインです

ボリュームへの読み取り / 書き込みアクセスが許可されていません。

- オンライン

ボリュームへの読み取り / 書き込みアクセスが許可されています。

- 制限

パリティの再構築などの一部の処理は許可されますが、データアクセスは許可されません。

- 混在

FlexGroup ボリュームに状態の異なるコンスティチュエントが混在しています。

- * セキュリティ形式 *

エクスポートされているボリュームのアクセス権限が表示されます。セキュリティ形式には、UNIX、Unified、NTFS、Mixed があります。

- UNIX（NFS クライアント）

ボリューム内のファイルおよびディレクトリに UNIX 権限が設定されています。

- 統合：

ボリューム内のファイルおよびディレクトリに unified セキュリティ形式が設定されています。

- NTFS（CIFS クライアント）

ボリューム内のファイルおよびディレクトリに Windows NTFS 権限が設定されています。

- 混在

ボリューム内のファイルおよびディレクトリに UNIX 権限または Windows NTFS 権限のどちらかを設定できます。

- * UNIX 権限 *

エクスポートされるボリュームに設定されている 8 進数の文字列形式の UNIX 権限ビットが表示されます。UNIX 形式の権限ビットと同様の形式です。

- * エクスポートポリシー *

エクスポートされているボリュームのアクセス権限を定義するルールが表示されます。リンクをクリックすると、エクスポートポリシーに関連付けられているルールについて、認証プロトコルやアクセス権限などの詳細を確認できます。

SMB Shares（SMB 共有）タブ

選択した Storage VM の SMB 共有に関する情報が表示されます。SMB 共有のステータス、共有名、Storage VM に関連付けられているパス、共有のジャンクションパスのステータス、コンテナオブジェクト、コンテナボリュームの状態、共有のセキュリティのデータ、共有に対して定義されているエクスポートポリシーなどの情報を参照できます。SMB 共有に相当する NFS パスが存在するかどうかを確認できます。



フォルダ内の共有は、SMB 共有タブには表示されません。

- * ユーザーマッピングの表示コマンドボタン *

[ユーザーマッピング（User Mapping）] ダイアログボックスを起動します。

Storage VM のユーザマッピングの詳細を確認できます。

- * ACL コマンドボタン * を表示します

共有の Access Control ダイアログボックスを開きます。

選択した共有のユーザおよび権限の詳細を表示できます。

- * ステータス *

共有の現在のステータスが表示されます。標準 (✓) またはエラー (!)。

- * 共有名 *

SMB 共有の名前が表示されます。

- * パス *

共有が作成されているジャンクションパスが表示されます。

- * ジャンクションパスがアクティブ *

共有にアクセスするパスがアクティブであるか非アクティブであるかが表示されます。

- * コンテナオブジェクト *

共有が属するコンテナオブジェクトの名前が表示されます。コンテナオブジェクトは、ボリュームまたは qtree のいずれかです。

リンクをクリックすると、該当する [詳細] ページでコンテナオブジェクトの詳細を表示できます。コンテナオブジェクトが qtree の場合、qtree とボリュームの両方のリンクが表示されます。

- * ボリュームの状態 *

エクスポートされるボリュームの状態が表示されます。「オフライン」、「オンライン」、「制限」、「混在」のいずれかです。

- オフラインです

ボリュームへの読み取り / 書き込みアクセスが許可されていません。

- オンライン

ボリュームへの読み取り / 書き込みアクセスが許可されています。

- 制限

パリティの再構築などの一部の処理は許可されますが、データアクセスは許可されません。

- 混在

FlexGroup ボリュームに状態の異なるコンスティチュエントが混在しています。

- * セキュリティ *

エクスポートされているボリュームのアクセス権限が表示されます。セキュリティ形式には、UNIX、Unified、NTFS、Mixed があります。

- UNIX（NFS クライアント）

ボリューム内のファイルおよびディレクトリに UNIX 権限が設定されています。

- 統合：

ボリューム内のファイルおよびディレクトリに unified セキュリティ形式が設定されています。

- NTFS（CIFS クライアント）

ボリューム内のファイルおよびディレクトリに Windows NTFS 権限が設定されています。

- 混在

ボリューム内のファイルおよびディレクトリに UNIX 権限または Windows NTFS 権限のどちらかを設定できます。

- * エクスポートポリシー *

共有に適用されているエクスポートポリシーの名前が表示されます。Storage VM にエクスポートポリシーが指定されていない場合は、「無効」と表示されます。

リンクをクリックすると、エクスポートポリシーに関連付けられているルールについて、アクセスプロトコルや権限などの詳細を確認できます。このリンクは、選択した Storage VM のエクスポートポリシーが無効になっている場合は無効になります。

- * NFS の同等機能 *

共有に NFS と同等の機能があるかどうかを示します。

SAN タブ

選択した Storage VM の LUN、イニシエータグループ、およびイニシエータに関する詳細が表示されます。デフォルトでは、LUNs ビューが表示されます。イニシエータグループの詳細は、イニシエータグループタブで確認できます。また、イニシエータタブでイニシエータの詳細を確認できます。

- * LUNs タブ *

選択した Storage VM に属する LUN に関する詳細が表示されます。LUN の名前、LUN の状態（オンラインまたはオフライン）、LUN が含まれているファイルシステム（ボリュームまたは qtree）の名前、ホストオペレーティングシステムのタイプ、LUN の合計データ容量とシリアル番号などの情報を参照できます。LUN Performance 列には、LUN / パフォーマンスの詳細ページへのリンクが表示されます。

LUN でシンプロビジョニングが有効になっているかどうかや、LUN がイニシエータグループにマッピングされているかどうかを確認できます。イニシエータにマッピングされている場合は、選択した LUN にマッピングされているイニシエータグループとイニシエータを表示できます。

- * イニシエータグループタブ *

イニシエータグループに関する詳細が表示されます。イニシエータグループの名前、アクセス状態、グル

ープ内のすべてのイニシエータで使用されているホストオペレーティングシステムのタイプ、サポートされるプロトコルなどの詳細を確認できます。アクセス状態の列のリンクをクリックすると、イニシエータグループの現在のアクセス状態を確認できます。

- * 標準 *

イニシエータグループは複数のアクセスパスに接続されています。

- * シングルパス *

イニシエータグループは単一のアクセスパスに接続されています。

- * パスなし *

イニシエータグループにアクセスパスが接続されていません。

イニシエータグループがすべてのインターフェイスにマッピングされているか、ポートセットを介して特定のインターフェイスにマッピングされているかを確認することができます[Mapped Interfaces] カラムのカウントリンクをクリックすると、すべてのインターフェイスが表示されるか、ポートセットの特定のインターフェイスが表示されます。ターゲットポータルを介してマッピングされているインターフェイスは表示されません。イニシエータグループにマッピングされているイニシエータと LUN の合計数が表示されます。

選択したイニシエータグループにマッピングされているLUNとイニシエータも確認できます。

- * イニシエータタブ *

選択した Storage VM のイニシエータの名前とタイプ、およびこのイニシエータにマッピングされているイニシエータグループの合計数が表示されます。

```
initiator groups that are mapped to the selected initiator group.
```

[関連注釈 (Related Annotations)] パネル

関連するアノテーションペインでは、選択した Storage VM に関連付けられているアノテーションの詳細を確認できます。これには、Storage VM に適用されるアノテーションの名前と値などの情報が含まれます。関連するアノテーションペインから手動アノテーションを削除することもできます。

Related Devices ペイン

Related Devices ペインでは、Storage VM に関連するクラスタ、アグリゲート、ボリュームを確認できます。

- * クラスタ *

Storage VM が属するクラスタの健全性ステータスが表示されます。

- * アグリゲート *

選択した Storage VM に属するアグリゲートの数が表示されます。最も高い重大度レベルに基づいて、アグリゲートの健全性ステータスも表示されます。たとえば、Storage VM に 10 個のアグリゲートがあ

り、5つのステータスが「警告」で残りの5つが「重大」の場合、ステータスは「重大」と表示されます。

- * 割り当て済みアグリゲート *

Storage VM に割り当てられているアグリゲートの数が表示されます。最も高い重大度レベルに基づいて、アグリゲートの健全性ステータスも表示されます。

- * ボリューム *

選択した Storage VM に属するボリュームの数と容量が表示されます。最も高い重大度レベルに基づいて、ボリュームの健全性ステータスも表示されます。Storage VM に FlexGroup がある場合は、FlexGroup の数も含まれます。FlexGroup コンスティチュエントは含まれません。

【関連グループ】ペイン

Related Groups ペインでは、選択した Storage VM に関連付けられているグループのリストを確認できます。

【関連アラート】ペイン

関連するアラートペインでは、選択した Storage VM に対して作成されたアラートのリストを確認できます。また、[* アラートの追加 *] リンクをクリックしてアラートを追加したり、アラート名をクリックして既存のアラートを編集したりすることもできます。

クラスタ / 健全性の詳細ページ

クラスタ / 健全性の詳細ページには、選択したクラスタについて、健全性、容量、設定の詳細などの情報が表示されます。クラスタのネットワークインターフェイス（LIF）、ノード、ディスク、関連するデバイス、および関連するアラートに関する情報も確認できます。

クラスタ名の横にあるステータス（「問題なし」など）は通信ステータスで、Unified Manager がクラスタと通信できるかどうかを示します。クラスタのフェイルオーバーステータスや全体的なステータスを表しているわけではありません。

コマンドボタン

選択したクラスタについて、各コマンドボタンを使用して次のタスクを実行できます。

- * パフォーマンスビューに切り替え *

クラスタ / パフォーマンスの詳細ページに移動できます。

- * アクション *

- アラートの追加：アラートの追加ダイアログボックスが開き、選択したクラスタにアラートを追加できます。
- 再検出：クラスタの手動更新が開始され、クラスタへの最新の変更を Unified Manager で検出できるようになります。

Unified Manager を OnCommand Workflow Automation と組み合わせて使用している場合、再検出処

理には WFA のキャッシュデータがあればそれが必要です。

再検出処理が開始されると、関連付けられているジョブの詳細へのリンクが表示され、ジョブステータスを追跡できるようになります。

◦ アノテーションの適用：選択したクラスタをアノテートできます。

• * クラスタを表示 *

健全性：すべてのクラスタビューに移動できます。

正常性タブ

ノード、SVM、アグリゲートなどのさまざまなクラスタオブジェクトのデータ可用性とデータ容量の問題に関する詳細な情報が表示されます。可用性の問題は、クラスタオブジェクトのデータ処理機能に関連した問題です。容量の問題は、クラスタオブジェクトのデータ格納機能に関連した問題です。

オブジェクトのグラフをクリックすると、フィルタリングされたオブジェクトのリストを表示できます。たとえば、警告が表示された SVM の容量のグラフをクリックすると、フィルタリングされた SVMs のリストを表示できます。このリストには、重大度レベルが「警告」の容量の問題があるボリュームまたは qtree を含む SVM が表示されます。また、警告が表示された SVM の可用性のグラフをクリックすると、重大度レベルが「警告」の可用性の問題がある SVM のリストが表示されます。

可用性の問題

可用性の問題があるオブジェクトとないオブジェクトの両方を含むオブジェクトの合計数が図で表示されます。グラフでは、問題の重大度レベルに応じて色が表示されます。グラフの下には、クラスタ内のデータの可用性に影響を及ぼす可能性がある問題とすでに影響を及ぼしている問題に関する詳細が表示されます。たとえば、停止しているディスクセルフやオフラインになっているアグリゲートの情報が表示されます。



SFO の棒グラフに表示されるデータは、ノードの HA の状態に基づきます。それ以外の棒グラフに表示されるデータは、生成されたイベントに基づいて計算されます。

容量の問題

容量の問題があるオブジェクトとないオブジェクトの両方を含むオブジェクトの合計数が図で表示されます。グラフでは、問題の重大度レベルに応じて色が表示されます。グラフの下には、クラスタ内のデータの容量に影響を及ぼす可能性がある問題とすでに影響を及ぼしている問題に関する詳細が表示されます。たとえば、設定されたしきい値を超える可能性があるアグリゲートの情報が表示されます。

Capacity（容量）タブ

選択したクラスタの容量に関する詳細情報が表示されます。

容量

割り当てられているすべてのアグリゲートの使用済み容量と使用可能容量を示すデータ容量のグラフが表示されます。

• 使用済み論理スペース

このクラスタのすべてのアグリゲートに格納されているデータの実際のサイズ。 ONTAP の Storage

Efficiency テクノロジによる削減を適用する前のサイズです。

- 使用済み

すべてのアグリゲート上のデータに使用されている物理容量。これには、パリティ、ライトサイジング、リザーベーション用に使用される容量は含まれません。

- 利用可能

データに使用できる容量が表示されます。

- スペア数

すべてのスペアディスクのストレージに使用できる格納可能容量が表示されます。

- プロビジョニング済み

基盤となるすべてのボリューム用にプロビジョニングされている容量が表示されます。

詳細

使用済み容量と使用可能容量に関する詳細情報が表示されます。この計算では、ルートアグリゲートデータは除外されます。

- 合計容量

クラスタの合計容量が表示されます。これには、パリティ用に割り当てられた容量は含まれません。

- 使用済み

データに使用されている容量が表示されます。これには、パリティ、ライトサイジング、リザーベーション用に使用される容量は含まれません。

- 利用可能

データに使用できる容量が表示されます。

- プロビジョニング済み

基盤となるすべてのボリューム用にプロビジョニングされている容量が表示されます。

- スペア数

すべてのスペアディスクのストレージに使用できる格納可能容量が表示されます。

クラウド階層

クラスタの FabricPool 対応アグリゲートについて、使用されているクラウド階層の合計容量、および接続されている各クラウド階層で使用されている容量が表示されます。FabricPool のライセンス設定またはライセンス設定は行われません。

ディスクタイプ別の物理容量内訳

ディスクタイプ別の物理容量ブレイクアウト領域には、クラスタ内のさまざまなタイプのディスクのディスク容量に関する詳細情報が表示されます。ディスクタイプをクリックすると、Disks（ディスク）タブにディスクタイプに関する詳細を表示できます。

- 使用可能な総容量

データディスクの使用可能容量とスペア容量が表示されます。

- HDD

クラスタ内のすべての HDD データディスクの使用済み容量と使用可能容量が図で表示されます。HDD のデータディスクのスペア容量は点線で表されます。

- フラッシュ

- SSD データ

クラスタ内の SSD データディスクの使用済み容量と使用可能容量が図で表示されます。

- SSD キャッシュ

クラスタ内の SSD キャッシュディスクの格納可能容量が図で表示されます。

- SSD スペア

クラスタ内の SSD、データ、およびキャッシュディスクのスペア容量が図で表示されます。

- 未割り当てディスク

クラスタ内の未割り当てのディスクの数が表示されます。

容量に問題があるアグリゲートのリストです

容量のリスクの問題があるアグリゲートの使用済み容量と使用可能容量に関する詳細が表形式で表示されます。

- ステータス

アグリゲートに容量に関連する特定の重大度の問題があることを示します。

ステータスにカーソルを合わせると、アグリゲートに対して生成されたイベントに関する詳細を確認できます。

アグリゲートのステータスが単一のイベントに基づく場合は、イベントの名前、イベントがトリガーされた日時、イベントが割り当てられている管理者の名前、イベントの原因などの情報が表示されます。イベントの詳細情報を表示するには、[* 詳細の表示 *] ボタンをクリックします。

アグリゲートのステータスが同じ重大度の複数のイベントに基づく場合は、上位の 3 つのイベントについて、イベントの名前、イベントがトリガーされた日時、イベントが割り当てられている管理者の名前などの情報が表示されます。イベント名をクリックすると、それらの各イベントの詳細を確認できます。また、「* すべてのイベントを表示 *」リンクをクリックして、生成されたイベントのリストを表示するこ

ともできます。



アグリゲートには、重大度が同じまたは異なる容量関連のイベントが複数ある場合もあります。ただし、表示されるのは最も高い重大度だけです。たとえば、重大度が「エラー」と「重大」の2つのイベントがアグリゲートにある場合、表示される重大度は「重大」だけです。

- アグリゲート

アグリゲートの名前が表示されます。

- 使用済みデータ容量

アグリゲートの容量の使用率に関する情報が図で表示されます。

- フルまでの日数

アグリゲートの容量がフルに達するまでの推定日数が表示されます。

【構成】タブ

選択したクラスタについて、IP アドレス、連絡先、場所などの詳細が表示されます。

クラスタの概要

- 管理インターフェイス

Unified Manager からクラスタへの接続に使用されるクラスタ管理 LIF が表示されます。インターフェイスの動作ステータスも表示されます。

- ホスト名または IP アドレス

Unified Manager からクラスタへの接続に使用されるクラスタ管理 LIF の FQDN、短縮名、または IP アドレスが表示されます。

- FQDN

クラスタの完全修飾ドメイン名（FQDN）が表示されます。

- OS バージョン

クラスタで実行されている ONTAP のバージョンが表示されます。クラスタ内の各ノードで異なるバージョンの ONTAP が実行されている場合は、最も古い ONTAP のバージョンが表示されます。

- 連絡先

クラスタで問題が発生した場合に連絡する管理者に関する詳細が表示されます。

- 場所

クラスタの場所が表示されます。

- パーソナリティ

オール SAN アレイ構成のクラスタかどうかを示します。

リモートクラスタの概要

MetroCluster 構成のリモートクラスタに関する詳細が表示されます。この情報は、MetroCluster 構成に対してのみ表示されます。

- クラスタ

リモートクラスタの名前が表示されます。クラスタ名をクリックすると、クラスタの詳細ページが表示されます。

- ホスト名または IP アドレス

リモートクラスタの FQDN、短縮名、または IP アドレスが表示されます。

- 場所

リモートクラスタの場所が表示されます。

MetroCluster の概要

MetroCluster over FCまたはMetroCluster over IP構成のローカルクラスタに関する詳細が表示されます。この情報は、MetroCluster over FCまたはIP構成についてのみ表示されます。

- を入力します

MetroCluster タイプが 2 ノードと 4 ノードのどちらであるかが表示されます。MetroCluster over IPでは、4ノードのみがサポートされます。

- 設定

FCおよびIPを使用したMetroCluster の設定が表示されます。次の値を指定できます。

- FCの場合*
- SAS ケーブルを使用したストレッチ構成
- FC-SAS ブリッジを使用したストレッチ構成
- FC スイッチを使用したファブリック構成



4 ノード MetroCluster の場合は、FC スイッチを使用するファブリック構成のみがサポートされます。

- IPの場合*
- イーサネットスイッチを使用したIP構成（クラスタの構成に応じてL2またはL3）
 - 自動計画外スイッチオーバー（AUSO）

ローカルクラスタで自動計画外スイッチオーバーが有効になっているかどうかが表示されます。Unified Manager のデフォルトの設定では、2 ノードの MetroCluster 構成の場合、すべてのクラスタで AUSO が有効になります。AUSO の設定はコマンドラインインターフェイスを使用して変更できます。これは、MetroCluster over FCでのみサポートされます。

- スwitchオーバーモード

MetroCluster over IP構成のスイッチオーバーモードを表示します。指定できる値は次のとおりです。Active、Negotiated Switchover`および`Automatic Unplanned Switchover。

ノード

- 可用性

稼働しているノードの数 (●) または down (●) をクラスタに追加します。

- OS のバージョン

ノードで実行されている ONTAP のバージョンと、そのバージョンの ONTAP を実行しているノードの数が表示されます。たとえば、「9.6 (2)、9.3 (1)」は、2 つのノードで ONTAP 9.6 が実行され、1 つのノードで ONTAP 9.3 が実行されていることを示します。

Storage Virtual Machine

- 可用性

稼働している SVM の数 (●) または down (●) をクラスタに追加します。

ネットワークインターフェイス

- 可用性

稼働している非データ LIF の数 (●) または down (●) をクラスタに追加します。

- クラスタ管理インターフェイス

クラスタ管理 LIF の数が表示されます。

- ノード管理インターフェイス

ノード管理 LIF の数が表示されます。

- クラスタインターフェイス

クラスタ LIF の数が表示されます。

- クラスタ間インターフェイス

クラスタ間 LIF の数が表示されます。

プロトコル

- データプロトコル

クラスタでライセンスが有効になっているデータプロトコルのリストが表示されます。データプロトコルには、iSCSI、CIFS、NFS、NVMe、FC / FCoE があります。

保護

- メディエーター

クラスタがメディエーターをサポートしているかどうかとメディエーターの接続ステータスを表示します。メディエーターが設定されているかどうかを示し、設定されている場合はメディエーターのステータスが表示されます。

- 該当なし

クラスタがメディエーターをサポートしていない場合に表示されます。

- 未設定

クラスタがメディエーターをサポートしているが、メディエーターが設定されていない場合に表示されます。

- IP アドレス

クラスタがメディエーターをサポートし、メディエーターが設定されている場合に表示されます。メディエーターのステータスは色で示されます。緑は、メディエーターのステータスが到達可能であることを示します。赤は、メディエーターのステータスが到達不能であることを示します。

クラウド階層

このクラスタが接続されているクラウド階層のリストが表示されます。それぞれのクラウド階層のタイプ（Amazon S3、Microsoft Azure クラウド、IBM Cloud Object Storage、Google Cloud Storage、Alibaba Cloud Object Storage、または StorageGRID）と状態（「使用可能」または「利用不可」）も表示されます。

MetroCluster 接続タブ

MetroCluster over FC構成のクラスタコンポーネントの問題と接続ステータスが表示されます。ディザスタリカバリパートナーに問題があるクラスタは赤い線で囲んで示されます。



MetroCluster 接続タブは、MetroCluster over FC構成のクラスタに対してのみ表示されます。

リモートクラスタの名前をクリックすると、リモートクラスタの詳細ページに移動できます。コンポーネント数のリンクをクリックして、コンポーネントの詳細を確認することもできます。たとえば、クラスタ内のノード数のリンクをクリックすると、クラスタの詳細ページにノードタブが表示されます。リモートクラスタのディスク数のリンクをクリックすると、リモートクラスタの詳細ページにディスクタブが表示されます。



8 ノード MetroCluster 構成を管理している場合、ディスクシェルフコンポーネントの個数のリンクをクリックすると、デフォルト HA ペアのローカルシェルフのみが表示されます。また、もう一方の HA ペアのローカルシェルフを表示する方法也没有ありません。

コンポーネントにカーソルを合わせると、問題の場合はクラスタの詳細と接続ステータスを確認でき、問題に対して生成されたイベントに関する詳細を確認できます。

コンポーネント間の接続問題のステータスが単一のイベントに基づく場合は、イベントの名前、イベントがトリガーされた日時、イベントが割り当てられている管理者の名前、イベントの原因などの情報が表示されます。[詳細の表示] ボタンをクリックすると、イベントの詳細が表示されます。

コンポーネント間の接続問題のステータスが同じ重大度の複数のイベントに基づく場合は、上位の 3 つのイベントについて、イベントの名前、イベントがトリガーされた日時、イベントが割り当てられている管理者の名前などの情報が表示されます。イベント名をクリックすると、それらの各イベントの詳細を確認できます。また、「* すべてのイベントを表示 *」リンクをクリックして、生成されたイベントのリストを表示することもできます。

MetroCluster レプリケーションタブ

MetroCluster over FC構成でレプリケートされているデータのステータスが表示されます。MetroCluster のレプリケーションタブを使用して、すでにピア関係が設定されたクラスタとデータを同期的にミラーリングすることで、データ保護を確保できます。ディザスタリカバリパートナーに問題があるクラスタは赤い線で囲って示されます。



MetroCluster レプリケーションタブは、MetroCluster over FC構成のクラスタに対してのみ表示されます。

MetroCluster 環境では、このタブを使用して、ローカルクラスタとリモートクラスタの間の論理接続やピア関係を検証できます。クラスタコンポーネントとその論理接続を客観的に捉えることができるため、これにより、メタデータやデータのミラーリングで発生する可能性がある問題を特定できます。

MetroCluster レプリケーションタブでは、選択したクラスタと MetroCluster パートナーがリモートクラスタを参照する詳細な図がローカルクラスタに表示されます。

Network Interfaces タブをクリックします

選択したクラスタに作成されているデータ LIF 以外のすべての LIF に関する詳細が表示されます。

Network Interface の略

選択したクラスタに作成されている LIF の名前が表示されます。

動作ステータス

インターフェイスの動作ステータスが表示されます。up (↑)、Down (↓)、または Unknown (?)。ネットワークインターフェイスの動作ステータスは、物理ポートのステータスで決まります。

管理ステータス

インターフェイスの管理ステータスが表示されます。up (↑)、Down (↓)、または Unknown (?)。設定を変更する際やメンテナンスを実施する際には、インターフェイスの管理ステータスを変更することができます。管理ステータスは、動作ステータスとは異なる場合があります。ただし、LIF の管理ステータス

が「停止」の場合、動作ステータスはデフォルトで「停止」になります。

IP アドレス

インターフェイスの IP アドレスが表示されます。

ロール

インターフェイスのロールが表示されます。「クラスタ管理 LIF」、「ノード管理 LIF」、「クラスタ LIF」、「クラスタ間 LIF」のいずれかです。

ホームポート

インターフェイスが最初に関連付けられていた物理ポートが表示されます。

現在のポート

インターフェイスが現在関連付けられている物理ポートが表示されます。LIF の移行後は、現在のポートがホームポートと同じでなくなることがあります。

フェイルオーバーポリシー

インターフェイスに設定されているフェイルオーバーポリシーが表示されます。

ルーティンググループ

ルーティンググループの名前が表示されます。ルーティンググループ名をクリックすると、ルートとデスティネーションゲートウェイに関する詳細を確認できます。

ルーティンググループは ONTAP 8.3 以降ではサポートされないため、それらのクラスタの列は空白になります。

フェイルオーバーグループ

フェイルオーバーグループの名前が表示されます。

[ノード (Nodes)] タブ

選択したクラスタ内のノードに関する情報が表示されます。HA ペア、ディスクシェルフ、およびポートに関する詳細情報を表示できます。

HAの詳細

HA ペアのノードの HA の状態と健全性ステータスが図で表示されます。ノードの健全性ステータスは次の色で示されます。

- * 緑 *

ノードは稼働しています。

- * 黄 *

ノードがパートナーノードをテイクオーバーしたか、環境に何らかの問題があります。

- * 赤 *

ノードは停止しています。

HA ペアの可用性に関する情報を確認して、リスクを回避するための必要な措置を講じることができます。たとえば、テイクオーバー処理が実行された可能性がある場合、「ストレージフェイルオーバー実行可能」というメッセージが表示されます。

ファン、電源装置、NVRAM バッテリ、フラッシュカード、サービスプロセッサ、およびディスクシェルフの接続。イベントがトリガーされた時刻を確認することもできます。

モデル番号など、ノード関連のその他の情報を確認することができます。

シングルノードクラスタがある場合は、ノードに関する詳細も確認できます。

ディスクシェルフ

HA ペアのディスクシェルフに関する情報が表示されます。

ディスクシェルフや環境コンポーネントに対して生成されたイベントも表示され、それらのイベントがトリガーされた時刻も確認できます。

- * シェルフ ID *

ディスクが配置されているシェルフの ID が表示されます。

- * コンポーネントステータス *

電源装置、ファン、温度センサー、電流センサー、ディスク接続など、ディスクシェルフの環境に関する詳細が表示されます。 および電圧センサー。環境の詳細は、次の色のアイコンで表示されます。

- * 緑 *

環境コンポーネントは適切に動作しています。

- * グレー *

環境コンポーネントについてのデータがありません。

- * 赤 *

一部の環境コンポーネントは停止しています。

- * 状態 *

ディスクシェルフの状態が表示されます。「オフライン」、「オンライン」、「ステータスなし」、「初期化が必要」、「見つからない」、「不明」のいずれかです

- * モデル *

ディスクシェルフのモデル番号が表示されます。

- * ローカルディスクシェルフ *

ディスクシェルフがローカルクラスタとリモートクラスタのどちらに配置されているかを示します。この列は、MetroCluster 構成のクラスタに対してのみ表示されます。

- * 一意の ID*

ディスクシェルフの一意の識別子が表示されます。

- * ファームウェアバージョン *

ディスクシェルフのファームウェアバージョンが表示されます。

ポート

関連付けられた FC、FCoE、およびイーサネットポートに関する情報が表示されます。ポートのアイコンをクリックすると、ポートとそれに関連付けられている LIF に関する詳細を確認できます。

ポートに対して生成されたイベントを確認することもできます。

ポートに関する次の詳細を確認できます。

- ポート ID

ポートの名前が表示されます。たとえば、e0M、e0a、e0b などです。

- ロール

ポートのロールが表示されます。「クラスタ」、「データ」、「クラスタ間」、「ノード管理」、「未定義」のいずれかです。

- を入力します

ポートに使用されている物理レイヤプロトコルが表示されます。「イーサネット」、「ファイバチャネル」、「FCoE」のいずれかです。

- WWPN

ポートの World Wide Port Name（WWPN；ワールドワイドポート名）が表示されます。

- ファームウェアリビジョン

FC / FCoE ポートのファームウェアのリビジョンが表示されます。

- ステータス

ポートの現在の状態が表示されます。「稼働」、「停止」、「リンク未接続」、「不明」()。

ポート関連イベントは、イベントリストで確認できます。関連付けられている LIF の詳細について、LIF の名前、動作ステータス、IP アドレスまたは WWPN、プロトコル、LIF に関連付けられている SVM の名前、現在のポート、フェイルオーバーポリシー、フェイルオーバーグループなどの情報も確認できます。

Disks（ディスク）タブ

選択したクラスタ内のディスクに関する詳細が表示されます。使用されているディスク、スペアディスク、破損ディスク、未割り当てディスクの数など、ディスク関連の情報を確認できます。ディスク名、ディスクタイプ、ディスクの所有者ノードなどの詳細も確認できます。

ディスクプールサマリ

実質的タイプ（FCAL、SAS、SATA、MSATA、SSD）別のディスク数が表示されます。NVMe SSD、SSD の容量、アレイ LUN、VMDISK）、ディスクの状態アグリゲート、共有ディスク、スペアディスク、破損ディスク、未割り当てディスクの数など、その他の詳細を確認することもできます。サポートされていないディスクで構成実質的ディスクタイプ数のリンクをクリックすると、選択した状態および実質的タイプのディスクが表示されます。たとえば、状態が「破損」で実質的タイプが「SAS」のディスク数のリンクをクリックすると、状態が「破損」で実質的タイプが「SAS」のすべてのディスクが表示されます。

ディスク

ディスクの名前が表示されます。

RAID グループ

RAID グループの名前が表示されます。

所有者ノード

ディスクが属するノードの名前が表示されます。ディスクが未割り当ての場合、この列に値は表示されません。

状態

ディスクの状態が表示されます。「アグリゲート」、「共有」、「スペア」、「破損」、「未割り当て」、サポートされていないか不明ですデフォルトでは、この列の状態は、「破損」、「未割り当て」、「サポート対象外」、「スペア」、「アグリゲート」の順にソートされて表示されます。共有。

ローカルディスク

ディスクがローカルクラスタに配置されているかリモートクラスタに配置されているかを示す「はい」または「いいえ」が表示されます。この列は、MetroCluster 構成のクラスタに対してのみ表示されます。

位置（**Position**）

コンテナタイプに基づいてディスクの位置が表示されます。たとえば、コピー、データ、パリティなどです。デフォルトでは、この列は表示されません。

影響を受けるアグリゲート

障害が発生したディスクの影響を受けるアグリゲートの数が表示されます。個数のリンクにカーソルを合わせると影響を受けるアグリゲートが表示され、アグリゲート名をクリックするとそのアグリゲートの詳細を確認できます。アグリゲート数をクリックして、影響を受けるアグリゲートのリストを「健全性：すべてのアグリゲート」ビューで確認することもできます。

次の場合、この列に値は表示されません。

- Unified Manager に追加されたクラスタに破損ディスクが含まれている場合
- 障害が発生したディスクがない場合

ストレージプール

SSD が属するストレージプールの名前が表示されます。ストレージプールの名前にカーソルを合わせると、ストレージプールの詳細を確認できます。

格納可能な容量

使用可能なディスク容量が表示されます。

物理容量

ライトサイジングや RAID 構成でフォーマットする前の raw ディスクの容量が表示されます。デフォルトでは、この列は表示されません。

を入力します

ディスクのタイプが表示されます。たとえば、ATA、SATA、FCAL、VMDISK などです。

実質的タイプ

ONTAP によって割り当てられたディスクタイプが表示されます。

ONTAP の特定のディスクタイプは、その作成、アグリゲートへの追加、およびスペアの管理を行う目的において同じタイプとみなされます。ONTAP は、各ディスクタイプに実質的ディスクタイプを割り当てます。

使用済みスペアブロック

SSD ディスクの使用済みのスペアブロックの割合が表示されます。この列は、SSD ディスク以外のディスクについては空白になります。

使用済み寿命

SSD の実際の使用状況とメーカーの想定寿命に基づいて、SSD の推定される使用済み寿命の割合が表示されます。この値が 99 を超えた場合、想定される耐久度に達したと考えられますが、必ずしも SSD で障害が発生しているとはかぎりません。値が不明なディスクについては省略されます。

ファームウェア

ディスクのファームウェアバージョンが表示されます。

rpm

ディスクの回転速度（rpm）が表示されます。デフォルトでは、この列は表示されません。

モデル

ディスクのモデル番号が表示されます。デフォルトでは、この列は表示されません。

ベンダー

ディスクベンダーの名前が表示されます。デフォルトでは、この列は表示されません。

シェルフ ID

ディスクが配置されているシェルフの ID が表示されます。

ベイ

ディスクが配置されているベイの ID が表示されます。

[関連注釈 (Related Annotations)] パネル

選択したクラスタに関連付けられているアノテーションの詳細を確認できます。これには、クラスタに適用されるアノテーションの名前と値などの情報が含まれます。関連するアノテーションペインから手動アノテーションを削除することもできます。

Related Devices ペイン

選択したクラスタに関連付けられているデバイスの詳細を確認できます。

これには、クラスタに接続されたデバイスのタイプ、サイズ、数、ヘルスステータスなどのプロパティが含まれます。個数のリンクをクリックすると、そのデバイスについてさらに詳しい分析を行うことができます。

MetroCluster のパートナーペインを使用すると、リモート MetroCluster パートナーの数や詳細、およびノード、アグリゲート、SVM などの関連するクラスタコンポーネントを取得できます。MetroCluster パートナーペインは、MetroCluster 構成のクラスタに対してのみ表示されます。

Related Devices ペインでは、クラスタに関連するノード、SVM、アグリゲートを確認し、それらに移動することができます。

MetroCluster パートナー

MetroCluster パートナーのヘルスステータスが表示されます。個数のリンクを使用して詳細に移動し、クラスタコンポーネントの健全性や容量に関する情報を確認できます。

ノード

選択したクラスタに属するノードの数、容量、および健全性ステータスが表示されます。容量は、総容量のうちの使用可能な合計容量を示します。

Storage Virtual Machine

選択したクラスタに属する SVM の数が表示されます。

アグリゲート

選択したクラスタに属するアグリゲートの数、容量、および健全性ステータスが表示されます。

【関連グループ】 ペイン

選択したクラスタを含むグループのリストを確認できます。

【関連アラート】 ペイン

関連するアラートペインでは、選択したクラスタのアラートのリストを確認できます。また、[Add Alert] リンクをクリックしてアラートを追加したり、アラート名をクリックして既存のアラートを編集したりすることもできます。

- 関連情報 *

["Volumes（ボリューム） ページ"](#)
["クラスタリストおよび詳細の表示"](#)

アグリゲート / 健全性の詳細ページ

アグリゲート / 健全性の詳細ページでは、選択したアグリゲートについて、容量、ディスク情報、設定の詳細、生成されたイベントなどの詳細情報を確認できます。また、そのアグリゲートに関連するオブジェクトやアラートに関する情報も参照できます。

コマンドボタン



FabricPool 対応アグリゲートを監視する場合、このページのコミット済み容量とオーバーコミット容量の値はローカルのパフォーマンス階層の容量のみに基づきます。クラウド階層で使用可能なスペースの量は、オーバーコミット容量の値に反映されません。同様に、アグリゲートのしきい値もローカルのパフォーマンス階層のみに対する値となります。

選択したアグリゲートについて、各コマンドボタンを使用して次のタスクを実行できます。

- * パフォーマンスビューに切り替え *

アグリゲート / パフォーマンスの詳細ページに移動できます。

- * アクション *

- アラートを追加します

選択したアグリゲートにアラートを追加できます。

- しきい値の編集

選択したアグリゲートのしきい値の設定を変更できます。

- * アグリゲートを表示 *

健全性：すべてのアグリゲートビューに移動できます。

Capacity（容量）タブ

容量タブには、選択したアグリゲートについて、容量、しきい値、日次増加率などの詳細情報が表示されます。

デフォルトでは、ルートアグリゲートについては容量のイベントは生成されません。また、Unified Manager で使用されるしきい値のノードのルートアグリゲートには適用されません。これらのイベントが生成されるように設定を変更できるのは、テクニカルサポート担当者だけです。テクニカルサポート担当者が設定を変更すると、しきい値がノードのルートアグリゲートにも適用されるようになります。

- * 容量 *

データ容量のグラフと Snapshot コピーのグラフに、アグリゲートの容量の詳細が表示されます。

- 使用済み論理スペース

アグリゲートに格納されているデータの実際のサイズ。ONTAP の Storage Efficiency テクノロジーによる削減を適用する前のサイズです。

- 使用済み

アグリゲートでデータに使用されている物理容量。

- オーバーコミット

アグリゲートのスペースがオーバーコミットされている場合、グラフにフラグとオーバーコミット容量が表示されます。

- 警告

警告しきい値が設定されている場所に点線が表示されます。つまり、アグリゲートのスペースがほぼフルです。このしきい値を超えると、「スペースがほぼフル」イベントが生成されます。

- エラー

エラーしきい値が設定された場所にある、アグリゲートのスペースがフルであることを示す実線が表示されます。このしきい値を超えると、「スペースがフル」イベントが生成されます。

- Snapshot コピーのグラフ

このグラフは、Snapshot 使用容量または Snapshot リザーブが 0 でない場合にのみ表示されます。

どちらのグラフにも、Snapshot 使用容量が Snapshot リザーブを超えている場合には超過分の使用容量が表示されます。

- * クラウド階層 *

FabricPool 対応アグリゲートについて、クラウド階層でデータに使用されているスペースが表示されます。FabricPool のライセンス設定またはライセンス設定は行われません。

クラウド階層が別のクラウドプロバイダ（「ミラーリング層」）にミラーリングされている場合、両方のクラウド階層がここに表示されます。

- * 詳細 *

容量に関する詳細情報が表示されます。

- 合計容量

アグリゲート内の合計容量が表示されます。

- データ容量

アグリゲートで使用されているスペース（使用済み容量）とアグリゲートの使用可能なスペース（空き容量）が表示されます。

- Snapshot リザーブ

アグリゲートの Snapshot の使用容量と空き容量が表示されます。

- オーバーコミット容量

アグリゲートオーバーコミットメントを表示します。アグリゲートオーバーコミットを使用すると、すべてのストレージが使用中でないかぎり、アグリゲートの実際の使用可能容量よりも多くのストレージを割り当てることができます。シンプロビジョニングを使用している場合、アグリゲート内のボリュームの合計サイズがアグリゲートの総容量を超えることがあります。



アグリゲートをオーバーコミットした場合は、アグリゲートの空きスペースを注意深く監視し、必要に応じてストレージを追加して、スペース不足による書き込みエラーを回避する必要があります。

- クラウド階層

FabricPool 対応アグリゲートについて、クラウド階層でデータに使用されているスペースが表示されます。FabricPool のライセンス設定またはライセンス設定は行われません。クラウド階層が別のクラウドプロバイダ（ミラー階層）にミラーリングされている場合、両方のクラウド階層が表示されます。

- 合計キャッシュスペース

Flash Pool アグリゲートに追加されているソリッドステートドライブ（SSD）の合計スペースが表示されます。アグリゲートで Flash Pool を有効にしているが、SSD が追加されていない場合、キャッシュスペースは 0KB と表示されます。



このフィールドは、アグリゲートで Flash Pool が無効になっている場合は表示されません。

- アグリゲートのしきい値

アグリゲートの容量に関する次のしきい値が表示されます

- ほぼフルのしきい値

アグリゲートがほぼフルであるとみなす割合を示します。

- フルのしきい値

アグリゲートがフルであるとみなす割合を示します。

- 「ほぼオーバーコミット」しきい値

アグリゲートがほぼオーバーコミットされているとみなす割合を示します。

- 「オーバーコミット」しきい値

アグリゲートがオーバーコミットされたとみなす割合を示します。

- その他の詳細：日次増加率

最後の 2 つのサンプル間の変更率が 24 時間続いた場合にアグリゲートで使用するディスクスペースが表示されます。

たとえば、アグリゲートのディスクスペースの使用量が午後 2 時に 10GB で、午後 6 時に 12GB であるとする、このアグリゲートの 1 日あたりの増加率は 2GB です。

- ボリューム移動

現在実行中のボリューム移動処理の数が表示されます。

- ボリュームが配置されました

アグリゲートから移動中のボリュームの数と容量が表示されます。

リンクをクリックすると、ボリューム名、ボリュームの移動先のアグリゲート、ボリューム移動処理のステータス、推定終了時刻などの詳細を確認できます。

- に表示されます

アグリゲートに移動中のボリュームの数と残りの移動容量が表示されます。

リンクをクリックすると、ボリューム名、ボリュームの移動元のアグリゲート、ボリューム移動処理のステータス、推定終了時刻などの詳細を確認できます。

- ボリューム移動後の推定使用容量

ボリューム移動処理完了後のアグリゲートの推定使用済みスペース（割合と KB、MB、GB など）が表示されます。

• * 容量の概要 - ボリューム *

アグリゲートに含まれるボリュームの容量に関する情報がグラフで表示されます。ボリュームで使用されているスペース（使用済み容量）とボリュームの使用可能なスペース（空き容量）が表示されます。シンプロビジョニングボリュームについて「シンプロビジョニングボリュームにスペースリスクあり」イベントが生成された場合は、ボリュームで使用されているスペース（使用済み容量）と、ボリュームで使用可能なスペースのうちアグリゲートの容量の問題が原因で使用できないスペース（使用不可の容量）が表示されます。

表示するグラフはドロップダウンリストから選択できます。グラフに表示されるデータをソートして、使用済みサイズ、プロビジョニングされたサイズ、使用可能な容量、1 日あたりの最大および最小増加率などの詳細を表示できます。アグリゲート内のボリュームを含む Storage Virtual Machine（SVM）でデータをフィルタリングできます。シンプロビジョニングボリュームの詳細を表示することもできます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。デフォルトでは、アグリゲート内の上位 30 個のボリュームがフィルタリングされて表示されます。

選択したアグリゲート内のディスクについて、RAID タイプとサイズ、アグリゲートで使用されているディスクのタイプなど、詳細な情報が表示されます。このタブには、RAID グループと使用されているディスクのタイプ（SAS、ATA、FCAL、SSD、VMDISK など）を示す図も表示されます。パリティディスクやデータディスクにカーソルを合わせると、ディスクのベイ、シェルフ、回転速度などの詳細を確認できます。

• * データ *

専用データディスク、共有データディスク、またはその両方の詳細が図で表示されます。データディスクに共有ディスクが含まれている場合は、共有ディスクの詳細が表示されます。専用ディスクと共有ディスクの両方が含まれているデータディスクの場合は、両方のディスクの詳細が表示されます。

◦ * RAID の詳細 *

専用ディスクの場合のみ、RAID の詳細が表示されます。

▪ を入力します

RAID タイプ（RAID 0、RAID 4、RAID-DP、または RAID-TEC）が表示されます。

▪ グループサイズ

RAID グループに含めることができるディスクの最大数が表示されます。

▪ グループ

アグリゲート内の RAID グループの数が表示されます。

◦ * 使用されているディスク *

▪ 実質的タイプ

データディスクの種類（ATA、SATA、FCAL、SSD、や VMDISK など）を追加します。

▪ データディスク

アグリゲートに割り当てられているデータディスクの数と容量が表示されます。データディスクの詳細は、アグリゲートに共有ディスクしか含まれていない場合は表示されません。

▪ パリティディスク

アグリゲートに割り当てられているパリティディスクの数と容量が表示されます。パリティディスクの詳細は、アグリゲートに共有ディスクしか含まれていない場合は表示されません。

▪ 共有ディスク

アグリゲートに割り当てられている共有データディスクの数と容量が表示されます。共有ディスクの詳細は、アグリゲートに共有ディスクが含まれている場合にのみ表示されます。

◦ * スペアディスク *

選択したアグリゲートのノードで使用できるスペアデータディスクの実質的タイプ、数、および容量が表示されます。



Unified Manager では、アグリゲートがパートナーノードにフェイルオーバーされた場合、アグリゲートと互換性があるすべてのスペアディスクが表示されないことがあります。

- * SSD キャッシュ *

専用キャッシュ SSD ディスクと共有キャッシュ SSD ディスクに関する詳細が表示されます。

専用キャッシュ SSD ディスクについては、次の詳細が表示されます。

- * RAID の詳細 *

- を入力します

RAID タイプ（RAID 0、RAID 4、RAID-DP、または RAID-TEC）が表示されます。

- グループサイズ

RAID グループに含めることができるディスクの最大数が表示されます。

- グループ

アグリゲート内の RAID グループの数が表示されます。

- * 使用されているディスク *

- 実質的タイプ

アグリゲートでキャッシュに使用されているディスクタイプとして「SSD」が表示されます。

- データディスク

キャッシュ用にアグリゲートに割り当てられているデータディスクの数と容量が表示されます。

- パリティディスク

キャッシュ用にアグリゲートに割り当てられているパリティディスクの数と容量が表示されます。

- * スペアディスク *

選択したアグリゲートのノードでキャッシュに使用できるスペアディスクの実質的タイプ、数、および容量が表示されます。



Unified Manager では、アグリゲートがパートナーノードにフェイルオーバーされた場合、アグリゲートと互換性があるすべてのスペアディスクが表示されないことがあります。

共有キャッシュについては、次の情報が表示されます。

- * ストレージプール *

ストレージプールの名前が表示されます。ストレージプールの名前にカーソルを合わせると、次の情報を確認できます。

- ステータス

ストレージプールのステータスが表示されます。正常であるか正常でないかがあります。

- 割り当て合計

ストレージプール内の合計割り当て単位とサイズが表示されます。

- 割り当て単位のサイズ

アグリゲートに割り当て可能なストレージプール内の最小スペースが表示されます。

- ディスク

ストレージプールの作成に使用されているディスクの数が表示されます。ストレージプールの列のディスク数と、そのストレージプールのディスク情報タブに表示されるディスク数が一致しない場合は、1つ以上のディスクが破損しており、ストレージプールが正常な状態でないことを示しています。

- 使用済みの割り当て

アグリゲートで使用されている割り当て単位の数とサイズが表示されます。アグリゲート名をクリックすると、アグリゲートの詳細を確認できます。

- 使用可能な割り当て

ノードで使用可能な割り当て単位の数とサイズが表示されます。ノード名をクリックすると、アグリゲートの詳細を確認できます。

- * 割り当て済みキャッシュ *

アグリゲートで使用されている割り当て単位のサイズが表示されます。

- * 割り当て単位 *

アグリゲートで使用されている割り当て単位の数が表示されます。

- * ディスク *

ストレージプールに含まれているディスクの数が表示されます。

- * 詳細 *

- ストレージプール

ストレージプールの数が表示されます。

- 合計サイズ

ストレージプールの合計サイズが表示されます。

- * クラウド階層 *

FabricPool 対応アグリゲートを設定している場合にクラウド階層の名前が表示され、使用済みの合計スペースが表示されます。クラウド階層が別のクラウドプロバイダ（ミラー階層）にミラーリングされている場合、両方のクラウド階層の詳細が表示されます

【構成】タブ

Configuration タブには、選択したアグリゲートについて、クラスタノード、ブロックタイプ、RAID タイプ、RAID サイズ、RAID グループ数などの詳細が表示されます。

• * 概要 *

◦ ノード

選択したアグリゲートが含まれるノードの名前が表示されます。

◦ ブロックタイプ（Block Type）

アグリゲートのブロック形式が表示されます。32 ビットまたは 64 ビットのいずれかになります。

◦ RAID タイプ

RAID タイプ（RAID 0、RAID 4、RAID-DP、RAID-TEC、または混在 RAID）が表示されます。

◦ RAID サイズ

RAID グループのサイズが表示されます。

◦ RAID グループ

アグリゲート内の RAID グループの数が表示されます。

◦ SnapLock タイプ

アグリゲートの SnapLock タイプが表示されます。

• * クラウド階層 *

FabricPool 対応アグリゲートの場合、クラウド階層の詳細が表示されます。一部のフィールドはストレージプロバイダによって異なります。クラウド階層が別のクラウドプロバイダ（「ミラーリング層」）にミラーリングされている場合、両方のクラウド階層がここに表示されます。

◦ プロバイダ

ストレージプロバイダの名前が表示されます。たとえば、StorageGRID、Amazon S3、IBM Cloud Object Storage、Microsoft Azure クラウド、Google Cloud Storage、Alibaba Cloud Object Storage などです。

◦ 名前

ONTAP での作成時に指定されたクラウド階層の名前が表示されます。

◦ サーバ

クラウド階層の FQDN が表示されます。

- ポート

クラウドプロバイダとの通信に使用されているポート。

- アクセスキーまたはアカウント

クラウド階層のアクセスキーまたはアカウントが表示されます。

- コンテナ名

クラウド階層のバケット名またはコンテナ名が表示されます。

- SSL

クラウド階層に対して SSL 暗号化が有効になっているかどうかが表示されます。

履歴領域

履歴領域には、選択したアグリゲートの容量に関する情報がグラフで表示されます。また、[* エクスポート *] ボタンをクリックして、表示しているチャートの CSV 形式でレポートを作成することもできます。

履歴ペインの上部にあるドロップダウンリストからグラフタイプを選択できます。1 週間、1 カ月、または 1 年のいずれかを選択して、特定の期間の詳細を表示することもできます。履歴グラフは傾向を確認するのに役立ちます。たとえば、アグリゲートの使用量が継続的に「ほぼフル」のしきい値を超えていれば、それに応じた措置を講じることができます。

履歴グラフには次の情報が表示されます。

- * アグリゲート - 使用容量 (%) *

折れ線グラフの形式で、アグリゲートの使用率とアグリゲートの容量使用履歴が縦軸 (y 軸) に表示されます。横軸 (x 軸) に期間が表示されます。期間は、1 週間、1 カ月、または 1 年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、折れ線グラフの表示と非表示を切り替えることができます。たとえば、Capacity Used の凡例をクリックすると、Capacity Used のグラフの線が非表示になります。

- * アグリゲート - 使用容量と総容量 *

折れ線グラフの形式で、アグリゲートの容量の使用履歴と使用済み容量および合計容量 (バイト、KB、MB) が表示されます。垂直 (y) 軸など。横軸 (x 軸) に期間が表示されます。期間は、1 週間、1 カ月、または 1 年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、折れ線グラフの表示と非表示を切り替えることができます。たとえば、「使用済みトレンド容量」の凡例をクリックすると、「使用済みトレンド容量」のグラフ行が非表示になります。

- * アグリゲート - 使用容量 (%) 対コミット容量 (%) *

折れ線グラフの形式で、アグリゲートの容量使用履歴とコミット済みスペースの割合が縦軸 (y 軸) に表示されます。横軸 (x 軸) に期間が表示されます。期間は、1 週間、1 カ月、または 1 年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、折れ線グラフの表示と非表示を切り替えることができます。たとえば、Space

Committed の凡例をクリックすると、Space Committed のグラフの線が非表示になります。

イベントのリスト

イベントリストには、新規イベントと確認済みイベントに関する詳細が表示されます。

- * 重大度 *

イベントの重大度が表示されます。

- * イベント *

イベント名が表示されます。

- * トリガー日時 *

イベントが生成されてからの経過時間が表示されます。1 週間を過ぎたイベントには、生成時のタイムスタンプが表示されます。

Related Devices ペイン

Related Devices ペインでは、アグリゲートに関連するクラスタノード、ボリューム、およびディスクを確認できます。

- * ノード *

アグリゲートが含まれるノードの容量と健全性ステータスが表示されます。容量は、総容量のうちの使用可能な合計容量を示します。

- * ノード内のアグリゲート *

選択したアグリゲートが含まれるクラスタノード内のアグリゲートの総数と容量が表示されます。最も高い重大度レベルに基づいて、アグリゲートの健全性ステータスも表示されます。たとえば、クラスタノードに 10 個のアグリゲートがあり、5 つのステータスが「警告」で残りの 5 つが「重大」の場合、ステータスは「重大」と表示されます。

- * ボリューム *

アグリゲート内の FlexVol ボリュームと FlexGroup ボリュームの数と容量が表示されます。FlexGroup コンスティチュエントは含まれません。最も高い重大度レベルに基づいて、ボリュームの健全性ステータスも表示されます。

- * リソースプール *

アグリゲートに関連するリソースプールが表示されます。

- * ディスク *

選択したアグリゲート内のディスクの数が表示されます。

【関連アラート】 ペイン

関連するアラートペインでは、選択したアグリゲートに対して作成されたアラートのリストを確認できます。また、[Add Alert] リンクをクリックしてアラートを追加したり、アラート名をクリックして既存のアラートを編集したりすることもできます。

- 関連情報 *

"ストレージプールの詳細を表示しています"

データを保護、リストア

保護関係の作成、監視、およびトラブルシューティング

Unified Manager では、保護関係の作成、管理対象クラスタに保存されているデータのミラー保護とバックアップ保護の監視とトラブルシューティング、および上書きされたデータや失われたデータのリストアを実行できます。

SnapMirror 保護のタイプ

導入するデータストレージのトポロジに応じて、複数のタイプの SnapMirror 保護関係を Unified Manager で設定できます。すべての種類の SnapMirror 保護では、フェイルオーバーによるディザスタリカバリ保護が提供されますが、パフォーマンス、バージョン依存性の解消、および複数のバックアップコピーによる保護については、提供される機能が異なります。

従来型の SnapMirror 非同期保護関係

従来型の SnapMirror 非同期保護では、ソースボリュームとデスティネーションボリューム間のブロックレプリケーションによるミラー保護が提供されます。

従来型の SnapMirror 関係では、ブロックレプリケーションに基づいてミラー処理が行われるため、他の SnapMirror 関係よりも高速なミラー処理が可能です。ただし、従来型の SnapMirror 保護では、デスティネーションボリュームで実行されている ONTAP ソフトウェアのマイナーバージョンがソースボリュームと同じかそれよりも新しい必要があります（バージョン 8.x から 8.x、9.x から 9.x など）。9.1 ソースから 9.0 デスティネーションへのレプリケーションはサポートされていません。これは、デスティネーションで古いメジャーバージョンが実行されているためです。

バージョンに依存しないレプリケーションを使用した SnapMirror 非同期保護

バージョンに依存しないレプリケーションを使用した SnapMirror 非同期保護では、ソースボリュームとデスティネーションボリューム間の論理レプリケーションによるミラー保護が提供されます。ボリュームで異なるバージョンの ONTAP 8.3 以降のソフトウェアを実行している場合でも同様です（バージョン 8.3 から 8.3.1、8.3 から 9.1、9.2 から 9.2.2 など）。

バージョンに依存しないレプリケーションを使用した SnapMirror 関係では、ミラー処理が従来型の SnapMirror 関係ほど高速ではありません。

実行速度が遅いため、バージョンに依存しないレプリケーション保護を使用する SnapMirror は、次の状況のどちらにも適していません。

- ・ソースオブジェクトには、保護対象のファイルが 1、000 万を超えています。
- ・保護対象データの目標復旧時点が 2 時間以下である。（つまり、ソースのデータからの遅れが 2 時間未満のリカバリ可能なミラーデータが常にデスティネーションに含まれている必要があります）。

これらのいずれかの状況では、デフォルトの SnapMirror 保護をより高速なブロックレプリケーションベースで実行する必要があります。

バージョンに依存しないレプリケーションとバックアップオプションを使用した **SnapMirror** 非同期保護

バージョンに依存しないレプリケーションとバックアップオプションを使用した SnapMirror 非同期保護では、ソースボリュームとデスティネーションボリューム間のミラー保護およびミラーデータの複数のコピーをデスティネーションに格納する機能が提供されます。

ストレージ管理者は、ソースからデスティネーションにミラーリングする Snapshot コピーを指定したり、ソースで削除されたコピーをデスティネーションに保持する期間を指定したりできます。

バージョンに依存しないレプリケーションとバックアップオプションを使用した SnapMirror 関係では、ミラー処理が従来型の SnapMirror 関係ほど高速ではありません。

SnapMirror ユニファイドレプリケーション（ミラーバックアップ）

SnapMirror ユニファイドレプリケーションを使用すると、同じデスティネーションボリュームでディザスタリカバリとアーカイブを設定できます。SnapMirror と同様に、一元化されたデータ保護機能の初回起動時に、ベースライン転送が実行されます。デフォルトの一元化されたデータ保護ポリシー「MirrorAllSnapshots」に基づくベースライン転送では、ソースボリュームの Snapshot コピーが作成され、そのコピーおよびコピーが参照するデータブロックがデスティネーションボリュームに転送されます。SnapVault と同様に、一元化されたデータ保護にはベースラインの古い Snapshot コピーは含まれません。

厳密な同期を使用した **SnapMirror** 同期保護

「stict」同期を使用した SnapMirror 同期保護では、プライマリボリュームとセカンダリボリュームが常に相互の完全なコピーになります。セカンダリボリュームへのデータの書き込みでレプリケーションエラーが発生すると、プライマリボリュームに対するクライアント I/O が中断されます。

通常の同期を使用した **SnapMirror** 同期保護

「ル」同期を使用した SnapMirror 同期保護では、プライマリボリュームとセカンダリボリュームが常に相互の完全なコピーである必要はないため、プライマリボリュームの可用性が確保されます。セカンダリボリュームへのデータの書き込みでレプリケーションエラーが発生すると、プライマリボリュームとセカンダリボリュームが同期されていない状態のまま、プライマリボリュームに対するクライアント I/O が継続されます。



同期保護関係を Health : All Volumes ビューまたは Volume/Health Details ページから監視する場合、Restore ボタンと Relationship 操作ボタンは使用できません。

SnapMirror Synchronous によるビジネス継続性

ONTAP 9.8 以降では、SnapMirror のビジネス継続性（SM-BC）機能を使用できます。また、この機能を使用して LUN でアプリケーションを保護できるため、アプリケーションのフェイルオーバーを透過的に実行し、災害発生時のビジネス継続性を確保できます。

クラスタおよび Storage Virtual Machine で使用される Consistency Groups（CG；整合グループ）の同期 SnapMirror 関係を Unified Manager から検出して監視できます。SM-BC は、AFF クラスタまたは All SAN Array（ASA）クラスタでサポートされます。プライマリクラスタとセカンダリクラスタは、AFF または ASA のどちらかになります。SM-BC は、iSCSI LUN または FCP LUN を使用してアプリケーションを保護します。

SM-BC 関係で保護されているボリュームと LUN を表示すると、保護関係の一元化されたビュー、ボリュームインベントリ内の整合グループ、整合グループ関係の保護トポロジの表示、1 年以内の整合グループ関係の履歴データの表示が可能になります。レポートをダウンロードすることもできます。また、整合グループ関係

の概要の表示、整合グループ関係のサポートの検索、整合グループで保護されているボリュームに関する情報の取得も可能です。

[関係] ページでは 'ソースストレージオブジェクトとデスティネーションストレージオブジェクト' およびコンシステンシグループによって保護されているそれらの関係の保護をソート 'フィルタ' および拡張することもできます

SnapMirror Synchronous のビジネス継続性の詳細については、を参照してください ["SM-BC に関する ONTAP 9 のマニュアル"](#)。

Unified Manager で保護関係をセットアップする

Unified Manager と OnCommand Workflow Automation を使用してデータを保護するための SnapMirror 関係と SnapVault 関係をセットアップするには、いくつかの手順を実行する必要があります。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- 2 つのクラスタまたは 2 つの Storage Virtual Machine (SVM) 間にピア関係を確立しておく必要があります。
- OnCommand Workflow Automation を Unified Manager に統合する必要があります。
 - ["OnCommand Workflow Automation をセットアップする"](#)。
 - ["Workflow Automation での Unified Manager データソースのキャッシングの確認"](#)。

手順

1. 作成する保護関係のタイプに応じて、次のいずれかを実行します。
 - ["SnapMirror 保護関係を作成する"](#)。
 - ["SnapVault 保護関係を作成する"](#)。
2. 関係のポリシーを作成する場合は、作成する関係タイプに応じて、次のいずれかを実行します。
 - ["SnapVault ポリシーを作成する"](#)。
 - ["SnapMirror ポリシーを作成する"](#)。
3. ["SnapMirror または SnapVault スケジュールを作成します"](#)。

Workflow Automation と Unified Manager の間の接続の設定

OnCommand Workflow Automation (WFA) と Unified Manager の間にセキュアな接続を確立することができます。Workflow Automation に接続することで、SnapMirror や SnapVault の設定ワークフロー、SnapMirror 関係の管理用コマンドなどの保護機能を使用できるようになります。

- 必要なもの *
- Workflow Automation のバージョン 5.1 以降がインストールされている必要があります。



WFA 5.1 には「WFA pack for managing Clustered Data ONTAP」が含まれています。したがって、以前のようにこのパックを NetAppStorage Automation Store からダウンロードして、WFA サーバに個別にインストールする必要はありません。["ONTAP を管理するための WFA パック"](#)

- WFA と Unified Manager の接続をサポートするために Unified Manager で作成したデータベースユーザの名前を確認しておく必要があります。

このデータベースユーザには、統合スキーマユーザロールが割り当てられている必要があります。

- Workflow Automation で Administrator ロールまたは Architect のロールが割り当てられている必要があります。
- ホストアドレス、ポート番号 443、および Workflow Automation セットアップのユーザ名とパスワードが必要です。
- アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* 一般 * > * Workflow Automation * をクリックします。
2. Workflow Automation ページ * の * データベースユーザ * 領域で、名前を選択し、Unified Manager 接続と Workflow Automation 接続をサポートするために作成したデータベースユーザのパスワードを入力します。
3. ページの * Workflow Automation Credentials * 領域に、ホスト名または IP アドレス（IPv4 または IPv6）、および Workflow Automation セットアップのユーザ名とパスワードを入力します。

Unified Manager サーバのポート（ポート 443）を使用する必要があります。

4. [保存（Save）] をクリックします。
5. 自己署名証明書を使用する場合は、[* はい] をクリックしてセキュリティ証明書を承認します。

Workflow Automation ページが表示されます。

6. Web UI をリロードして Workflow Automation の機能を追加するには、「* Yes 」をクリックします。

◦ 関連情報 *

["ネットアップのマニュアル：OnCommand Workflow Automation（現在のリリース）"](#)

Workflow Automation での Unified Manager データソースのキャッシングの確認

Unified Manager データソースのキャッシングが正しく機能しているかどうかを判別するには、Workflow Automation でデータソースの取得が正常に行われているかどうかを確認します。Workflow Automation を Unified Manager に統合する際にこの操作を実行して、統合後に Workflow Automation の機能が利用可能になることを確認できます。

- 必要なもの *

このタスクを実行するには、Workflow Automation で Administrator ロールまたは Architect ロールが割り当てられている必要があります。

手順

1. Workflow Automation の UI から、* Execution * > * Data Sources * を選択します。
2. Unified Manager データソースの名前を右クリックし、* 今すぐ取得 * を選択します。
3. 取得が正常に完了してエラーが発生しないことを確認します

Workflow Automation を Unified Manager に統合するためには、収集エラーを解決する必要があります。

OnCommand Workflow Automation を再インストールまたはアップグレードするとどうなりますか

OnCommand Workflow Automation を再インストールまたはアップグレードする前に、OnCommand Workflow Automation と Unified Manager の間の接続を削除し、実行中のすべての OnCommand Workflow Automation またはスケジュールされたジョブが停止されていることを確認する必要があります。

また、OnCommand Workflow Automation から Unified Manager を手動で削除する必要があります。

OnCommand Workflow Automation を再インストールまたはアップグレードしたら、Unified Manager との接続を再度セットアップする必要があります。

OnCommand Workflow Automation セットアップを **Unified Manager** から削除しています

Workflow Automation が不要となった場合は、Unified Manager から OnCommand Workflow Automation のセットアップを削除できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、左の [セットアップ] メニューの [一般 > Workflow Automation *] をクリックします。
2. [* Workflow Automation*] ページで、[セットアップの削除] をクリックします。

保護関係のフェイルオーバーとフェイルバックを実行する

ハードウェア障害や災害が原因で保護関係のソースボリュームが無効になっている場合は、Unified Manager の保護関係機能を使用して保護デスティネーションの読み取り / 書き込みアクセスを可能にし、ソースがオンラインに戻るまでそのボリュームにフェイルオーバーすることができます。その後、データの提供に使用できる元のソースにフェイルバックできます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- この処理を実行するには、OnCommand Workflow Automation をセットアップしておく必要があります。

手順

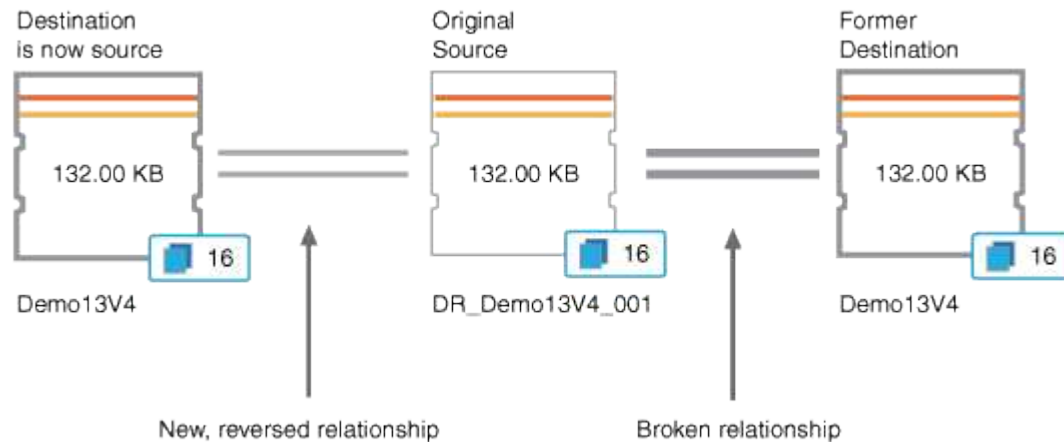
1. "SnapMirror 関係を解除".

デスティネーションをデータ保護ボリュームから読み書き可能ボリュームに変換する前、および関係を反転する前に、関係を解除する必要があります。

2. "保護関係を反転する".

元のソースボリュームが再び使用可能になったら、ソースボリュームをリストアして元の保護関係を再確立できます。ソースをリストアする前に、以前のデスティネーションに書き込まれたデータとソースを同期させる必要があります。逆再同期処理を使用して新しい保護関係を作成するには、元の関係のロールを反転し、ソースボリュームと以前のデスティネーションを同期させます。新しい関係に対して新しいベースライン Snapshot コピーが作成されます。

反転関係は、カスケード関係に似ています。



3. "反転する SnapMirror 関係を解除する".

元のソースボリュームが再同期され、再びデータを提供できるようになったら、解除処理を使用して反転関係を解除します。

4. "関係を削除します".

反転関係が不要になった場合は、元の関係を再確立する前に反転関係を削除する必要があります。

5. "関係を再同期します".

再同期処理を使用して、ソースからデスティネーションにデータを同期し、元の関係を再確立します。

ボリューム / 健全性の詳細ページから **SnapMirror** 関係を解除します

保護関係をボリューム / 健全性の詳細ページから解除して、SnapMirror 関係にあるソースボリュームとデスティネーションボリューム間のデータ転送を停止することができます。関係の解除は、データを移行する場合、ディザスタリカバリやアプリケーションのテストなどの目的で行うことがあります。デスティネーションボリュームは読み書き可能ボリュームに変わります。SnapVault 関係を解除することはできません。

• 必要なもの *

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

手順

1. ボリューム / 健全性 * の詳細ページの * 保護 * タブで、解除する SnapMirror 関係をトポロジから選択します。
2. 目的地を右クリックして、メニューから * ブレーク * を選択します。

[関係の解除 (Break Relationship)] ダイアログボックスが表示されます。

3. 「 * Continue * 」をクリックして関係を解除します。
4. トポロジで、関係が解除されていることを確認します。

ボリューム / 健全性の詳細ページで保護関係を反転しています

災害によって保護関係のソースボリュームが機能しなくなった場合は、ソースの修理や交換を行う間、デスティネーションボリュームを読み書き可能に変換してデータの提供を継続することができます。ソースがデータを受信できる状態に戻ったら、逆再同期処理を使用して逆方向の関係を確立し、ソースのデータを読み書き可能なデスティネーションのデータと同期できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。
- SnapVault 関係は使用できません。
- 保護関係がすでに存在している必要があります。
- 保護関係が解除されている必要があります。
- ソースとデスティネーションの両方がオンラインになっている必要があります。
- ソースが別のデータ保護ボリュームのデスティネーションになっていることはできません。
- このタスクを実行すると、共通の Snapshot コピーのデータよりも新しいソースのデータは削除されます。
- 逆再同期した関係に対して作成されるポリシーとスケジュールは、元の保護関係と同じになります。

ポリシーとスケジュールが存在しない場合は作成されます。

手順

1. ボリューム / 健全性 * の詳細ページの * 保護 * タブで、トポロジからソースとデスティネーションを反転する SnapMirror 関係を探して右クリックします。
2. メニューから * 逆再同期 * を選択します。

逆再同期 (Reverse Resync) ダイアログボックスが表示されます。

3. 逆再同期を実行する関係が * 逆再同期 * (Reverse Resync *) ダイアログボックスに表示されていることを確認し、 * 送信 * (Submit *) をクリックします。

逆再同期（Reverse Resync）ダイアログボックスが閉じ、ボリューム / 健全性の詳細ページの上部にジョブのリンクが表示されます。

4. * オプション： * Volume/Health * details ページで * View Jobs * をクリックして、各逆再同期ジョブのステータスを追跡します。

フィルタリングされたジョブのリストが表示されます。

5. * オプション：ブラウザの * 戻る * 矢印をクリックして、 * 音量 / ヘルス * の詳細ページに戻ります。

すべてのタスクが正常に完了すれば逆再同期処理は終了です。

ボリューム / 健全性の詳細ページから保護関係を削除しています

保護関係を削除すると、選択したソースとデスティネーションの間の既存の関係を完全に削除することができます。これは、たとえば別のデスティネーションを使用して関係を作成する場合などに行います。この処理ではすべてのメタデータが削除され、元に戻すことはできません。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

手順

1. ボリューム / 健全性 * の詳細ページの * 保護 * タブで、削除する SnapMirror 関係をトポロジから選択します。
2. 目的地の名前を右クリックし、メニューから * 削除 * を選択します。

[関係の削除（Remove Relationship）] ダイアログボックスが表示されます。

3. [* 続行] をクリックして、関係を削除します。

関係がボリューム / 健全性の詳細ページから削除されます。

ボリューム / 健全性の詳細ページから保護関係を再同期しています

SnapMirror 関係や SnapVault 関係を解除してデスティネーションが読み書き可能になったあとに、ソースのデータとデスティネーションのデータが一致するようにデータを再同期することができます。再同期は、必要な共通の Snapshot コピーがソースボリュームで削除されたために SnapMirror や SnapVault の更新が失敗する場合にも実行することがあります。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- OnCommand Workflow Automation のセットアップが完了している必要があります。

手順

1. ボリューム / 健全性 * の詳細ページの * 保護 * タブで、再同期する保護関係をトポロジから探して右クリックします。
2. メニューから * Resynchronize * を選択します。

または、* Actions * メニューから * Relationship * > * Resynchronize * を選択して、現在詳細を表示している関係を再同期します。

再同期化ダイアログボックスが表示されます。

3. [* Resynchronization Options] * タブで、転送の優先順位と最大転送速度を選択します。
4. [* ソース Snapshot コピー *] をクリックし、[* Snapshot コピー *] 列で [* デフォルト *] をクリックします。

Select Source Snapshot Copy (ソース Snapshot コピーの選択) ダイアログボックスが表示されます。

5. デフォルトの Snapshot コピーを転送するのではなく、既存の Snapshot コピーを指定する場合は、* 既存の Snapshot コピー * をクリックし、リストから Snapshot コピーを選択します。
6. [Submit (送信)] をクリックします。

再同期ダイアログボックスに戻ります。

7. 再同期するソースを複数選択した場合は、既存の Snapshot コピーを指定する次のソースに対して * Default * をクリックします。
8. Submit * をクリックして、再同期ジョブを開始します。

再同期ジョブが開始されると、ボリューム / 健全性の詳細ページに戻り、ページの上部にジョブのリンクが表示されます。

9. * オプション: * Volume/Health details * ページで * View Jobs * をクリックして、各再同期ジョブのステータスを追跡します。

フィルタリングされたジョブのリストが表示されます。

10. * オプション: ブラウザの * 戻る * 矢印をクリックして、* 音量 / ヘルス * の詳細ページに戻ります。

すべてのタスクが正常に完了すれば再同期ジョブは終了です。

保護ジョブの失敗を解決する

このワークフローでは、Unified Manager のダッシュボードで保護ジョブの失敗を特定して解決する方法の例を示します。

• 必要なもの *

このワークフローの一部のタスクは管理者ロールでログインする必要があるため、さまざまな機能を使用するために必要なロールを把握しておく必要があります。

このシナリオでは、ダッシュボードページにアクセスして、保護ジョブに問題がないかどうかを確認します。保護インシデント領域には、ボリュームで保護ジョブの失敗エラーが表示され、ジョブ終了インシデントがあることがわかりました。このエラーを調査して、原因と潜在的な解決策を特定します。

手順

1. [未解決のインシデントとリスクのダッシュボード] 領域の [保護インシデント] パネルで、[保護ジョブの失敗 *] イベントをクリックします。



イベントのリンクされたテキストがフォームに書き込まれます

object_name:/object_name - Error Name`など

`cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed。

失敗した保護ジョブのイベントの詳細ページが表示されます。

2. 「概要」エリアの「原因」フィールドのエラーメッセージを確認して、問題を特定し、考えられる対処方法を評価します。

を参照してください "[保護ジョブが失敗した場合の問題の特定と対処策の実施](#)"。

保護ジョブが失敗した場合の問題の特定と対処策の実施

原因の詳細ページでジョブエラーのエラーメッセージを確認し、 Snapshot コピーのエラーが原因でジョブが失敗したことを確認します。次に、ボリューム / 健全性の詳細ページに移動して詳細情報を収集します。

- 必要なもの *

アプリケーション管理者のロールが必要です。

イベントの詳細ページの原因フィールドに表示されるエラーメッセージには、失敗したジョブに関する次のテキストが含まれています。

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

このメッセージには次の情報が表示されます。

- バックアップジョブまたはミラージョブが正常に完了しませんでした。

ジョブにソースボリューム間の保護関係が関係しています cluster2_src_vol2 仮想サーバ cluster2_src_svm デスティネーションボリュームを指定します managed_svc2_vol3 という名前の仮想サーバ上にある cluster3_dst_svm。

- に対する Snapshot コピージョブが失敗しました 0426cluster2_src_vol2snap ソースボリューム cluster2_src_svm:/cluster2_src_vol2。

このシナリオでは、ジョブが失敗した場合の原因と潜在的な対処策を特定できます。ただし、失敗を解決する

には、System Manager Web UI または ONTAP CLI コマンドを使用する必要があります。

手順

1. エラーメッセージを確認し、ソースボリュームで Snapshot コピージョブが失敗していることから、おそらくソースボリュームに問題があると判断します。

必要に応じて、エラーメッセージの最後にある * Job Details * リンクをクリックしてもかまいませんが、このシナリオでは、そのような操作を行わないように選択します。

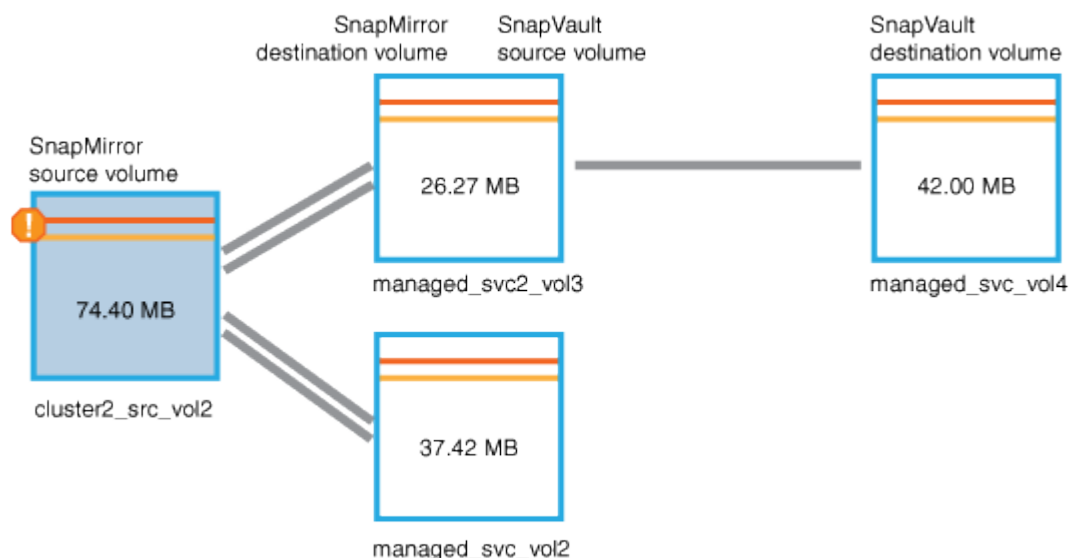
2. イベントを解決するために、次の作業を行います。
 - a. [* Assign to * (* への割り当て)] ボタンをクリックし、メニューから [* Me* (* Me *)] を選択します
 - b. [* Acknowledge * (確認)] ボタンをクリックして、イベントにアラートが設定されている場合は、繰り返しアラート通知を受信しないようにします。
 - c. 必要に応じて、イベントに関するメモを追加することもできます。
3. [Summary] * ペインで [Source] * フィールドをクリックして、ソース・ボリュームの詳細を表示します。

「* Source *」フィールドには、ソースオブジェクトの名前が表示されます。この場合は、Snapshot コピージョブがスケジュールされたボリュームが表示されます。

のボリューム/健全性の詳細ページが表示されます `cluster2_src_vol2` をクリックすると、Protectionタブの内容が表示されます。

4. 保護トポロジのグラフを見ると、トポロジ内の最初のボリューム（SnapMirror 関係のソースボリューム）に関連付けられているエラーアイコンが表示されます。

また、ソースボリュームアイコンに水平のバーが表示され、そのボリュームに設定されている警告とエラーのしきい値が表示されます。



5. エラーアイコンにカーソルを合わせると、ポップアップダイアログが開いてしきい値の設定が表示され、ボリュームがエラーしきい値を超えて容量の問題を示していることがわかります。
6. [容量 *] タブをクリックします。

ボリュームの容量情報 `cluster2_src_vol2` を表示します。

7. 容量 * パネルの棒グラフに、ボリュームの容量がボリュームに設定されたしきい値のレベルを超えたことを示すエラーアイコンが再び表示されます。
8. 容量グラフの下には、ボリュームの自動拡張が無効になっていることと、ボリュームのスペースギャランティが設定されていることが示されています。

自動拡張を有効にすることもできますが、このシナリオの目的上、さらに調査を進めてから、容量の問題を解決する方法を決定することになります。

9. 下にスクロールして「* Events」リストを表示し、「Protection Job Failed」、「Volume Days Until Full」、「Volume Space Full」の各イベントが生成されたことを確認します。
10. イベントのリストで、「* ボリュームスペースがフル *」イベントをクリックして詳細を確認します。このイベントは容量問題に最も関連しているように見えます。

イベントの詳細ページには、ソースボリュームで「ボリュームスペースがフル」イベントが表示されます。

11. [サマリー* (Summary *)] 領域で、イベントの[プロパティ (原因)] フィールドを確認します。The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.
12. サマリー領域の下に推奨される対処方法が表示されます。



Suggested Corrective Actions は一部のイベントについてのみ表示されるため、すべてのタイプのイベントについてこの領域が表示されるわけではありません。

「ボリュームスペースがフル」イベントを解決するために実施する推奨対処策をクリックしていきます。

- このボリュームで自動拡張を有効にします。
 - ボリュームのサイズを変更する。
 - このボリュームで重複排除を有効にして実行する。
 - このボリュームで圧縮を有効にして実行する。
13. ボリュームの自動拡張を有効にすることにしましたが、これを行うには、親アグリゲート上の使用可能な空きスペースと現在のボリューム増加率を確認する必要があります。
 - a. 親アグリゲートを確認します。`cluster2_src_aggr1`をクリックします。



アグリゲートの名前をクリックすると、アグリゲートに関する詳細を確認できます。

ボリュームに自動拡張を有効にするための十分なスペースがあることを確認します。

- b. ページの上部で、重要なインシデントを示すアイコンを確認し、アイコンの下のテキストを確認します。

「フルまでの日数：1 日未満 | 日次増加率：5.4%」と指定します。

14. System ManagerまたはONTAP CLIにアクセスしてを有効にします `volume autogrow` オプション



ボリュームとアグリゲートの名前をメモしておいて、自動拡張を有効にするときに参照できるようにします。

15. 容量問題を解決したら、Unified Manager のイベント * 詳細ページに戻り、イベントを解決済みとマークします。

遅延の問題を解決する

このワークフローでは、遅延問題を解決する方法の例を示します。このシナリオでは、管理者またはオペレータが Unified Manager のダッシュボードページにアクセスして、保護関係に問題がないかどうかを確認し、問題がある場合は解決策を探します。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

ダッシュボードページで、未解決のインシデントとリスク領域を確認し、保護ペインの保護リスクの下に SnapMirror 遅延エラーが表示されます。

手順

1. ダッシュボード * ページの * 保護 * ペインで、SnapMirror 関係の遅延エラーを探してクリックします。

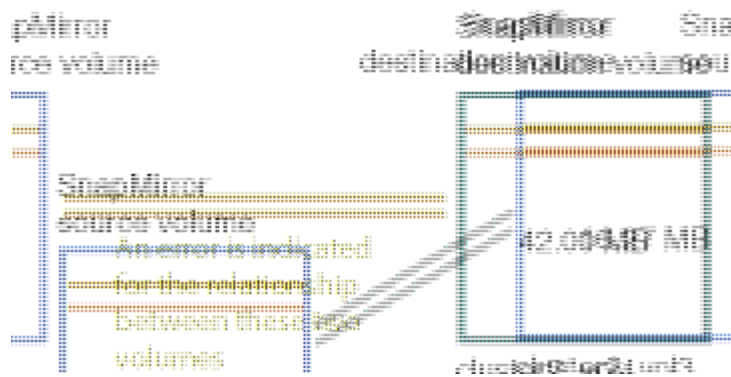
遅延エラーイベントのイベントの詳細ページが表示されます。

2. イベント * の詳細ページでは、次のタスクを 1 つ以上実行できます。
 - 概要領域の原因フィールドのエラーメッセージを確認して、推奨される対処方法があるかどうかを判断します。
 - ボリュームの詳細を確認するには、サマリー領域のソースフィールドでオブジェクト名（この場合はボリューム）をクリックします。
 - このイベントに関して追加されたメモを探します。
 - イベントにメモを追加します。
 - イベントを特定のユーザに割り当てます。
 - イベントに応答するか、またはイベントを解決します。
3. このシナリオでは、サマリー * 領域のソースフィールドでオブジェクト名（この場合はボリューム）をクリックすると、ボリュームの詳細が表示されます。

ボリューム / 健全性の詳細ページの保護タブが表示されます。

4. [* 保護 *] タブでは、トポロジ図を確認します。

3 つのボリュームで構成される SnapMirror カスケードの最後のボリュームで遅延エラーが発生していることがわかりました。選択したボリュームがダークグレーの線で囲まれます。ソースボリュームから延びるオレンジ色の二重線は、SnapMirror 関係のエラーを示しています。



5. SnapMirror カスケード内の各ボリュームをクリックします。

各ボリュームを選択すると、サマリ、トポロジ、履歴、イベント、関連デバイス、および関連するアラート領域が変更され、選択したボリュームに関連する詳細が表示されます。

6. サマリ * 領域を表示し、各ボリュームの * スケジュールの更新 * フィールドの情報アイコンにカーソルを合わせます。

このシナリオでは、SnapMirror ポリシーが DPDefault であり、SnapMirror スケジュールが毎時 5 分に更新されます。関係内のすべてのボリュームが同時に SnapMirror 転送を試行することがわかりました。

7. 遅延問題を解決するには、カスケードされたボリュームのうちの 2 つのスケジュールを変更して、ソースが転送を完了したあとにデスティネーションが SnapMirror 転送を開始するようにします。

保護関係を管理および監視する

Active IQ Unified Manager では、保護関係の作成、管理対象クラスタでの SnapMirror 関係と SnapVault 関係の監視とトラブルシューティング、および上書きされたデータや失われたデータのリストアを実行できます。

SnapMirror 処理には、2つのレプリケーションタイプがあります。

- 非同期

プライマリボリュームからセカンダリボリュームへのレプリケーションはスケジュールに従って実行されます。

- 同期

レプリケーションはプライマリボリュームとセカンダリボリュームで同時に実行されます。

保護ジョブは、パフォーマンスに影響を及ぼすことなく最大 10 件まで同時に実行できます。11~30 件のジョブを同時に実行すると、パフォーマンスが低下することがあります。30 を超えるジョブを同時に実行することは推奨されません。

ボリュームの保護ステータスを表示しています

データ保護ページには、単一クラスタまたはデータセンター内のすべてのクラスタで保護されているすべてのボリュームのデータ保護の詳細が全体的なビューで表示されま

す。

手順

1. 左側のナビゲーションペインで、* ダッシュボード * をクリックします。
2. すべての監視対象クラスタのデータ保護ステータスを表示するか、1つのクラスタのデータ保護ステータスを表示するかに応じて、* すべてのクラスタ * を選択するか、ドロップダウンメニューから1つのクラスタを選択します。
3. データ保護パネルの上部にある右矢印をクリックします。[データ保護]ページが表示されます。

データセンターで1つまたはすべてのクラスタを選択した場合は、SnapshotコピーまたはSnapMirrorポリシーで保護されているボリュームのデータ保護ステータスと、保護されていないボリュームの数が表示されます。

個々のクラスタリストからクラスタを選択すると、そのクラスタ内で保護されているボリュームのSnapshot保護とSnapMirror関係のステータスが表示されます。

このページでイベントをクリックすると、イベントの詳細ページが表示されます。[すべて表示 *] リンクをクリックすると、[イベント管理] イベントリページですべてのアクティブな保護イベントを表示できます。マウスのカーソルを合わせると、それぞれのカウントと凡例を表示できます。次のいずれかをクリックできます。

- 保護されていないボリュームとSnapshotコピーで保護されているボリュームの棒グラフ。ボリュームのページに移動して詳細を確認できます。
- すべての関係の棒グラフが関係ページに表示され、詳細はソースクラスタでフィルタリングされます。

Snapshotコピーで保護されているボリュームの保護ステータスを表示します


- Snapshotコピーの概要*：次のような、Snapshotコピーで保護されているボリュームの概要
- 保護されているが Snapshot コピーで保護されていないボリュームの総数。
- Snapshot コピーのリザーブスペースを使用中または超えているボリュームの合計数。
- Snapshot Copies Analysis * には、次の情報が含まれています。
- Snapshot コピーの個々のイベント。過去 24 時間に生成されたイベントも含まれます。
- 保護されているボリュームと Snapshot コピーで保護されていないボリュームの詳細チャート。
- ボリュームが、リザーブされている Snapshot コピー容量を使用、使用、および超えています。
- Snapshot コピー数に関するボリューム数の内訳。

Snapshotコピーについてはメモを指定します

- Snapshotコピーで保護されているボリュームの数をカウントする場合、ソースボリュームとデスティネーションボリュームの両方が考慮されます。
- 返される Snapshot コピーの数は、オンラインで使用可能なボリュームの数だけです。
- Snapshotコピー数のグラフの範囲は動的です。この値は、選択したクラスタに存在するSnapshotの数に基づいて生成されます。
- ボリュームを保護対象とする場合は、ボリュームの Snapshot コピーのスケジュールを有効にする必要があります。
- Snapshotコピーのリザーブスペースの値は、使用されているディスクスペースの量を確認したり、1つ以

上のSnapshotコピーを削除した場合に再利用可能なスペースを計算する場合に重要です。

SnapMirror関係の保護ステータスを表示します

- SnapMirror の概要 * : 次のような、 SnapMirror ポリシーで保護されているボリュームの概要。
- Volume SnapMirror 関係、 Storage VM ディザスタリカバリ (SVM-DR) 、およびその組み合わせなど、それぞれの SnapMirror ポリシーで保護されているボリュームの数。
- 遅延ステータスに基づいて、目標復旧時点 (RPO) の遅延が発生しているSnapMirror関係の総数。
- SnapMirror Analysis * には、次の情報が詳細に含まれています。
- SnapMirror 関係に対して発生した個々のイベント。過去 24 時間に発生したイベントも含まれます
- 各タイプのSnapMirrorポリシーで保護されているボリュームの数。
- 非同期ミラー、非同期バックアップ、非同期ミラーバックアップ、StricxtSync、SnapMirror Business Continuity (SMBC) 整合グループ、同期など、SnapMirror関係で保護される関係の数。
- 健全でない関係の数。
- ボリューム関係の数を表示します。グラフはRPOの遅延時間とステータスで切り替えることができます。
- 管理対象外の関係の遅延しきい値。設定アイコン () をクリックして、遅延しきい値を設定します。詳細については、[を参照してください "管理対象外の保護関係の遅延しきい値を設定しています"](#)。

SnapMirror関係については、メモを指定します

- SnapMirror関係のカウントでは、読み取りと書き込みが有効なソースボリュームがカウントされます。デスティネーションボリュームとルートボリュームは考慮されません。
- SnapMirror関係の場合、ソースクラスタのイベントが表示されます。
- SnapMirror関係の数には、ソースとデスティネーションが同じクラスタまたは異なるクラスタにあるボリュームの数が含まれます。
- データレプリケーションにおけるRPOの遅延時間は、SnapMirror関係に基づいています。ステータスは次のように分類されます ok、`warning`または`error`を選択します。ステータスを確認して、パラメータが想定どおりに機能しているかどうか、または問題 に対処する必要があるかどうかを判断できます。
- ボリュームに複数のSnapMirror関係がある場合、RPO遅延には各関係タイプがカウントされます。
- ソースとデスティネーションの間でデータレプリケーションに問題がある場合、たとえば関係が解除されたときなど、ボリューム関係は正常な状態でないとみなされます。

MetroCluster 構成で保護されているクラスタを表示します

[データ保護]ページの[* MetroCluster Protection]パネルには、MetroCluster over FCまたはIP構成で保護または保護されていないクラスタの数が表示されます。このパネルの棒グラフをクリックすると、クラスタページが開き、保護されているクラスタまたは保護されていないクラスタに基づいてクラスタの詳細がフィルタリングされます。MetroCluster 設定の監視については、[を参照してください "MetroCluster 構成を監視しています"](#)。

ボリュームの保護関係を表示しています

Relationship : All Relationships ビューと Volume Relationships ページで、既存のボリュームの SnapMirror 関係と SnapVault 関係のステータスを確認できます。転送と遅延の

ステータス、ソースとデスティネーションの詳細、スケジュールとポリシーの情報など、保護関係の詳細も確認できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

このページから、関係に関するコマンドを開始することもできます。

手順

1. 左側のナビゲーションペインで、*** Storage *** > *** Volumes *** をクリックします。
2. [表示] メニューから、[*** 関係 ***] > [*** すべての関係 ***] を選択します。

[関係：すべての関係] ビューが表示されます。

3. 次のいずれかの方法を選択してボリュームの保護の詳細を表示します。

- すべてのボリューム関係に関する現在の情報を表示するには、デフォルトの *** すべての関係 *** ページのままにします。
- 一定期間のボリューム転送の傾向に関する詳細情報を表示するには、表示メニューで、関係：過去 1 カ月の転送ステータスビューを選択します。
- ボリューム転送アクティビティに関する詳細情報を 1 日単位で表示するには、表示メニューで、関係：過去 1 カ月の転送速度ビューを選択します。



ボリューム転送のビューには、非同期関係にあるボリュームの情報のみが表示されます。同期関係にあるボリュームは表示されません。

コンシステンシグループ関係の **LUN** を監視しています

ONTAP 環境で、LUN を使用してアプリケーションを保護するために SnapMirror のビジネス継続性（SM-BC）がサポートされている場合は、Active IQ Unified Manager でそれらの LUN を表示および監視できます。

SM-BC は、SAN 環境でのフェイルオーバー時に Recovery Time Objective（RTO；目標復旧時間）をゼロにします。SM-BC をサポートする一般的な環境では、ボリューム上の LUN は整合グループ関係で保護されます。

これらのプライマリ LUN とセカンダリ LUN は、複合 LUN か、同じ UUID とシリアル番号を持つレプリカ LUN ペアです。I/O 処理（読み取りと書き込みの両方）がこれらの複合 LUN 上のソースサイトとデスティネーションサイト間で多重化されるため、透明性が確保されます。

複数の LUN を表示する場合は、整合グループ関係の一部である LUN を含むプライマリクラスタとセカンダリクラスタの両方を Unified Manager で追加して検出する必要があります。iSCSI LUN と FCP LUN のみがサポートされます。

SM-BC の詳細については、を参照してください ["SM-BC に関する ONTAP 9 のマニュアル"](#)。

環境内のコンポジット LUN を表示するには、次の手順を実行します。

手順

1. 左側のナビゲーションペインで、* Storage * > * LUNs * をクリックします。
2. [表示] メニューから、[* 関係 > すべての LUN*] を選択します。

Relationship : All LUNs ビューが表示されています。

LUN の名前、ボリューム、LUN をホストしている Storage VM、クラスタ、整合グループ、パートナー LUN など、LUN の詳細を確認できます。これらの各コンポーネントをクリックすると、詳細ビューにドリルダウンできます。コンシステンシ・グループをクリックすると [関係] ページが表示されます

パートナー LUN をクリックすると、そのパートナー LUN がホストされている Storage VM の Storage VM の詳細ページの SAN タブで設定の詳細を確認できます。パートナー LUN のイニシエータやイニシエータグループなどの情報が表示されます。

環境内の保護対象 LUN のレポートをソート、フィルタ、生成、およびアップロードするための、グリッドレベルの標準機能を実行できます。

「健全性：すべてのボリューム」ビューで **SnapVault** 保護関係を作成します

健全性：すべてのボリュームビューを使用して、同じ Storage VM 上の 1 つ以上のボリュームの SnapVault 関係を作成し、データを保護するためのデータバックアップを有効にすることができます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

次の場合、* Protect * メニューは表示されません。

- RBAC の設定で休止操作が許可されていない場合：オペレータの権限しかない場合など
- ボリューム ID が不明な場合：クラスタ間関係が確立されているがデスティネーションクラスタが検出されていない場合など

手順

1. 左側のナビゲーションペインで、* Storage * > * Volumes * をクリックします。
2. [* 正常性：すべてのボリューム *] ビューで、保護するボリュームを選択し、[* 保護] をクリックします。

または、同じ Storage Virtual Machine (SVM) 上に複数の保護関係を作成するには、Health : All Volumes ビューで 1 つ以上のボリュームを選択し、ツールバーの * Protect * をクリックします。

3. メニューから * SnapVault * を選択します。

Configure Protection (保護の設定) ダイアログボックスが開きます。

4. SnapVault * をクリックして、* SnapVault * タブを表示し、セカンダリ・ボリューム情報を設定します。
5. [* 詳細設定 *] をクリックして、必要に応じて重複排除、圧縮、自動拡張、およびスペースギャランティを設定し、[* 適用 *] をクリックします。

6. [* SnapVault *（接続先情報）] タブの [* 接続先情報 *] 領域と [* 関係設定 *] 領域に入力します。

7. [適用（Apply）] をクリックします。

Health : All Volumes ビューに戻ります。

8. 「* Health : All Volumes」ビューの上部にある保護設定ジョブのリンクをクリックします。

保護関係を1つだけ作成する場合は、ジョブの詳細ページが表示されます。ただし、複数の保護関係を作成する場合は、保護処理に関連付けられているすべてのジョブのフィルタされたリストが表示されます。

9. 次のいずれかを実行します。

- ジョブが1つしかない場合は、[* 更新 *] をクリックして、保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認します。
- ジョブが複数ある場合は、次の手順を実行します。
 - i. ジョブリストでジョブをクリックします。
 - ii. 保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認するには、[* Refresh] をクリックします。
 - iii. フィルタリングされたリストに戻り、別のジョブを表示するには、「* 戻る」ボタンを使用します。

ボリューム / 健全性の詳細ページから **SnapVault** 保護関係を作成しています

ボリュームでデータバックアップを有効にして保護するために、ボリューム / 健全性の詳細ページを使用して SnapVault 関係を作成することができます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- このタスクを実行するには、Workflow Automation をセットアップしておく必要があります。

次の場合、* Protect * メニューは表示されません。

- RBAC の設定で休止操作が許可されていない場合：オペレータの権限しかない場合など
- ボリューム ID が不明な場合：クラスター間関係が確立されているがデスティネーションクラスターが検出されていない場合など

手順

1. [* Volume/Health*（ボリューム / ヘルス * の詳細）] ページの [* 保護] タブで、保護するボリュームをトポロジビューで右クリックします。
2. メニューから * Protect * > * SnapVault * を選択します。

Configure Protection（保護の設定）ダイアログボックスが開きます。

3. SnapVault * をクリックして、* SnapVault * タブを表示し、セカンダリ・リソース情報を設定します。

4. [* 詳細設定 *] をクリックして、必要に応じて重複排除、圧縮、自動拡張、およびスペースギャランティを設定し、[* 適用 *] をクリックします。

5. [保護の設定 *] ダイアログボックスの [接続先情報 *] 領域と [関係設定 *] 領域に入力します。

6. [適用 (Apply)] をクリックします。

ボリューム / 健全性の詳細ページに戻ります。

7. 「 * Volume/Health * details 」 ページの上部にある保護設定ジョブのリンクをクリックします。

ジョブの詳細ページが表示されます。

8. 保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認するには、[* Refresh] をクリックします。

ジョブのタスクが完了すると、新しい関係がボリューム / 健全性の詳細ページのトポロジビューに表示されます。

ケンセンセイ：スヘテノホリユウムヒユウカラノ **SnapMirror** ホコカンケイノサクセイ

Health：All Volumes ビューでは、同じ Storage VM 上にある複数のボリュームを選択して、複数の SnapMirror 保護関係を一度に作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

次の場合、* Protect * メニューは表示されません。

- RBAC の設定で休止操作が許可されていない場合：オペレータの権限しかない場合など
- ボリューム ID が不明な場合：クラスタ間関係が確立されているがデスティネーションクラスタが検出されていない場合など

手順

1. [* 正常性：すべてのボリューム *] ビューで、保護するボリュームを選択します。

または、同じ SVM 上に複数の保護関係を作成するには、Health：All Volumes ビューで 1 つ以上のボリュームを選択し、ツールバーの * Protect * > * SnapMirror * をクリックします。

Configure Protection（保護の設定）ダイアログボックスが表示されます。

2. 「 * SnapMirror * 」 をクリックして、「 * SnapMirror * 」 タブを表示し、デスティネーション情報を設定します。

3. 必要に応じて「 * 詳細設定 * 」 をクリックしてスペースギャランティを設定し、「 * 適用 * 」 をクリックします。

4. [* SnapMirror *] タブの [* デスティネーション情報 *] 領域と [* 関係設定 *] 領域に入力します。

5. [適用 (Apply)] をクリックします。

Health：All Volumes ビューに戻ります。

6. 「* Health : All Volumes」ビューの上部にある保護設定ジョブのリンクをクリックします。

保護関係を 1 つだけ作成する場合は、ジョブの詳細ページが表示されます。ただし、複数の保護関係を作成する場合は、保護処理に関連付けられているすべてのジョブのリストが表示されます。

7. 次のいずれかを実行します。

- ジョブが 1 つしかない場合は、[* 更新 *] をクリックして、保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認します。
- ジョブが複数ある場合は、次の手順を実行します。
 - i. ジョブリストでジョブをクリックします。
 - ii. 保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認するには、[* Refresh] をクリックします。
 - iii. フィルタリングされたリストに戻り、別のジョブを表示するには、「* 戻る」ボタンを使用します。

設定で指定したデスティネーション SVM と詳細設定で有効にしたオプションに応じて、次のいずれかの SnapMirror 関係が作成されます。

- ソースボリュームと同じかそれよりも新しいバージョンの ONTAP で実行されているデスティネーション SVM を指定した場合、デフォルトではブロックレプリケーションベースの SnapMirror 関係が作成されます。
- ソースボリュームと同じかそれよりも新しいバージョンの ONTAP で実行されているデスティネーション SVM を指定し、詳細設定でバージョンに依存しないレプリケーションを有効にした場合、バージョンに依存しないレプリケーションを使用した SnapMirror 関係が作成されます。
- ソースボリュームよりも前のバージョンの ONTAP で実行されているデスティネーション SVM を指定した場合、以前のバージョンでバージョンに依存しないレプリケーションがサポートされていれば、バージョンに依存しないレプリケーションを使用した SnapMirror 関係が自動的に作成されます。

ボリューム / 健全性の詳細ページから **SnapMirror** 保護関係を作成しています

データレプリケーションを有効にしてデータを保護するために、ボリューム / 健全性の詳細ページを使用して SnapMirror 関係を作成することができます。SnapMirror レプリケーションを使用すると、ソースでデータ損失が発生した場合にデスティネーションボリュームからデータをリストアできます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

次の場合、* Protect * メニューは表示されません。

- RBAC の設定で休止操作が許可されていない場合：オペレータの権限しかない場合など
- ボリューム ID が不明な場合：クラスタ間関係が確立されているがデスティネーションクラスタが検出されていない場合など

保護ジョブは、パフォーマンスに影響を及ぼすことなく最大 10 件まで同時に実行できます。11~30 件のジョブを同時に実行すると、パフォーマンスが低下することがあります。30 を超えるジョブを同時に実行するこ

とは推奨されません。

手順

1. [* Volume/Health * (ボリューム / ヘルス * の詳細)] ページの [* 保護] タブ * で、保護するボリュームの名前をトポロジビューで右クリックします。
2. メニューから * Protect * > * SnapMirror * を選択します。

Configure Protection (保護の設定) ダイアログボックスが表示されます。

3. 「 * SnapMirror * 」をクリックして、「 * SnapMirror * 」タブを表示し、デスティネーション情報を設定します。
4. 必要に応じて「 * 詳細設定 * 」をクリックしてスペースギャランティを設定し、「 * 適用 * 」をクリックします。
5. [保護の設定 *] ダイアログボックスの [接続先情報 *] 領域と [関係設定 *] 領域に入力します。
6. [適用 (Apply)] をクリックします。

ボリューム / 健全性の詳細ページに戻ります。

7. 「 * Volume/Health * details 」 ページの上部にある保護設定ジョブのリンクをクリックします。

ジョブのタスクと詳細がジョブの詳細ページに表示されます。

8. [* ジョブ * の詳細] ページで、[* 更新 *] をクリックして、保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認します。
9. ジョブのタスクが完了したら、ブラウザの * 戻る * をクリックして * 音量 / ヘルス * の詳細ページに戻ります。

新しい関係がボリューム / 健全性の詳細ページのトポロジビューに表示されます。

設定で指定したデスティネーション SVM と詳細設定で有効にしたオプションに応じて、次のいずれかの SnapMirror 関係が作成されます。

- ソースボリュームと同じかそれよりも新しいバージョンの ONTAP で実行されているデスティネーション SVM を指定した場合、デフォルトではブロックレプリケーションベースの SnapMirror 関係が作成されます。
- ソースボリュームと同じかそれよりも新しいバージョンの ONTAP で実行されているデスティネーション SVM を指定し、詳細設定でバージョンに依存しないレプリケーションを有効にした場合、バージョンに依存しないレプリケーションを使用した SnapMirror 関係が作成されます。
- ONTAP の以前のバージョン、またはソースボリュームよりも新しいバージョンで実行されているデスティネーション SVM を指定した場合、以前のバージョンではバージョンに依存しないレプリケーションがサポートされていれば、バージョンに依存しないレプリケーションを使用した SnapMirror 関係が自動で作成されます。

バージョンに依存しないレプリケーションを使用して **SnapMirror** 関係を作成する

バージョンに依存しないレプリケーションを使用して SnapMirror 関係を作成できます。バージョンに依存しないレプリケーションを使用すると、ソースボリュームとデスティネーションボリュームが異なるバージョンの ONTAP で実行されている場合でも、

SnapMirror 保護を実装できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。
- ソースとデスティネーションの SVM でそれぞれ、SnapMirror ライセンスが有効になっている必要があります。
- ソースとデスティネーションの SVM がそれぞれ、バージョンに依存しないレプリケーションをサポートするバージョンの ONTAP ソフトウェアで実行されている必要があります。

バージョンに依存しないレプリケーションを使用する SnapMirror では、すべてのストレージが 1 つのバージョンの ONTAP で実行されていない異機種混在ストレージ環境でも SnapMirror 保護を実装できます。ただし、バージョンに依存しないレプリケーションを使用する SnapMirror で実行されるミラー処理は、従来のブロックレプリケーションによる SnapMirror で実行されるミラー処理ほど高速ではありません。

手順

1. 保護するボリュームの * 保護の設定 * ダイアログボックスを表示します。
 - ボリューム / 健全性の詳細ページの保護タブを表示している場合は、保護するボリュームの名前を含むトポロジビューを右クリックし、メニューから * 保護 * > * SnapMirror * を選択します。
 - Health : All Volumes (すべてのボリューム) ビューを表示している場合は、保護するボリュームを探して右クリックし、メニューから * Protect * > * SnapMirror * * を選択します。Configure Protection (保護の設定) ダイアログボックスが表示されます。
2. 「* SnapMirror *」をクリックして、「* SnapMirror *」タブを表示します。
3. [保護の設定 *] ダイアログボックスの [接続先情報 *] 領域と [関係設定 *] 領域に入力します。

保護するソースボリュームよりも前のバージョンの ONTAP で実行されるデスティネーション SVM を指定し、その前のバージョンでバージョンに依存しないレプリケーションがサポートされる場合は、SnapMirror にバージョンに依存しないレプリケーションが自動的に設定されます。

4. ソースボリュームと同じバージョンの ONTAP で実行されているデスティネーション SVM を指定し、バージョンに依存しないレプリケーションで SnapMirror を設定する場合は、* アドバンスド * をクリックしてバージョンに依存しないレプリケーションを有効にし、* 適用 * をクリックします。
5. [適用 (Apply)] をクリックします。

ボリューム / 健全性の詳細ページに戻ります。

6. 「* Volume/Health * details」ページの上部にある保護設定ジョブのリンクをクリックします。

ジョブのタスクと詳細がジョブの詳細ページに表示されます。

7. [* ジョブ * の詳細] ページで、[* 更新 *] をクリックして、保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認します。
8. ジョブのタスクが完了したら、ブラウザの * 戻る * をクリックして * 音量 / ヘルス * の詳細ページに戻ります。

新しい関係がボリューム / 健全性の詳細ページのトポロジビューに表示されます。

バージョンに依存しないレプリケーションとバックアップオプションを使用した SnapMirror 関係の作成

バージョンに依存しないレプリケーションとバックアップオプション機能を使用して SnapMirror 関係を作成できます。バックアップオプション機能を使用すると、SnapMirror 保護を実装できます。また、デスティネーションの場所でバックアップコピーの複数のバージョンを保持することもできます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。
- ソースとデスティネーションの SVM でそれぞれ、SnapMirror ライセンスが有効になっている必要があります。
- ソースとデスティネーションの SVM でそれぞれ、SnapVault ライセンスが有効になっている必要があります。
- ソースとデスティネーションの SVM がそれぞれ、バージョンに依存しないレプリケーションをサポートするバージョンの ONTAP ソフトウェアで実行されている必要があります。

SnapMirror にバックアップオプション機能を設定すると、ボリュームのフェイルオーバー機能などの SnapMirror ディザスタリカバリ機能を使用してデータを保護できるだけでなく、複数のバックアップコピーによる保護などの SnapVault 機能を利用できます。

手順

1. 保護するボリュームの * 保護の設定 * ダイアログボックスを表示します。
 - ボリューム / 健全性の詳細ページの保護タブを表示している場合は、トポロジビューで保護するボリュームの名前を右クリックし、メニューから * Protect * > * SnapMirror * を選択します。
 - Health : All Volumes (すべてのボリューム) ビューを表示している場合は、保護するボリュームを探して右クリックし、メニューから * Protect * > * SnapMirror * を選択します。Configure Protection (保護の設定) ダイアログボックスが表示されます。
2. 「* SnapMirror *」をクリックして、「* SnapMirror *」タブを表示します。
3. [保護の設定 *] ダイアログボックスの [接続先情報 *] 領域と [関係設定 *] 領域に入力します。
4. 「* 詳細設定 *」をクリックして、「* 詳細設定 *」ダイアログボックスを表示します。
5. バージョンに依存しないレプリケーション * チェックボックスがまだ選択されていない場合は、ここで選択します。
6. バックアップオプション機能を有効にするには、* バックアップオプション * 付きチェックボックスを選択し、* 適用 * をクリックします。
7. [適用 (Apply)] をクリックします。

ボリューム / 健全性の詳細ページに戻ります。

8. 「* Volume/Health * details」ページの上にある保護設定ジョブのリンクをクリックします。

ジョブのタスクと詳細がジョブの詳細ページに表示されます。

9. [* ジョブ * の詳細] ページで、[* 更新 *] をクリックして、保護設定ジョブに関連するタスクリストとタ

スクの詳細を更新し、ジョブが完了したかどうかを確認します。

10. ジョブのタスクが完了したら、ブラウザの * 戻る * をクリックして * 音量 / ヘルス * の詳細ページに戻ります。

新しい関係がボリューム / 健全性の詳細ページのトポロジビューに表示されます。

デスティネーションの効率化設定を行います

デスティネーションの詳細設定ダイアログボックスを使用して、保護デスティネーションの重複排除、圧縮、自動拡張、スペースギャランティなどの効率化設定を行うことができます。デスティネーションまたはセカンダリボリュームでスペースの利用率を最大限に高める場合にこれらの設定を使用します。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

デフォルトでは、効率化設定はソースボリュームの設定に対応します。ただし、SnapVault 関係の圧縮設定は例外で、この設定はデフォルトで無効になっています。

手順

1. 構成する関係のタイプに応じて、[保護の構成 *] ダイアログボックスの [* SnapMirror *] タブまたは [* SnapVault *] タブをクリックします。
2. [* Destination Information* (目的地情報 *)] 領域で [* Advanced* (詳細設定 *)] [拡張宛先設定] ダイアログボックスが開きます。
3. 必要に応じて、重複排除、圧縮、自動拡張、およびスペースギャランティの効率化設定を有効または無効にします。
4. [* 適用 * (Apply *)] をクリックして選択内容を保存し、[* 保護の設定 * (Configure Protection *)] ダイアログボックスに戻ります。

SnapMirror スケジュールと SnapVault スケジュールを作成

SnapMirror および SnapVault の基本または詳細スケジュールを作成して、ソースボリュームまたはプライマリボリュームで自動データ保護転送を有効にすることができます。ボリュームでのデータ変更の頻度に応じて、転送の実行頻度を調整することができます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- [保護の設定] ダイアログボックスの [宛先情報] 領域に、すでに入力されている必要があります。
- このタスクを実行するには、Workflow Automation をセットアップしておく必要があります。

手順

1. [保護の設定] ダイアログ・ボックスの [* SnapMirror *] タブまたは [* SnapVault *] タブで、[* 関係設定

] 領域の [スケジュールの作成] リンクをクリックします。

Create Schedule (スケジュールの作成) ダイアログボックスが表示されます。

2. [* スケジュール名*] フィールドに、スケジュールに付ける名前を入力します。

3. 次のいずれかを選択します。

- * 基本 *

間隔で指定する基本的なスケジュールを作成する場合に選択します。

- * 詳細 *

cron 形式のスケジュールを作成する場合に選択します。

4. [作成 (Create)] をクリックします。

新しいスケジュールは、SnapMirror Schedule または SnapVault Schedule ドロップダウンリストに表示されます。

カスケード関係またはファンアウト関係を作成して、既存の保護関係から保護を拡張します

既存の関係のソースボリュームからのファンアウトまたはデスティネーションボリュームからのカスケードを作成することで、既存の関係から保護を拡張できます。この処理は、1つのサイトから複数のサイトにデータをコピーする必要がある場合や、バックアップをさらに作成して追加の保護を提供する必要がある場合に実行します。

複数のボリュームを保持するコンテナである整合グループを使用してボリュームの保護を拡張することで、すべてのボリュームを1つのエンティティとして管理できます。SnapMirror のビジネス継続性 (SM-BC) 整合グループと同期整合性グループの関係は、Unified Manager の関係のページで確認できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

手順

1. [* 保護 >]、[関係*] の順にクリックします。または、ボリュームの詳細ページで関係を確認します。
2. * Volume Relationships * ページで、保護の拡張元の SnapMirror 関係を選択します。
3. アクションバーで、* 保護の拡張 * をクリックします。
4. メニューで、ソースからファンアウト関係を作成するか、デスティネーションからカスケード関係を作成するかに応じて、ソースから * を選択するか、デスティネーションから * を選択します。
5. 作成する保護関係のタイプに応じて、「* with SnapMirror *」または「* with SnapVault *」のいずれかを選択します。

[保護の設定* (Configure Protection*)] ダイアログボックスが表示されます。



これは、一元化された関係 / ボリューム関係とボリューム / 健全性の詳細ページから実行できます。

6. [保護の設定 *] ダイアログボックスに示されている情報を入力します。

ボリューム関係ページで保護関係を編集する

既存の保護関係を編集して、最大転送速度、保護ポリシー、保護スケジュールを変更することができます。関係の編集は、転送に使用する帯域幅を制限したり、データが頻繁に変更されるためにスケジュールされた転送の実行頻度を増やす場合などに行います。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

保護関係のデスティネーションであるボリュームを選択する必要があります。ソースボリューム、負荷共有ボリューム、または SnapMirror 関係や SnapVault 関係のデスティネーションでないボリュームが選択されている場合、関係を編集することはできません。

手順

1. ボリューム関係 * ページで、関係設定を編集する同じ SVM 内の 1 つ以上のボリュームのリストからボリュームを選択し、ツールバーから * 編集 * を選択します。

[関係の編集 (Edit Relationship)] ダイアログボックスが表示されます。

2. [関係の編集 *] ダイアログボックスで、必要に応じて最大転送速度、保護ポリシー、または保護スケジュールを編集します。
3. [適用 (Apply)] をクリックします。

選択した関係に変更が適用されます。

ボリューム / 健全性の詳細ページで保護関係を編集しています

既存の保護関係を編集して、現在の最大転送速度、保護ポリシー、保護スケジュールを変更することができます。関係の編集は、転送に使用する帯域幅を制限したり、データが頻繁に変更されるためにスケジュールされた転送の実行頻度を増やす場合などに行います。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のインストールと設定が完了している必要があります。

保護関係のデスティネーションであるボリュームを選択する必要があります。ソースボリューム、負荷共有ボリューム、または SnapMirror 関係や SnapVault 関係のデスティネーションでないボリュームが選択されている場合、関係を編集することはできません。

手順

1. ボリューム / 健全性 * の詳細ページの * 保護 * タブで、編集する保護関係をトポロジから探して右クリックします。
2. メニューから「* 編集 *」を選択します。

または、[* アクション * (* Actions *)]メニューから[* 関係 * (Relationship *)]>[* 編集 * (* Edit *)]を選択して、現在詳細を表示している関係を編集します。

[関係の編集 * (Edit Relationship *)] ダイアログボックスが表示されます。

3. 関係の編集ダイアログボックスで、最大転送速度、保護ポリシー、または保護スケジュールを必要に応じて編集します。
4. [適用 (Apply)] をクリックします。

選択した関係に変更が適用されます。

転送効率を最大化するために、**SnapMirror** ポリシーを作成します

SnapMirror ポリシーを作成して、保護関係における SnapMirror 転送の優先順位を指定することができます。SnapMirror ポリシーで優先度を割り当てて、優先度が低い転送を通常の優先度の転送よりもあとに実行するようにスケジュールすることで、ソースからデスティネーションへの転送効率を最大化できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。
- このタスクでは、[保護の設定] ダイアログボックスの [宛先情報] 領域がすでに完了していることを前提としています。

手順

1. Configure Protection * (保護の設定) ダイアログボックスの * SnapMirror * タブで、* Relationship Settings * (関係設定 *) 領域の * Create Policy * (ポリシーの作成) リンクをクリックします。

SnapMirror ポリシーの作成ダイアログボックスが表示されます。

2. [* ポリシー名 *] フィールドに、ポリシーに付ける名前を入力します。
3. [* 転送優先度 *] フィールドで、ポリシーに割り当てる転送優先度を選択します。
4. [* コメント * (* Comment *)] フィールドに、ポリシーのオプションのコメントを入力します。
5. [作成 (Create)] をクリックします。

新しいポリシーが SnapMirror ポリシーのドロップダウンリストに表示されます。

転送効率を最大化するための **SnapVault** ポリシーを作成する

新しい SnapVault ポリシーを作成して SnapVault 転送の優先度を設定できます。ポリシーを使用することで、保護関係におけるプライマリからセカンダリへの転送効率を最大

化できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。
- [保護の設定] ダイアログボックスの [接続先情報] 領域が既に完了している必要があります。

手順

1. [保護の設定 *] ダイアログボックスの [SnapVault ポリシーの作成 *] タブで、[関係設定 *] 領域の [ポリシーの作成 *] リンクをクリックします。

SnapVault タブが表示されます。

2. [* ポリシー名 *] フィールドに、ポリシーに付ける名前を入力します。
3. [* 転送優先度 *] フィールドで、ポリシーに割り当てる転送優先度を選択します。
4. * オプション： * [* コメント * (* Comment *)] フィールドに、ポリシーのコメントを入力します。
5. レプリケーションラベル * 領域で、必要に応じてレプリケーションラベルを追加または編集します。
6. [作成 (Create)] をクリックします。

新しいポリシーが [Create Policy] ドロップダウンリストに表示されます。

ボリューム関係ページからのアクティブなデータ保護転送を中止します

実行中の SnapMirror レプリケーションを中止する場合、アクティブなデータ保護転送を中止することができます。ベースライン転送後の以降の転送については、再開チェックポイントを消去することもできます。転送を中止する状況としては、ボリューム移動などの別の処理と競合する場合などがあります。



整合性グループによって保護されているボリューム関係は中止できません。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

中止処理は、次の場合は表示されません。

- RBAC の設定で休止操作が許可されていない場合：オペレータの権限しかない場合など
- ボリューム ID が不明な場合：クラスター間関係が確立されているがデスティネーションクラスターが検出されていない場合など

ベースライン転送の再開チェックポイントは消去できません。

手順

1. 1 つ以上の保護関係の転送を中止するには、* ボリューム関係 * ページで 1 つ以上のボリュームを選択

し、ツールバーで * 中止 * をクリックします。

転送の中止ダイアログボックスが表示されます。

2. ベースライン転送以外の転送の再開チェックポイントをクリアする場合は、「* チェックポイントのクリア *」を選択します。
3. [* Continue (続行)] をクリックします

転送の中止ダイアログボックスが閉じ、ボリューム関係ページの上部に中止ジョブのステータスとジョブの詳細へのリンクが表示されます。

4. * オプション: * View details * リンクをクリックして、* Job * details ページで詳細を確認し、ジョブの進捗状況を確認します。

ボリューム / 健全性の詳細ページからアクティブなデータ保護転送を中止します

実行中の SnapMirror レプリケーションを中止する場合、アクティブなデータ保護転送を中止することができます。ベースライン転送以外の転送の再開チェックポイントを消去することもできます。転送を中止する状況としては、ボリューム移動などの別の処理と競合する場合などがあります。



整合性グループによって保護されているボリューム関係は中止できません。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

中止処理は、次の場合は表示されません。

- RBAC の設定で休止操作が許可されていない場合：オペレータの権限しかない場合など
- ボリューム ID が不明な場合：クラスタ間関係が確立されているがデスティネーションクラスタが検出されていない場合など

ベースライン転送の再開チェックポイントは消去できません。

手順

1. [* Volume/Health *] の詳細ページの [* Protection *] タブで、中止するデータ転送のトポロジビューで関係を右クリックし、[* Abort *] を選択します。

転送の中止ダイアログボックスが表示されます。

2. ベースライン転送以外の転送の再開チェックポイントをクリアする場合は、「* チェックポイントのクリア *」を選択します。
3. [* Continue (続行)] をクリックします

転送の中止ダイアログボックスが閉じ、ボリューム / 健全性の詳細ページの上部に中止処理のステータスとジョブの詳細へのリンクが表示されます。

4. * オプション： * View details * リンクをクリックして、 * Job * details ページで詳細を確認し、ジョブの進捗状況を確認します。
5. 各ジョブタスクをクリックすると、その詳細が表示されます。
6. ブラウザの戻る矢印をクリックして、 * 音量 / ヘルス * の詳細ページに戻ります。

すべてのタスクが正常に完了すれば中止処理は終了です。

ボリューム関係ページで保護関係を休止しています

ボリューム関係ページでは、保護関係を休止してデータ転送を一時的に停止できます。関係の休止は、データベースを含む SnapMirror デスティネーションボリュームの Snapshot コピーを作成する場合に、Snapshot コピーの処理中にデータベースコンテンツの安定を確保する目的で行うことがあります。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

次の場合は休止操作が表示されません。

- RBAC の設定で休止操作が許可されていない場合：オペレータの権限しかない場合など
- ボリューム ID が不明な場合：クラスタ間関係が確立されているがデスティネーションクラスタが検出されていない場合など
- Workflow Automation と Unified Manager を連携させていない場合

手順

1. 1 つ以上の保護関係の転送を休止するには、 * ボリューム関係 * ページで 1 つ以上のボリュームを選択し、ツールバーで * 休止 * をクリックします。

休止（Quiesce）ダイアログボックスが表示されます。

2. [* Continue（続行）] をクリックします

休止ジョブのステータスは、ボリューム / 健全性の詳細ページの上部にジョブの詳細へのリンクとともに表示されます。

3. [* 詳細の表示 *] リンクをクリックして、[* ジョブ * 詳細] ページに移動し、詳細とジョブの進捗状況を確認します。
4. * オプション：ブラウザの * 戻る * 矢印をクリックして、 * ボリューム関係 * ページに戻ります。

すべてのジョブタスクが正常に完了すれば休止ジョブは終了です。

ボリューム / 健全性の詳細ページで保護関係を休止しています

保護関係を休止してデータ転送を一時的に停止できます。関係の休止は、データベースを含む SnapMirror デスティネーションボリュームの Snapshot コピーを作成する場合

に、Snapshot コピーの実行中にデータベースコンテンツの安定を確保する目的で行うことがあります。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

次の場合は休止操作が表示されません。

- RBAC の設定で許可されていない場合：オペレータの権限しかない場合など
- ボリューム ID が不明な場合：クラスタ間関係が確立されているがデスティネーションクラスタが検出されていない場合など
- Workflow Automation と Unified Manager を連携させていない場合

手順

1. ボリューム / 健全性 * の詳細ページの * 保護 * タブで、休止する保護関係のトポロジビューで関係を右クリックします。
2. メニューから「* 休止」を選択します。
3. 続行するには、[はい] をクリックします。

休止ジョブのステータスは、ボリューム / 健全性の詳細ページの上部にジョブの詳細へのリンクとともに表示されます。

4. [* 詳細の表示 *] リンクをクリックして、[* ジョブ * 詳細] ページに移動し、詳細とジョブの進捗状況を確認します。
5. * オプション：ブラウザの [戻る] 矢印をクリックして、* Volume/Health * の詳細ページに戻ります。

すべてのジョブタスクが正常に完了すれば休止ジョブは終了です。

ボリューム関係ページから **SnapMirror** 関係を解除します

保護関係を解除して、SnapMirror 関係にあるソースボリュームとデスティネーションボリュームの間のデータ転送を停止することができます。関係の解除は、データを移行する場合、ディザスタリカバリやアプリケーションのテストなどの目的で行うことがあります。デスティネーションボリュームは読み書き可能ボリュームに変わります。SnapVault 関係を解除することはできません。


- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

手順

1. [* ボリューム関係 *] ページで、データ転送を停止する保護関係のある 1 つ以上のボリュームを選択し、ツールバーの [* 解除 *] をクリックします。

[関係の解除 (Break Relationship)] ダイアログボックスが表示されます。

2. 「 * Continue * 」をクリックして関係を解除します。
3. ボリューム関係 * ページで、 * 関係状態 * 列に関係が解除されていることを確認します。

デフォルトでは、[関係の状態 (Relationship State)] 列は非表示になっているため、[列の表示 / 非表示 (Show/Hide Column)] リストで選択する必要がある場合があります .

ボリューム関係ページから保護関係を削除します

ボリューム関係ページでは、保護関係を削除して、選択したソースとデスティネーションの間の既存の関係を完全に削除できます。たとえば、別のデスティネーションを使用して関係を作成する場合などです。この処理ではすべてのメタデータが削除され、元に戻すことはできません。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

手順

1. [* ボリューム関係 * (* Volume Relationships *)] ページで、保護関係を削除する 1 つ以上のボリュームを選択し、ツールバーで [* 削除 * (* Remove *)] をクリックします。

[関係の削除 (Remove Relationship)] ダイアログボックスが表示されます。

2. [* 続行] をクリックして、関係を削除します。

関係がボリューム関係ページから削除されます。

休止中の関係のスケジュールされた転送をボリューム関係ページで再開しています

関係を休止してスケジュールされた転送の実行を停止したあと、 * Resume * を使用してスケジュールされた転送を再度有効にし、ソースボリュームまたはプライマリボリュームのデータを保護することができます。スケジュールされた次の転送時に、チェックポイントが存在する場合は、チェックポイントから転送が再開されます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

転送を再開する休止中の関係を 10 個まで選択できます。

手順

1. Volume * Relationships * (ボリューム * 関係 *) ページで、関係が休止されているボリュームを 1 つ以上選択し、ツールバーで * Resume * (続行) をクリックします。
2. [* Resume * (続行)] ダイアログボックスで、[* Continue * (続行)] をクリックします。

ボリューム関係のページに戻ります。

3. 関連するジョブタスクを表示してその進捗状況を追跡するには、* ボリューム関係 * ページの上部に表示されるジョブのリンクをクリックします。
4. 次のいずれかを実行します。
 - ジョブが 1 つだけ表示されている場合は、ジョブの詳細ページで「* 更新 *」をクリックして、保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認します。
 - 複数のジョブが表示される場合は、
 - i. [ジョブ] ページで、詳細を表示するジョブをクリックします。
 - ii. [ジョブの詳細] ページで、[*Refresh] をクリックして、保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認します。ジョブが完了すると、次のスケジュールされた転送の実行時にデータ転送が再開されます。

休止中の関係のスケジュールされた転送をボリューム / 健全性の詳細ページで再開します

関係を休止してスケジュールされた転送の実行を停止したあと、ボリューム / 健全性の詳細ページで * Resume * を使用してスケジュールされた転送を再び有効にし、ソースボリュームまたはプライマリボリュームのデータを保護します。スケジュールされた次の転送時に、チェックポイントが存在する場合は、チェックポイントから転送が再開されます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

手順

1. ボリューム / 健全性 * の詳細ページの * 保護 * タブで、トポロジビューを右クリックして再開する休止中の関係を選択します。

または、* Actions * > * Relationship * メニューから * Resume * を選択します。

2. [* Resume * (続行)] ダイアログボックスで、[* Continue * (続行)] をクリックします。

ボリューム / 健全性の詳細ページに戻ります。

3. 関連するジョブタスクを表示してその進捗状況を追跡するには、* Volume/Health * の詳細ページの上部に表示されるジョブのリンクをクリックします。
4. [* ジョブ * の詳細] ページで、[* 更新 *] をクリックして、保護設定ジョブに関連するタスクリストとタスクの詳細を更新し、ジョブが完了したかどうかを確認します。

ジョブが完了すると、次のスケジュールされた転送の実行時にデータ転送が再開されます。

ボリューム関係ページから保護関係を初期化または更新しています

ボリューム関係ページでは、新しい保護関係で最初のベースライン転送を実行できます。また、すでに初期化された関係でスケジュールされていない増分更新を手動で実行してすぐに転送する場合は、関係を更新できます。



整合グループで保護されているボリュームは初期化または更新できません。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- OnCommand Workflow Automation のセットアップが完了している必要があります。

手順

1. [* ボリューム関係 *] ページでボリュームを右クリックし、更新または初期化する関係を持つ 1 つ以上のボリュームを選択して、ツールバーの [* 初期化 / 更新 *] をクリックします。

[Initialize] / [Update] * ダイアログボックスが表示されます。

2. 転送オプション * タブで、転送の優先順位と最大転送速度を選択します。
3. [* ソース Snapshot コピー *] をクリックし、[* Snapshot コピー *] 列で [* デフォルト *] をクリックします。

Select Source Snapshot Copy (ソース Snapshot コピーの選択) ダイアログボックスが表示されます。

4. デフォルトの Snapshot コピーを転送するのではなく、既存の Snapshot コピーを指定する場合は、* 既存の Snapshot コピー * をクリックし、リストから Snapshot コピーを選択します。
5. [Submit (送信)] をクリックします。

[Initialize] / [Update] * ダイアログボックスに戻ります。

6. 初期化または更新するソースを複数選択した場合は、既存の Snapshot コピーを指定する次のソースに対して「 * Default * 」をクリックします。
7. [Submit] をクリックして、初期化ジョブまたは更新ジョブを開始します。

初期化ジョブまたは更新ジョブが開始されると、ボリューム関係ページに戻り、ページの上部にジョブのリンクが表示されます。

8. * オプション： * ヘルス：すべてのボリューム * ビューで * ジョブを表示 * クリックすると、各初期化ジョブまたは更新ジョブのステータスが追跡されます。

フィルタリングされたジョブのリストが表示されます。

9. * オプション： * 各ジョブをクリックすると詳細が表示されます。
10. * オプション：ブラウザの * 戻る * 矢印をクリックして、* ボリューム関係 * ページに戻ります。

すべてのタスクが正常に終了すれば初期化処理または更新処理は終了です。

ボリューム / 健全性の詳細ページから保護関係を初期化または更新しています

新しい保護関係で最初のベースライン転送を実行できます。また、すでに初期化された関係でスケジュールされていない増分更新を手動で実行してデータをただちに転送する場合は、関係を更新できます。

- 注：コンシステンシ・グループで保護されているボリュームは ' 初期化または更新できません
- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- OnCommand Workflow Automation のセットアップが完了している必要があります。

手順

1. ボリューム / 健全性 * の詳細ページの * 保護 * タブで、初期化または更新する保護関係をトポロジから探して右クリックします。
2. メニューから [Initialize] / [Update] を選択します。

または、* アクション * メニューから * 関係 * > * 初期化 / 更新 * を選択して、現在詳細を表示している関係を初期化または更新します。

Initialing/Update ダイアログボックスが表示されます。

3. 転送オプション * タブで、転送の優先順位と最大転送速度を選択します。
4. [* ソース Snapshot コピー *] をクリックし、[* Snapshot コピー *] 列で [* デフォルト *] をクリックします。

Select Source Snapshot Copy (ソース Snapshot コピーの選択) ダイアログボックスが表示されます。

5. デフォルトの Snapshot コピーを転送するのではなく、既存の Snapshot コピーを指定する場合は、* 既存の Snapshot コピー * をクリックし、リストから Snapshot コピーを選択します。
6. [Submit (送信)] をクリックします。

Initialing/Update ダイアログボックスに戻ります。

7. 複数のソースを選択して初期化または更新する場合は、既存の Snapshot コピーを指定する次の読み取り / 書き込みソースに対して「* Default 」をクリックします。

データ保護ボリュームには別の Snapshot コピーを選択できません。

8. [Submit] をクリックして、初期化ジョブまたは更新ジョブを開始します。

初期化ジョブまたは更新ジョブが開始されると、ボリューム / 健全性の詳細ページに戻り、ページの上部にジョブのリンクが表示されます。

9. * オプション：* Volume/Health * の詳細ページで * View Jobs * をクリックして、各初期化ジョブまたは更新ジョブのステータスを追跡します。

フィルタリングされたジョブのリストが表示されます。

10. * オプション：* 各ジョブをクリックすると詳細が表示されます。

11. * オプション：ブラウザの [戻る] 矢印をクリックして、* Volume/Health * の詳細ページに戻ります。

すべてのタスクが正常に完了すれば初期化处理または更新処理は終了です。

ボリューム関係ページから保護関係を再同期しています

ボリューム関係ページで関係を再同期することができます。これは、ソースボリュームを機能しないイベントからリカバリする場合や、現在のソースを別のボリュームに変更する場合に行います。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。

手順

1. ボリュームの関係 * ページで、関係が休止中のボリュームを 1 つ以上選択し、ツールバーの * 再同期 * をクリックします。

再同期化ダイアログボックスが表示されます。

2. [* Resynchronization Options] * タブで、転送の優先順位と最大転送速度を選択します。
3. [* ソース Snapshot コピー *] をクリックし、[* Snapshot コピー *] 列で [* デフォルト *] をクリックします。

Select Source Snapshot Copy（ソース Snapshot コピーの選択）ダイアログボックスが表示されます。

4. デフォルトの Snapshot コピーを転送するのではなく、既存の Snapshot コピーを指定する場合は、* 既存の Snapshot コピー * をクリックし、リストから Snapshot コピーを選択します。
5. [Submit（送信）] をクリックします。

再同期ダイアログボックスに戻ります。

6. 再同期するソースを複数選択した場合は、既存の Snapshot コピーを指定する次のソースに対して * Default * をクリックします。
7. Submit * をクリックして、再同期ジョブを開始します。

再同期ジョブが開始されると、ボリューム関係ページに戻り、ページの上部にジョブのリンクが表示されます。

8. * オプション：* Volume Relationships * ページで * View Jobs * をクリックして、各再同期ジョブのステータスを追跡します。

フィルタリングされたジョブのリストが表示されます。

9. * オプション：ブラウザの * 戻る * 矢印をクリックして、* ボリューム関係 * ページに戻ります。

すべてのタスクが正常に終了すれば再同期処理は終了です。

ボリューム関係ページで保護関係を反転しています

災害によって保護関係のソースボリュームが機能しなくなった場合は、ソースの修理や交換を行う間、デスティネーションボリュームを読み書き可能ボリュームに変換してデータの提供を継続することができます。ソースがデータを受信できる状態に戻ったら、逆再同期処理を使用して逆方向の関係を確立し、ソースのデータを読み書き可能なデスティネーションのデータと同期できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automation のセットアップが完了している必要があります。
- SnapVault 関係は使用できません。
- 保護関係がすでに存在している必要があります。
- 保護関係が解除されている必要があります。
- ソースとデスティネーションの両方がオンラインになっている必要があります。
- ソースが別のデータ保護ボリュームのデスティネーションになっていることはできません。
- このタスクを実行すると、共通の Snapshot コピーのデータよりも新しいソースのデータは削除されます。
- 逆再同期した関係に対して作成されるポリシーとスケジュールは、元の保護関係と同じになります。

ポリシーとスケジュールが存在しない場合は作成されます。

手順

1. [* ボリューム関係 * (* Volume Relationships *)] ページで、反転する関係を持つ 1 つ以上のボリュームを選択し、ツールバーで [* 逆再同期 * (* Reverse Resync *)] をクリックします。

逆再同期 (Reverse Resync) ダイアログボックスが表示されます。

2. 逆再同期を実行する関係が * 逆再同期 * (Reverse Resync *) ダイアログボックスに表示されていることを確認し、 * 送信 * (Submit *) をクリックします。

逆再同期処理が開始されると、ボリューム関係ページに戻り、ページの上部にジョブのリンクが表示されます。

3. * オプション : * Volume Relationships * ページで * View Jobs * をクリックして、各逆再同期ジョブのステータスを追跡します。

この処理に関連するジョブがフィルタリングされて表示されます。

4. * オプション : ブラウザの * 戻る * 矢印をクリックして、 * ボリューム関係 * ページに戻ります。

すべてのタスクが正常に完了すれば逆再同期処理は終了です。

ボリュームおよびボリューム/健全性の詳細ページを使用したデータのリストア

ボリュームとボリューム/健全性の詳細ページでリストア機能を使用することで、上書きまたは削除したファイルやディレクトリ、またはボリューム全体をSnapshotコピーからリストアすることができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。



次の点に注意してください。

- NTFS ファイルストリームはリストアできません。
- リストアオプションは、次の場合は使用できません。
 - ボリューム ID が不明な場合：クラスタ間関係が確立されているがデスティネーションクラスタが検出されていない場合など。
 - ボリュームが SnapMirror 同期レプリケーションの対象に設定されている場合。

手順

1. 左側のナビゲーションペインで、* Storage > Volumes *の順に選択します。
2. ボリュームを選択し、* Restore （復元） ボタンをクリックします。または、ボリュームをクリックして、Volume/Health details > Actions > Restore *に移動します。[復元] ダイアログボックスが表示されます。このページの詳細については、を参照してください "[リストアダイアログボックス](#)"。
3. デフォルトの設定と異なる場合は、データをリストアするボリュームと Snapshot コピーを選択します。
4. ソースLUNなど、リストアする項目を選択します。

ボリューム全体をリストアすることも、リストアするフォルダやファイルを指定することもできます。

5. 選択したアイテムを復元する場所を選択します。* 元の場所 * または * 代替の既存の場所 * のいずれかを選択します。
6. 別の既存の場所を選択した場合は、次のいずれかを実行します。
 - [リストアパス] テキストフィールドに、データを復元する場所のパスを入力し、[* ディレクトリの選択 *] をクリックします。
 - **[Browse]** をクリックして [Browse Directories] ダイアログボックスを起動し、次の手順を実行します。
 - i. リストア先のデスティネーションクラスタ、Storage VM (SVM) 、およびボリュームを選択します。
 - ii. 名前(Name)テーブルで'リストアする必要のあるディレクトリ名'を選択します
 - iii. [* ディレクトリの選択 *] をクリックします。
7. [* リストア] をクリックします。

リストアプロセスが開始されます。リストアプロセスを完了するためにバックエンドでジョブが作成されます。

8. ジョブの進捗状況を表示するには、左側のナビゲーションペインで* Protection > Jobs *と進み、リストア
・ジョブのステータスをジョブのリストから確認します。



Cloud Volumes ONTAP HA クラスタ間のリストア処理が NDMP のエラーで失敗する場合は、ソースシステムのクラスタ管理 LIF と通信できるように、デスティネーションクラスタで明示的な AWS ルートを追加しなければならないことがあります。この設定手順は、BlueXPを使用して実行します。

リソースプールとは

リソースプールは、Unified Manager を使用してストレージ管理者が作成するアグリゲートのグループであり、バックアップ管理用のパートナーアプリケーションにプロビジョニングを提供します。

リソースは、パフォーマンス、コスト、物理的な場所、可用性などの属性に基づいてプールにまとめることができます。関連するリソースをプールにグループ化すると、監視とプロビジョニングでそのプールを 1 つのユニットとして扱うことができます。これにより、リソースの管理が簡易化され、柔軟かつ効率的にストレージを使用できるようになります。

Unified Manager では、セカンダリストレージのプロビジョニングの際に、リソースプールから保護に最適なアグリゲートが次の基準で選択されます。

- ・アグリゲートはデータアグリゲート（ルートアグリゲートではない）で、オンラインになっています。
- ・ONTAP のバージョンがソースクラスタのメジャーバージョンと同じかそれ以上であるデスティネーションクラスタノード上にアグリゲートがあります。
- ・リソースプール内のすべてのアグリゲートのうち、使用可能なスペースが最も大きいアグリゲートを使用しています。
- ・デスティネーションボリュームのプロビジョニング後、アグリゲートのスペースがアグリゲートに対して定義された「ほぼフル」および「ほぼオーバーコミット」のしきい値（グローバルまたはローカルのしきい値、該当する場合）内に収まっていることを確認します。
- ・デスティネーションノードの FlexVol ボリュームの数がプラットフォームの制限を超えないようにする必要があります。

リソースプールを作成しています

[Create Resource Pool] ダイアログボックスを使用すると、プロビジョニングのためにアグリゲートをグループ化できます。

- ・必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

リソースプールには異なるクラスタのアグリゲートを含めることができますが、同じアグリゲートが異なるリソースプールに属することはできません。

1. 左側のナビゲーションペインで、* 保護 * > * リソースプール * をクリックします。

2. [* リソースプール] ページで、[* 作成] をクリックします。
3. Create Resource Pool * ダイアログボックスの手順に従って、名前と概要を指定し、作成するリソースプールにメンバーとしてアグリゲートを追加します。

リソースプールを編集しています

リソースプールの名前や概要を変更する場合は、既存のリソースプールを編集することができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

- Edit * ボタンは、1つのリソースプールが選択されている場合にのみ有効になります。複数のリソースプールが選択されている場合、* Edit * ボタンは無効になります。

手順

1. 左側のナビゲーションペインで、* 保護 * > * リソースプール * をクリックします。
2. リストから1つのリソースプールを選択します。
3. [編集 (Edit)] をクリックします。

[Edit Resource Pool] ウィンドウが表示されます。

4. 必要に応じて、リソースプール名と概要を編集します。
5. [保存 (Save)] をクリックします。

リソースプールのリストに新しい名前と概要が表示されます。

リソースプールインベントリの表示

リソースプールページを使用して、リソースプールのインベントリを表示したり、各リソースプールの残りの容量を監視したりできます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

ステップ

1. 左側のナビゲーションペインで、* 保護 * > * リソースプール * をクリックします。

リソースプールのインベントリが表示されます。

リソースプールのメンバーを追加しています

リソースプールは、複数のメンバーアグリゲートで構成されます。既存のリソースプールにアグリゲートを追加して、セカンダリボリュームのプロビジョニングに使用できる

スペースを増やすことができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

リソースプールに一度に追加できるアグリゲートの数は 200 個までです。アグリゲートダイアログボックスに表示されるアグリゲートは他のリソースプールに属していません。

手順

1. 左側のナビゲーションペインで、* 保護 * > * リソースプール * をクリックします。
2. リソースプール * リストからリソースプールを選択します。

リソースプールのリストの下領域に、リソースプールのメンバーが表示されます。

3. リソースプールのメンバー領域で、* 追加 * をクリックします。

アグリゲートダイアログボックスが表示されます。

4. 1 つ以上のアグリゲートを選択します。
5. [追加 (Add)] をクリックします。

ダイアログボックスが閉じ、選択したリソースプールのメンバーのリストにアグリゲートが表示されます。

リソースプールからアグリゲートを削除しています

アグリゲートを他の目的に使用したい場合などに、既存のリソースプールからアグリゲートを削除することができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

リソースプールのメンバーは、リソースプールが選択されている場合にのみ表示されます。

手順

1. 左側のナビゲーションペインで、* 保護 * > * リソースプール * をクリックします。
2. メンバーアグリゲートを削除するリソースプールを選択します。

メンバーアグリゲートのリストがメンバーペインに表示されます。

3. 1 つ以上のアグリゲートを選択します。

「* 削除」ボタンが有効になっています。

4. [削除] をクリックします。 *

警告のダイアログボックスが表示されます。

5. 続行するには、[はい] をクリックします。

選択したアグリゲートがメンバーペインから削除されます。

リソースプールを削除しています

不要になったリソースプールを削除できます。たとえば、1 つのリソースプールから他の複数のリソースプールにメンバーアグリゲートを再配分したあと、元のリソースプールを廃止状態にすることができます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

[削除 *] ボタンは、少なくとも 1 つのリソースプールが選択されている場合にのみ有効になります。

手順

1. 左側のナビゲーションペインで、* 保護 * > * リソースプール * をクリックします。
2. 削除するリソースプールを選択します。
3. [削除 (Delete)] をクリックします。

リソースプールがリソースプールのリストから削除され、そのアグリゲートがメンバーのリストから削除されます。

Storage VM ディザスタリカバリ保護関係を監視しています

Active IQ Unified Manager では、Storage VM ディザスタリカバリ関係の監視がサポートされており、ディザスタリカバリは Storage VM レベルできめ細かく実行できます。Storage VM ディザスタリカバリを使用すると、Storage VM のコンスティチュエントボリュームに存在するデータをリカバリしたり、Storage VM の設定をリカバリしたりできます。

非同期のディザスタリカバリを実現するために、ソース Storage VM からデスティネーション Storage VM への Storage VM DR 関係が作成されます。クラスタのセットアップに基づいて、データボリュームと一緒に Storage VM の設定をすべてレプリケートするか一部だけ（ネットワークとプロトコルの設定を除く）レプリケートするかを選択できます。

Storage VM ディザスタリカバリ関係の設定後、ハードウェア障害や環境障害が原因でソース Storage VM が使用できなくなったときに、デスティネーション Storage VM が起動し、最小限のシステム停止でデータへのアクセスが提供されます。同様に、ソース Storage VM が使用可能になると、デスティネーション Storage VM と再同期され、ソースからデータの提供が再開されます。SnapMirror コマンドを使用して、Storage VM ディザスタリカバリ関係を設定および管理できます。

カンケイヘエシヨウシヨウシタ **Storage VM** ノカンシ

Storage VM ディザスタリカバリ関係は、インベントリの保護セクションにある関係ページで監視できます。デフォルトでは、関係ページには、コンスティチュエント関係のフ

フィルタが適用されたときの最上位の関係だけが表示されます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

フィルタを使用して Storage VM ディザスタリカバリ関係を表示します。

手順

1. 左側のナビゲーションペインで、 * protection * > * Relationships * （保護 * > * 関係 * ）をクリックします。

ボリューム、整合性グループ、Storage VM 関係のすべてのタイプの関係が表示されます。

2. フィルタ * をクリックし、* 関係オブジェクトタイプ * および * Storage VM * を選択して、Storage VM のディザスタリカバリ関係のみを表示します。
3. [フィルタを適用（Apply Filter）] をクリックする。



保護関係をすべて表示するには、コンスチチュエント関係のフィルタをクリアする必要があります。

Storage VM ディザスタリカバリ関係のみが表示されます。

Storage VM ページで保護関係を表示します

Storage VMS ページを使用して、既存の Storage VM の災害復旧関係のステータスを表示できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

転送と遅延のステータス、ソース、デスティネーションの詳細など、保護関係の詳細も確認できます。レポートのスケジュールを設定したり、必要な形式で既存のレポートをダウンロードしたりできます。[* 表示 / 非表示 * （Show/Hide * ）] ボタンを使用すると、デフォルトでは表示されないように、必要な列をレポートに追加できます。

手順

1. 左側のナビゲーションペインで、 * storage * > * Storage VM * をクリックします。
2. * VIEW * メニューから * Relationship * > * All Relationships * を選択します。

設定されているすべての Storage VM について、「関係：すべての関係」ビューが表示されます。

保護ステータスに基づいた **Storage VM** の表示

インベントリの Storage VM ページを使用して Active IQ Unified Manager 内のすべての Storage VM を表示し、保護ステータスに基づいて Storage VM をフィルタリングできます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

Storage VM ビューに Protection Role という新しい列が追加され、Storage VM が保護されているか保護されていないかを示す情報が表示されます。



ソースクラスタが Active IQ Unified Manager に追加されていない場合、そのクラスタに関連するすべての情報がグリッドで使用できなくなります。

手順

1. 左側のナビゲーションペインで、* storage * > * Storage VM* をクリックします。
2. view * メニューから * Health * > * All Storage VM* を選択します。

Health : All Storage VM が表示されます。

3. 「* Filter *」をクリックして、次のいずれかの Storage VM を表示します。

をクリックしてください	フィルタ値
• 保護された Storage VM*	• 保護役割 * は保護されています *
• 保護されていない Storage VM *	• 保護ロール * は保護されていません *



保護されている Storage VM と保護されていない Storage VM の両方を同時に表示することはできません。新しいフィルタオプションを再適用するには、既存のフィルタをクリアする必要があります。

4. [フィルタを適用 (Apply Filter)] をクリックする。

保存されていないビューには、選択したフィルタに基づいて、Storage VM ディザスタリカバリで保護されているか保護されていないすべての Storage VM が表示されます。

Storage VMの関連付けの概要

Storage Virtual Machine (Storage VM) の関連付けは、ソースStorage VMからデスティネーションStorage VMへのマッピングであり、リソースの選択やセカンダリボリュームのプロビジョニングのためにパートナーアプリケーションで使用されます。

デスティネーションStorage VMがセカンダリデスティネーションか3次デスティネーションかに関係なく、ソースStorage VMとデスティネーションStorage VMの間で関連付けが作成されます。セカンダリデスティネーションStorage VMをソースとして使用して、3番目のデスティネーションStorage VMとの関連付けを作成することはできません。

アプリケーション管理者またはストレージ管理者は、環境内のStorage VMの関連付けを* Protection > Storage VM Associations *ページで確認できます。

SVMを関連付ける方法は3つあります。

- 任意の**Storage VM**に関連付け：任意のプライマリソースStorage VMと1つ以上のデスティネーションSVMの間に関連付けを作成できます。つまり、現時点で保護を必要とする既存のすべてのSVMおよび今後作成されるすべてのSVMが指定したデスティネーションSVMに関連付けられます。たとえば、異なる場所にある複数のソースのアプリケーションを1箇所にある1つ以上のデスティネーションSVMにバックアップできます。
- 特定の**Storage VM**に関連付け：特定のソースStorage VMと1つ以上の特定のデスティネーションSVMの間に関連付けを作成できます。たとえば、データを互いに分離する必要がある多数のクライアントにストレージサービスを提供する場合は、このオプションを選択して、特定のソース Storage VM を、対象のクライアントにのみ割り当てられる特定のデスティネーション Storage VM に関連付けることができます。
- 外部**Storage VM**と関連付け：ソースStorage VMとデスティネーションStorage VMの外部のフレキシブルボリュームとの間に関連付けを作成できます。

Storage VMの関連付けを作成します

Create Storage Virtual Machine Associationsウィザードでは、パートナーの保護アプリケーションを使用して、ソースStorage VMをデスティネーションStorage VMに関連付けて、SnapMirror関係とSnapVault 関係で 사용할 수 있습니다。パートナーアプリケーションでは、デスティネーションボリュームの最初のプロビジョニングの際にこれらの関連付けを使用して、.ddを選択するリソースを特定します

- 必要なもの *
- 関連付ける Storage VM がすでに存在している必要があります。
- アプリケーション管理者またはストレージ管理者のロールが必要です。

すべてのソース Storage VM と関係タイプについて、各デスティネーションクラスターでデスティネーション Storage VM を 1 つだけ選択できます。

削除機能と作成機能を使用した関連付けの変更は、以降のプロビジョニング処理にのみ反映されます。既存のデスティネーションボリュームは移動されません。

手順

1. 左側のナビゲーションペインで、* Protection > Storage VM Associations *をクリックします。
2. [* Storage VM Associations]ページで、[* Create]をクリックします。

Create Storage Virtual Machine Associations *ウィザードが起動します。

3. 次のいずれかのソースを選択します。

◦ * 任意 *

任意のプライマリ Storage VM ソースと 1 つ以上のデスティネーション Storage VM の間に関連付けを作成する場合に、このオプションを選択します。つまり、現時点で保護を必要とする既存のすべての Storage VM と、以降に作成されるすべての Storage VM が、指定したデスティネーション Storage VM に関連付けられます。たとえば、異なる場所にある複数のソースのアプリケーションを 1 箇所にある 1 つ以上のデスティネーション Storage VM にバックアップできます。

◦ * シングル *

1 つ以上のデスティネーション Storage VM に関連付けられている特定のソース Storage VM を選択する場合に、このオプションを選択します。たとえば、データを互いに分離する必要がある多数のクライアントにストレージサービスを提供する場合は、このオプションを選択して、特定の Storage VM ソースを、対象のクライアントにのみ割り当てられる特定の Storage VM デスティネーションに関連

付けます。

- * なし (外部) *

ソース Storage VM とデスティネーション Storage VM の外部のフレキシブルボリュームの間で関連付けを作成する場合に、このオプションを選択します。

4. 作成する保護関係タイプとして、次のいずれかまたは両方を選択します。

- * SnapMirror *
- * SnapVault *

5. 「* 次へ *」をクリックします。

6. Storage VM 保護デスティネーションを 1 つ以上選択してください。

7. [完了] をクリックします。

Storage VMの関連付けを削除します

パートナーアプリケーションに対するStorage VMの関連付けを削除して、ソースとデスティネーションのStorage VM間のセカンダリプロビジョニング関係を削除することができます。この処理は、たとえば、デスティネーションStorage VMがいっぱいになり、Storage VMの保護の関連付けを新たに作成する場合などに行います。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

Delete *ボタンは、Storage VMとの関連付けが少なくとも1つ選択されるまで無効になります。関連付けの削除と追加による変更は、以降のプロビジョニング処理にのみ反映されます。既存のデスティネーションボリュームが移動されることはありません。

手順

1. 左側のナビゲーションペインで、* Protection > Storage VM Associations *をクリックします。
2. Storage VMの関連付けを少なくとも1つ選択してください。
 - Delete * (削除) ボタンが有効になっています。
3. [削除] をクリックします。 *

警告のダイアログボックスが表示されます。

4. 続行するには、[はい] をクリックします。

選択したStorage VMの関連付けがリストから削除されます。

ストレージサービスをサポートするための SVM とリソースプールの要件

ストレージサービスに固有の SVM の関連付けやリソースプールの要件を確認する場合は、パートナーアプリケーションへの準拠を適切に確保することができます。たとえば、SVM を関連付けて Unified Manager でリソースプールを作成すると、パートナーアプリケーションから提供されるストレージサービスの保護トポロジがサポートされま

す。

一部のアプリケーションは、Unified Manager サーバと連携し、ソースボリュームとセカンダリストレージまたは 3 番目のストレージにある保護ボリュームとの間で SnapMirror または SnapVault によるバックアップ保護を自動的に設定して実行するサービスを提供します。このような保護ストレージサービスをサポートするには、Unified Manager を使用して、必要な SVM の関連付けとリソースプールを設定する必要があります。

ストレージサービスのシングルホップ保護またはカスケード保護をサポートするため、SnapMirror ソースまたは SnapVault プライマリボリュームから、セカンダリまたは 3 番目の場所にあるデスティネーション SnapMirror または SnapVault バックアップボリュームへのレプリケーションを含むには、次の要件を確認してください。

- SnapMirror ソースまたは SnapVault プライマリボリュームを含む SVM と、セカンダリボリュームまたは 3 番目のボリュームが配置されている SVM の間で SVM の関連付けが設定されている必要があります。
 - たとえば、ソースボリューム Vol_A が SVM_1 に配置されている保護トポロジで SnapMirror セカンダリデスティネーションボリューム Vol_B が SVM_2 に配置されている場合は、3 番目の SnapVault バックアップボリューム Vol_C は SVM_3 に配置されています。SVM_1 と SVM_2 の間の SnapMirror の関連付けと、SVM_1 と SVM_3 の間の SnapVault バックアップの関連付けを設定するには、Unified Manager Web UI を使用する必要があります。
- この例では、SVM_2 と SVM_3 の間の SnapMirror の関連付けまたは SnapVault バックアップの関連付けは不要なため、使用されません。
- ソースボリューム Vol_A と SnapMirror デスティネーションボリューム Vol_B の両方が SVM_1 に配置されている保護トポロジをサポートするには、SVM_1 と SVM_1 の間に SnapMirror の関連付けを設定する必要があります。
- リソースプールには、関連付けられた SVM で使用可能なクラスタのアグリゲートリソースが含まれている必要があります。

Unified Manager Web UI でリソースプールを設定し、パートナーアプリケーションを使用してストレージサービスのセカンダリターゲットノードと 3 番目のターゲットノードを割り当てます。

ジョブとは

ジョブは、Unified Manager を使用して監視できる一連のタスクです。ジョブとその関連タスクを表示すると、それらが正常に完了したかどうかを確認できます。

SnapMirror 関係と SnapVault 関係の作成時、関係の操作（解除、編集、休止、削除、再開、再同期、逆再同期）、データのリストアタスクを実行したとき、クラスタにログインしたときなど。

ジョブを開始すると、ジョブページおよびジョブの詳細ページを使用して、ジョブおよび関連するジョブタスクの進捗状況を監視できます。

ジョブの監視

ジョブページでは、ジョブステータスを監視したり、ストレージサービスのタイプ、状態、送信日時、完了日時などのジョブプロパティを表示したりして、ジョブが正常に完了したかどうかを判断できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* 保護 * > * ジョブ * をクリックします。

Jobs ページが表示されます。

2. 現在実行中のジョブのステータスを確認するには、* State * 列を表示します。
3. 特定のジョブの詳細を表示するには、そのジョブ名をクリックします。

ジョブの詳細ページが表示されます。

ジョブの詳細を表示します

ジョブを開始したら、ジョブの詳細ページでその進捗状況を追跡し、関連タスクにエラーの可能性がないかどうかを監視できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* 保護 * > * ジョブ * をクリックします。
2. [ジョブ] ページで、[名前] 列のジョブ名をクリックして、ジョブに関連するタスクのリストを表示します。
3. タスクをクリックすると、タスクの詳細 * ペインとタスクリストの右側にある * タスクメッセージ * ペインに追加情報が表示されます。

ジョブを中止しています

[ジョブ] ページを使用して、ジョブの終了に時間がかかりすぎている場合、多数のエラーが発生している場合、または不要になった場合にジョブを中止できます。中止できるのは、ジョブの中止がステータスとタイプで許可されている場合のみです。実行中のジョブはすべて中止できます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* 保護 * > * ジョブ * をクリックします。
2. ジョブのリストからジョブを 1 つ選択し、* 中止 * をクリックします。
3. 確認のプロンプトで「* はい *」をクリックして、選択したジョブを中止します。

失敗した保護ジョブを再試行します

失敗した保護ジョブを修正するための対策を行ったら、* Retry * を使用してジョブを再実行できます。ジョブを再試行すると、元のジョブ ID を使用して新しいジョブが作成されます。

- 必要なもの *

アプリケーション管理者またはストレージ管理者のロールが必要です。

失敗したジョブは一度に 1 つずつ再試行できます。複数のジョブを選択すると、* Retry * ボタンが無効になります。再試行できるのは、タイプが Protection Configuration および Protection Relationship Operation のジョブだけです。

手順

1. 左側のナビゲーションペインで、* 保護 * > * ジョブ * をクリックします。
2. ジョブのリストから、タイプが Protection Configuration または Protection Relationship Operation の失敗したジョブを 1 つだけ選択します。

[* Retry * (再試行)] ボタンが有効になります。

3. [* 再試行 *] をクリックします。

ジョブが再開されます。

保護関係の概要のウィンドウとダイアログボックス

リソースプール、SVM の関連付け、保護ジョブなど、保護に関連する詳細を表示および管理できます。適切な健全性しきい値ページを使用して、アグリゲート、ボリューム、および関係のグローバルな健全性しきい値を設定できます。

リソースプールページ

リソースプールページには、既存のリソースプールとそのメンバーが表示されます。また、プロビジョニングのためにリソースプールを作成、監視、管理することもできます。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * 作成 *。

[リソースプールの作成] ダイアログボックスが開きます。このダイアログボックスを使用して、リソースプールを作成できます。

- * 編集 *。

作成するリソースプールの名前と概要を編集できます。

- * 削除 *

1 つ以上のリソースプールを削除できます。

リソースプールのリスト

[リソースプール] リストには、既存のリソースプールのプロパティが表形式で表示されます。

- * リソースプール *

リソースプールの名前が表示されます。

- * 概要 *

リソースプールについて説明します。

- * SnapLock タイプ *

リソースプール内のアグリゲートで使用されている SnapLock タイプが表示されます。SnapLock タイプの有効な値は、Compliance、Enterprise、および Non-SnapLock です。リソースプールに含めることができる SnapLock タイプは 1 つだけです。

- * 合計容量 *

リソースプールの合計容量（MB、GB など）が表示されます。

- * 使用容量 *

リソースプールで使用されているスペース（MB、GB など）が表示されます。

- * 使用可能容量 *

リソースプールで使用可能なスペース（MB、GB など）が表示されます。

- * 使用済み % *

リソースプールで使用されているスペースの割合が表示されます。

メンバーはコマンドボタンを一覧表示します

メンバーリストのコマンドボタンを使用して、次のタスクを実行できます。

- * 追加 *。

リソースプールにメンバーを追加できます。

- * 削除 *

リソースプールから 1 つ以上のメンバーを削除できます。

メンバーリスト

リソースプールを選択すると、メンバーリストにリソースプールメンバーとそのプロパティが表形式で表示されます。

• * ステータス *

メンバーアグリゲートの現在のステータスが表示されます。ステータスは Critical (❌)、エラー (💡)、警告 (⚠️)、または標準 (✅)。

• * アグリゲート名 *

メンバーアグリゲートの名前が表示されます。

• * 状態 *

アグリゲートの現在の状態が表示されます。次のいずれかになります。

◦ オフラインです

読み取り / 書き込みアクセスが許可されていません。

◦ オンライン

このアグリゲートでホストされているボリュームへの読み取りおよび書き込みアクセスが許可されます。

◦ 制限

一部の処理（パリティの再構築など）は許可されますが、データアクセスは許可されません。

◦ 作成中です

アグリゲートを作成中です。

◦ 破棄しています

アグリゲートを削除中です。

◦ 失敗しました

アグリゲートをオンラインにできません。

◦ フリーズしました

アグリゲートが（一時的に）要求に応答していません。

◦ 不整合

アグリゲートが破損とマークされています。テクニカルサポートにお問い合わせください。

◦ Iron 使用不可

アグリゲートで診断ツールを実行できません。

- マウント中

アグリゲートがマウント中です。

- 一部有効です

アグリゲート用のディスクが少なくとも 1 つ見つかりましたが、複数のディスクが不足しています。

- 休止中です

アグリゲートを休止中です。

- 休止中です

アグリゲートが休止されています。

- リバート済み

アグリゲートのリバートが完了しました。

- アンマウントされました

アグリゲートがアンマウントされました。

- アンマウント中です

アグリゲートをオフラインにしています。

- 不明です

アグリゲートが検出されましたが、Unified Manager サーバでアグリゲートの情報がまだ取得されていません。

デフォルトでは、この列は表示されません。

- * クラスタ *

アグリゲートが属するクラスタの名前が表示されます。

- * ノード *

アグリゲートが配置されているノードの名前が表示されます。

- * 合計容量 *

アグリゲートの合計容量（MB、GB など）が表示されます。

- * 使用容量 *

アグリゲートで使用されているスペース（MB、GB など）が表示されます。

- * 使用可能容量 *

アグリゲートで使用可能なスペース（MB、GB など）が表示されます。

- * 使用済み %*

アグリゲートで使用されているスペースの割合が表示されます。

- * ディスクタイプ *

RAID 構成タイプが表示されます。次のいずれかになります。

- RAID0 :すべての RAID グループのタイプが RAID 0 です。
- RAID4 :すべての RAID グループのタイプが RAID 4 です。
- RAID-DP :すべての RAID グループのタイプが RAID-DP です。
- RAID-TEC :すべての RAID グループのタイプが RAID-TEC です。
- Mixed RAID :アグリゲートに RAID タイプ（RAID 0、RAID 4、RAID-DP、RAID-TEC）が異なる複数の RAID グループが含まれています。デフォルトでは、この列は表示されません。

CreateResourcePool ダイアログボックス

Create Resource Pool ダイアログボックスを使用して、新しいリソースプールの名前と説明を指定し、そのリソースプールに対してアグリゲートを追加および削除することができます。

リソースプール名

テキストボックスを使用して、リソースプールを作成するための次の情報を追加できます。

リソースプール名を指定できます。

説明

リソースプールの説明を指定できます。

メンバー

リソースプールのメンバーが表示されます。メンバーを追加および削除することもできます。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * 追加 *

アグリゲートダイアログボックスを開きます。このダイアログボックスで、特定のクラスタのアグリゲートをリソースプールに追加できます。異なるクラスタからアグリゲートを追加できますが、同じアグリゲートを複数のリソースプールに追加することはできません。

- * 削除 *

選択したアグリゲートをリソースプールから削除できます。

- * 作成 *。

リソースプールを作成します。このボタンは、リソースプール名または概要フィールドに情報が入力されるまで有効になりません。

- * キャンセル *

変更内容を破棄して [Create Resource Pool] ダイアログボックスを閉じます。

EditResourcePool タイアロクホツクス

Edit Resource Pool ダイアログボックスを使用して、既存のリソースプールの名前と概要を変更できます。たとえば、元の名前や概要が正確でない場合や正しくない場合は、より正確になるように名前を変更できます。

テキストボックス

テキストボックスを使用して、選択したリソースプールに関する次の情報を変更できます。

- * リソースプール名 *

新しい名前を入力できます。

- * 概要 *

新しい概要を入力できます。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * 保存 *

リソースプール名および概要の変更内容を保存します。

- * キャンセル *

変更内容を破棄して [Edit Resource Pool] ダイアログボックスを閉じます。

Aggregates タイアロクホツクス

アグリゲートダイアログボックスを使用して、リソースプールに追加するアグリゲートを選択できます。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * 追加 *。

選択したアグリゲートをリソースプールに追加します。追加ボタンは、少なくとも 1 つのアグリゲートが選択されるまで有効になりません。

- * キャンセル *

変更内容を破棄してから、アグリゲートのダイアログボックスを閉じます。

アグリゲートのリスト

アグリゲートリストには、監視対象のアグリゲートの名前とプロパティが表形式で表示されます。

- * ステータス *

ボリュームの現在のステータスが表示されます。ステータスは Critical (❌)、エラー (🚫)、警告 (⚠️)、または標準 (✅)。

ステータスにカーソルを合わせると、ボリュームに対して生成されたイベントに関する詳細を確認できます。

- * アグリゲート名 *

アグリゲートの名前が表示されます。

- * 状態 *

アグリゲートの現在の状態が表示されます。次のいずれかになります。

- オフラインです

読み取り / 書き込みアクセスが許可されていません。

- 制限

一部の処理（パリティの再構築など）は許可されますが、データアクセスは許可されません。

- オンライン

このアグリゲートでホストされているボリュームへの読み取りおよび書き込みアクセスが許可されます。

- 作成中です

アグリゲートを作成中です。

- 破棄しています

アグリゲートを削除中です。

- 失敗しました

アグリゲートをオンラインにできません。

- フリーズしました

アグリゲートが（一時的に）要求に応答していません。

- 不整合

アグリゲートが破損とマークされています。テクニカルサポートにお問い合わせください。

- Iron 使用不可

アグリゲートで診断ツールを実行できません。

- マウント中

アグリゲートがマウント中です。

- 一部有効です

アグリゲート用のディスクが少なくとも 1 つ見つかりましたが、複数のディスクが不足しています。

- 休止中です

アグリゲートを休止中です。

- 休止中です

アグリゲートが休止されています。

- リバート済み

アグリゲートのリバートが完了しました。

- アンマウントされました

アグリゲートがオフラインです。

- アンマウント中です

アグリゲートをオフラインにしています。

- 不明です

アグリゲートが検出されましたが、Unified Manager サーバでアグリゲートの情報がまだ取得されていません。

• * クラスタ *

アグリゲートが配置されているクラスタの名前が表示されます。

• * ノード *

アグリゲートが含まれるストレージコントローラの名前が表示されます。

- * 合計容量 *

アグリゲートの合計データサイズ（MB、GB など）が表示されます。デフォルトでは、この列は表示されません。

- * コミット容量 *

アグリゲート内のすべてのボリュームに対してコミットされているスペースの合計（MB、GB など）が表示されます。デフォルトでは、この列は表示されません。

- * 使用容量 *

アグリゲートで使用されているスペース（MB、GB など）が表示されます。

- * 使用可能容量 *

アグリゲートでデータに使用できるスペース（MB、GB など）が表示されます。デフォルトでは、この列は表示されません。

- * 使用可能 % *

アグリゲートでデータに使用できるスペースの割合が表示されます。デフォルトでは、この列は表示されません。

- * 使用済み % *

アグリゲートでデータに使用されているスペースの割合が表示されます。

- * RAID タイプ *

選択したボリュームの RAID タイプが表示されます。RAID タイプには、RAID 0、RAID 4、RAID-DP、RAID-TEC、Mixed RAID のいずれかを指定できます。

「ジョブ」ページ

Jobs ページでは、現在実行中のすべてのパートナーアプリケーション保護ジョブの現在のステータスとその他の情報、および完了したジョブを表示できます。この情報から、実行中のジョブと、ジョブが成功したか失敗したかを確認できます。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * 中止 *

選択したジョブを中止します。このオプションは、選択したジョブが実行中の場合にのみ使用できます。

- * 再試行 *

Protection Configuration タイプまたは Protection Relationship Operation タイプの失敗したジョブを再起動します。失敗したジョブは一度に 1 つずつ再試行できます。複数の失敗したジョブが選択されている場合、* Retry * ボタンは無効になります。ストレージサービスジョブは、失敗しても再試行できません。



- * 更新 *

ジョブのリストとジョブに関連付けられている情報を更新します。

「ジョブ」リスト

ジョブリストには、進行中のジョブのリストが表形式で表示されます。デフォルトでは、過去 1 週間に生成されたジョブのみがリストに表示されます。列のソートやフィルタリングを使用して、表示するジョブをカスタマイズできます。

- * ステータス *

ジョブの現在のステータスを表示します。ステータスは、Error () または標準 ()。

- * ジョブ ID *

ジョブの ID 番号が表示されます。デフォルトでは、この列は表示されません。

ジョブ ID 番号は一意であり、ジョブの開始時にサーバによって割り当てられます。列フィルタのテキストボックスにジョブ ID 番号を入力すると、特定のジョブを検索できます。

- * 名前 *

ジョブの名前を表示します。

- * タイプ *

ジョブタイプが表示されます。ジョブタイプは次のとおりです。

- * クラスタの取得 *

Workflow Automation ジョブがクラスタを再検出しています。

- * 保護設定 *

保護ジョブは、cron スケジュール、SnapMirror ポリシーの作成などの Workflow Automation ワークフローを開始しています。

- * 保護関係の操作 *

保護ジョブが SnapMirror 処理を実行しています。

- * 保護ワークフローチェーン *

Workflow Automation ジョブが複数のワークフローを実行しています。

- * 復元 *

リストアジョブを実行しています。

- * クリーンアップ *

リストアに必要ななくなったストレージサービスメンバーのアーティファクトをジョブがクリーンアップしています。

◦ * 適合 *

ジョブがストレージサービスメンバーの設定をチェックして準拠していることを確認しています。

◦ * 破棄 *

ジョブがストレージサービスを削除しています。

◦ * インポート *

ジョブが管理対象外のストレージオブジェクトを既存のストレージサービスにインポートしています。

◦ * 変更 *

ジョブが既存のストレージサービスの属性を変更しています。

◦ * 予約購読 *

ジョブがストレージサービスにメンバーをサブスクライブしています。

◦ * 配信停止 *

ジョブがストレージサービスからメンバーをサブスクライブ解除しています。

◦ * アップデート *

保護更新ジョブを実行しています。

◦ * WFA の設定 *

Workflow Automation ジョブが、クラスタのクレデンシャルをプッシュし、データベースキャッシュを同期しています。

• * 状態 *

ジョブの実行状態を表示します。状態のオプションは次のとおりです。

◦ * 中止しました *

ジョブが中止されました。

◦ * 中止中 *

ジョブの中止処理が進行中です。

◦ * 完了 *

ジョブが完了しました。

◦ * 実行中 *

ジョブが実行中です。

• * 送信時刻 *

ジョブが送信された時刻を表示します。

• * 期間 *

ジョブの完了までにかかった時間が表示されます。この列はデフォルトで表示されます。

• * 完了時間 *

ジョブが終了した時刻が表示されます。デフォルトでは、この列は表示されません。

ジョブの詳細ページ

ジョブの詳細ページでは、実行中の特定の保護ジョブタスク、キューに登録されたタスク、完了したタスクに関するステータスやその他の情報を確認できます。この情報は、保護ジョブの進捗の監視やジョブが失敗した場合のトラブルシューティングに役立ちます。

ジョブの概要

ジョブの概要として次の情報が表示されます。

- ジョブ ID
- を入力します
- 状態
- 送信時刻
- 完了時刻
- 期間

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

• * 更新 *

タスクリストと各タスクに関連付けられているプロパティを更新します。

• * ジョブの表示 *

[ジョブ] ページに戻ります。

ジョブタスクリスト

[ジョブタスク] リストは、特定のジョブに関連付けられているすべてのタスクと、各タスクに関連するプロパティを表形式で表示します。

- * 開始時間 *

タスクが開始された日時が表示されます。デフォルトでは、列の上部に最新のタスクが表示され、古いタスクについては下部に表示されます。

- * タイプ *

タスクのタイプが表示されます。

- * 状態 *

特定のタスクの状態：

- * 完了 *

完了したタスクです。

- * キューイング済み *

実行待ちのタスクです。

- * 実行中 *

実行中のタスクです。

- * 待機中 *

ジョブが送信され、一部の関連タスクがキューへの登録と実行を待機しています。

- * ステータス *

タスクのステータスが表示されます。

- * エラー (🚫) *

失敗したタスクです。

- * 正常 (✅) *

成功したタスクです。

- * スキップ (🔄) *

失敗したために後続のタスクがスキップされたタスクです。

- * 期間 *

タスクが開始されてからの経過時間が表示されます。

- * 完了時間 *

タスクが完了した時刻が表示されます。デフォルトでは、この列は表示されません。

- * タスク ID *

ジョブの個々のタスクを識別する GUID が表示されます。列はソートおよびフィルタできます。デフォルトでは、この列は表示されません。

- * 依存順序 *

グラフ内のタスクのシーケンスを表す整数が表示されます。最初のタスクには 0 が割り当てられます。デフォルトでは、この列は表示されません。

- * タスクの詳細ペイン *

各ジョブタスクに関する追加情報が表示されます。これには、タスク名、タスク概要、タスクが失敗した場合は失敗の理由などが含まれます。

- * タスク・メッセージ・パネル *

選択したタスクに固有のメッセージが表示されます。エラーの理由や推奨される解決方法などが含まれます。すべてのタスクにタスクメッセージが表示されるわけではありません。

Advanced Secondary Settings ダイアログボックス

Advanced Secondary Settings ダイアログボックスを使用して、セカンダリボリュームのバージョンに依存しないレプリケーション、複数コピーバックアップ、およびスペース関連設定を有効にすることができます。Advanced Secondary Settings ダイアログボックスを使用して、現在の設定を有効または無効にすることができます。

スペース関連設定には、重複排除、データ圧縮、自動拡張、スペースギャランティなど、格納できるデータの量を最大限に増やすための設定が含まれます。

このダイアログボックスには次のフィールドがあります。

- * バージョンに依存しないレプリケーション * を有効にします

バージョンに依存しないレプリケーションで SnapMirror を有効にします。バージョンに依存しないレプリケーションでは、デスティネーションボリュームで実行している ONTAP のバージョンがソースボリュームよりも古い場合でも、ソースボリュームの SnapMirror 保護が可能です。

- バックアップを有効にします

バージョンに依存しないレプリケーションを有効にすると、SnapMirror ソースデータの複数の Snapshot コピーを SnapMirror デスティネーションに転送して保持することができます。

- * 重複排除を有効にする *

SnapVault 関係のセカンダリボリュームで重複排除を有効にして、重複するデータブロックを排除してスペースを削減できるようにします。重複排除は、スペース削減率が 10% 以上で、データが頻繁には書きされない場合に効果を期待できます。重複排除は、仮想環境、ファイル共有、バックアップのデータに

よく使用されます。この設定は、デフォルトでは無効になっています。有効にすると、転送が完了するたびにこの処理が開始されます。

- 圧縮を有効にします

透過的なデータ圧縮を有効にします。圧縮は、スペース削減率が 10% 以上で、潜在的なオーバーヘッドを許容でき、ピーク時以外の時間帯に圧縮を完了できるだけの十分なシステムリソースがある場合に効果を期待できます。SnapVault 関係では、この設定はデフォルトで無効になっています。圧縮は、重複排除を選択した場合にのみ使用できます。

- インラインで圧縮します

ディスクに書き込む前にデータを圧縮することで、スペース削減効果を即座に実現できます。インライン圧縮は、システムのピーク時の利用率が 50% 以下で、ピーク時に書き込みや CPU が多少増えても許容できる場合に効果を期待できます。この設定は、「圧縮を有効にする」が選択されている場合にのみ使用できます。

- * 自動拡張を有効にします。 *

空きスペースの割合が指定したしきい値を下回ったときに、関連付けられているアグリゲートに使用可能なスペースが残っていれば、デスティネーションボリュームを自動的に拡張できます。

- * 最大サイズ *

ボリュームを最大で何パーセントまで拡張できるかを設定します。デフォルトでは、ソースボリュームのサイズよりも 20% まで大きくできます。現在のボリュームサイズがこの値以上の場合、そのボリュームは自動的に拡張されません。このフィールドは、自動拡張の設定を有効にした場合にのみ有効になります。

- * 増分サイズ *

ボリュームの自動拡張で何パーセントずつ拡張するかを指定します。ソースボリュームの割合で示した最大サイズに達するまで、この割合で自動的に拡張されます。

- * スペース保証 *

データ転送が常に成功するようにセカンダリボリュームに十分なスペースを割り当てます。スペースギャランティの設定は次のいずれかです。

- ファイル。

- ボリューム

- none + たとえば、200GB のボリュームに合計 50GB のファイルが格納されており、それらのファイルに実際に格納されているデータは 10GB だけとします。ボリュームギャランティでは、ソースの内容に関係なく、デスティネーションボリュームに 200GB が割り当てられます。ファイルギャランティでは、ソース上のファイルに十分なスペースが確保されるように 50GB が割り当てられます。このシナリオで None を選択した場合、ソース上のファイルデータで使用する実際のスペースに対して、デスティネーションには 10GB だけが割り当てられます。

スペースギャランティはデフォルトでボリュームに設定されています。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * 適用 *

選択した効率化設定を保存し、[保護の設定] ダイアログボックスで[適用]をクリックしたときに適用します。

- * キャンセル *

選択内容を破棄して、[Advanced Destination Settings] ダイアログボックスを閉じます。

Advanced Destination Settings ダイアログボックス

デスティネーションボリュームのスペースギャランティの設定を有効にするには、詳細設定ダイアログボックスを使用します。詳細設定は、ソースではスペースギャランティが無効になっている状況において、デスティネーションでスペースギャランティを有効にする場合に使用します。SnapMirror 関係の重複排除、圧縮、および自動拡張の設定はソースボリュームから継承され、変更することはできません。

スペースギャランティ

データ転送が常に成功するようにデスティネーションボリュームに十分なスペースを割り当てます。スペースギャランティの設定は次のいずれかです。

- ファイル。
- ボリューム
- なし

たとえば、200GB のボリュームに合計 50GB のファイルが格納されており、それらのファイルに実際に格納されているデータは 10GB だけであるとします。ボリュームギャランティでは、ソースの内容に関係なく、デスティネーションボリュームに 200GB が割り当てられます。ファイルギャランティでは、デスティネーションのソースファイル用に十分なスペースが確保されるように 50GB が割り当てられます。このシナリオで「なし」を選択すると、ソースのファイルデータで使用する実際のスペース用に、デスティネーションには 10GB しか割り当てられません。

スペースギャランティはデフォルトでボリュームに設定されています。

リストアダイアログボックス

リストアダイアログボックスを使用すると、特定の Snapshot コピーからボリュームにデータをリストアできます。

からリストアします

Restore from 領域では、データをリストアする場所を指定できます。

- * 音量 *

データのリストア元のボリュームを指定します。デフォルトでは、リストア操作を開始したボリュームが選択されます。リストア操作を開始したボリュームと保護関係にあるすべてのボリュームを表示するドロップダウンリストから別のボリュームを選択することもできます。

- * Snapshot コピー *

データのリストアに使用する Snapshot コピーを指定します。デフォルトでは、最新の Snapshot コピーが選択されます。ドロップダウンリストから別の Snapshot コピーを選択することもできます。Snapshot コピーのリストが、選択したボリュームに応じて変更されます。


- * 最大 995 個のファイルとディレクトリ * を表示します

デフォルトでは、最大 995 個のオブジェクトがリストに表示されます。選択したボリューム内のすべてのオブジェクトを表示する場合は、このチェックボックスを選択解除できます。アイテムの数が非常に多い場合は、この処理に時間がかかることがあります。

リストアする項目を選択します

リストアするアイテムを選択領域では、ボリューム全体、またはリストアする特定のファイルとフォルダを選択できます。最大 10 個のファイル、フォルダ、またはその組み合わせを選択できます。アイテムの最大数を選択すると、アイテム選択チェックボックスは無効になります。

- * パスフィールド *

リストアするデータのパスが表示されます。リストアするフォルダとファイルに移動するか、パスを入力できます。このフィールドは、パスを選択または入力するまで空になります。をクリックします  パスを選択すると、ディレクトリ構造の 1 つ上のレベルに移動します。

- * フォルダーとファイルリスト *

入力したパスの内容が表示されます。デフォルトでは、最初にルートフォルダが表示されます。フォルダ名をクリックすると、そのフォルダの内容が表示されます。

リストアする項目は次のように選択できます。

- パスフィールドに特定のファイル名を指定してパスを入力すると ' 指定したファイルがフォルダとファイルに表示されます
- 特定のファイルを指定せずにパスを入力すると、フォルダの内容がフォルダとファイルリストに表示され、最大 10 個のファイル、フォルダ、またはその組み合わせを選択してリストアできます。

フォルダに 995 個を超えるアイテムが含まれている場合は、アイテムが多すぎて表示できないことを通知するメッセージが表示され、そのまま処理を続行すると、指定したフォルダ内のすべてのアイテムがリストアされます。選択したボリューム内のすべてのオブジェクトを表示する場合は、「最大 995 個のファイルとディレクトリを表示」チェックボックスをオフにできます。



NTFS ファイルストリームはリストアできません。

にリストアします

Restore to 領域では、データをリストアする場所を指定できます。

- * Volume_Name 内の元の場所 *

選択したデータを、データのバックアップが行われたソース上のディレクトリにリストアします。

- * 別の場所 *

選択したデータを新しい場所にリストアします。

- リストアパス

選択したデータをリストアする代替パスを指定します。既存のパスを指定する必要があります。「* Browse *」ボタンを使用して、データをリストアする場所に移動したり、cluster : //SVM/volume/path の形式でパスを手動で入力したりできます。

- ディレクトリ階層を維持します

このチェックボックスをオンにすると、元のファイルまたはディレクトリの構造が保持されます。たとえば、ソースが「/A/B/C/ myfile.txt」で、デスティネーションが「/X/Y/Z」である場合、Unified Manager はデスティネーションでディレクトリ構造「/X/Y/Z/A/B/C/myFile.txt」を使用してデータをリストアします。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * キャンセル *

選択内容を破棄して、[復元] ダイアログボックスを閉じます。

- * 復元 *

選択内容を適用してリストアプロセスを開始します。

BrowseDirectories タイアロクホツクス

元のソースとは異なるクラスタおよび SVM 上のディレクトリにデータをリストアする場合は、[Browse Directories] ダイアログボックスを使用します。元のソースクラスタとボリュームがデフォルトで選択されます。

[Browse Directories] ダイアログボックスでは、データのリストア先となるクラスタ、SVM、ボリューム、およびディレクトリパスを選択できます。

- * クラスタ *

リストア先として指定できるクラスタのリストが表示されます。デフォルトでは元のソースボリュームのクラスタが選択されます。

- * SVM ドロップダウンリスト *

選択したクラスタで使用可能な SVM のリストが表示されます。デフォルトでは元のソースボリュームの SVM が選択されます。


- * 音量 *

選択した SVM 内の読み書き可能なボリュームがすべて表示されます。ボリュームは、名前および使用可能なスペースでフィルタできます。最もスペースが大きいボリュームから順に一覧表示されます。デフォルトでは元のソースボリュームが選択されます。

- * ファイルパステキストボックス *

データのリストア先となるファイルパスを入力できます。既存のパスを入力する必要があります。

- * 名前 *

選択したボリュームで利用できるフォルダの名前が表示されます。[名前] リストでフォルダをクリックすると、サブフォルダがある場合はそのサブフォルダが表示されます。フォルダに含まれているファイルは表示されません。をクリックします  フォルダを選択すると、ディレクトリ構造の 1 つ上のレベルに移動します。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * 「ディレクトリ」を選択します。 *

選択内容を適用して、[ディレクトリの参照] ダイアログボックスを閉じます。ディレクトリが選択されていない場合、このボタンは無効になります。

- * キャンセル *

選択内容を破棄して、[ディレクトリの参照] ダイアログボックスを閉じます。

Configure Protection（保護の設定）ダイアログボックス

保護の設定ダイアログボックスを使用して、クラスタ上のすべての読み取り、書き込み、データ保護のボリュームに対して SnapMirror 関係と SnapVault 関係を作成し、ソースボリュームまたはプライマリボリューム上のデータをレプリケートできます。

[ソース] タブ

- * トポロジビュー *

作成する関係が視覚的に表示されます。デフォルトでは、トポロジ内のソースが強調表示されます。

- * ソース情報 *

選択したソースボリュームに関する詳細が表示されます。次の情報が含まれます。

- ソースクラスタ名
- ソース SVM 名
- ボリュームの累積合計サイズ

選択したすべてのソースボリュームの合計サイズが表示されます。

- ボリュームの累積使用サイズ

選択したすべてのソースボリュームの累積使用サイズが表示されます。

- ソースボリューム

次の情報を表形式で表示します。

- ソースボリューム

選択したソースボリュームの名前が表示されます。

- を入力します

ボリュームタイプが表示されます。

- SnapLock タイプ

ボリュームの SnapLock タイプが表示されます。「 Compliance 」、「 Enterprise 」、「 Non-SnapLock 」のいずれかです。

- Snapshot コピー

ベースライン転送に使用される Snapshot コピーが表示されます。ソースボリュームが読み取り / 書き込みの場合、Snapshot コピーの列の default の値は、新しい Snapshot コピーがデフォルトで作成され、ベースライン転送に使用されることを示します。ソースボリュームがデータ保護ボリュームの場合、Snapshot コピー列の default の値は新しい Snapshot コピーが作成されないことを示し、既存のすべての Snapshot コピーがデスティネーションに転送されます。Snapshot コピーの値をクリックすると Snapshot コピーのリストが表示され、ベースライン転送に使用する既存の Snapshot コピーを選択できます。ソースタイプがデータ保護の場合、別のデフォルトの Snapshot コピーを選択することはできません。

SnapMirror タブ

保護関係のデスティネーションクラスタ、 Storage Virtual Machine （ SVM ）、アグリゲート、および SnapMirror 関係を作成する際のデスティネーションの命名規則を指定できます。SnapMirror ポリシーとスケジュールを指定することもできます。

- * トポロジビュー *

作成する関係が視覚的に表示されます。デフォルトでは、トポロジ内の SnapMirror のデスティネーションリソースが強調表示されます。

- * 目的地情報 *

保護関係のデスティネーションリソースを選択できます。

- 詳細リンク

SnapMirror 関係の作成時に、詳細なデスティネーション設定ダイアログボックスを表示します。

- クラスタ

保護デスティネーションホストとして使用できるクラスタが表示されます。このフィールドは必須です。

- Storage Virtual Machine (SVM)

選択したクラスタで使用可能な SVM が表示されます。このリストに SVM を表示するには、クラスタを選択する必要があります。このフィールドは必須です。

- アグリゲート

選択した SVM で使用できるアグリゲートが表示されます。このリストにアグリゲートを表示するには、クラスタを選択する必要があります。このフィールドは必須です。アグリゲートリストには、次の情報が表示されます。

- ランク

複数のアグリゲートがデスティネーションの要件をすべて満たす場合、この順位は、次の条件に従ってアグリゲートを表示する優先順位を示します。

- A. ソースボリュームのノードとは異なるノードに配置されているアグリゲートが優先され、障害ドメインの分離が可能になります。
 - B. ボリューム数が少ないノード上のアグリゲートが優先され、クラスタ内のノード間での負荷分散が可能になります。
 - C. 他のアグリゲートよりも空きスペースの多いアグリゲートが優先され、容量の分散が可能になります。順位 1 は、この 3 つの条件に従っているアグリゲートが最も優先されることを示します。

- アグリゲート名

アグリゲートの名前

- 使用可能容量
 - アグリゲートでデータに使用できるスペースの量
 - リソースプール

アグリゲートが属するリソースプールの名前

- 命名規則

デスティネーションボリュームに適用されるデフォルトの命名規則を指定します。用意されている命名規則をそのまま使用することも、カスタムの命名規則を作成することもできます。命名規則には、%C、%M、%V、%N という属性を指定できます。%C はクラスタ名、%M は SVM 名、%V はソースボリューム、%N はトポロジのデスティネーションノード名です。

入力が無効な場合、命名規則のフィールドが赤で強調表示されます。「名前のプレビュー」リンクをクリックすると、入力した命名規則のプレビューが表示され、テキストフィールドに命名規則を入力するとプレビューテキストが動的に更新されます。関係を作成すると、001～999 のサフィックスが宛先名に付加されます。プレビューテキストに表示される nnn は置き換えられ、001 が最初に割り当てられ、002 が 2 番目に割り当てられます。

• * 関係設定 *

保護関係で使用する最大転送速度、 SnapMirror ポリシー、およびスケジュールを指定できます。

◦ 最大転送速度

ネットワークを介してクラスタ間でデータを転送する最大速度を指定します。最大転送速度を指定しない場合は、関係間でベースライン転送が制限されません。

◦ SnapMirror ポリシー

関係の ONTAP SnapMirror ポリシーを指定します。デフォルトは DPDefault です。

◦ ポリシーの作成

SnapMirror ポリシーの作成ダイアログボックスが開きます。このダイアログボックスで、新しい SnapMirror ポリシーを作成して使用できます。

◦ SnapMirror スケジュール

関係の ONTAP SnapMirror ポリシーを指定します。スケジュールは、「None」、「5min」、「8hour」、「daily」、「hourly」、毎週、デフォルトは「None」で、関係にスケジュールが関連付けられません。スケジュールが設定されていない関係については、ストレージサービスに属している場合を除き、遅延ステータスの値は表示されません。

◦ スケジュールを作成します

スケジュールの作成ダイアログボックスが開きます。このダイアログボックスで、新しい SnapMirror スケジュールを作成できます。

SnapVault タブ

保護関係のセカンダリクラスタ、SVM、アグリゲート、および SnapVault 関係を作成する際のセカンダリボリュームの命名規則を指定できます。SnapVault ポリシーとスケジュールを指定することもできます。

• * トポロジビュー *

作成する関係が視覚的に表示されます。デフォルトでは、トポロジ内の SnapVault セカンダリリソースが強調表示されます。

• * 二次情報 *

保護関係のセカンダリリソースを選択できます。

◦ 詳細リンク

Advanced Secondary Settings ダイアログボックスを起動します。

◦ クラスタ

セカンダリ保護ホストとして使用できるクラスタが表示されます。このフィールドは必須です。

- Storage Virtual Machine (SVM)

選択したクラスタで使用可能な SVM が表示されます。このリストに SVM を表示するには、クラスタを選択する必要があります。このフィールドは必須です。

- アグリゲート

選択した SVM で使用できるアグリゲートが表示されます。このリストにアグリゲートを表示するには、クラスタを選択する必要があります。このフィールドは必須です。アグリゲートリストには、次の情報が表示されます。

- ランク

複数のアグリゲートがデスティネーションの要件をすべて満たす場合、この順位は、次の条件に従ってアグリゲートを表示する優先順位を示します。

- A. プライマリボリュームのノードとは異なるノードに配置されているアグリゲートが優先され、障害ドメインの分離が可能になります。
 - B. ボリューム数が少ないノード上のアグリゲートが優先され、クラスタ内のノード間での負荷分散が可能になります。
 - C. 他のアグリゲートよりも空きスペースの多いアグリゲートが優先され、容量の分散が可能になります。順位 1 は、この 3 つの条件に従っているアグリゲートが最も優先されることを示します。

- アグリゲート名

アグリゲートの名前

- 使用可能容量

- アグリゲートでデータに使用できるスペースの量

- リソースプール

アグリゲートが属するリソースプールの名前

- 命名規則

セカンダリボリュームに適用されるデフォルトの命名規則を指定します。用意されている命名規則をそのまま使用することも、カスタムの命名規則を作成することもできます。命名規則には、%C、%M、%V、%N という属性を指定できます。%C はクラスタ名、%M は SVM 名、%V はソースボリューム、%N はトポロジのセカンダリノード名です。

入力が無効な場合、命名規則のフィールドが赤で強調表示されます。「名前のプレビュー」リンクをクリックすると、入力した命名規則のプレビューが表示され、テキストフィールドに命名規則を入力するとプレビューテキストが動的に更新されます。無効な値を入力すると、プレビュー領域に無効な情報が赤の疑問符として表示されます。リレーションが作成されると、001 ~ 999 の接尾辞がセカンダリ名に付加されます。プレビューテキストに表示される nnn は置き換えられ、001 が最初に割り当てられ、002 が 2 番目に割り当てられます。

- * 関係設定 *

保護関係で使用する最大転送速度、SnapVault ポリシー、および SnapVault スケジュールを指定できます。

- 最大転送速度

ネットワークを介してクラスタ間でデータを転送する最大速度を指定します。最大転送速度を指定しない場合は、関係間でベースライン転送が制限されません。

- SnapVault ポリシー

関係の ONTAP SnapVault ポリシーを指定します。デフォルトは XDPDefault です。

- ポリシーの作成

Create SnapVault Policy ダイアログボックスが開きます。このダイアログボックスで、新しい SnapVault ポリシーを作成して使用できます。

- SnapVault スケジュール

関係の ONTAP SnapVault スケジュールを指定します。スケジュールは、「None」、「5min」、「8hour」、「daily」、「hourly」、毎週、デフォルトは「None」で、関係にスケジュールが関連付けられません。スケジュールが設定されていない関係については、ストレージサービスに属している場合を除き、遅延ステータスの値は表示されません。

- スケジュールを作成します

スケジュールの作成ダイアログボックスが開きます。このダイアログボックスで、SnapVault スケジュールを作成できます。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * キャンセル *

選択内容を破棄して、Configure Protection ダイアログボックスを閉じます。

- * 適用 *

選択項目を適用して保護プロセスを開始します。

スケジュールの作成ダイアログボックス

スケジュールの作成ダイアログボックスでは、SnapMirror 関係と SnapVault 関係の転送の基本または詳細な保護スケジュールを作成できます。データ更新を頻繁に行うために、データ転送の頻度を増やすための新しいスケジュールを作成できます。データがあまり変更されない場合は、少ない頻度のスケジュールを作成することもできます。

SnapMirror 同期関係にスケジュールを設定することはできません。

- * デスティネーションクラスタ *

保護の設定ダイアログボックスの SnapVault タブまたは SnapMirror タブで選択したクラスタの名前。

- * スケジュール名 *

スケジュールに指定する名前。スケジュール名には、A~Z、a~z、0~9、および次の特殊文字を使用できます。!@#\$% { キャレット } &* () _ -。スケジュール名には、以下の文字は使用できません。

- * Basic または Advanced *

使用するスケジュールモード。

基本モードには、次の要素が含まれます。

- 繰り返します

スケジュールされた転送が発生する頻度。時間単位、日単位、週単位のいずれかを選択できます。

- 日

「Weekly」の繰り返しを選択した場合に転送が発生する曜日。

- 時間

「毎日」または「毎週」を選択した場合に転送が発生する時刻。

詳細モードには、次の要素が含まれます。

- 月

カンマで区切った数値のリスト。月を表します。有効な値は0~11です。0は1月を表し、以降も同様です。この要素はオプションです。このフィールドを空にすると、毎月転送が発生します。

- 日

カンマで区切った数値のリスト。日にちを表します。有効な値は1~31です。この要素はオプションです。このフィールドを空にすると、指定した月に毎日転送が発生します。

- 平日

カンマで区切った数値のリスト。曜日を表します。有効な値は0~6です。0は日曜を表し、以降も同様です。この要素はオプションです。このフィールドを空にすると、指定した週に毎日転送が発生します。曜日を指定し、日にちを指定していない場合は、毎日ではなく指定した曜日にのみ転送が実行されます。

- 時間

カンマで区切った数値のリスト。1日のうちの時間数を表します。有効な値は0~23です。0は午前0時を表します。この要素はオプションです。

- 分

カンマで区切った数値のリスト。1時間のうちの分数を表します。有効な値は0~59です。この要素は必須です。

SnapMirror ポリシーの作成ダイアログボックス

SnapMirror ポリシーの作成ダイアログボックスでは、SnapMirror 転送の優先度を設定するポリシーを作成できます。ポリシーを使用することで、ソースからデスティネーションへの転送効率を最大化できます。

- * デスティネーションクラスタ *

Configure Protection（保護の設定）ダイアログボックスの SnapMirror（SnapMirror）タブで選択したクラスタの名前。

- * デスティネーション SVM *

保護の設定ダイアログボックスの SnapMirror タブで選択した SVM の名前。

- * ポリシー名 *

新しいポリシーに指定する名前。ポリシー名には、A~Z、a~z、0~9、ピリオド（.）、ハイフン（-）、とアンダースコア（_）

- * 転送優先順位 *

非同期操作の転送を実行する優先順位。標準または低を選択できます。転送の優先順位として「標準」を指定したポリシーを使用する関係の転送は、「低」を指定したポリシーを使用する関係の転送の前に実行されます。

- * コメント *

オプションのフィールド。ポリシーに関するコメントを追加できます。

- * 転送再開 *

中止処理によって転送が中断された場合や、ネットワーク停止などの何らかの障害によって転送が中断された場合に実行する再開処理を指定します。次のいずれかを選択できます。

- 常に

転送を再開する前に新しい Snapshot コピーを作成し、既存の Snapshot コピーが存在する場合は、チェックポイントから転送を再開して、そのあとに新しく作成した Snapshot コピーに基づく差分転送を実行するように指定します。

- なし

中断された転送を再開しないように指定します。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * キャンセル *

選択内容を破棄して、Configure Protection ダイアログボックスを閉じます。

- * 適用 *

選択項目を適用して保護プロセスを開始します。

Create SnapVault Policy ダイアログボックス

Create SnapVault Policy ダイアログボックスでは、SnapVault 転送の優先度を設定するポリシーを作成できます。ポリシーを使用することで、プライマリからセカンダリボリュームへの転送効率を最大化できます。

- * デスティネーションクラス *

[保護の構成] ダイアログ・ボックスの [保護の構成] タブで選択 SnapVault したクラスタの名前

- * デスティネーション SVM *

保護の設定ダイアログボックスの SnapVault タブで選択した SVM の名前。

- * ポリシー名 *

新しいポリシーに指定する名前。ポリシー名には、A~Z、a~z、0~9、ピリオド (.)、ハイフン (-)、とアンダースコア (_)

- * 転送優先順位 *

転送を実行する優先順位。標準または低を選択できます。転送の優先順位として「標準」を指定したポリシーを使用する関係の転送は、「低」を指定したポリシーを使用する関係の転送の前に実行されます。デフォルト設定は Normal です。

- * コメント *

オプションのフィールド。SnapVault ポリシーに関するコメントを 255 文字以内で追加できます。

- * アクセス時間を無視 *

アクセス時間だけが変更されたファイルを差分転送で無視するかどうかを指定します。

- * レプリケーションラベル *

ONTAP で選択された Snapshot コピーに関連付けられているルールを表形式で示します。この Snapshot コピーのポリシーには特定のレプリケーションラベルが指定されています。次の情報とアクションも利用できます。

- コマンドボタン

各コマンドボタンを使用して次の操作を実行できます。

- 追加 (Add)

Snapshot コピーラベルと保持数を作成できます。

- 保持数を編集

既存の Snapshot コピーラベルの保持数を変更できます。保持数は 1~251 の数値にする必要があります。すべてのルールすべての保持数の合計は 251 個以下でなければなりません。

- 削除

既存の Snapshot コピーラベルを削除できます。

- Snapshot コピーラベル

Snapshot コピーラベルが表示されます。同じローカル Snapshot コピーポリシーを使用する 1 つ以上のボリュームを選択すると、ポリシー内の各ラベルのエントリが表示されます。2 つ以上のローカル Snapshot コピーポリシーを使用する複数のボリュームを選択すると、すべてのポリシーのすべてのラベルがテーブルに表示されます

- スケジュール

各 Snapshot コピーラベルに関連付けられているスケジュールが表示されます。ラベルに複数のスケジュールが関連付けられている場合は、そのラベルのスケジュールがカンマで区切ったリストに表示されます。同じラベルでスケジュールが異なる複数のボリュームを選択すると、スケジュールには「Various」と表示され、選択したボリュームに複数のスケジュールが関連付けられていることが示されます。

- デスティネーションの保持数

SnapVault セカンダリに保持されている、指定したラベルを持つ Snapshot コピーの数が表示されます。複数のスケジュールを使用するラベルの保持数として、各ラベルとスケジュールのペアの保持数の合計が表示されます。2 つ以上のローカル Snapshot コピーポリシーを使用する複数のボリュームを選択した場合、保持数は空になります。

関係の編集ダイアログボックス

既存の保護関係を編集して、最大転送速度、保護ポリシー、保護スケジュールを変更することができます。

宛先情報

- * デスティネーションクラスタ *

選択したデスティネーションクラスタの名前です。

- * デスティネーション SVM *

選択した SVM の名前

- * 関係設定 *

保護関係で使用する最大転送速度、SnapMirror ポリシー、およびスケジュールを指定できます。

- 最大転送速度

ネットワークを介してクラスタ間でベースラインデータを転送する最大速度を指定します。選択すると、ネットワーク帯域幅は指定した値に制限されます。数値を入力してから、KBps（1 秒あたりの

キロバイト数)、MBps (1秒あたりのメガバイト数)、GBps (1秒あたりのギガバイト数)、TBps (1秒あたりのテラバイト数)のいずれかの単位を選択できます。最大転送速度は1KBps~4TBpsの範囲で指定する必要があります。最大転送速度を指定しない場合は、関係間でベースライン転送が制限されません。この設定は、プライマリクラスタとセカンダリクラスタが同じ場合は無効になります。

- SnapMirror ポリシー

関係の ONTAP SnapMirror ポリシーを指定します。デフォルトは DPDefault です。

- ポリシーの作成

SnapMirror ポリシーの作成ダイアログボックスが開きます。このダイアログボックスで、新しい SnapMirror ポリシーを作成して使用できます。

- SnapMirror スケジュール

関係の ONTAP SnapMirror ポリシーを指定します。スケジュールは、「None」、「5min」、「8hour」、「daily」、「hourly」、毎週、デフォルトは「None」で、関係にスケジュールが関連付けられません。スケジュールが設定されていない関係については、ストレージサービスに属している場合を除き、遅延ステータスの値は表示されません。

- スケジュールを作成します

スケジュールの作成ダイアログボックスが開きます。このダイアログボックスで、新しい SnapMirror スケジュールを作成できます。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * キャンセル *

選択内容を破棄して、Configure Protection ダイアログボックスを閉じます。

- * 送信 *

選択内容を適用して、[関係の編集] ダイアログボックスを閉じます。

Initialize/Update ダイアログボックスが表示されます

Initialize/Update ダイアログボックスでは、新しい保護関係で最初のベースライン転送を実行できます。また、すでに初期化されている関係でスケジュールされていない増分更新を手動で実行する場合は、関係を更新できます。

[転送オプション] タブ

[転送オプション] タブでは、転送の初期設定の優先順位を変更したり、転送中に使用される帯域幅を変更したりできます。

- * 転送優先順位 *

転送を実行する優先順位。標準または低を選択できます。関係のポリシーで転送の優先順位「Normal」が指定されている場合、その関係は転送の優先順位「Low」が指定された関係より先に実行デフォルトでは「Normal」が選択されます。

- * 最大転送速度 *

ネットワークを介してクラスタ間でデータを転送する最大速度を指定します。最大転送速度を指定しない場合は、関係間でベースライン転送が制限されません。最大転送速度が異なる複数の関係を選択する場合は、次の最大転送速度設定のいずれかを指定できます。

- 個々の関係のセットアップまたは編集で指定した値を使用します

このオプションを選択すると、各関係の作成時または編集時に指定された最大転送速度が初期化処理と更新処理で使用されます。このフィールドは、転送速度が異なる複数の関係を初期化または更新する場合にのみ使用できます。

- 無制限

関係間の転送に帯域幅の制限がないことを示します。このフィールドは、転送速度が異なる複数の関係を初期化または更新する場合にのみ使用できます。

- 帯域幅をに制限します

選択すると、ネットワーク帯域幅は指定した値に制限されます。数値を入力してから、KBps（1秒あたりのキロバイト数）、MBps（1秒あたりのメガバイト数）、GBps（1秒あたりのギガバイト数）、TBps（1秒あたりのテラバイト数）のいずれかの単位を選択できます。最大転送速度は1KBps~4TBpsの範囲で指定する必要があります。

ソース Snapshot コピータブ

ソース Snapshot コピータブには、ベースライン転送に使用されるソース Snapshot コピーに関する次の情報が表示されます。

- * ソースボリューム *

対応するソースボリュームの名前が表示されます。

- * デスティネーションボリューム *

選択したデスティネーションボリュームの名前が表示されます。

- * ソースタイプ *

ボリュームタイプが表示されます。「読み取り / 書き込み」または「データ保護」のいずれかです。

- * Snapshot コピー *

データ転送に使用される Snapshot コピーが表示されます。Snapshot コピーの値をクリックすると、Select Source Snapshot Copy ダイアログボックスが表示されます。このダイアログボックスでは、使用している保護関係のタイプおよび実行している処理に応じて、転送する特定の Snapshot コピーを選択できます。データ保護タイプのソースについては、別の Snapshot コピーを指定できません。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * キャンセル *

選択内容を破棄して [Initialize] / [Update] ダイアログボックスを閉じます。

- * 送信 *

選択内容を保存し、初期化ジョブまたは更新ジョブを開始します。

Resynchronize タイアロクホツクス

再同期ダイアログボックスを使用すると、以前に解除した SnapMirror 関係や SnapVault 関係のデータを、デスティネーションが読み書き可能ボリュームになったあとに再同期できます。再同期は、必要な共通の Snapshot コピーがソースボリュームで削除されたために SnapMirror や SnapVault の更新が失敗する場合にも実行することがあります。

再同期オプションタブ

再同期オプションタブでは、再同期する保護関係の転送の優先順位と最大転送速度を設定できます。

- * 転送優先順位 *

転送を実行する優先順位。標準または低を選択できます。関係のポリシーで転送の優先順位「Normal」が指定されている場合、その関係は転送の優先順位「Low」が指定された関係より先に実行されます。

- * 最大転送速度 *

ネットワークを介してクラスタ間でデータを転送する最大速度を指定します。選択すると、ネットワーク帯域幅は指定した値に制限されます。数値を入力してから、KBps（1秒あたりのキロバイト数）、MBps（1秒あたりのメガバイト数）、GBps（1秒あたりのギガバイト数）、TBps（1秒あたりのテラバイト数）のいずれかの単位を選択できます。最大転送速度を指定しない場合は、関係間でベースライン転送が制限されません。

ソース Snapshot コピータブ

ソース Snapshot コピータブには、ベースライン転送に使用されるソース Snapshot コピーに関する次の情報が表示されます。

- * ソースボリューム *

対応するソースボリュームの名前が表示されます。

- * デスティネーションボリューム *

選択したデスティネーションボリュームの名前が表示されます。

- * ソースタイプ *

ボリュームタイプが表示されます。読み取り / 書き込みまたはデータ保護のいずれかです。

- * Snapshot コピー *

データ転送に使用される Snapshot コピーが表示されます。Snapshot コピーの値をクリックすると、Select Source Snapshot Copy ダイアログボックスが表示されます。このダイアログボックスでは、保護関係のタイプおよび実行中の処理に応じて、転送する特定の Snapshot コピーを選択できます。

コマンドボタン

- * 送信 *

再同期プロセスを開始して、再同期ダイアログボックスを閉じます。

- * キャンセル *

選択内容をキャンセルして再同期ダイアログボックスを閉じます。

SelectSourceSnapshotCopy ダイアログボックス

ソース Snapshot コピーの選択ダイアログボックスを使用して、保護関係間でデータを転送する特定の Snapshot コピーを選択するか、デフォルトの動作を選択します。選択するオプションは、関係を初期化、更新、再同期するかどうか、および関係が SnapMirror と SnapVault のどちらであるかによって異なります。

デフォルト

SnapVault 関係および SnapMirror 関係の初期化、更新、転送の再同期に使用される Snapshot コピーを決定する際のデフォルトの動作を選択できます。

SnapVault 転送を実行する場合、各処理のデフォルトの動作は次のとおりです。

操作	ソースが読み取り / 書き込みの場合のデフォルトの SnapVault の動作	ソースがデータ保護（ DP ）の場合のデフォルトの SnapVault の動作
初期化します	新しい Snapshot コピーを作成して転送します。	最後にエクスポートされた Snapshot コピーを転送します。
更新	ポリシーの指定に従って、ラベルが設定された Snapshot コピーだけを転送します。	最後にエクスポートされた Snapshot コピーを転送します。
再同期	最も新しい共通の Snapshot コピーのあとに作成され、ラベルが設定されたすべての Snapshot コピーを転送します	ラベルが設定された最新の Snapshot コピーを転送します。

SnapMirror 転送を実行する場合、各処理のデフォルトの動作は次のとおりです。

操作	デフォルトの SnapMirror の動作	関係が SnapMirror-to-SnapMirror カスケードの 2 番目のホップである場合の、デフォルトの SnapMirror の動作
初期化します	新しい Snapshot コピーを作成して、その Snapshot コピーおよびその前に作成されたすべての Snapshot コピーを転送します。	ソースから Snapshot コピーをすべて転送します。
更新	新しい Snapshot コピーを作成して、その Snapshot コピーおよびその前に作成されたすべての Snapshot コピーを転送します。	すべての Snapshot コピーを転送します。
再同期	新しい Snapshot コピーを作成して、ソースから Snapshot コピーをすべて転送します。	セカンダリボリュームから 3 番目のボリュームにすべての Snapshot コピーを転送し、最も新しい共通の Snapshot コピーの作成後に追加されたデータを削除します。

既存の **Snapshot** コピー

リストから既存の Snapshot コピーを選択できます（その処理で Snapshot コピーを選択できる場合）。

- * Snapshot コピー *

転送用に選択可能な既存の Snapshot コピーが表示されます。

- * 作成日 *

Snapshot コピーが作成された日時が表示されます。最新の Snapshot コピーがリストの先頭に表示されます。

SnapVault 転送の実行時に、ソースからデスティネーションに転送する既存の Snapshot コピーを選択する場合、各処理の動作は次のようになります。

操作	Snapshot コピーを指定する場合の SnapVault の動作	カスケード構成の Snapshot コピーを指定する場合の SnapVault の動作
初期化します	指定した Snapshot コピーを転送します。	データ保護ボリュームに対しては、ソース Snapshot コピーの選択がサポートされません。
更新	指定した Snapshot コピーを転送します。	データ保護ボリュームに対しては、ソース Snapshot コピーの選択がサポートされません。

操作	Snapshot コピーを指定する場合の SnapVault の動作	カスケード構成の Snapshot コピーを指定する場合の SnapVault の動作
再同期	選択した Snapshot コピーを転送します。	データ保護ボリュームに対しては、ソース Snapshot コピーの選択がサポートされません。

SnapMirror 転送の実行時に、ソースからデスティネーションに転送する既存の Snapshot コピーを選択する場合、各処理の動作は次のようになります。

操作	Snapshot コピーを指定する場合の SnapMirror の動作	カスケード構成の Snapshot コピーを指定する場合の SnapMirror の動作
初期化します	ソース上のすべての Snapshot コピーを、指定した Snapshot コピーまで転送します。	データ保護ボリュームに対しては、ソース Snapshot コピーの選択がサポートされません。
更新	ソース上のすべての Snapshot コピーを、指定した Snapshot コピーまで転送します。	データ保護ボリュームに対しては、ソース Snapshot コピーの選択がサポートされません。
再同期	すべての Snapshot コピーをソースから選択した Snapshot コピーまで転送し、新しい共通の Snapshot コピーの作成後に追加されたデータを削除します。	データ保護ボリュームに対しては、ソース Snapshot コピーの選択がサポートされません。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

• * 送信 *

選択内容を送信して、Select Source Snapshot Copy（ソース Snapshot コピーの選択）ダイアログボックスを閉じます。

• * キャンセル *

選択内容を破棄して、Select Source Snapshot Copy ダイアログボックスを閉じます。

ReverseResync ダイアログボックス

ソースボリュームが機能しなくなったために保護関係を解除して、デスティネーションを読み書き可能なボリュームにした場合は、逆再同期によって関係の方向を反転させて、デスティネーションを新しいソースにし、ソースを新しいデスティネーションにすることができます。

災害によって保護関係のソースボリュームが機能しなくなった場合は、ソースの修理や交換、ソースの更新、および関係の再確立を行う間、デスティネーションボリュームを読み書き可能に変換してデータの提供を継続することができます。逆再同期処理を実行すると、共通の Snapshot コピーのデータよりも新しいソース上のデータは削除されます。

逆再同期前

逆再同期処理を実行する前の関係のソースとデスティネーションが表示されます。

- * ソースボリューム *

逆再同期処理を実行する前のソースボリュームの名前と場所。

- * デスティネーションボリューム *

逆再同期処理を実行する前のデスティネーションボリュームの名前と場所。

逆再同期後

リザーブ再同期処理を実行したあとの関係のソースとデスティネーションが表示されます。

- * ソースボリューム *

逆再同期処理を実行したあとのソースボリュームの名前と場所。

- * デスティネーションボリューム *

逆再同期処理を実行したあとのデスティネーションボリュームの名前と場所。

コマンドボタン

各コマンドボタンを使用して次の操作を実行できます。

- * 送信 *

逆再同期プロセスを開始します。

- * キャンセル *

逆再同期処理を開始せずに逆再同期ダイアログボックスを閉じます。

関係：すべての関係ビュー

Relationship : All Relationships ビューには、ストレージシステム上の保護関係に関する情報が表示されます。

デフォルトでは、関係ページにアクセスすると、ボリュームと Storage VM の両方の最上位の保護関係が表示されます。ページの上部にあるコントロールを使用すると、特定のビューの選択、特定のオブジェクトの検索の実行、フィルタの作成および適用による表示データのリストの絞り込み、ページ上の列の追加 / 削除 / 並べ替え、ページ上のデータの .csv、.pdf または .xlsx ファイル。カスタマイズしたページをカスタムビューとして保存し、データのレポートを定期的に生成して E メールで送信するようにスケジュール設定できます。

デフォルトでは、[* 関係 *]メニューを選択すると、レポートにはデータセンター内のボリュームと Storage VM の両方の保護関係が表示されます。「* フィルタ *」オプションを使用すると、ボリュームのみ、または Storage VM のみなど、選択したストレージシステムのみを表示できます。ストレージページと、選択したストレージエンティティについてのみ、同じレポートが表示されます。ボリュームまたは Storage VM の関係を表示するには、* Storage * > * Volumes * > * Relationship : All Relationships * ページまたはアクセス * Protection * > * Relationships * > * Relationship : すべての関係 *。フィルタ * の * 関係オブジェクトタイプ * オプションを使用して、ボリュームまたは Storage VM のデータのみをフィルタリングします。

すべての保護関係のリストが表示される関係ページには、デスティネーションクラスタのリンク * System Manager * が表示されます。このリンクを使用すると、ONTAP System Manager で同じオブジェクトを表示できます。

- * ステータス *

保護関係の現在のステータスが表示されます。

ステータスは、Error (❗)、警告 (⚠)、または OK (✅)。

- * ソース Storage VM *

ソース SVM の名前が表示されます。SVM 名をクリックすると、ソース SVM の詳細が表示されます。

クラスタに SVM があり、Unified Manager インベントリにまだ追加されていない場合、またはクラスタの前の更新後に SVM が作成されている場合、このフィールドは空になります。SVM の存在を確認するか、またはクラスタで再検出を実行してリソースのリストを更新する必要があります。

- * 出典 *

選択した内容に基づいて保護されているソースボリュームまたはソース Storage VM が表示されます。ソースボリュームまたは Storage VM の名前をクリックすると、ソースボリュームまたは Storage VM の詳細が表示されます。

というメッセージが表示されます Resource-key not discovered が表示される場合は、クラスタに存在するボリュームが Unified Manager インベントリにまだ追加されていないか、または最後のクラスタ更新の後にボリュームが作成された可能性があります。ボリュームの存在を確認するか、またはクラスタで再検出を実行してリソースのリストを更新する必要があります。

- * デスティネーション Storage VM *

デスティネーション SVM の名前が表示されます。SVM 名をクリックすると、デスティネーション SVM の詳細が表示されます。

- * 目的地 *

選択内容に基づいて、デスティネーションボリュームまたは Storage VM の名前が表示されます。それぞれのオブジェクト名をクリックすると、デスティネーションボリュームまたは Storage VM の詳細を確認できます。

- * 関係オブジェクトタイプ *

Storage VM、ボリューム、整合グループなど、関係で使用されているオブジェクトのタイプが表示されます。整合性関係にあるオブジェクトの場合は、ソースとデスティネーションの関係に整合グループが表示され、クリックすると LUN ページに移動して関係が表示されます。

• * ポリシー *

SnapMirror 関係の保護ポリシーの名前が表示されます。ポリシー名をクリックすると、そのポリシーに関連付けられた詳細について次の情報を確認できます。

◦ 転送の優先順位

非同期操作の転送を実行する優先度を指定します。転送の優先順位は「中」または「低」です。優先順位が「中」の転送は、優先順位が「低」の転送よりも先デフォルトは Normal です。

◦ アクセス時間を無視します

SnapVault 関係にのみ適用されます。アクセス時間だけが変更されたファイルを差分転送で無視するかどうかを指定します。値は True または False のいずれかです。デフォルトは False です。

◦ 関係が同期されていない場合

同期関係を同期できない場合に ONTAP で実行する処理を指定します。StrictSync 関係の場合、セカンダリボリュームとの同期に失敗すると、プライマリボリュームへのアクセスが制限されます。Sync 関係の場合、セカンダリとの同期に失敗しても、プライマリへのアクセスは制限されません。

◦ 最大試行回数

SnapMirror 関係の手動またはスケジュールされた各転送を試行する最大回数を指定します。デフォルトは 8. です。

◦ コメント

選択したポリシーに関するコメントを示すテキストフィールドが表示されます。

◦ SnapMirror ラベル

Snapshot コピーポリシーに関連付ける第 1 のスケジュールの SnapMirror ラベルを指定します。SnapMirror ラベルは、Snapshot コピーを SnapVault デスティネーションにバックアップするときに、SnapVault サブシステムによって使用されます。

◦ 保持設定

バックアップを保持する期間を、バックアップの時刻または数で指定します。

◦ 実際の Snapshot コピー

このボリューム上の、指定したラベルと一致する Snapshot コピーの数を指定します。

◦ Snapshot コピーを保持

ポリシーの上限に達した場合でも自動的に削除されない SnapVault Snapshot コピーの数を指定します。値は True または False のいずれかです。デフォルトは False です。

◦ 保持の警告しきい値

Snapshot コピー数の制限を指定します。この上限に達すると、保持数の上限に近づいていることを通知する警告が送信されます。

- * 遅延時間 *

ミラーのデータがソースより遅延している時間が表示されます。

遅延時間は、StrictSync 関係については 0 またはそれに近い値になります。

- * 遅延ステータス *

管理対象の関係の遅延ステータスと、スケジュールが関連付けられている管理対象外の関係の遅延ステータスが表示されます。遅延ステータスは次のいずれかになります。

- エラー

遅延時間が遅延エラーしきい値と同じか、それを上回っています。

- 警告

遅延時間が遅延警告しきい値と同じか、それを上回っています。

- わかりました

遅延時間が正常範囲内です。

- 該当なし

同期関係については、スケジュールを設定できないため、遅延ステータスは適用されません。

- * 前回成功した更新 *

SnapMirror または SnapVault の処理に最後に成功した時刻が表示されます。

同期関係については、前回成功した更新は適用されません。

- * コンスティチュエント関係 *

選択したオブジェクトにボリュームが含まれているかどうかが表示されます。

- * 関係タイプ *

ボリュームをレプリケートするために使用される関係タイプが表示されます。関係タイプは次のとおりです。

- 非同期ミラー

- 非同期バックアップ

- 非同期ミラーバックアップ

- StrictSync のサポート

- 同期

- * 転送ステータス *

保護関係の転送ステータスが表示されます。転送ステータスは、次のいずれかになります。

- 中止しています

SnapMirror 転送は有効ですが、チェックポイントの削除を含む転送の中止処理が進行中です。

- チェック中です

デスティネーションボリュームの診断チェックを実行中で、実行中の転送はありません。

- 最終処理中です

SnapMirror 転送が有効になっています。現在 SnapVault 増分転送の転送後のフェーズです。

- アイドル

転送が有効になっており、実行中の転送はありません。

- 同期中

同期関係にある 2 つのボリュームのデータが同期されています。

- 非同期

デスティネーションボリュームのデータがソースボリュームと同期されていません。

- 準備中

SnapMirror 転送が有効になっています。現在 SnapVault 増分転送の転送前のフェーズです。

- キューに登録され

SnapMirror 転送が有効になっています。実行中の転送はありません。

- 休止中です

SnapMirror 転送が無効になっています。実行中の転送はありません。

- 休止中です

SnapMirror 転送を実行中です。追加の転送は無効になります。

- 転送中です

SnapMirror 転送が有効になっており、転送を実行中です。

- 移行中

ソースボリュームからデスティネーションボリュームへの非同期のデータ転送が完了し、同期処理への移行が開始されています。

- 待機中です

SnapMirror 転送は開始されましたが、一部の関連タスクのキュー登録を待っています。

- * 前回の転送時間 *

前回のデータ転送が完了するまでの時間が表示されます。

StrictSync 関係については、転送が同時に行われるため、転送時間は適用されません。

- * 最後の転送サイズ *

前回のデータ転送のサイズがバイト単位で表示されます。

StrictSync 関係については、転送サイズは適用されません。

- メディエーター

メディエーターのステータスが表示されます。

- 該当なし

クラスタがSnapMirror Business Continuityをサポートしていない場合。

- 未設定

このオプションが設定されていない場合や設定されているがデスティネーションクラスタのみが追加されていて、ソースクラスタがUnified Managerに追加されていない場合。

- メディエーターのIPアドレス

設定されている場合は、ソースとデスティネーションの両方のクラスタがUnified Managerに追加されます。

- * 状態 *

SnapMirror 関係または SnapVault 関係の状態が表示されます。「未初期化」、「SnapMirror 済み」、「切断」のいずれかです。ソースボリュームを選択した場合は、関係の状態は適用されず表示されません。

- * 関係の健全性 *

クラスタの関係の健全性が表示されます。

- * 正常でない理由 *

関係が正常な状態でない理由が表示されます。

- * 転送優先順位 *

転送を実行する優先度が表示されます。転送の優先順位は「中」または「低」です。優先順位が「中」の転送は、優先順位が「低」の転送よりも先

同期関係については、すべての転送が同じ優先度で扱われるため、転送の優先度は適用されません。

- * スケジュール *

関係に割り当てられている保護スケジュールの名前が表示されます。

同期関係については、スケジュールは適用されません。

- * バージョンに依存しないレプリケーション *

[はい]、[バックアップオプションあり]、または [なし] のいずれかを表示します。

- * ソースクラスタ *

SnapMirror 関係のソースクラスタの FQDN、短縮名、または IP アドレスが表示されます。

- * ソースクラスタ FQDN *

SnapMirror 関係のソースクラスタの名前が表示されます。

- * ソースノード *

ボリュームの SnapMirror 関係のソースノード名リンクの名前が表示されます。オブジェクトが Storage VM または整合グループの場合は、SnapMirror 関係のノード数リンクが表示されます。

カスタムビューでノード名のリンクをクリックすると、SM-BC 関係に属する整合グループのボリュームを含むストレージオブジェクトの保護を表示および拡張できます。

ノード数のリンクをクリックすると、該当するノードとその関係に関連付けられているノードのページが表示されます。ノード数が 0 の場合、関係に関連付けられているノードがないため、値は表示されません。

- * 宛先ノード *

ボリュームの SnapMirror 関係のデスティネーションノード名リンクの名前が表示されます。オブジェクトが Storage VM または整合グループの場合は、SnapMirror 関係のノード数リンクが表示されます。

ノード数のリンクをクリックすると、該当するノードとその関係に関連付けられているノードのページが表示されます。ノード数が 0 の場合、関係に関連付けられているノードがないため、値は表示されません。

- * デスティネーションクラスタ *

SnapMirror 関係のデスティネーションクラスタの名前が表示されます。

- * デスティネーションクラスタ FQDN *

SnapMirror 関係のデスティネーションクラスタの FQDN、短縮名、または IP アドレスが表示されます。

- * 保護者 *

さまざまな関係が表示されます。この列には、クラスタおよび Storage Virtual Machine のボリュームと整合性グループの関係について、次の順序で表示できます。

- SnapMirror
- Storage VM DR
- SnapMirror、Storage VM DR
- 整合グループ

◦ SnapMirror、整合グループ

- 関連情報 *
- Relationship : MetroCluster *ビューの詳細については、を参照してください "[MetroCluster 構成を監視しています](#)".
- 「* Relationship : Last 1 Month Transfer Status *」ビューの詳細については、を参照してください "[関係 : 過去 1 カ月の転送ステータス画面](#)".
- 「* Relationship : All Relationships *」ビューの詳細については、を参照してください "[関係 : 過去 1 カ月の転送速度ビュー](#)".

関係 : 過去 1 カ月の転送ステータス画面

Relationship : Last 1 month Transfer Status ビューを使用すると、非同期関係にあるボリュームと Storage VM の一定期間の転送の傾向を分析できます。また、転送が成功したか失敗したかが表示されます。

ページの上部にあるコントロールを使用すると、特定のオブジェクトを検索したり、フィルタを作成したり適用して、表示されるデータのリストを絞り込んだり、ページの列を追加/削除/並べ替えたり、ページのデータをエクスポートしたりできます。 .csv、.pdf、または .xlsx ファイル。カスタマイズしたページをカスタムビューとして保存し、データのレポートを定期的に生成して E メールで送信するようにスケジュール設定できます。「* フィルタ *」オプションを使用すると、ボリュームのみ、または Storage VM のみなど、選択したストレージシステムのみを表示できます。ストレージページと、選択したストレージエンティティについてのみ、同じレポートが表示されます。たとえば、ボリューム関係を表示する場合は、Storage VM の Relationship : Last 1 Month Transfer Status レポートにアクセスできます。このレポートは、Storage * > * Storage VM * > * Relationship : Last 1 Month Transfer Status * メニューまたは * Protection * > * Relationships * > * Relationship : Last 1 Month Transfer Status * メニュー。 * Filter * を使用して、ボリュームのデータのみを表示します。

- * ソースボリューム *

ソースボリューム名が表示されます。

- * デスティネーションボリューム *

デスティネーションボリューム名が表示されます。

- * 操作タイプ *

ボリューム転送のタイプが表示されます。

- * 操作結果 *

ボリューム転送が成功したかどうかが表示されます。

- * 転送開始時間 *

ボリューム転送の開始時間が表示されます。

- * 転送終了時間 *

ボリューム転送の終了時間が表示されます。

- * 転送時間 *

ボリューム転送が完了するまでの所要時間（時間）が表示されます。

- * 転送サイズ *

転送されたボリュームのサイズ（MB）が表示されます。

- * ソース SVM *

Storage Virtual Machine（SVM）名が表示されます。

- * ソースクラスタ *

ソースクラスタ名が表示されます。

- * デスティネーション SVM *

デスティネーション SVM 名が表示されます。

- * デスティネーションクラスタ *

デスティネーションクラスタ名が表示されます。

- 関連情報 *

- 「* Relationship：All Relationships *」ビューの詳細については、を参照してください ["関係：すべての関係ビュー"](#)。
- Relationship：metrocluster *ビューの詳細については、を参照してください ["MetroCluster 構成を監視しています"](#)。
- 「* Relationship：All Relationships *」ビューの詳細については、を参照してください ["関係：過去 1 カ月の転送速度ビュー"](#)。

関係：過去 1 カ月の転送速度ビュー

Relationship：Last 1 month Transfer Rate ビューを使用すると、非同期関係にあるボリュームについて、転送されるデータボリュームの量を 1 日単位で分析できます。また、このページには、毎日の転送に関する詳細およびボリュームと Storage VM の転送処理を完了するために必要な時間が表示されます。

ページ上部のコントロールを使用すると、特定のオブジェクトの検索、フィルタの作成と適用による表示データの絞り込み、ページ上の列の追加と削除 / 並べ替え、ページ上のデータの .csv、.pdf、.xlsx ファイルへのエクスポートを実行できます。カスタマイズしたページをカスタムビューとして保存し、データのレポートを定期的に生成して E メールで送信するようにスケジュール設定できます。たとえば、ボリュームの関係を表示するには、* Storage * > * Volumes * > * Relationship：Last 1 Month Transfer Rate * メニュー、または * Protection * > * Relationships：Last 1 Month Transfer Rate * メニューのいずれかにアクセスし、* Filter * を使用してボリュームのデータのみを表示できます。

- * 合計転送サイズ *

ボリューム転送の合計サイズがギガバイト単位で表示されます。

- * 日 *

ボリューム転送が開始された日にちが表示されます。

- * 終了時間 *

ボリューム転送が終了した日時が表示されます。

- 関連情報 *

- Relationship : metrocluster *ビューの詳細については、を参照してください "[MetroCluster 構成を監視しています](#)"。
- 「* Relationship : Last 1 Month Transfer Status *」 ビューの詳細については、を参照してください "[関係：過去 1 カ月の転送ステータス画面](#)"。
- 「* Relationship : All Relationships *」 ビューの詳細については、を参照してください "[関係：過去 1 カ月の転送速度ビュー](#)"

カスタムレポートを生成

Unified Manager のレポート機能

Active IQ Unified Manager（旧 OnCommand Unified Manager）では、ONTAP ストレージシステムのレポートを表示、カスタマイズ、ダウンロード、およびスケジュール設定できます。レポートには、ストレージシステムの容量、健全性、パフォーマンス、セキュリティ、保護関係に関する詳細を表示できます。

Active IQ Unified Manager 9.6 で導入された新しい Unified Manager レポート作成機能およびスケジュール設定機能は、Unified Manager バージョン 9.5 で廃止された以前のレポート作成エンジンに代わるものです。

レポート機能は、ネットワークのさまざまなビューを提供し、容量、健全性、パフォーマンス、セキュリティ、保護データに関する実用的な情報を提供します。列の表示、非表示、再配置、データのフィルタリング、データのソート、検索結果を表示します。カスタムビューは、再利用できるように保存したり、レポートとしてダウンロードしたりできます。また、定期的なレポートとしてスケジュールを設定して、E メールで配布することもできます。

Microsoft® Excel 形式のビューをダウンロードしてカスタマイズできます。複雑な並べ替え、レイヤーフィルター、ピボットテーブル、グラフなど、Excel の高度な機能を使用できます。結果の Excel レポートに問題がなければ、レポートがスケジュールされて共有されるたびに使用する Excel ファイルをアップロードできます。

Unified Manager では、ユーザインターフェイスからレポートを生成する以外にも、次の方法を使用して健全性、セキュリティ、およびパフォーマンスのデータを抽出できます。

- Open Database Connectivity（ODBC）および ODBC のツールを使用してデータベースに直接アクセスし、クラスタ情報を取得する
- Unified Manager REST API を使用して確認したい情報を取得する

このリリースの Active IQ Unified Manager では、レポートの機能が次のように拡張されています。

- 設定したスケジュールに従ってレポートの E メールが送信されます。オンデマンドレポートを生成した場合でも、E メールが送信されます。
- レポートのファイル名とレポートのメタデータには、レポートの生成元のホスト名が含まれます。ファイル名が変更された場合でも、この機能強化によりレポートの生成元のホスト名を特定できます。

レポートを生成するためのアクセスポイント

クラスタに関する情報を Unified Manager で収集して、UI、MySQL データベースクエリ、REST API からレポートを作成できます。

ここでは、Unified Manager の UI を使用したレポート作成とスケジュール設定について説明します。

Unified Manager が提供するレポート機能には、次の 3 つの方法でアクセスできます。

- UI のインベントリページからデータを直接抽出する。
- Open Database Connectivity（ODBC）および ODBC のツールを使用して、使用可能なすべてのオブジ

ェクトにアクセスする。

- Unified Manager REST API を使用して確認したい情報を取得する。

ここでは、Unified ManagerのUIを使用したレポート作成とスケジュール設定について説明します。

カスタムレポートを作成するために **Unified Manager** データベースにアクセスできる

Unified Manager では、監視対象のクラスタからのデータを MySQL データベースを使用して格納します。データは MySQL データベースのさまざまなスキーマに永続化されます。

次のデータベースからすべてのテーブルデータを使用できます。

データベース	説明
NetApp _ モデル	ONTAP コントローラのオブジェクトに関するデータ。
NetApp_model_view	レポートツールの消費に適した、ONTAP コントローラ上のオブジェクトに関するデータ。
パフォーマンス	クラスタ固有のパフォーマンスカウンタ。
ocum	Unified Manager のアプリケーションデータと、UI で一部の派生フィールドのフィルタ、ソート、計算に使用される情報。
ocum_report	インベントリの設定と容量に関連する情報のデータ。
ocum_report_BIRT	レポートツールの消費に適した、インベントリの構成と容量に関連するデータのビュー。
OPM	パフォーマンスの設定としきい値の情報。
頭皮管理者	Unified Manager のアプリケーションの健全性とパフォーマンスの問題に関するデータ。
vmware_model	ネットアップストレージでホストされているデータストアの VMware オブジェクトデータ。
vmware_model_view	ネットアップストレージにホストされているデータストアの VMware オブジェクトデータ用ビュー。レポートツールの利用に適しています。
VMWARE_performance	ネットアップストレージでホストされているデータストアの VMware パフォーマンスカウンタデータ。

レポートスキーマロールを持つデータベースユーザーであるレポートユーザーは、これらのテーブルのデータにアクセスできます。このユーザには、レポートおよびその他のデータベースビューに Unified Manager データベースから直接アクセスするための読み取り専用アクセスが付与されます。このユーザには、ユーザデータやクラスタクレデンシャル情報を含むテーブルにアクセスする権限はありません。

レポート作成に使用できる Unified Manager REST API

REST API を使用すると、Unified Manager で収集された健全性、容量、パフォーマンス、セキュリティの情報を確認することができ、クラスタの管理に便利です。

REST API は Swagger Web ページから利用できます。Unified Manager REST API ドキュメントを表示する場合、および API 呼び出しを手動で問題する場合は、Swagger Web ページにアクセスします。Unified Manager Web UI のメニューバーで、* ヘルプ * ボタンをクリックし、* API ドキュメント * を選択します。Unified Manager REST API については、を参照してください "[Active IQ Unified Manager REST API の使用を開始する](#)"。

REST API にアクセスするには、オペレータ、ストレージ管理者、またはアプリケーション管理者のロールが必要です。

レポートの概要

レポートには、ストレージ、ネットワーク、サービス品質、および保護関係に関する詳細情報が表示されます。これにより、潜在的な問題を発生前に特定して解決することができます。

ビューをカスタマイズする場合は、後で使用できるように一意の名前で保存できます。このビューに基づいてレポートを定期的に行うようにスケジュール設定し、他のユーザと共有することができます。また、Excel 形式のビューをダウンロードして高度な Excel 機能を使用してカスタマイズし、そのファイルを Unified Manager にアップロードし直すこともできます。そのビューを使用してレポートをスケジュールすると、アップロードした Excel ファイルを使用して、共有可能な堅牢なレポートが作成されます。

スケジュールされたすべてのレポートは、[Report Schedules] ページで管理できます。



レポートを管理するには、アプリケーション管理者またはストレージ管理者のロールが必要です。

レポートは、カンマ区切り値（CSV）、Excel、または PDF ファイルとしてダウンロードできます。

ビューとレポートの関係を理解する必要があります

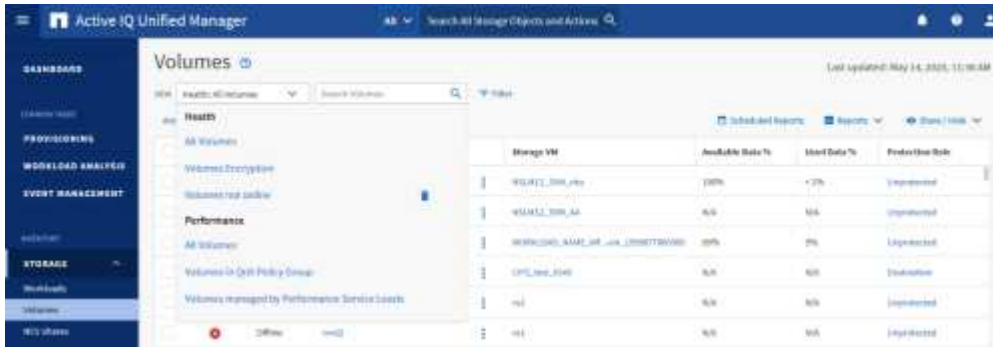
ビューとインベントリページは、ダウンロードまたはスケジュール設定したレポートになります。

ビューとインベントリページはカスタマイズして保存し、再利用することができます。Unified Manager で表示できるほぼすべての情報を、レポートとして保存、再利用、カスタマイズ、スケジュール設定、共有できます。

ビューのドロップダウンでは、削除アイコンが表示されている項目は、自分または他のユーザーが作成した既存のカスタムビューです。アイコンのない項目は、Unified Manager のデフォルトビューです。デフォルトビューは変更または削除できません。



- リストからカスタムビューを削除すると、そのビューを使用する Excel ファイルやスケジュール済みレポートも削除されます。
- カスタムビューを変更した場合、そのビューを使用するレポートに変更が反映されるのは、レポートスケジュールに従って次回レポートが生成されて E メールで送信されることです。ビューを変更するときは、レポートに使用される関連する Excel のカスタマイズが変更されていることを確認してください。必要に応じて、Excel ファイルをダウンロードして必要な変更を加え、ビューの新しい Excel カスタマイズとしてアップロードすることで、Excel ファイルを更新できます。



削除アイコンが表示され、ビューやスケジュール済みレポートを変更したり削除したりできるのは、アプリケーション管理者ロールまたはストレージ管理者ロールのユーザだけです。

レポートのタイプ

この表には、カスタマイズ、ダウンロード、およびスケジュール設定が可能なレポートとして使用できるビューとインベントリページの包括的なリストが表示されます。

Active IQ Unified Manager レポート

を入力します	ストレージまたはネットワークオブジェクト
容量	クラスタ アグリゲート 個のボリューム qtree

を入力します	ストレージまたはネットワークオブジェクト
健全性	クラスタ ノード アグリゲート Storage VMs 個のボリューム SMB/CIFS 共有 NFS 共有
パフォーマンス	クラスタ ノード アグリゲート Storage VMs 個のボリューム LUN NVMe ネームスペース ネットワークインターフェイス（LIF） ポート
Quality of Service の略	従来の QoS ポリシーグループ アダプティブ QoS ポリシーグループ パフォーマンスサービスレベルポリシーグループ
ボリューム保護関係（Volumes（ボリューム）ページで確認可能）	すべての関係 過去 1 カ月の転送ステータス 過去 1 カ月の転送速度です
セキュリティ	Storage VMs クラスタ

レポート機能の制限事項

Active IQ Unified Manager の新しいレポート機能には、注意が必要な制限事項があります。

以前のバージョンの **Unified Manager** で作成した既存のレポート

スケジュールと受信者を編集できるのは、Unified Manager 9.5 以前のリリースで作成およびインポートされた既存のレポート（.rptdesign ファイル）のみです。Unified Manager 9.5 以前の標準レポートをカスタマイズしたレポートは、新しいレポートツールにインポートされません。

rptdesign ファイルからインポートした既存のレポートを編集する必要がある場合は、次のいずれかの操作を行って、インポートしたレポートを削除します。

- 新しいビューを作成し、そのビューからレポートのスケジュールを設定する（推奨）
- レポートにカーソルを合わせ、SQL をコピーして、外部ツールを使用してデータを抽出します

デフォルトビューは、カスタマイズすることなくレポートとして生成できます。新しいレポート用解決策を使用して、カスタムレポートを再作成できます。

スケジュールとレポートの関係

保存したレポートごとに、受信者を任意に組み合わせて複数のスケジュールを作成できます。ただし、スケジュールを複数のレポートで再利用することはできません。

レポートの保護

適切な権限を持つユーザは、レポートを編集または削除できます。保存したビューやスケジュールを他のユーザが削除または変更できないようにする方法はありません。

イベントレポート

イベントビューをカスタマイズしてレポートを CSV 形式でダウンロードすることはできますが、イベントレポートを繰り返し生成して配信するようにスケジュール設定することはできません。

レポートの添付

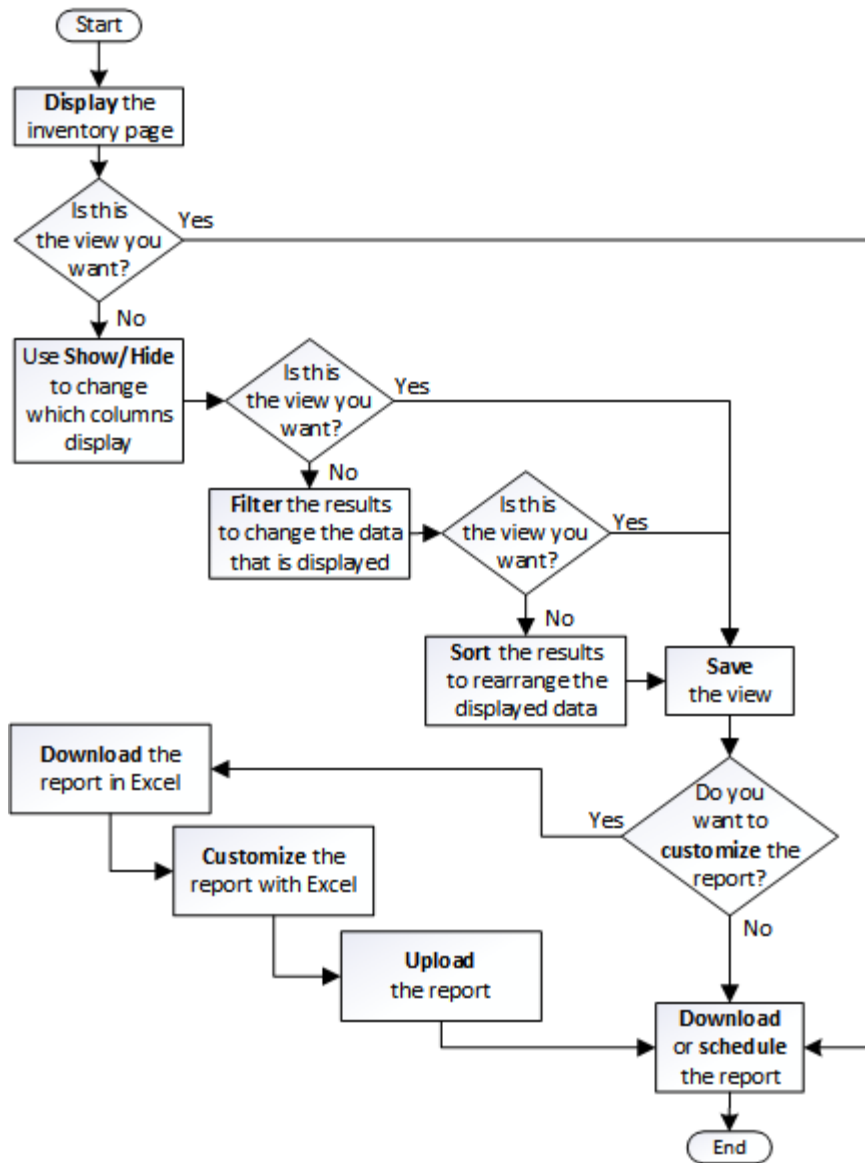
レポートを E メール本文として送信することはできません。代わりに、レポートは PDF、Excel、または CSV 形式の添付ファイルとしてのみ送信されます。

レポートの操作

共有可能なスケジュール済みレポートにインベントリページビューを見つけてカスタマイズする方法について説明します。

レポートワークフロー

レポートのワークフローを説明するデシジョンツリー。



レポートのクイックスタート

サンプルのカスタムレポートを作成して、各ビューの内容とレポートのスケジュール設定について学びます。このクイックスタートのレポートでは、アクセス頻度の低いワールドデータが相当量あり、クラウド階層への移動を検討するボリュームを特定します。Performance : All Volumes ビューを開き、フィルタと列を使用してビューをカスタマイズし、カスタムビューをレポートとして保存し、レポートを週に 1 回共有するようにスケジュール設定します。

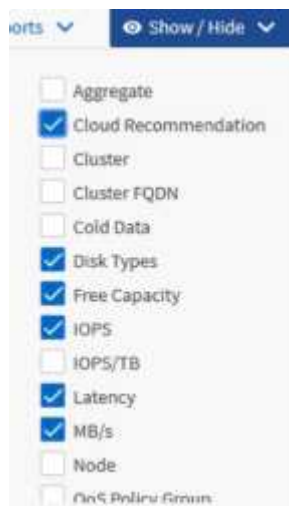
- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- FabricPool アグリゲートを設定しておく必要があります。また、それらのアグリゲート上にボリュームが必要です。

以下の手順に従って、次の操作を実行します。

- デフォルトビューを開きます
- データをフィルタおよびソートして列をカスタマイズします
- ビューを保存します
- カスタムビューに対して生成されるようにレポートをスケジュール設定します

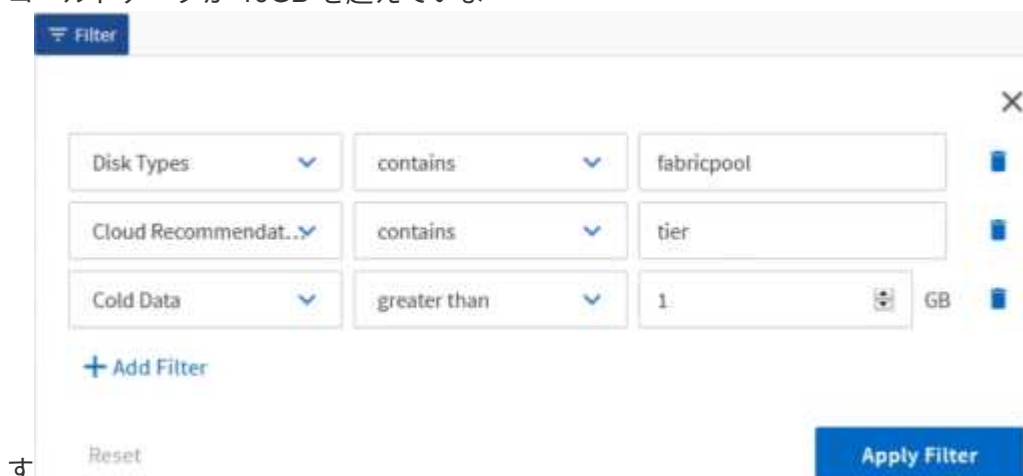
手順

1. 左側のナビゲーションペインで、 * Storage * > * Volumes * をクリックします。
2. [表示] メニューで、 [* パフォーマンス > すべてのボリューム *] を選択します。
3. 「ディスクタイプ」列がビューに表示されることを確認するには、「 * 表示 / 非表示 * 」をクリックします。



他の列を追加または削除して、レポートに必要なフィールドを含むビューを作成します。

4. 「クラウドのおすすめ」列の横にある「ディスクの種類」列をドラッグします。
5. フィルタアイコンをクリックして次の 3 つのフィルタを追加し、 * フィルタの適用 * をクリックします。
 - ディスクタイプには FabricPool が含まれます
 - クラウドに関する推奨事項に階層が含まれて
 - コールドデータが 10GB を超えています



各フィルタは論理積で結合され、すべての条件を満たすボリュームだけが返されます。最大 5 つのフィルタを追加できます。

6. コールドデータ列の上部をクリックして結果をソートし、コールドデータが最も多いボリュームがビューの上部に表示されるようにします。
7. ビューをカスタマイズすると、ビュー名は [保存されていないビュー] になります。ビューに表示されているビューを反映する名前を付けますたとえば 'Vols change tiering policy' のように指定します完了したら、チェックマークをクリックするか、* Enter * キーを押してビューを新しい名前で保存します。

Volumes - Performance / Vols change tiering policy ⓘ Last updated: Feb 8, 2019, 12:26 PM ↻

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View Vols change tiering policy 🔍 Search Volumes ⚙️

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports Reports Show/Hide

Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagntsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

8. レポートを * CSV *、* Excel *、または * PDF * ファイルとしてダウンロードし、スケジュール設定または共有する前に出力を確認します。

Microsoft Excel（CSV または Excel）や Adobe Acrobat（PDF）などのインストールされているアプリケーションでファイルを開くか、ファイルを保存します。



ビューを Excel ファイルとしてダウンロードすると、複雑なフィルタ、ソート、ピボットテーブル、グラフを使用してレポートをさらにカスタマイズできます。Excel でファイルを開いたら、高度な機能を使用してレポートをカスタマイズします。問題がなければ、Excel ファイルをアップロードします。このファイルはカスタマイズされており、レポートの実行時にビューに適用されます。

Excel を使用したレポートのカスタマイズの詳細については、_ Microsoft Excel レポートのサンプル _ を参照してください。

9. インベントリページの * スケジュール済みレポート * ボタンをクリックします。オブジェクトに関連するスケジュール済みレポート（この場合はボリューム）がすべてリストに表示されます。

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports

Volumes - Scheduled Reports View all Scheduled Reports

Add Schedule

Schedule Name	View	Recipients	Frequency	Format	
Weekly / Vols c... tiering policy	Performance / V... tiering policy	user@company.com	Weekly - Monday 1:00 PM	CSV	⋮

10. [レポートスケジュール] ページに新しい行を追加して、新しいレポートのスケジュール特性を定義できるようにするには、[スケジュールの追加] をクリックします。
11. レポートの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

CSV 形式のサンプルレポートを次に示します。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:52 PM - March 28, 2019, 12:52 PM)																
2	Generated At: March 28, 2019, 12:52 PM																
3																	
4	Status	Volume	Volume Id	Tiering Po	Cold Data	Free Capa	Total Capa	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id				
5	Ok	kjagnfsdst	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040				
6	Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141				
	performance-volumes-28-Mar-2019																

PDF 形式のサンプルレポートを次に示します。

Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:51 PM - March 28, 2019, 12:51 PM)
Generated At: March 28, 2019, 12:51 PM

Status	Volume	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	Cluster	Node	Aggregate
Ok	kjagnfsdst	Snapshot Only	28.01	121.32	150	ocum-mo	ocum-mo	aggr5_vs
Ok	nfs_vol4	Snapshot Only	379.64	2676.57	3072	ocum-mo	ocum-mo	aggr4

レポートに表示された結果を基に、ONTAP システムマネージャまたは ONTAP CLI を使用して、特定のボリュームの階層化ポリシーを「auto」または「all」に変更し、より多くのコールドデータをクラウド階層にオフロードできます。

スケジュール済みレポートを検索しています

スケジュール済みレポートは、名前、ビュー名、オブジェクトタイプ、または受信者で検索できます。

1. 左側のナビゲーションペインで、* ストレージ管理 * > * レポートスケジュール * をクリックします。
2. [スケジュール済みレポートの検索 *] テキストフィールドを使用します。

レポートを検索する条件	試用してください
スケジュール名	レポートスケジュール名の一部を入力します。
ビュー名	レポートビュー名の一部を入力します。デフォルトビューとカスタムビューがビューリストに表示されます。
受信者	E メールアドレスの一部を入力します。
ファイルタイプ	「PDF」、「CSV」、または「XLSX」と入力します。

3. 列見出しをクリックすると、その列でスケジュール名や形式などのレポートを昇順または降順でソートできます。

レポートのカスタマイズ

さまざまな方法でビューをカスタマイズして、ONTAP クラスターの管理に必要なすべて

の情報を含むレポートを作成できます。

デフォルトのインベントリページまたはカスタムビューで開始し、列の追加や削除、列の順序変更、データのフィルタリング、特定の列での昇順または降順のソートなどを行ってカスタマイズします。

Unified Manager 9.8 以降では、Excel のビューをダウンロードして、高度な機能を使用してカスタマイズすることもできます。完了したら、カスタマイズした Excel ファイルをアップロードします。そのビューを使用してレポートをスケジュールすると、カスタマイズした Excel ファイルを使用して、共有可能な堅牢なレポートが作成されます。

Excel を使用したレポートのカスタマイズの詳細については、[_ Microsoft Excel レポートのサンプル _](#)を参照してください。



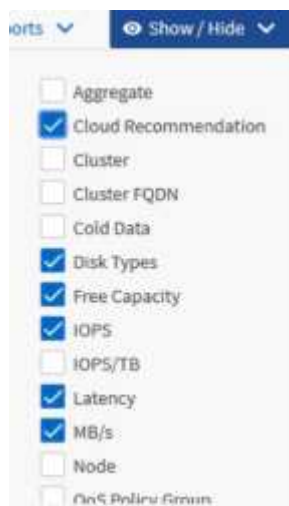
レポートを管理するには、アプリケーション管理者またはストレージ管理者のロールが必要です。

列のカスタマイズ

***Show/Hide *** を使用して、レポートで使用する列を選択します。インベントリページで列をドラッグして並べ替えることができます。

手順

1. 列を追加または削除するには、*** 表示 / 非表示 *** をクリックします。



2. インベントリページで、列をドラッグしてレポートに必要な順序に並べ替えます。
3. 保存されていないビューに名前を付けて変更を保存します。

データのフィルタリング

データをフィルタして、レポートの要件を満たしていることを確認します。フィルタリングすることで関心のあるデータのみを表示できます。

手順

1. フィルタアイコンをクリックして、表示する結果を絞り込むフィルタを追加し、*** フィルタの適用 *** をクリックします。

Filter

Disk Types	contains	fabricpool
Cloud Recommendation	contains	tier
Cold Data	greater than	1 GB

+ Add Filter

Reset Apply Filter

2. 保存されていないビューに名前を付けて変更を保存します。

データのソート

結果をソートするには、列をクリックし、昇順または降順を指定します。データをソートすることで、レポートに必要な情報に優先順位を付けることができます。

手順

1. 列の上部をクリックして結果をソートし、最も重要な情報がビューの上部に表示されるようにします。
2. 保存されていないビューに名前を付けて変更を保存します。

検索を使用してビューを絞り込みます

目的のビューが表示されたら、[検索] フィールドを使用してレポートに含める結果を絞り込むことができます。

手順

1. レポートのベースとして使用するカスタムビューまたはデフォルトビューを開きます。
2. 検索フィールドに入力して、ビューに表示されるデータを絞り込みます。表示されている任意の列に部分データを入力できます。たとえば、名前に「US_East」を含むノードを検索するには、全ノードのリストを絞り込むことができます。

検索結果はカスタムビューに保存され、スケジュール済みレポートで使用されます。

3. 保存されていないビューに名前を付けて変更を保存します。

Excel を使用してレポートをカスタマイズする

ビューを保存したら、Excel ワークブック形式（.xlsx）でダウンロードできます。Excel ファイルを開くと、Excel の高度な機能を使用してレポートをカスタマイズできます。

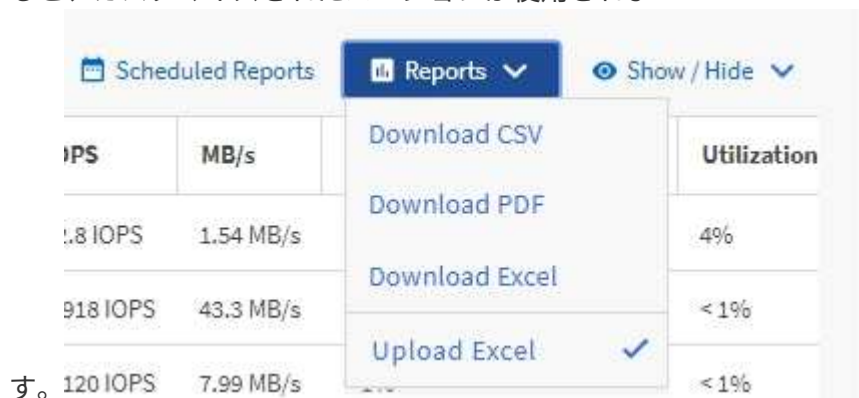
- 必要なもの *

アップロードできるのは、拡張子が .xlsx の Excel ブックファイルのみです。

たとえば、レポートで使用できる Excel の高度な機能には、次のものがあります。

- 複数列ソート
- 複雑なフィルタリング
- ピボットテーブル
- グラフ

- ダウンロードした Excel ファイルでは、保存した名前ではなく、ビューのデフォルトのファイル名が使用されます。
 - の形式で指定します <View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx.
 - たとえば、という名前のカスタム保存ビューがあります Volumes-not online には、というファイル名が付けられています health-volumes-05-May-2020-19-18-00.xlsx その日時に保存した場合。
- Excel ファイルにシートを追加できますが、既存のシートは変更しないでください。
 - 既存のシート、データ、および情報は変更しないでください。代わりに、作成した新しいページにデータをコピーします。
 - 上記の規則の例外の 1 つは、「data」ページで数式を作成できることです。データページの数式を使用して、新しいページにグラフを作成します。
 - 新しいシートデータや情報に名前を付けしないでください。
- カスタマイズされた Excel ファイルが存在する場合は、[* レポート > Excel * のアップロード]メニュー項目の横にチェックマークが表示されます。Excel ファイルをダウンロードすると、カスタマイズされたバージョンが使用されま



手順

1. レポートのベースとして使用するデフォルトビュー、カスタムビュー、または保存ビューを開きます。
2. [* レポート >] > [Excel のダウンロード *] を選択します。
3. ファイルを保存します。ファイルがダウンロードフォルダに保存されます。
4. 保存したファイルを Excel で開きます。ファイルを新しい場所に移動しないでください。別の場所で作業を行っている場合は、ファイルをアップロードする前に元のファイル名を使用してファイルを元の場所に保存し直してください。
5. 複雑な並べ替え、レイヤーフィルター、ピボットテーブル、グラフなどの Excel 機能を使用して、ファイルをカスタマイズします。詳細については、Microsoft® Excel のマニュアルを参照してください。

6. *Reports *>*Upload Excel * を選択し、変更したファイルを選択します。最新のダウンロード済みファイルは、同じファイルの場所からアップロードされます。
7. スケジュールレポート機能を使用して、テストレポートを送信します。

レポートのダウンロード

レポートをダウンロードして、データをカンマ区切り値（CSV）ファイル、Microsoft Excel（.xlsx）ファイル、または PDF ファイルとしてローカルドライブまたはネットワークドライブに保存できます。CSV ファイルと XLSX ファイルは、Microsoft Excel などのスプレッドシートアプリケーションで、PDF ファイルは Adobe Acrobat などのリーダーで開くことができます。

手順

1. [*Reports] ボタンをクリックして、次のいずれかの方法でレポートをダウンロードします。

を選択します	目的
CSV をダウンロードします	レポートを CSV ファイルとして保存します。
PDF をダウンロードします	レポートを .pdf ファイルで保存します。
Excel をダウンロードします	レポートを Microsoft Excel (XLSX) ファイルとして保存します。

レポートのスケジュール設定

レポートとして再利用して共有したいビューがある場合は、Active IQ Unified Manager を使用してそのビューをスケジュール設定できます。スケジュールされたレポートの管理、各レポートスケジュールの受信者と配信頻度の変更が可能です。

Unified Manager では、ほとんどのビューまたはインベントリページをスケジュール設定できます。ただしイベントだけは例外で、CSV ファイルとしてダウンロードすることはできますが、スケジュール設定して再生成および共有することはできません。また、ダッシュボード、お気に入り、設定ページをダウンロードしたり、スケジュール設定したりすることもできません。

Active IQ Unified Manager 9.8 以降では、Microsoft® Excel 形式のビューをダウンロードしてカスタマイズできます。複雑な並べ替え、レイヤーフィルター、ピボットテーブル、グラフなど、Excel の高度な機能を使用できます。結果の Excel レポートに問題がなければ、レポートがスケジュールされて共有されるたびに使用する Excel ファイルをアップロードできます。

組み込みのビューまたはカスタマイズしたビューをスケジュールできます。送信するファイルの種類として、CSV、PDF、または XSLX を選択できます。初めてレポートをスケジュールする場合は、レポートをダウンロードして自分だけを受信者に割り当て、受信者に表示されるレポートを確認することができます。

レポートのスケジュール設定

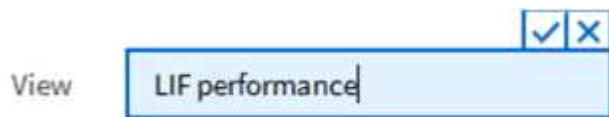
定期的に生成および配布するようにスケジュールするビューまたは Excel ファイルがある場合は、レポートのスケジュールを設定できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- レポート作成エンジンがリスト内の受信者に Unified Manager サーバから E メール添付ファイルとしてレポートを送信できるように、* General * > * Notifications * ページで SMTP サーバを設定しておく必要があります。
- 生成された E メールで添付ファイルを送信できるように E メールサーバを設定する必要があります。

次の手順に従って、ビューに対して生成するレポートをテストし、スケジュール設定します。使用するビューを選択またはカスタマイズします。次の手順ではネットワークインターフェイスのパフォーマンスを表示するネットワークビューを使用していますが、任意のビューを使用できます。

手順

1. ビューを開きます。この例では、LIF のパフォーマンスを表示するデフォルトのネットワークビューを使用します。左側のナビゲーションペインで、* Network > Network Interfaces * をクリックします。
2. 組み込みの Unified Manager 機能を使用して、必要に応じてビューをカスタマイズします。
3. カスタマイズしたビューは、[* 表示 * (* View *)] フィールドに一意の名前を入力し、チェックマークをクリックして保存できます。



4. Microsoft® Excel の高度な機能を使用して、レポートをカスタマイズできます。詳細については、["Excel を使用してレポートをカスタマイズする"](#)を参照してください。
5. 出力をスケジュールまたは共有する前に表示するには、次の手順を実行します。

オプション	説明
• レポートのカスタマイズに Excel を使用した場合 *	ダウンロードした既存の Excel ファイルを表示します。
• レポートのカスタマイズに Excel を使用しなかった場合 *	レポートを * CSV *、* PDF *、または * XLSX * ファイルとしてダウンロードします。

Microsoft Excel（CSV/XSLX）や Adobe Acrobat（PDF）など、インストールされているアプリケーションでファイルを開きます。

6. レポートに問題がなければ、[スケジュール済みレポート] をクリックします。
7. [レポートスケジュール] ページで、[スケジュールの追加] をクリックします。
8. ビュー名と頻度を組み合わせたデフォルト名をそのまま使用するか、または * スケジュール名 * をカスタマイズします。

9. スケジュール済みレポートを初めてテストするには、自分自身を * Recipient * としてだけ追加します。問題がなければ、すべてのレポート受信者の E メールアドレスを追加します。
10. レポートを生成して受信者に送信する頻度を指定します。「* Daily 」、「* Weekly 」、または「* Monthly 」、を選択できます。
11. フォーマットとして、**PDF**、**csv**、または**XSLX**を選択します。



Excel を使用してコンテンツをカスタマイズしたレポートの場合は、常に「* XSLX*」を選択します。

12. チェックマーク (✓) をクリックしてレポートスケジュールを保存します。

LIFs - Scheduled Reports View all Scheduled Reports

Add Schedule

Schedule Name	View	Recipients	Frequency	Format
Weekly / LIF performar	Performance / LIF pe ▼	test@inetapp.com	Weekly ▼ Thursda ▼ 4:30 PM ▼	PDF ▼

✓ ✕

レポートはテストとしてすぐに送信されます。その後、スケジュールされた頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

インポートした .rptdesign レポートのスケジュール設定

以前のリリースの Unified Manager で作成およびインポートした既存のレポートをスケジュールできます。

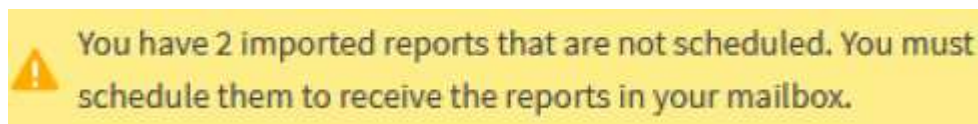
インポートしたレポートをスケジュール設定するには、次のもの

- 以前の Unified Manager リリースで設計し、インポートした .rptdesign ファイルレポート
- Unified Manager 9.6 GA 以降にアップグレードする場合に該当します

Unified Manager 9.6 GA 以降にアップグレードすると、レポートスケジュールページにインポートしたレポートが表示されます。これらのレポートのスケジュールを編集して、受信者の E メールアドレス、頻度、形式（PDF または CSV）を指定できます。これらの編集をしていないレポートは、Unified Manager UI で編集または表示できません。

手順

1. [レポートスケジュール] ページを開きます。インポートしたレポートがある場合は、メッセージが表示されます。



2. **View** 名をクリックして、レポートの生成に使用されている SQL クエリを表示します。

**Imported Report**

This report is generated using following database query:

```
SELECT c.name AS 'Cluster', m.name AS 'SVM', v.name AS 'Volume', s.name AS 'Share',
s.path AS 'Path', q.name AS 'Qtree', s.shareProperties AS 'Properties', a.userOrGroup
AS 'User', a.permission AS 'Permission' FROM ocum_report.cifsshare s JOIN
ocum_report.cifsshareacl a ON s.id = a.cifsShareId JOIN ocum_report.cluster c ON
s.clusterId = c.id JOIN ocum_report.svm m ON s.svmId = m.id JOIN
ocum_report.volume v ON s.volumeId = v.id JOIN ocum_report.qtree q ON s.qtreeId =
q.id
```

3. [詳細] アイコンをクリックします ⓘ をクリックし、* Edit * をクリックしてレポートスケジュールの詳細を定義し、レポートを保存します。



[詳細] アイコンから不要なレポートを削除することもできます ⓘ。

レポートスケジュールの管理

レポートスケジュールは、[Report Schedules] ページで管理できます。既存のスケジュールは、表示、変更、または削除することができます。

- 必要なもの *



[レポートスケジュール] ページから新しいレポートをスケジュールすることはできません。スケジュール済みレポートは、オブジェクトインベントリページからのみ追加できます。

- アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* ストレージ管理 * > * レポートスケジュール * をクリックします。
2. [レポートスケジュール (Report Schedules)] ページで、次

状況	作業
既存のスケジュールを表示します	スクロールバーとページコントロールを使用して、既存のレポートのリストをスクロールします。

状況	作業
既存のスケジュールを編集します	<ol style="list-style-type: none"> [詳細] アイコンをクリックします  をクリックします。 [編集 (Edit)] をクリックします。 必要な変更を行います。 チェックマークをクリックして変更を保存します。
既存のスケジュールを削除します	<ol style="list-style-type: none"> [詳細] アイコンをクリックします  をクリックします。 [削除 (Delete)] をクリックします。 操作を確定します。

スケジュール済みレポートの編集

スケジュールされたレポートは、[レポートスケジュール] ページで編集できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、 * ストレージ管理 * > * レポートスケジュール * をクリックします。


Scheduled Reports

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Search Scheduled Reports					
Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	



適切な権限があれば、システム内のすべてのレポートとそのスケジュールを変更できます。

2. [詳細] アイコンをクリックします  をクリックします。
3. [編集 (Edit)] をクリックします。
4. レポートスケジュールの * スケジュール名 *、* 受信者 * リスト、* 頻度 *、* 形式 * を変更できます。
5. 完了したら、チェックマークをクリックして変更を保存します。

スケジュール済みレポートの削除

スケジュールされたレポートは、[レポートスケジュール] ページから削除できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、* ストレージ管理 * > * レポートスケジュール * をクリックします。

Scheduled Reports ⓘ

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Search Scheduled Reports					
Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	⋮
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	⋮
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	⋮



適切な権限があれば、システム内のすべてのレポートとそのスケジュールを削除できます。

2. [詳細] アイコンをクリックします ⋮ をクリックします。
3. [削除 (Delete)] をクリックします。
4. 操作を確定します。

スケジュール済みレポートがリストから削除され、設定したスケジュールで生成および配布されなくなります。



インベントリページからカスタムビューを削除すると、そのビューを使用するカスタム Excel ファイルまたはスケジュール済みレポートもすべて削除されます。

サンプルのカスタムレポート

以下に記載するサンプルのカスタムレポートを使用して、潜在的な問題を発生前に特定して対処することができます。

このセクションのレポートリストはすべてのレポートを網羅しているわけではなく、今後も増えていきます。このセクションに追加して欲しいカスタムレポートがあれば、ドキュメントに関するフィードバックの形で提案していただくことができます。



レポートを管理するには、アプリケーション管理者またはストレージ管理者のロールが必要です。

クラスタストレージレポートのカスタマイズ

このセクションのクラスタストレージレポートは、それぞれのストレージシステムリソースの監視に役立つクラスタ容量に関するレポートの作成方法を説明するためのサンプルです。

容量をクラスタモデル別に表示するレポートの作成

クラスタのストレージ容量と使用状況をストレージシステムモデルに基づいて分析するためのレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、クラスタモデル別に容量を表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、*** Storage * > * Clusters *** をクリックします。
2. 表示メニューで、*** 容量 * > * すべてのクラスタ *** を選択します。
3. 「クラスタ FQDN」や「OS バージョン」など、レポートに不要な列を削除するには、「*** 表示 / 非表示 ***」を選択します。
4. 「合計物理容量」列、「モデル / ファミリー」列、および「クラスタ」列の近くにある 3 つの集計列をドラッグします。
5. 「**Model/Family**」列の上部をクリックして、クラスタタイプ別に結果をソートします。
6. 表示されているビューの名前を反映した名前で見えを保存します（例：「**Capacity by Cluster Model**」）。
7. インベントリページの *** スケジュール済みレポート *** ボタンをクリックします。
8. [*** スケジュールの追加 ***] をクリックして、新しいレポートのスケジュール特性を定義できるように、[**レポートスケジュール ***] ページに新しい行を追加します。
9. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、特定のクラスタに容量を追加したり、古いクラスタモデルをアップグレードしたりすることができます。

未割り当ての LUN 容量が最も多いクラスタを特定するレポートの作成

未割り当ての LUN 容量が 5 TB を超えているクラスタを検出するレポートを作成して、ワークロードを追加できる場所を特定できます。

- 必要な情報 ** アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、未割り当ての LUN 容量が最も多いクラスタを表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Clusters * をクリックします。
2. 表示メニューで、* 容量 * > * すべてのクラスタ * を選択します。
3. レポートに不要な列を削除するには、[* 表示 / 非表示 *]を選択します。
4. 「未割り当ての LUN 容量」列を「HA ペア」列の近くにドラッグします。
5. フィルタアイコンをクリックして次のフィルタを追加し、* フィルタの適用 * をクリックします。
 - 未割り当ての LUN 容量が 0.5TB を超えている
6. 未割り当ての LUN 容量が多い順に結果をソートするには '未割り当ての LUN 容量列の上部をクリックします
7. ビューに表示されている内容を反映した特定の名前でビューを保存します (「配分されていない LUN の容量」など)。チェックマーク (✓) をクリックします。
8. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
9. [レポートスケジュール] ページに新しい行を追加して、新しいレポートのスケジュール特性を定義できるようにするには、[スケジュールの追加] をクリックします。
10. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、クラスタの未割り当て LUN 容量を使用できます。

使用可能な容量が最も多い HA ペアを表示するレポートの作成

新しいボリュームや LUN のプロビジョニングに使用できる容量が最も多いハイアベイラビリティ (HA) ペアを検出するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、新しいボリュームや LUN のプロビジョニングに使用できる容量が多い順に HA ペアをソートして表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Clusters * をクリックします。
2. 表示メニューで、* 容量 * > * すべてのクラスタ * を選択します。
3. レポートに不要な列を削除するには、[* 表示 / 非表示 *]を選択します。
4. 「アグリゲート未使用容量」列を「HA ペア」列の近くにドラッグします。
5. フィルタアイコンをクリックして次のフィルタを追加し、* フィルタの適用 * をクリックします。

。アグリゲートの未使用容量が 0.5TB を超えている

6. 「アグリゲート - 未使用容量」列の上部をクリックして、未使用のアグリゲート容量が多い順に結果をソートします。
7. ビューに表示されているビューの名前（「最も使用されていないアグリゲート容量」など）を反映した名前を付けて保存し、チェックマーク () をクリックします (✓)。
8. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
9. [レポートスケジュール] ページに新しい行を追加して、新しいレポートのスケジュール特性を定義できるようにするには、[スケジュールの追加] をクリックします。
10. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、アグリゲートの容量に基づいて HA ペアのバランスを調整できます。

古いバージョンの **ONTAP** を実行しているノードを表示するレポートの作成

すべてのクラスタノードにインストールされている ONTAP ソフトウェアのバージョンを表示するレポートを作成して、アップグレードが必要なノードを確認できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、古いバージョンの ONTAP を実行しているノードを表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Nodes * をクリックします。
2. レポートに不要な列を削除するには、[* 表示 / 非表示 *] を選択します。
3. "OS バージョン" 列を " ノード " 列の近くにドラッグします。
4. 「 OS バージョン」列の上部をクリックして、ONTAP の最も古いバージョンで結果をソートします。
5. ビューに表示されている内容を反映した名前でビューを保存します (例 : ONTAP バージョンごとのノード)
6. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
7. [レポートスケジュール] ページに新しい行を追加して、新しいレポートのスケジュール特性を定義できるようにするには、[スケジュールの追加] をクリックします。
8. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、古いバージョンの ONTAP を実行しているノードをアップグレードできま

す。

アグリゲート容量レポートのカスタマイズ

以下に記載するサンプルのカスタムレポートを使用して、アグリゲートのストレージ容量に関連する潜在的な問題を特定して対処することができます。

このセクションのレポートは、それぞれのストレージシステムリソースの監視に役立つアグリゲート容量レポートの作成方法を説明するためのサンプルです。

容量がフルに達しているアグリゲートを表示するレポートの作成

容量がフルに近づいているアグリゲートを検出するレポートを作成して、容量を追加したり、ワークロードを他のアグリゲートに移動したりできます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、容量がフルに近づいているアグリゲートを表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Aggregates * をクリックします。
2. 表示メニューで、* 容量 * > * すべてのアグリゲート * を選択します。
3. レポートに不要な列を削除するには、[* 表示 / 非表示 *]を選択します。
4. フィルタアイコンをクリックして次のフィルタを追加し、* フィルタの適用 * をクリックします。
 - フルまでの日数が 45 日未満
5. 「フルまで」列の上部をクリックして、容量がフルに達するまでの残り日数が最も少ない順に結果をソートします。
6. ビューに表示されている内容を表す特定の名前を付けてビューを保存します。たとえば、「フルアグリゲート容量に到達するまでの時間」のように入力し、チェックマーク (✓) をクリックします。
7. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
8. [* スケジュールの追加 *] をクリックして、新しいレポートのスケジュール特性を定義できるように、[レポートスケジュール *] ページに新しい行を追加します。
9. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、容量がフルに近づいているアグリゲートのストレージを拡張できます。また、アグリゲートのスペースが少なくなった場合に早めにイベントを受信して対応できるように、「フルまでの日数」容量しきい値をデフォルトの 7 日より多い日数に引き上げることができます。

80% 以上フルのアグリゲートを表示するレポートの作成

80% 以上フルのアグリゲートを表示するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、80% 以上フルのアグリゲートを表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Aggregates * をクリックします。
2. 表示メニューで、* 容量 * > * すべてのアグリゲート * を選択します。
3. レポートに不要な列を削除するには、[* 表示 / 非表示 *]を選択します。
4. 「使用可能なデータ %」列と「使用済みデータ %」列を「アグリゲート」列の近くにドラッグします。
5. フィルタアイコンをクリックして次のフィルタを追加し、* フィルタの適用 * をクリックします。
 - 使用済みデータが 80% を超えています
6. 「Used Data %」列の上部をクリックして、結果を容量の割合でソートします。
7. ビューに表示されている内容を反映した名前を付けて 'ビューを保存しますたとえば' アグリゲートがフルに近づいていますチェック・マークをクリックします (✓)。
8. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
9. [レポートスケジュール] ページに新しい行を追加して、新しいレポートのスケジュール特性を定義できるようにするには、[スケジュールの追加] をクリックします。
10. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、一部のアグリゲートからデータを移動できます。

オーバーコミットされたアグリゲートを表示するレポートの作成

アグリゲートのストレージ容量と使用状況を分析するために、オーバーコミットされたアグリゲートを表示するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、オーバーコミットのしきい値を超えているアグリゲートを表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Aggregates * をクリックします。

2. 表示メニューで、* 容量 * > * すべてのアグリゲート * を選択します。
3. レポートに不要な列を削除するには、[* 表示 / 非表示 *]を選択します。
4. 「オーバーコミット容量」列を「アグリゲート」列の近くにドラッグします。
5. フィルタアイコンをクリックして次のフィルタを追加し、* フィルタの適用 * をクリックします。
 - オーバーコミット容量が 100% を超えています
6. 「オーバーコミット容量 %」列の上部をクリックして、結果を容量の割合でソートします。
7. ビューに表示されている内容を反映した名前 (「アグリゲートがオーバーコミット」など) でビューを保存し、チェックマーク (✓)。
8. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
9. [レポートスケジュール] ページに新しい行を追加して、新しいレポートのスケジュール特性を定義できるようにするには、[スケジュールの追加] をクリックします。
10. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、アグリゲートに容量を追加したり、特定のアグリゲートからデータを移動したりすることができます。

ボリューム容量レポートのカスタマイズ

以下に記載するサンプルのカスタムレポートを使用して、ボリュームの容量とパフォーマンスに関連する潜在的な問題を特定して対処することができます。

Snapshot の自動削除がオフで容量がフルに近づいているボリュームを特定するレポートの作成

Snapshot の自動削除機能が無効になっていて容量がフルに近づいているボリュームをリストするレポートを作成できます。このレポートは、Snapshot の自動削除を設定する必要があるボリュームを特定するのに役立ちます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、必要な列を正しい順序で表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Volumes * をクリックします。
2. 表示メニューで、* 容量 * > * すべてのボリューム * を選択します。
3. レポートに不要な列を削除するには、[* 表示 / 非表示 *]を選択します。
4. 「スナップショットの自動削除」列と「フル」列を「使用可能なデータ容量」列の近くにドラッグアンドドロップします。

5. フィルタアイコンをクリックして次の 2 つのフィルタを追加し、* フィルタの適用 * をクリックします。
 - フルまでの日数が 30 日未満
 - Snapshot の自動削除が無効になりました
6. 残り日数が最も少ないボリュームがリストの先頭に表示されるように、「フルまでの日数」列の上部をクリックします。
7. ビューに表示されている内容を反映した名前（たとえば「Vols near capacity」）でビューを保存します。
8. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
9. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク（✓）をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、ボリュームで Snapshot の自動削除を有効にしたり、使用可能なスペースを増やす方法を特定したりすることができます。

シンプロビジョニングが無効なボリュームが使用しているスペースを確認するレポートの作成

シンプロビジョニングされていないボリュームは、ボリューム作成時に定義されたスペースの全容量をディスク上で占有します。シンプロビジョニングが無効になっているボリュームを特定することで、特定のボリュームでシンプロビジョニングを有効にするかどうかを判断できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、必要な列を正しい順序で表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Volumes * をクリックします。
2. 表示メニューで、* 容量 * > * すべてのボリューム * を選択します。
3. レポートに不要な列を削除するには、[* 表示 / 非表示 *] を選択します。
4. [使用済みデータ %] 列と [シンプロビジョニング済み] 列を [使用可能なデータ容量] 列の近くにドラッグ・アンド・ドロップします
5. フィルタアイコンをクリックして次のフィルタを追加し、「シンプロビジョニング済み」「* なし」の「* フィルタの適用」をクリックします。
6. 「Used Data %」列の上部をクリックして、割合が最も高いボリュームがリストの先頭に表示されるように結果をソートします。
7. ビューに表示されている内容を反映する名前を付けてビューを保存します（例：「Vols no thin provisioning」）。
8. インベントリページの * スケジュール済みレポート * ボタンをクリックします。

9. [* スケジュールの追加 *] をクリックして、新しいレポートのスケジュール特性を定義できるように、[レポートスケジュール *] ページに新しい行を追加します。
10. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク () をクリックします (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、特定のボリュームでシンプロビジョニングを有効にすることができます。

クラウド階層へのデータの移動が必要な **FabricPool** アグリゲート上のボリュームを特定するレポートの作成

現在 FabricPool アグリゲートにあるボリューム、クラウド階層に関する推奨事項があり、さらに大量のコールドデータがあるボリュームのリストを記載したレポートを作成できます。このレポートは、特定のボリュームの階層化ポリシーを「auto」または「all」に変更して、より多くのコールド（非アクティブ）データをクラウド階層にオフロードする必要があるかどうかを判断するのに役立ちます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- FabricPool アグリゲートを設定しておく必要があります。また、それらのアグリゲート上にボリュームが必要です。

次の手順に従って、必要な列を正しい順序で表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Volumes * をクリックします。
2. [表示] メニューで、[* パフォーマンス > すべてのボリューム *] を選択します。
3. コラムセレクトで、ビューに「ディスクタイプ」列が表示されていることを確認します。

他の列を追加または削除して、レポートにとって重要なビューを作成します。

4. 「クラウドのおすすめ」列の近くにある「ディスクの種類」列をドラッグアンドドロップします。
5. フィルタアイコンをクリックして次の 3 つのフィルタを追加し、* フィルタの適用 * をクリックします。
 - ディスクタイプにFabricPool が含まれています
 - クラウドに関する推奨事項に階層が含まれて
 - コールドデータが 10GB を超えています

6. コールドデータ列の上部をクリックして、コールドデータが最も多いボリュームをビューの上部に表示します。
7. ビューに表示されている内容を反映する名前を付けてビューを保存しますたとえば 'Vols change tiering policy' です

Volumes - Performance / Vols change tiering policy

Last updated: Feb 8, 2019, 12:26 PM

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View Vols change tiering policy Search Volumes 3

Assign Performance Threshold Policy		Clear Performance Threshold Policy		Schedule Report		
Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagnfsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

8. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
9. [レポートスケジュール] ページに新しい行を追加して、新しいレポートのスケジュール特性を定義できるようにするには、[スケジュールの追加] をクリックします。
10. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、System Manager または ONTAP CLI を使用して、特定のボリュームの階層化ポリシーを「auto」または「all」に変更し、より多くのコールドデータをクラウド階層にオフロードできます。

qtree 容量レポートのカスタマイズ

以下に記載するサンプルのカスタムレポートを使用して、qtree 容量に関連する潜在的な問題を特定して対処することができます。

ほぼフルの qtree を表示するレポートの作成

qtree のストレージ容量と使用状況を分析するために、ほぼフルの qtree を表示するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、ほぼフルの qtree を表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Qtrees * をクリックします。
2. レポートに不要な列を削除するには、[* 表示 / 非表示 *] を選択します。
3. 「qtree」列の近くに「ディスク使用量 %」列をドラッグします。
4. フィルタアイコンをクリックして次のフィルタを追加し、* フィルタの適用 * をクリックします。
 - 使用済みディスクが 75% を超えている
5. 「使用済みディスク %」列の上部をクリックして、結果を容量の割合でソートします。
6. ビューに表示されている内容を反映した名前でビューを保存します（例：「qtree がフルに近づいています」）。チェックマーク () をクリックします (✓)。
7. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
8. [* スケジュールの追加 *] をクリックして、新しいレポートのスケジュール特性を定義できるように、[レポートスケジュール *] ページに新しい行を追加します。
9. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、ディスクのハードリミットやソフトリミットを調整したり（設定されている場合）、qtree 間でデータのバランスを調整したりすることができます。

NFS 共有レポートのカスタマイズ

NFS 共有レポートをカスタマイズして、ストレージシステム上のボリュームの NFS エクスポートポリシーおよびルールに関する情報を分析できます。たとえば、アクセスできないマウントパスがあるボリュームやデフォルトのエクスポートポリシーを使用するボリュームを表示するように、レポートをカスタマイズできます。

マウントパスにアクセスできないボリュームを表示するレポートの作成

マウントパスにアクセスできないボリュームを特定するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、マウントパスにアクセスできないボリュームのカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * NFS Shares * をクリックします。
2. レポートに不要な列を削除するには、[* 表示 / 非表示 *]を選択します。
3. フィルタアイコンをクリックして次のフィルタを追加し、* フィルタの適用 * をクリックします。
 - マウントパスがアクティブではありません
4. ビューに表示されている内容を反映した名前でビューを保存しますたとえば 'アクセスできないマウント・パスを持つボリュームなどの名前を付けて 'チェック・マーク () をクリックします (✓)。
5. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
6. [レポートスケジュール] ページに新しい行を追加して、新しいレポートのスケジュール特性を定義できるようにするには、[スケジュールの追加] をクリックします。
7. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、アクセスできないマウントパスを修正できます。

デフォルトのエクスポートポリシーを使用しているボリュームを表示するレポートの作成

デフォルトのエクスポートポリシーを使用しているボリュームを検出するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、デフォルトのエクスポートポリシーを使用しているボリュームのカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * NFS Shares * をクリックします。
2. レポートに不要な列を削除するには、[* 表示 / 非表示 *]を選択します。
3. 「ボリューム」列の近くにある「エクスポートポリシー」列をドラッグします。
4. フィルタアイコンをクリックして次のフィルタを追加し、* フィルタの適用 * をクリックします。

。エクスポートポリシーに default が含まれる

5. ビューに表示されている内容を反映した名前でビューを保存しますたとえば 'ボリュームにデフォルトのエクスポート・ポリシーが適用されている場合' チェック・マーク () をクリックします (✓)。
6. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
7. [レポートスケジュール] ページに新しい行を追加して、新しいレポートのスケジュール特性を定義できるようにするには、[スケジュールの追加] をクリックします。
8. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、カスタムのエクスポートポリシーを設定できます。

Storage VM レポートのカスタマイズ

Storage VM レポートを作成して、ボリューム情報を分析したり、全体の健全性とストレージの可用性を確認したりできます。たとえば、レポートを作成して、ボリューム数の上限に達した SVM を表示したり、停止した SVM を分析したりできます。

ボリューム数が上限に達している **Storage VM** を表示するレポートの作成

ボリューム数が上限に達している SVM を検出するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、ボリューム数が上限に達している Storage VM を表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Storage VM* をクリックします。
2. レポートに不要な列を削除するには、[* 表示 / 非表示 *] を選択します。
3. 「ボリューム数」列と「最大許容ボリューム数」列を「Storage VM」列の近くにドラッグします。
4. 「ボリュームの最大許容数」列の上部をクリックして、ボリュームの最大数で結果をソートします。
5. ビューに表示されている内容を反映した名前を付けてビューを保存します。たとえば、「最大ボリュームに達している VM」のように、チェックマーク () をクリックします (✓)。
6. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
7. [* スケジュールの追加 *] をクリックして、新しいレポートのスケジュール特性を定義できるように、[レポートスケジュール *] ページに新しい行を追加します。
8. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の

受信者に E メールで送信されます。

レポートに表示された結果を基に、Storage VM に割り当てるボリュームを調整できます。また、可能であれば、ONTAP System Manager を使用して許容される最大ボリューム数を変更することができます。

停止している **Storage VM** を表示するレポートの作成

停止しているすべての SVM のリストを表示するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、停止している Storage VM を表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Storage VM* をクリックします。
2. 表示メニューで、* Health * > * All Storage VM* を選択します。
3. レポートに不要な列を削除するには、[* 表示 / 非表示 *] を選択します。
4. 「Storage VM」列の近くにある「分版」列をドラッグします。
5. フィルタアイコンをクリックして次のフィルタを追加し、* フィルタの適用 * をクリックします。
 - 状態は stopped になります
6. ビューに表示されているビューを表す特定の名前を付けて保存します。たとえば、「SVM のトップ」と入力し、チェックマーク (✓)。
7. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
8. [* スケジュールの追加 *] をクリックして、新しいレポートのスケジュール特性を定義できるように、[レポートスケジュール *] ページに新しい行を追加します。
9. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、SVM が停止した理由を調査して、停止している SVM の再起動が必要かどうかを確認できます。

ボリューム関係レポートのカスタマイズ

ボリューム関係インベントリレポートでは、クラスタ内のストレージインベントリの詳細を分析できるほか、ボリュームに必要な保護レベルを把握したり、障害の原因、パターン、スケジュールに基づいてボリュームの詳細をフィルタリングしたりできます。

ボリューム関係を障害の原因別にグループ化するレポートの作成

関係が正常な状態でない理由別にボリュームをグループ化するレポートを作成できま

す。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、ボリュームを障害の原因別にグループ化するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Volumes * をクリックします。
2. [表示] メニューで、 [* 関係 > すべての関係 *] を選択します。
3. [リレーションシップの状態] 列と [不健康な理由] 列がビューに表示されることを確認するには [* Show/Hide *] を選択します

他の列を追加または削除して、レポートにとって重要なビューを作成します。

4. 「 Relationship Health 」 列と 「 Unhealthy Reason 」 列を 「 'S tate' 」 列の近くにドラッグします。
5. フィルタアイコンをクリックして次のフィルタを追加し、 * フィルタの適用 * をクリックします。
 - 関係の健全性に問題があります
6. 「正常でない理由」列の上部をクリックして、ボリューム関係を障害の原因別にグループ化します。
7. ビューには '失敗によるボリューム関係など' 表示されているビューの名前が反映された名前を付けて保存します
8. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
9. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、障害のタイプごとに原因と影響を調査できます。

ボリューム関係を問題別にグループ化するレポートの作成

ボリューム関係を問題別にグループ化するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、ボリューム関係を問題別にグループ化するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Volumes * をクリックします。
2. [表示] メニューで、 [* 関係 > すべての関係 *] を選択します。
3. レポートに不要な列を削除するには、 [* 表示 / 非表示 *] を選択します。

4. 「不健全な理由」列を「日付」列の近くにドラッグします。
5. [Unhealthy Reason] 列の上部をクリックして ' ボリュームを問題別にグループ化します
6. ビューに表示されているビューの名前を反映した名前を付けて ' ビューを保存しますたとえば 'Vol relationships by 問題などです
7. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
8. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、各タイプの問題の原因と影響を調査できます。

特定の期間のボリューム転送の傾向を表示するレポートの作成

特定の期間のボリューム転送の傾向を表示するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、特定の期間のボリュームを表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Volumes * をクリックします。
2. [表示] メニューで、 [* 関係 * > * 過去 1 カ月の転送ステータス *] を選択します。
3. レポートに不要な列を削除するには、 [* 表示 / 非表示 *] を選択します。
4. [転送時間] 列を [運用結果] 列の近くにドラッグします。
5. フィルタアイコンをクリックして次のフィルタを追加し、 * フィルタの適用 * をクリックします。
 - 転送終了時間が過去 7 日間以内です
6. 「転送時間」列の上部をクリックして、ボリュームを時間間隔でソートします。
7. ビューに表示されている内容を反映した特定の名前でビューを保存しますたとえば ' デュレーションごとのボリュームなどです
8. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
9. レポートスケジュールの名前を入力し、頻度を「 * Weekly * 」に設定して、他のレポートフィールドに情報を入力し、チェックマーク (✓) をクリックします (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、転送期間を調査できます。

失敗または成功したボリューム転送を表示するレポートの作成

ボリューム転送のステータスを表示するレポートを作成できます。このレポートでは、失敗したボリューム転送と成功したボリューム転送の両方を確認できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、失敗した転送と成功した転送を表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Volumes * をクリックします。
2. [表示] メニューで、[* 関係 * > * 過去 1 カ月の転送ステータス *] を選択します。
3. レポートに不要な列を削除するには、[* 表示 / 非表示 *] を選択します。
4. 「操作結果」列を「分列」列の近くにドラッグします。
5. [操作結果]列の上部をクリックして、ボリュームをステータスでソートします。
6. ビューに表示されている内容を反映した名前でビューを保存しますたとえば '転送ステータスによるボリューム' などです
7. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
8. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、転送ステータスを調査できます。

ボリューム転送を転送サイズに基づいて表示するレポートの作成

ボリューム転送を転送サイズに基づいて表示するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、ボリューム転送を転送サイズに基づいて表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Volumes * をクリックします。
2. 表示メニューで、* 関係 * > * 過去 1 カ月の転送速度 * を選択します。
3. 「合計転送サイズ」列の上部をクリックして、ボリューム転送をサイズでソートします。
4. ビューに表示されている内容を反映した名前でビューを保存しますたとえば '転送サイズによるボリューム' などです

5. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
6. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、ボリューム関係を転送サイズ別に調査できます。

ボリューム転送を日付別に表示するレポートの作成

ボリューム転送を日付別に表示するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、ボリューム転送を日付別に表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Volumes * をクリックします。
2. 表示メニューで、 * 関係 * > * 過去 1 カ月の転送速度 * を選択します。
3. ボリューム転送を日付で並べ替えるには、「` `」列の上部をクリックします。
4. 表示内容を反映した名前で作成したビューを保存しますたとえば ' 毎日のボリューム転送' などです
5. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
6. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、ボリューム転送を日付別に調査できます。

ボリュームパフォーマンスレポートのカスタマイズ

以下に記載するサンプルのカスタムレポートを使用して、ボリュームのパフォーマンスに関連する潜在的な問題を特定して対処することができます。

FabricPool 対応でないアグリゲート上の大量のコールドデータを含むボリュームを表示するレポートの作成

FabricPool 以外のアグリゲート上のコールドデータを大量に含むボリュームを表示するレポートを作成できます。このレポートから、FabricPool アグリゲートに移動する必要があるボリュームを特定できます。

- 必要なもの *

- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、FabricPool 対応でないアグリゲート上のコールドデータを大量に含むボリュームを表示するカスタムビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーションペインで、* Storage * > * Volumes * をクリックします。
2. [表示] メニューで、[* パフォーマンス > すべてのボリューム *] を選択します。
3. 「ディスクタイプ」列がビューに表示されるようにするには、「* 表示 / 非表示 *」を選択します。

他の列を追加または削除して、レポートにとって重要なビューを作成します。

4. 「コールドデータ」列の近くにある「ディスクタイプ」列をドラッグします。
5. フィルタアイコンをクリックして次のフィルタを追加し、* フィルタの適用 * をクリックします。
 - コールドデータが 100GB を超えています
 - ディスクタイプに SSD が含まれています
6. 「ディスクタイプ」列の上部をクリックして、ディスクタイプ SSD (FabricPool) が一番下になるようにボリュームをディスクタイプでソートします。
7. ビューに表示されている内容を反映した名前でビューを保存します (たとえば「FabricPool ではないコールドデータボリューム」)。
8. インベントリページの * スケジュール済みレポート * ボタンをクリックします。
9. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、FabricPool アグリゲートへの移動に適したボリュームを特定できます。

Microsoft Excel レポートの例

このサンプルの Microsoft Excel レポートは、Excel の高度な機能を使用して利用できるレポートオプションを紹介することを目的としています。

Excel の高度な機能を使用すると、ニーズに合わせてさまざまなレポートを作成できます。Excel の使用方法の詳細については、製品マニュアルを参照してください。



レポートを管理するには、アプリケーション管理者またはストレージ管理者のロールが必要です。

アグリゲートの容量の表とグラフを表示するレポートの作成

合計とクラスタ化された棒グラフ形式を使用して、Excel ファイルの容量を分析するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、健全性を開きます。すべてのアグリゲートビュー、Excel でのビューのダウンロード、使用可能な容量グラフの作成、カスタマイズした Excel ファイルのアップロード、最終レポートのスケジュール設定を行います。

手順

1. 左側のナビゲーションペインで、* Storage * > * Aggregates * をクリックします。
2. [* レポート >] > [Excel のダウンロード *] を選択します。



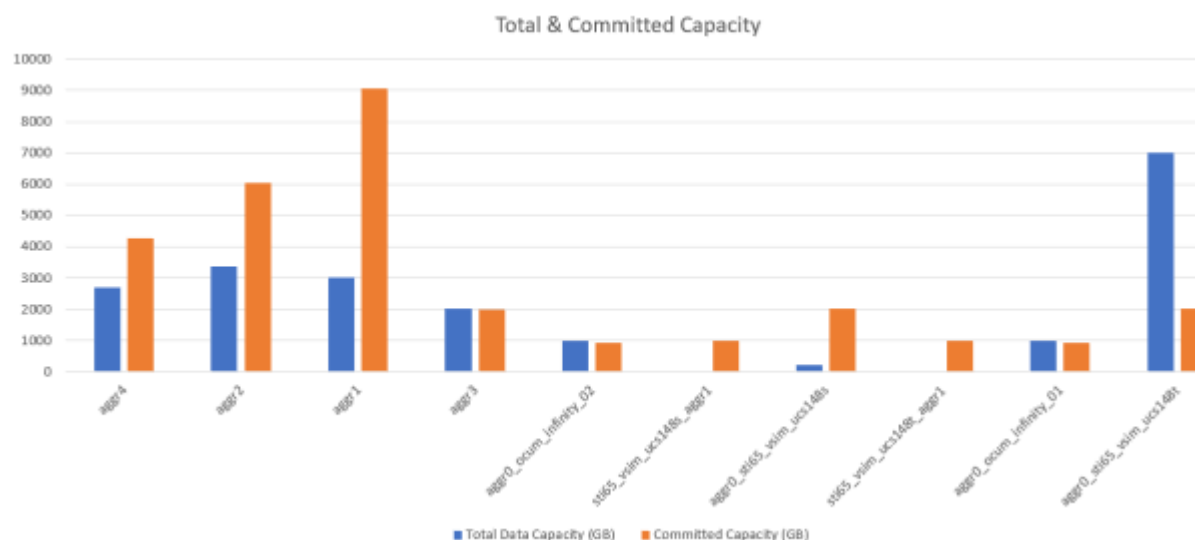
ブラウザによっては、ファイルを保存するために * OK * をクリックする必要があります。

3. 必要に応じて、* 編集を有効にする * をクリックします。
4. Excel で、ダウンロードしたファイルを開きます。
5. 新しいシートを作成します (⊕) をクリックします data シート名と名前*総データ容量*。
6. 新しい合計データ容量シートに次の列を追加します。
 - a. 合計データ容量 (GB)
 - b. コミット済み容量 (GB)
 - c. 使用済みデータ容量 (GB)
 - d. 使用可能なデータ容量 (GB)
7. 各列の最初の行に、次の式を入力します。この式では、データシート (data!) が参照されていることを確認し、取得したデータに対して正しい列と行の指定子が参照されていることを確認します (合計データ容量では、列 E、行 2 から 20 までのデータが取得されます)。
 - a. = 合計 (DATA ! E\$2 : DATA ! E\$20)
 - b. = 合計 (DATA ! F\$2 : DATA ! F\$50)
 - c. = 合計 (DATA ! G\$2 : DATA ! G\$50)
 - d. = 合計 (データ ! H\$2 : データ ! H\$50)

数式は、現在のデータに基づいて各列の合計を計算します。

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. データシートで、列 [合計データ容量 (GB)] および [コミット容量 (GB)] * を選択します。
2. [* 挿入 * (Insert *)] メニューから [* 推奨チャート * (Recommended Charts *)] を選択し、[* クラスタ化された列 * (* Clustered Column
3. グラフを右クリックし、[グラフの移動]を選択して、グラフをに移動します Total Data Capacity シート (Sheet) :
4. グラフを選択したときに使用できる * デザイン * および * フォーマット * メニューを使用して、グラフの外観をカスタマイズできます。
5. 必要に応じて、ファイルに変更を保存します。ファイルの名前や場所は変更しないでください。



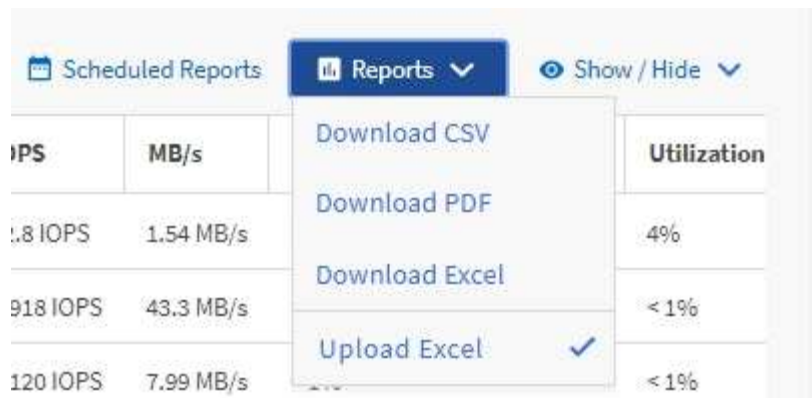
6. Unified Manager で、* Reports * > * Upload Excel * を選択します。



Excel ファイルをダウンロードしたときと同じビューに表示されていることを確認します。

7. 変更した Excel ファイルを選択します。
8. * 開く * をクリックします。
9. [Submit (送信)] をクリックします。

[Reports>*Upload Excel*] メニュー項目の横にチェックマークが表示されます。



10. [スケジュール済みレポート] をクリックします。
11. [レポートスケジュール] ページに新しい行を追加して、新しいレポートのスケジュール特性を定義できるようにするには、[スケジュールの追加] をクリックします。



レポートの **XLSX** 形式を選択します。

12. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、ネットワーク全体で使用可能な容量を最大限に活用する方法を調査できます。

アグリゲートの合計容量と使用可能容量のグラフを表示するレポートの作成

ストレージの合計容量とコミット済み容量を Excel グラフ形式で分析するレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

健全性を開くには、次の手順を実行します。すべてのアグリゲートビュー、Excel でのビューのダウンロード、合計容量とコミット済み容量のグラフの作成、カスタマイズした Excel ファイルのアップロード、最終レポートのスケジュール設定。

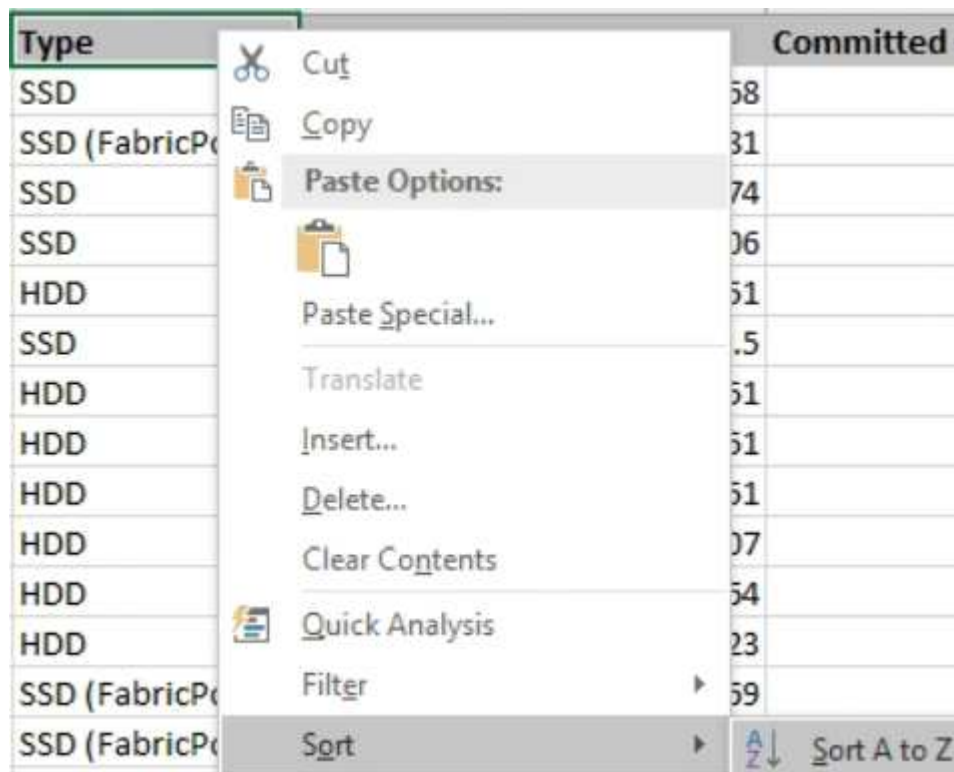
手順

1. 左側のナビゲーションペインで、* Storage * > * Aggregates * をクリックします。
2. [* レポート >] > [Excel のダウンロード *] を選択します。



ブラウザによっては、ファイルを保存するために * OK * をクリックする必要があります。

3. Excel で、ダウンロードしたファイルを開きます。
4. 必要に応じて、* 編集を有効にする * をクリックします。
5. データシートで、[タイプ (Type)] 列を右クリックし、[* 並べ替え * (Sort)] > [* 昇順 (* Sort a to Z)] を選択します。

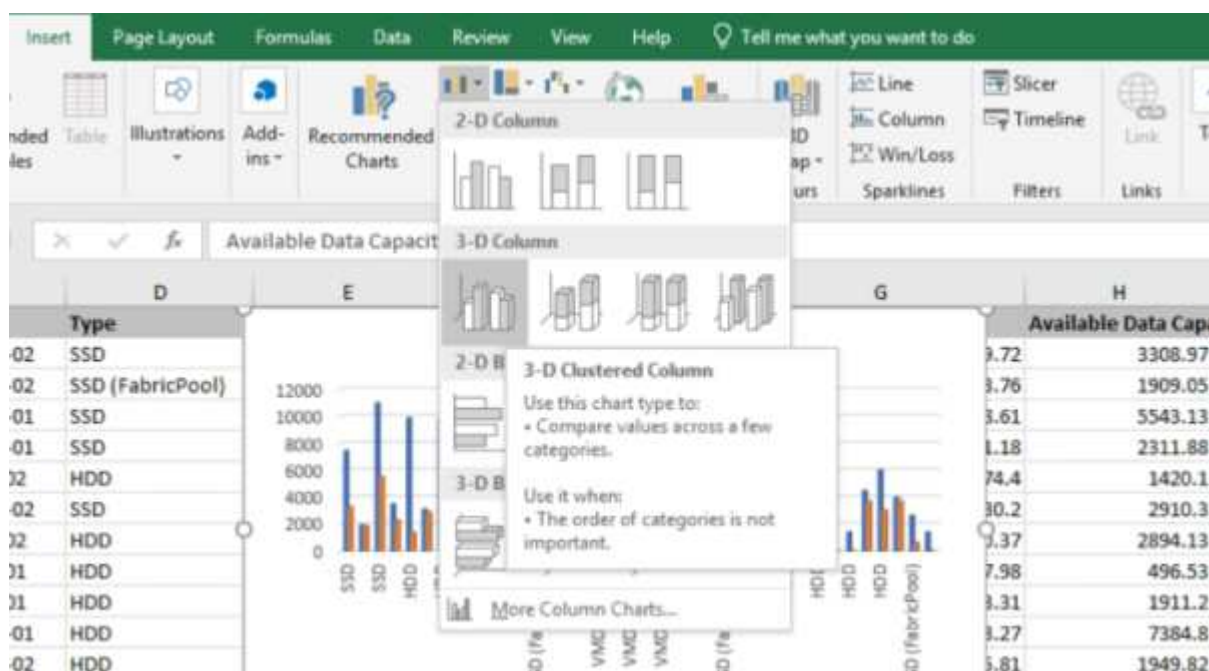


これにより、次のようなストレージタイプ別にデータが配置されます。

- HDD
- ハイブリッド
- SSD の場合
- SSD (FabricPool)

6. を選択します Type, Total Data Capacity, および Available Data Capacity 列 (Columns) :
7. [挿入 (Insert *)]メニューで、を選択します 3-D column チャート。

グラフがデータシートに表示されます。

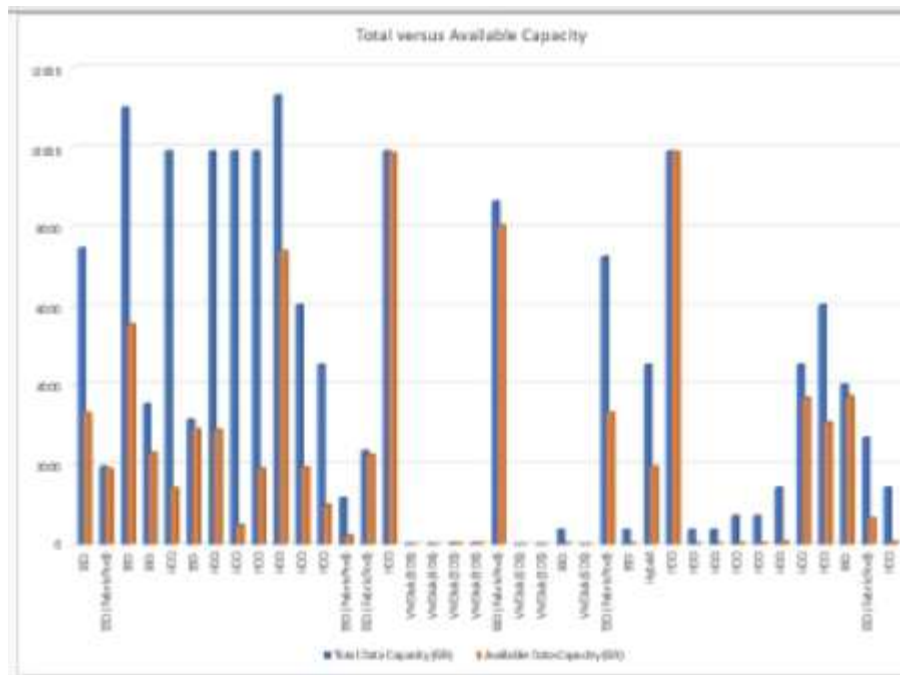


8. グラフを右クリックして、*チャートの移動*を選択します。
9. [新規シート*]を選択し、シートに「Total Storage Charts*」という名前を付けます。



インフォメーションシートとデータシートの後に新しいシートが表示されることを確認します。

10. グラフのタイトルに「* Total versus available Capacity *」と入力します。
11. グラフを選択したときに使用できる *デザイン* および *フォーマット* メニューを使用して、グラフの外観をカスタマイズできます。
12. 必要に応じて、ファイルに変更を保存します。ファイルの名前や場所は変更しないでください。

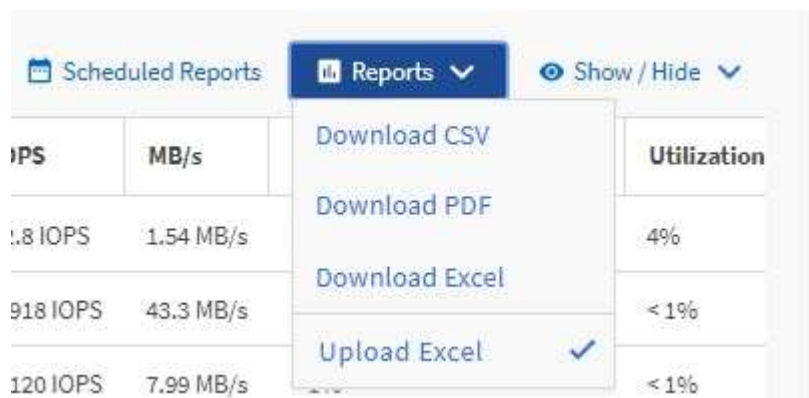


13. Unified Manager で、 * Reports * > * Upload Excel * を選択します。

Excel ファイルをダウンロードしたときと同じビューに表示されていることを確認します。

14. 変更した Excel ファイルを選択します。
15. * 開く * をクリックします。
16. [Submit (送信)] をクリックします。

[**Reports**>*Upload Excel*] メニュー項目の横にチェックマークが表示されます。



17. [スケジュール済みレポート]をクリックします。
18. [* スケジュールの追加*]をクリックして、新しいレポートのスケジュール特性を定義できるように、[レポートスケジュール*]ページに新しい行を追加します。

レポートの **XLSX** 形式を選択します。

19. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、アグリゲートの負荷を分散できます。

使用可能なボリューム容量グラフを表示するレポートの作成

Excel グラフで使用可能なボリューム容量を分析するためのレポートを作成できます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、健全性を開きます。すべてのボリュームビュー、Excel でのビューのダウンロード、使用可能な容量グラフの作成、カスタマイズした Excel ファイルのアップロード、最終レポートのスケジュール設定を行います。

手順

1. 左側のナビゲーションペインで、* Storage * > * Volumes * をクリックします。
2. [* レポート >] > [Excel のダウンロード *] を選択します。



ブラウザによっては、ファイルを保存するために * OK * をクリックする必要があります。

3. 必要に応じて、* 編集を有効にする * をクリックします。
4. Excel で、ダウンロードしたファイルを開きます。
5. をクリックします data シートで、で使用するデータを選択します Volume および Available Data % 列。
6. [挿入 (Insert *)] メニューで、を選択します 3-D piechart.

使用可能なスペースが最も多いボリュームがチャートに表示されます。グラフがデータシートに表示されます。

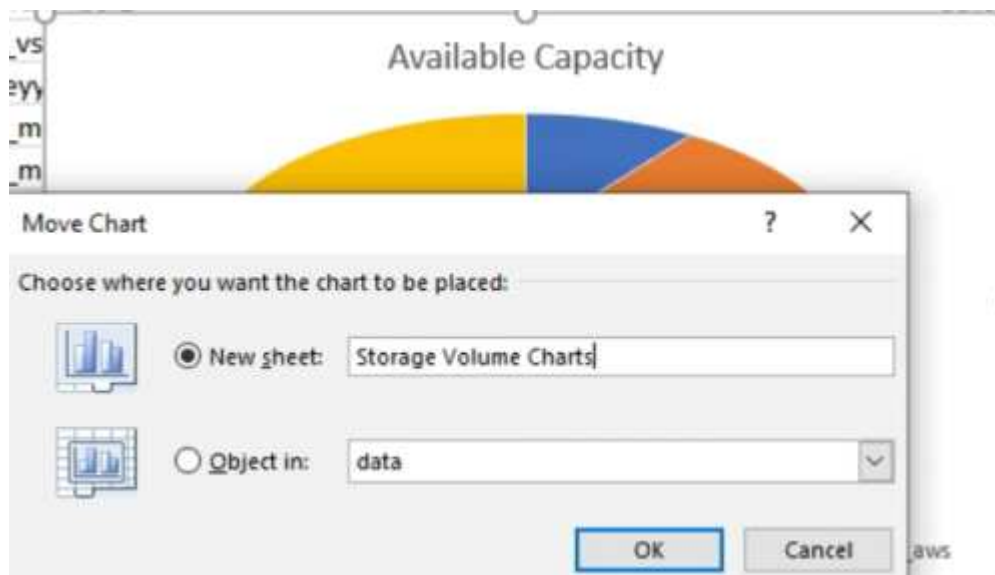


ネットワーク構成によっては、列全体またはデータ行が多すぎると、円グラフが読めなくなることがあります。このサンプルでは 3-D 円グラフを使用していますが、任意のグラフタイプを使用できます。最適なグラフには、キャプチャするデータが表示されます。

7. グラフのタイトルに「 * Available Capacity 」という名前を付けます。
8. グラフを右クリックして、 * チャートの移動 * を選択します。
9. [新規シート *] を選択し、シートに「 * ストレージ容量チャート * 」という名前を付けます。



インフォメーションシートとデータシートの後に新しいシートが表示されることを確認します。



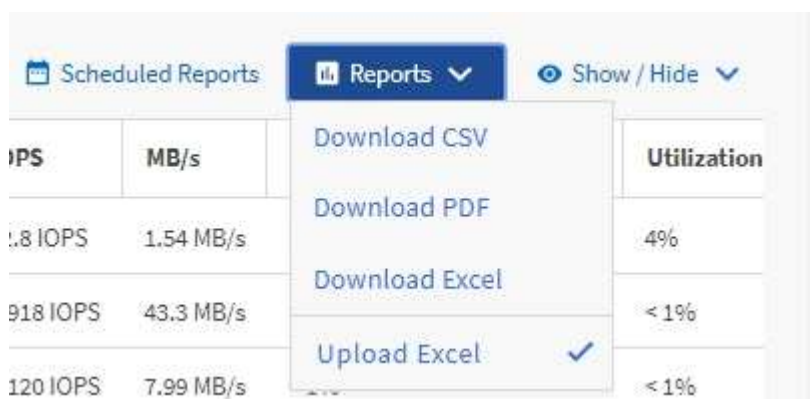
10. グラフを選択したときに使用できる * デザイン * および * フォーマット * メニューを使用して、グラフの外観をカスタマイズできます。
11. 必要に応じて、ファイルに変更を保存します。
12. Unified Manager で、 * Reports * > * Upload Excel * を選択します。



Excel ファイルをダウンロードしたときと同じビューに表示されていることを確認します。

13. 変更した Excel ファイルを選択します。
14. * 開く * をクリックします。
15. [Submit (送信)] をクリックします。

[Reports>*Upload Excel*] メニュー項目の横にチェックマークが表示されます。



16. [スケジュール済みレポート] をクリックします。
17. [* スケジュールの追加 *] をクリックして、新しいレポートのスケジュール特性を定義できるように、[レポートスケジュール *] ページに新しい行を追加します。
18. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。



レポートの **XLSX** 形式を選択します。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、ボリュームに負荷を分散できます。

IOPS が最も高いアグリゲートを表示するレポートの作成

このレポートには、新しいワークロードをプロビジョニングできるアグリゲートタイプごとの IOPS が最も使用可能なアグリゲートが表示されます。

- 必要なもの *
- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、健全性を開きます。すべてのボリュームビュー、Excel でのビューのダウンロード、使用可能な容量グラフの作成、カスタマイズした Excel ファイルのアップロード、最終レポートのスケジュール設定を行います。

手順

1. 左側のナビゲーションペインで、* Storage * > * Aggregates * をクリックします。
2. View * ドロップダウンから * Performance : All aggregates * を選択します。
3. を表示するには、*表示/非表示*を選択します Available IOPS を表示および非表示にします Cluster FQDN, Inactive Data Reporting, および Threshold Policy 列 (Columns) :
4. をドラッグアンドドロップします Available IOPS および Free Capacity の横にある列 Type 列 (Column) :
5. カスタムビューに名前を付けて保存します Available IOPS Per Aggr.
6. [* レポート >] > [Excel のダウンロード *] を選択します。



ブラウザによっては、ファイルを保存するために * OK * をクリックする必要があります。

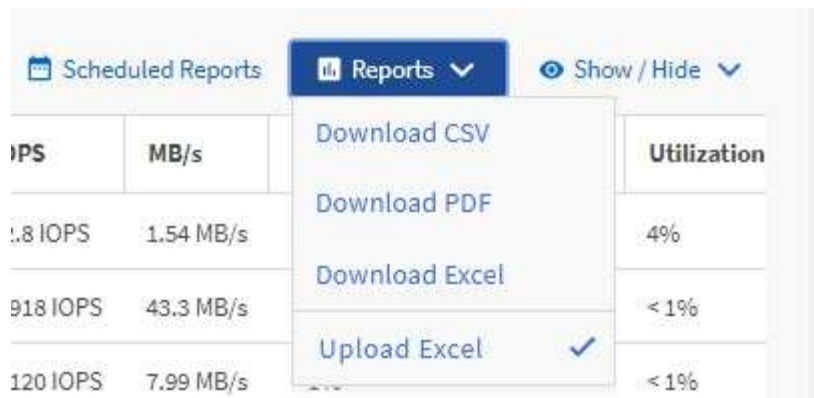
7. 必要に応じて、* 編集を有効にする * をクリックします。
8. Excel で、ダウンロードしたファイルを開きます。
9. データシートの左上にある小さな三角形をクリックして、シート全体を選択します。
10. [データ]リボンで、から[並べ替え]を選択します Sort & Filter area.
11. 次のソートレベルを設定します。
 - a. 「並べ替え基準」を指定します Available IOPS (IOPS) 。 * Sort on * as Cell Values, および*注文* AS Largest to Smallest.
 - b. [レベルの追加] をクリックします。
 - c. 「並べ替え基準」を指定します Type、ソートオン*を指定します **Cell Values**, および*注文 AS z to A.
 - d. [レベルの追加] をクリックします。
 - e. 「並べ替え基準」を指定します Free Capacity (GB), [ソートオン (* Sort On * As)] Cell Values, および*注文* AS Largest to Smallest.
 - f. [OK] をクリックします。
12. Excel ファイルを保存して閉じます。
13. Unified Manager で、* Reports * > * Upload Excel * を選択します。



Excel ファイルをダウンロードしたときと同じビューに表示されていることを確認します。

14. 変更したExcelファイルを選択します (この場合) performance-aggregates-<date>.xlsx.
15. * 開く * をクリックします。
16. [Submit (送信)] をクリックします。

[Reports>*Upload Excel*] メニュー項目の横にチェックマークが表示されます。



17. [スケジュール済みレポート] をクリックします。
18. [レポートスケジュール] ページに新しい行を追加して、新しいレポートのスケジュール特性を定義できるようにするには、[スケジュールの追加] をクリックします。
19. レポートスケジュールの名前を入力し、他のレポートフィールドに情報を入力して、チェックマーク (✓) をクリックします。



レポートの **XLSX** 形式を選択します。

レポートはテストとしてすぐに送信されます。その後、指定した頻度でレポートが生成され、リスト内の受信者に E メールで送信されます。

レポートに表示された結果を基に、使用可能な IOPS が最も高いアグリゲートに新しいワークロードをプロビジョニングできます。

REST API を使用してストレージを管理できます

Active IQ Unified Manager REST APIの使用を開始する

Active IQ Unified Manager には、サポート対象のストレージシステム上のストレージリソースを RESTful Web サービスインターフェイスを介して管理するための一連の API が用意されており、サードパーティ製品との統合に使用できます。

これらのトピックでは、Unified Manager APIに関する情報、特定の問題を解決するためのサンプルワークフロー、および一部のサンプルコードについて説明します。この情報を使用して、ネットアップシステムを管理するためのネットアップ管理ソフトウェアソリューションを備えたRESTfulクライアントを作成できます。API は、Representational State Transfer (REST) アーキテクチャスタイルに基づいています。Create、Read、Update、Delete (CRUD と呼ばれる) の 4 つすべての REST 処理がサポートされています。

このコンテンツの対象読者

ここでは、REST APIを使用してActive IQ Unified Manager ソフトウェアと連携するアプリケーションを作成する開発者を対象としています。

ストレージ管理者とストレージ設計者は、この情報を参照して、Unified Manager REST APIを使用してネットアップストレージシステムを管理および監視するためのクライアントアプリケーションを構築する方法の基本的な知識を得ることができます。

ストレージプロバイダ、ONTAP クラスタ、および管理APIを使用してストレージを管理する場合は、この情報を使用する必要があります。



オペレータ、ストレージ管理者、またはアプリケーション管理者のいずれかのロールが割り当てられている必要があります。REST API を実行する Unified Manager サーバの IP アドレスまたは完全修飾ドメイン名を確認しておく必要があります。

Active IQ Unified Manager API アクセスおよびカテゴリ

Active IQ Unified Manager API を使用して、環境内のストレージオブジェクトを管理およびプロビジョニングできます。Unified Manager Web UI にアクセスして、これらの機能の一部を実行することもできます。

REST API に直接アクセスするための URL の作成

REST API には、Python、C#、C {pp}、JavaScript などのプログラミング言語を使用して直接アクセスできます。など。以下の形式でホスト名または IP アドレスと URL を入力して、REST API にアクセスします

+ <https://<hostname>/api+>



デフォルトのポートは 443 です。環境に応じてポートを設定できます。

オンラインの **API** ドキュメントページにアクセスする

製品に付属の `_API Documentation_reference` コンテンツページにアクセスして API ドキュメントを表示することも、（Swagger などのインターフェイス上の）API 呼び出しを手動で問題することもできます。このドキュメントにアクセスするには、`* メニューバー *` > `* ヘルプボタン *` > `* API ドキュメント *` をクリックします

または、以下の形式でホスト名または IP アドレスと URL を入力して、REST API ページにアクセスします

+ <https://<hostname>/docs/api/>+

カテゴリ

API 呼び出しは、領域またはカテゴリに基づいて機能的に分類されます。特定の API を検索するには、該当する API カテゴリをクリックします。

Unified Manager に付属の REST API を使用して、管理、監視、およびプロビジョニングの各機能を実行できます。API は、次のカテゴリに分類されます。

- `* データセンター *`

このカテゴリには、Work Flow Automation や Ansible などのツールを使用したデータセンターストレージの管理と分析に役立つ API が含まれています。このカテゴリの REST API は、クラスタ、ノード、アグリゲート、ボリューム、LUN、データセンター内のファイル共有、ネームスペース、その他の要素。

- `* management-server *`

management-server カテゴリの API には、が含まれています jobs, system, および events API: ジョブとは、Unified Manager でのストレージオブジェクトまたはワークロードの管理に関連して、非同期の実行がスケジュールされている処理のことです。。 events API は、データセンターおよびイベントを返します system API が Unified Manager インスタンスの詳細を返します。

- `* ストレージ・プロバイダ *`

このカテゴリには、ファイル共有、LUN、パフォーマンスサービスレベル、およびストレージ効率化ポリシーの管理とプロビジョニングに必要なすべてのプロビジョニング API が含まれています。また、アクセスエンドポイントや Active Directory を設定したり、ストレージワークロードにパフォーマンスサービスレベルとストレージ効率化ポリシーを割り当てたりすることもできます。

- `* 管理 *`

このカテゴリには、バックアップの設定の維持、Unified Manager データソースの信頼ストア証明書の表示、ONTAP クラスタを Unified Manager のデータソースとして管理するなどの管理タスクを実行するために使用する API が含まれます。

- `* ゲートウェイ *`

Unified Manager では、ゲートウェイカテゴリの API を使用して ONTAP REST API を呼び出し、データセンター内のストレージオブジェクトを管理できます。


- `* セキュリティ *`

このカテゴリには、Unified Manager ユーザを管理するための API が含まれています。

Active IQ Unified Manager で提供される REST サービス

Active IQ Unified Manager API の使用を開始する前に、提供される REST サービスと処理について理解しておく必要があります。

API サーバの設定に使用されるプロビジョニング API と管理 API では、読み取り（GET）処理または書き込み（POST、PATCH、DELETE）処理がサポートされます。API でサポートされる GET、PATCH、POST、および DELETE 処理のいくつかの例を次に示します。

- GETの例：GET /datacenter/cluster/clusters データセンター内のクラスタの詳細を取得します。によって返されるレコードの最大数 GET 動作は1000です。
- 

API を使用すると、レコードをサポートされている属性でフィルタ、ソート、および並べ替えることができます。
- POSTの例：POST /datacenter/svm/svms カスタムのStorage Virtual Machine（SVM）を作成します。
 - PATCHの例：PATCH /datacenter/svm/svms/{key} 一意のキーを使用してSVMのプロパティを変更します。
 - 削除の例：DELETE /storage-provider/access-endpoints/{key} 一意のキーを使用して、LUN、SVM、またはファイル共有からアクセスエンドポイントを削除します。

API を使用して実行できる REST 処理は、オペレータ、ストレージ管理者、またはアプリケーション管理者ユーザのロールによって異なります。

ユーザロール	サポートされている REST メソッド
演算子	データへの読み取り専用アクセス。このロールのユーザは、すべての GET 要求を実行できます。
ストレージ管理者	すべてのデータへの読み取りアクセス。このロールのユーザは、すべての GET 要求を実行できます。 また、管理、ストレージサービスオブジェクト、ストレージ管理オプションなどの特定のアクティビティを実行するための書き込みアクセス（PATCH、POST、および DELETE 要求を実行するため）が可能です。
アプリケーション管理者	すべてのデータへの読み取りおよび書き込みアクセス。このロールのユーザは、すべての機能に対する GET、PATCH、POST、および DELETE 要求を実行できます。

すべての REST 処理の詳細については、_ オンラインの API ドキュメントを参照してください。

Active IQ Unified Manager の API バージョン

Active IQ Unified Manager の REST API URI には、バージョン番号が指定されます。例

： /v2/datacenter/svm/svms. バージョン番号 v2 インチ
/v2/datacenter/svm/svms 特定のリリースで使用されているAPIのバージョン。バージョン番号を指定することで、クライアントが処理可能な応答が返されるため、APIの変更によるクライアントソフトウェアへの影響が最小限に抑えられます。

このバージョン番号の数値部分は、リリースごとに増分されます。URI にバージョン番号を指定すると、今後のリリースで下位互換性を維持するための一貫したインターフェイスが提供されます。たとえば、バージョンを持たない同じAPIもあります /datacenter/svm/svms, これはバージョンがないベースAPIを示します。ベースAPIは常に最新バージョンのAPIです。



Swagger インターフェイスの右上の領域で、使用するAPIのバージョンを選択できます。デフォルトでは、最新バージョンが選択されています。特定のAPIについて、Unified Manager インスタンスで使用可能な（最も大きな数字の）最新バージョンを使用することを推奨します。

すべての要求に対して、使用するAPIバージョンを明示的に指定する必要があります。バージョン番号が指定されている場合、アプリケーションが処理するように設計されていない応答要素は返されません。REST 要求には、バージョンパラメータを含める必要があります。以前のバージョンのAPIは、数回のリリース後、最終的に廃止されます。このリリースでは、がサポートされます v1 APIのバージョンは廃止されました。

ONTAP のストレージリソース

ONTAP のストレージリソースは、*physical storage resources* や *_logical* ストレージリソースに大きく分類できます。_Active IQ Unified Manager で提供されるAPIを使用してONTAPシステムを効率的に管理するには、ストレージリソースモデルおよびさまざまなストレージリソース間の関係を理解しておく必要があります。

• * 物理ストレージ・リソース *

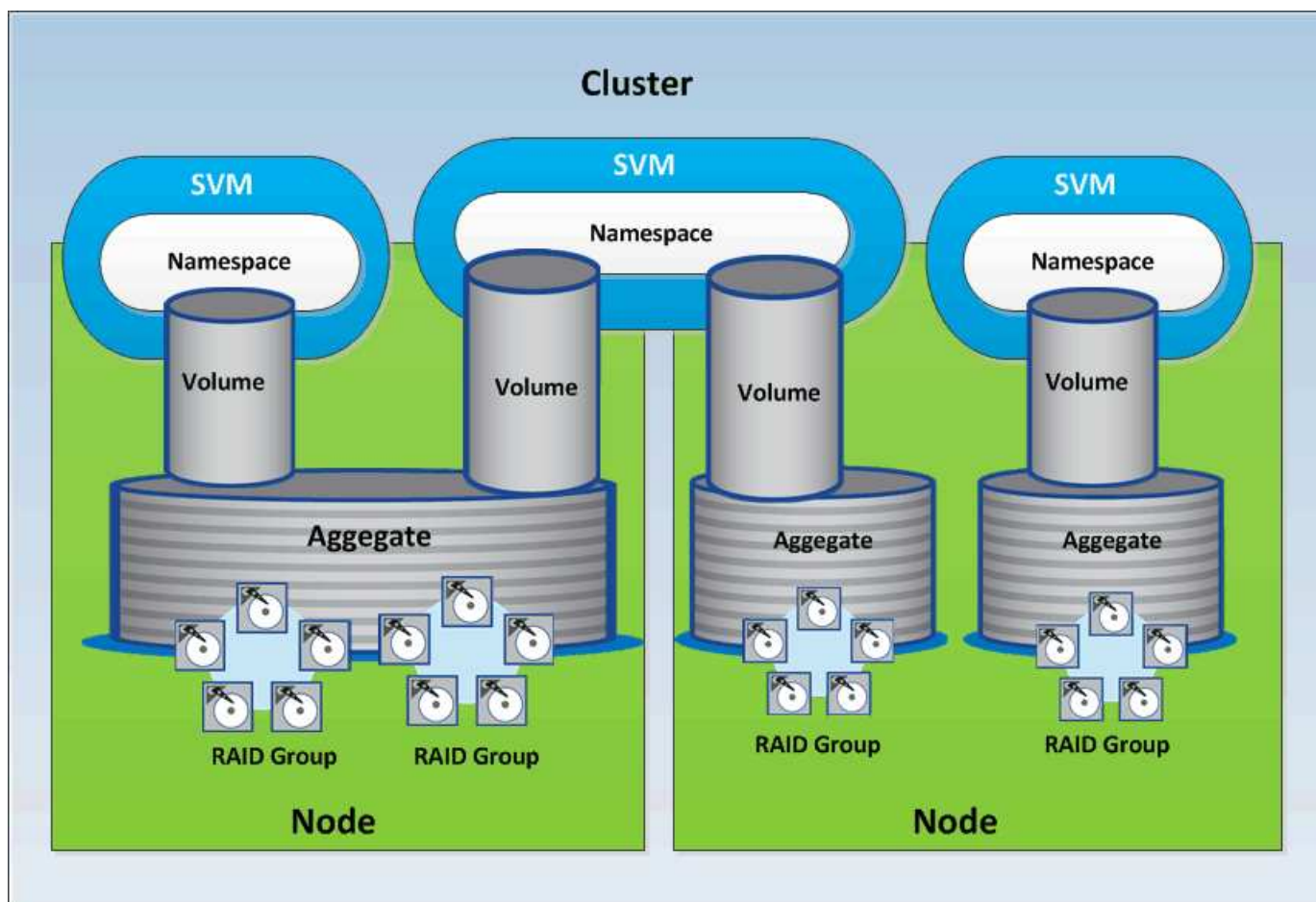
ONTAP が提供する物理ストレージオブジェクトのことです。物理ストレージリソースには、ディスク、クラスタ、ストレージコントローラ、ノード、およびアグリゲートがあります。

• * 論理ストレージ・リソース *

物理リソースに関連付けられていない、ONTAP が提供するストレージリソースのことです。これらのリソースは Storage Virtual Machine (SVM、旧 Vserver) に関連付けられており、ディスク、アレイ LUN、アグリゲートなどの特定の物理ストレージリソースには紐づけられていません。

論理ストレージリソースには、すべてのタイプのボリュームと qtree だけでなく、Snapshot コピー、重複排除、圧縮、クォータなど、これらのリソースで使用できる機能および設定も含まれます。

次の図は、2 ノードクラスタのストレージリソースを示しています。



Active IQ Unified Manager での REST API へのアクセスおよび認証

Active IQ Unified Manager REST APIには、基本のHTTP認証メカニズムを使用して問題 HTTP要求を実行できるRESTクライアントまたはプログラミングプラットフォームを使用してアクセスできます。

要求と応答の例：

• * リクエスト *

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

• * 応答 *

```
{
  "records": [
    {
```

```

    "key": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
    "name": "fas8040-206-21",
    "uuid": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
    "contact": null,
    "location": null,
    "version": {
      "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33
UTC 2019",
      "generation": 9,
      "major": 5,
      "minor": 0
    },
    "isSanOptimized": false,
    "management_ip": "10.226.207.25",
    "nodes": [
      {
        "key": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
        "uuid": "12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
        "name": "fas8040-206-21-01",
        "_links": {
          "self": {
            "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-00a0985badbb"
          }
        },
        "location": null,
        "version": {
          "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
          "generation": 9,
          "major": 5,
          "minor": 0
        },
        "model": "FAS8040",
        "uptime": 13924095,
        "serial_number": "701424000157"
      },
      {
        "key": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-00a0985bb9b7",
        "uuid": "1ed606ed-2e3a-11e9-a270-00a0985bb9b7",

```



```

        "name": "fas8040-206-21-02",
        "_links": {
            "self": {
                "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-00a0985bb9b7"
            }
        },
        "location": null,
        "version": {
            "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33 UTC 2019",
            "generation": 9,
            "major": 5,
            "minor": 0
        },
        "model": "FAS8040",
        "uptime": 14012386,
        "serial_number": "701424000564"
    }
},
    "_links": {
        "self": {
            "href": "/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb"
        }
    }
}
},

```

- *IP address/hostname* は、APIサーバのIPアドレスまたは完全修飾ドメイン名（FQDN）です。
- ポート 443

443 は、デフォルトの HTTPS ポートです。必要に応じて、HTTPS ポートをカスタマイズできます。

Webブラウザから問題 HTTP要求を行うには、REST API ブラウザプラグインを使用する必要があります。cURL や Perl などのスクリプトプラットフォームを使用して、REST API にアクセスすることもできます。

認証

Unified Manager では、API の基本的な HTTP 認証方式がサポートされます。情報の流れ（要求と応答）をセキュリティで保護するために、REST API には HTTPS 経由でのみアクセスできます。API サーバは、サーバ検証のためにすべてのクライアントに自己署名 SSL 証明書を提供します。この証明書は、カスタム証明書（または CA 証明書）で置き換えることができます。

REST API を呼び出すには、API サーバへのユーザアクセスを設定する必要があります。ユーザには、ローカ

ルユーザ（ローカルデータベースに格納されているユーザプロファイル）または LDAP ユーザ（LDAP 経由で認証するように API サーバを設定している場合）を指定できます。Unified Manager Administration Console のユーザインターフェイスにログインして、ユーザアクセスを管理できます。

Active IQ Unified Manager で使用される HTTP ステータスコード

API の実行時や問題のトラブルシューティング時には、Active IQ Unified Manager API で使用されるさまざまな HTTP ステータスコードとエラーコードについて理解しておく必要があります。

次の表に、認証に関連するエラーコードを示します。

HTTP ステータスコード	ステータスコードタイトル	説明
200	わかりました	同期 API 呼び出しの実行に成功した場合に返されます。
201	作成済み	Active Directory の設定など、同期呼び出しによって新しいリソースが作成されたことを示します。
202	承認済み	LUN やファイル共有の作成など、プロビジョニング機能の非同期呼び出しの実行が成功したときに返されます。
400	無効な要求です	入力検証に失敗したことを示します。ユーザは、要求の本文に有効なキーを指定するなど、入力を修正する必要があります。
401	不正な要求です	リソースを表示する権限がありません / 権限がありません。
403	禁止された要求です	アクセスしようとしていたリソースへのアクセスは禁止されています。
404	リソースが見つかりません	アクセスしようとしているリソースが見つかりません。
405	メソッドを使用できません	メソッドを使用できません
429	要求が多すぎます	指定した時間内にユーザが送信した要求が多すぎる場合に返されます。

HTTP ステータスコード	ステータスコードタイトル	説明
500	内部サーバエラー。	内部サーバエラー。サーバから応答を取得できませんでした。この内部サーバエラーは、永続的な場合とそうでない場合があります。たとえば、を実行するとします GET または GET ALL このエラーが表示された場合は、この処理を5回以上繰り返すことを推奨します。永続的なエラーの場合、引き続きステータスコード 500 が返されます。処理が成功すると、ステータスコード 200 が返されます。

Active IQ Unified Manager で API を使用する際の推奨事項です

Active IQ Unified Manager で API を使用するときは、特定の推奨される方法に従ってください。

- 有効に実行するには、すべての応答コンテンツタイプが次の形式である必要があります。

```
application/json
```

- API のバージョン番号は、製品のバージョン番号とは関係ありません。Unified Manager インスタンスで使用可能な最新バージョンの API を使用する必要があります。Unified Manager API のバージョンの詳細については、「Active IQ Unified Manager での ST API のバージョン管理」を参照してください。
- Unified Manager API を使用して配列値を更新する場合は、値の文字列全体を更新する必要があります。配列に値を付加することはできません。既存のアレイのみを交換できます。
- パイプ (|) やワイルドカード (+*+) などのフィルタ演算子をすべてのクエリパラメータに使用できます。ただし、指標 API の IOPS やパフォーマンスなど、二重値は除きます。
- フィルタ演算子のワイルドカード (*) とパイプ (|) を組み合わせてオブジェクトを照会しないでください。間違った数のオブジェクトが取得される可能性があります。
- フィルタに値を使用する場合は、値に何も含まれていないことを確認してください？を押します。これは、SQL インジェクションのリスクを軽減するためです。
- を参照してください GET (all) APIに対する要求は、最大1000レコードを返します。を設定してクエリを実行した場合も同様です max_records パラメータを1000より大きい値に設定すると、1000レコードのみが返されます。
- 管理機能を実行する場合は、Unified Manager UI を使用することを推奨します。

トラブルシューティング用のログ

システムログを使用して、API の実行中に発生する可能性のある障害の原因を分析し、問題のトラブルシューティングを行うことができます。

API 呼び出しに関連する問題のトラブルシューティングを行うには、次の場所からログを取得します。

ログの場所	使用
/var/log/ocie/access_log.log	<p>API を呼び出しているユーザ名、開始時刻、実行時間、ステータス、URL など、API 呼び出しに関するすべての詳細情報が含まれます。</p> <p>このログファイルを使用して、頻繁に使用される API を確認したり、GUI ワークフローのトラブルシューティングを行ったりできます。また、実行時間に基づいて分析の規模を調整することもできます。</p>
/var/log/ocum/ocumserver.log	<p>すべての API 実行ログが含まれます。</p> <p>このログファイルを使用して、API 呼び出しのトラブルシューティングとデバッグを行うことができます。</p>
/var/log/ocie/server.log	<p>すべての Wildfly サーバ構成と、サービスの開始 / 停止に関連するログが含まれています。</p> <p>このログファイルを使用して、Wildfly サーバの開始、停止、または導入時に発生する問題のルート原因を見つけることができます。</p>
/var/log/ocie/au.log	<p>Acquisition Unit 関連のログが含まれます。</p> <p>このログファイルは、ONTAP でオブジェクトを作成、変更、または削除したときに使用できますが、Active IQ Unified Manager REST API には反映されません。</p>

ジョブオブジェクトの非同期プロセス

Active IQ Unified Manager は、を提供します `jobs` 他のAPIの実行中に実行されたジョブに関する情報を取得するAPI。非同期処理がジョブオブジェクトを使用してどのように動作するかを理解しておく必要があります。

一部の API 呼び出し、特にリソースの追加や変更を使用される API 呼び出しは、他の呼び出しよりも完了に時間がかかることがあります。Unified Manager は、これらの長時間実行されている要求を非同期的に処理します。

ジョブオブジェクトを使用して記述された非同期要求

非同期的に実行される API 呼び出しを行うと、HTTP 応答コード 202 が返されます。この応答コードは、要求が正常に検証され受け入れられたものの、まだ完了していないことを示します。要求はバックグラウンドタスクとして処理され、クライアントへの最初の HTTP 応答後も引き続き実行されます。応答には、要求に対応するジョブオブジェクトと、その一意の識別子が含まれます。

API 要求に関連付けられたジョブオブジェクトの照会

HTTP 応答で返されるジョブオブジェクトには、いくつかのプロパティが含まれています。状態プロパティを照会して、要求が正常に完了したかどうかを確認できます。ジョブオブジェクトは次のいずれかの状態になります。

- NORMAL
- WARNING
- PARTIAL_FAILURES
- ERROR

ジョブオブジェクトをポーリングするときに、タスクの終了状態（成功または失敗）を検出するために使用できる 2 つの方法があります。

- 標準のポーリング要求：現在のジョブの状態がすぐに返されます。
- ロングポーリング要求：ジョブの状態がになったとき NORMAL, ERROR, または PARTIAL_FAILURES.

非同期要求の手順

非同期 API 呼び出しを完了する大まかな手順を次に示します。

1. 問題：非同期 API 呼び出し。
2. 要求が正常に受け取られたことを示す HTTP 応答 202 を受信します。
3. 応答の本文からジョブオブジェクトの識別子を抽出します。
4. ループ内で、ジョブオブジェクトが終了状態になるまで待ちます NORMAL, ERROR, または PARTIAL_FAILURES.
5. ジョブの終了状態を確認し、ジョブの結果を取得します。

Hello API server 」と入力します

Hello API server は、シンプルな REST クライアントを使用して Active IQ Unified Manager で REST API を呼び出す方法を示すサンプルプログラムです。このサンプルプログラムでは、APIサーバに関する基本的な詳細情報をJSON形式で提供しています（サーバでのみサポートされます） application/json 形式）。

使用するURIは次のとおりです。 <https://<hostname>/api/datacenter/svm/svms>。このサンプルコードでは、次の入力パラメータを使用します。

- API サーバの IP アドレスまたは FQDN
- オプション：ポート番号（デフォルト： 443 ）
- ユーザ名
- パスワード
- 応答の形式 (application/json)

REST API を呼び出すために、 Jersey や RESTEasy など他のスクリプトを使用して Active IQ Unified

Manager 用の Java REST クライアントを作成することもできます。サンプルコードに関して、次の点に注意する必要があります。

- Active IQ Unified Manager への HTTPS 接続を使用して、指定した REST URI を呼び出します
- Active IQ Unified Manager から提供される証明書を無視します
- ハンドシェイク中にホスト名の検証をスキップします
- 使用 `javax.net.ssl.HttpsURLConnection` URI接続の場合
- サードパーティのライブラリを使用します (`org.apache.commons.codec.binary.Base64`) を使用して、HTTPベーシック認証で使用するBase64エンコード文字列を作成します

サンプルコードをコンパイルして実行するには、Java コンパイラ 1.8 以降を使用する必要があります。

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpsURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import org.apache.commons.codec.binary.Base64;

public class HelloApiServer {

    private static String server;
    private static String user;
    private static String password;
    private static String response_format = "json";
    private static String server_url;
    private static String port = null;

    /*
     * * The main method which takes user inputs and performs the *
    necessary steps
     * to invoke the REST URI and show the response
    */ public static void main(String[] args) {
        if (args.length < 2 || args.length > 3) {
            printUsage();
            System.exit(1);
        }
        setUserArguments(args);
        String serverBaseUrl = "https://" + server;
```

```

        if (null != port) {
            serverBaseUrl = serverBaseUrl + ":" + port;
        }
        server_url = serverBaseUrl + "/api/datacenter/svm/svms";
        try {
            HttpsURLConnection connection =
getAllTrustingHttpsURLConnection();
            if (connection == null) {
                System.err.println("FATAL: Failed to create HTTPS
connection to URL: " + server_url);
                System.exit(1);
            }
            System.out.println("Invoking API: " + server_url);
            connection.setRequestMethod("GET");
            connection.setRequestProperty("Accept", "application/" +
response_format);
            String authString = getAuthorizationString();
            connection.setRequestProperty("Authorization", "Basic " +
authString);
            if (connection.getResponseCode() != 200) {
                System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
+ connection.getResponseMessage());
                System.exit(1);
            }
            BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
            String response;
            System.out.println("Response:");
            while ((response = br.readLine()) != null) {
                System.out.println(response);
            }
            connection.disconnect();
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    /* Print the usage of this sample code */ private static void
printUsage() {
        System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
        System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
        System.out.println("\tHelloApiServer 10.22.12.34:8320 admin
password");
    }

```

```

        System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
        System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
        System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
    }

    /* * Set the server, port, username and password * based on user
inputs. */ private static void setUserArguments(
        String[] args) {
        server = args[0];
        user = args[1];
        password = args[2];
        if (server.contains(":")) {
            String[] parts = server.split(":");
            server = parts[0];
            port = parts[1];
        }
    }

    /*
    * * Create a trust manager which accepts all certificates and * use
this trust
    * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
    * SSL Context and skip * server hostname verification during SSL
handshake. * *
    * Note: Trusting all certificates or skipping hostname verification *
is not
    * required for API Services to work. These are done here to * keep
this sample
    * REST Client code as simple as possible.
    */ private static HttpsURLConnection
getAllTrustingHttpsURLConnection() {
    HttpsURLConnection conn =
null;
    try {
        /* Creating a trust manager that does not
validate certificate chains */
        TrustManager[]
trustAllCertificatesManager = new
TrustManager[]{new
X509TrustManager() {
            public X509Certificate[] getAcceptedIssuers(){return null;}
            public void checkClientTrusted(X509Certificate[]
certs, String authType){}
            public void checkServerTrusted(X509Certificate[]
certs, String authType){}
        }};
        /* Initialize the
SSLContext with the all-trusting trust manager */
        SSLContext sslContext = SSLContext.getInstance("TLS");

```



```

sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
URLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));
URL url = new URL(server_url);
conn =
(HttpURLConnection) url.openConnection();
/* Do not perform an
actual hostname verification during SSL Handshake.
Let all
hostname pass through as verified.*/
conn.setHostnameVerifier(new HostnameVerifier() {
public
boolean verify(String host, SSLSession session) {
return true;
});
} catch (Exception e)
{
e.printStackTrace();
return conn;
}

/*
* * This forms the Base64 encoded string using the username and
password *
* provided by the user. This is required for HTTP Basic
Authentication.
*/
private static String getAuthorizationString() {
String userPassword = user + ":" + password;
byte[] authEncodedBytes =
Base64.encodeBase64(userPassword.getBytes());
String authString = new String(authEncodedBytes);
return authString;
}
}

```

Unified Manager REST API

ここでは、Active IQ Unified Manager 用の REST API をカテゴリ別に示します。

Unified Manager インスタンスから、すべての REST API 呼び出しの詳細を含むオンラインドキュメントページを表示できます。このドキュメントでは、オンラインドキュメントの詳細については説明しません。このドキュメントに記載または説明されている各 API 呼び出しには、ドキュメントページで呼び出しを検索するために必要な情報のみが含まれています。特定の API 呼び出しを検索すると、入力パラメータ、出力形式、HTTP ステータスコード、要求処理タイプなど、その呼び出しのすべての詳細を確認できます。

ワークフロー内の各 API 呼び出しについて、ドキュメントページで検索するのに役立つ次の情報が含まれています。

- カテゴリ

ドキュメントページでは、機能的な関連領域またはカテゴリ別に API 呼び出しが分類されています。特定の API 呼び出しを検索するには、ページの一番下までスクロールし、該当する API カテゴリをクリックします。

- HTTP 動詞（呼び出し）

HTTP 動詞は、リソースに対して実行する操作を示します。各 API 呼び出しは、単一の HTTP 動詞を使用して実行されます。

- パス

パスは、呼び出しの実行時に操作が使用する特定のリソースを指定します。パス文字列がコア URL に追加され、リソースを識別する完全な URL が形成されます。

APIを使用してデータセンター内のストレージオブジェクトを管理する

の REST API `datacenter` カテゴリを使用すると、クラスタ、ノード、アグリゲート、Storage VM など、データセンター内のストレージオブジェクトを管理できます。ボリューム、LUN、ファイル共有、ネームスペース。これらの API はオブジェクトの設定を照会でき、一部の API を使用してオブジェクトの追加、削除、または変更の処理を実行できます。

これらの API のほとんどはクラスタをまたいだ集計値を提供する GET 呼び出しで、フィルタ、ソート、およびページ付けをサポートします。これらの API を実行すると、データベースからデータが返されます。したがって、新たに作成されたオブジェクトは、次の取得サイクルで検出されるまで応答に表示されません。

特定のオブジェクトの詳細を照会するには、そのオブジェクトの一意の ID を入力する必要があります。たとえば、ストレージオブジェクトの指標や分析情報については、を参照してください ["パフォーマンス指標の表示"](#)。

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```



cURL コマンド、例、要求、および API への応答は、Swagger API インターフェイスで参照できます。Swagger にも記載されているとおり、結果を特定のパラメータでフィルタおよび順序付けすることができます。これらの API を使用して、クラスタ、ボリューム、Storage VM などの特定のストレージオブジェクトについての結果をフィルタリングできます。

データセンター内のストレージオブジェクト用の API

HTTP 動詞	パス	説明
GET	<code>/datacenter/cluster/clusters</code> <code>/datacenter/cluster/clusters/{key}</code>	このメソッドを使用して、データセンター全体の ONTAP クラスタの詳細を表示できます。API は、クラスタの IPv4 アドレスや IPv6 アドレス、ノードの健全性、パフォーマンス容量、ハイアベイラビリティ（HA）ペアなどのノードに関する情報を返し、クラスタがオール SAN アレイかどうかを示します。

HTTP 動詞	パス	説明
GET	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	データセンター内のクラスタにインストールされているライセンスの詳細を返します。必要な条件に基づいて結果をフィルタできます。ライセンスキー、クラスタキー、有効期限、ライセンス範囲などの情報が返されます。ライセンスキーを入力すると、特定のライセンスの詳細を取得できます。
GET	/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}	このメソッドを使用して、データセンター内のノードの詳細を表示できます。ノードのクラスタ、ノードの健全性、パフォーマンス容量、およびハイアベイラビリティ（HA）ペアに関する情報を表示できます。
GET	/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}	このメソッドを使用して、データセンター内の CIFS 共有の詳細を表示できます。クラスタ、SVM、およびボリュームの詳細以外にも、アクセス制御リスト（ACL）に関する情報が返されます。
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	<p>このメソッドを使用して、サポートされている NFS サービスのエクスポートポリシーの詳細を表示できます。</p> <p>このメソッドを使用して、クラスタまたは Storage VM のエクスポートポリシーを照会し、NFS ファイル共有のプロビジョニングに使用できます。ワークロードでのエクスポートポリシーの割り当てと再利用の詳細については、「CIFS および NFS ファイル共有のプロビジョニング」を参照してください。</p>

HTTP 動詞	パス	説明
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	このメソッドを使用して、データセンター内のすべてのアグリゲートまたは特定のアグリゲートを表示し、ワークロードのプロビジョニングや監視を行うことができます。クラスタとノードの詳細、使用済みパフォーマンス容量、使用可能なスペースと使用済みのスペース、Storage Efficiency などの情報が返されます。
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	このメソッドを使用して、データセンター全体のすべての LUN を表示できます。クラスタと SVM の詳細、QoS ポリシー、igroup など、LUN に関する情報を表示できます。
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	このメソッドを使用して、データセンター内のストレージオブジェクトに適用可能なすべての QoS ポリシーの詳細を表示できます。クラスタと SVM の詳細、固定またはアダプティブのポリシーの詳細、そのポリシーに該当するオブジェクトの数などの情報が返されます。
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	このメソッドを使用して、すべての FlexVol または FlexGroup ボリュームについて、データセンター全体の qtree の詳細を表示できます。クラスタと SVM の詳細、FlexVol ボリューム、エクスポートポリシーなどの情報が返されます。

HTTP 動詞	パス	説明
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	<p>このメソッドを使用して、データセンター内のすべてのボリュームを表示できます。SVM とクラスタの詳細、QoS ポリシーとエクスポートポリシー、ボリュームのタイプが読み書き可能、データ保護、負荷共有のいずれであるかなど、ボリュームに関する情報が返されます。</p> <p>FlexVol および FlexClone ボリュームについては、それぞれのアグリゲートに関する情報を表示できます。FlexGroup ボリュームの場合、コンスティチュエントアグリゲートのリストが表示されます。</p>
GET POST DELETE PATCH	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}	<p>特定の LUN ターゲットへのアクセスを許可されたイニシエータグループ（igroup）を割り当てることができます。既存の igroup がある場合は、その igroup を割り当てることができます。igroup を作成して、LUN に割り当てすることもできます。</p> <p>これらのメソッドを使用して、igroup の照会、作成、削除、および変更を実行できます。</p> <p>注意事項：</p> <ul style="list-style-type: none"> • POST: igroupの作成中に、アクセスを割り当てるStorage VMを指定できます。 • DELETE: 特定のigroupを削除するには、入力パラメータとしてigroupキーを指定する必要があります。すでに LUN に割り当てられている igroup は削除できません。 • PATCH: 特定のigroupを変更するには、入力パラメータとしてigroupキーを指定する必要があります。また、更新するプロパティとその値を入力する必要があります。

HTTP 動詞	パス	説明
GET	/datacenter/svm/svms	<p>これらのメソッドを使用して、Storage Virtual Machine（Storage VM）を表示、作成、削除、および変更できます。</p> <ul style="list-style-type: none"> • POST: 作成するStorage VMオブジェクトを入力パラメータとして指定する必要があります。カスタムの Storage VM を作成して、必要なプロパティを割り当てることができます。 • DELETE: 特定のStorage VMを削除するには、Storage VMキーを指定する必要があります。 • PATCH: 特定のStorage VMを変更するには、Storage VMキーを指定する必要があります。また、更新するプロパティとその値を入力する必要があります。
POST	/datacenter/svm/svms/{key}	
DELETE		
PATCH		



注意事項：

環境で SLO ベースのワークロードプロビジョニングを有効にしている場合、Storage VM を作成する際には、CIFS または SMB、NFS、FCP など、LUN とファイル共有のプロビジョニングに必要なすべてのプロトコルがこの環境でサポートされていることを確認してください。および iSCSI などです。Storage VM が必要なサービスをサポートしていないと、プロビジョニングワークフローが失敗することがあります。対応するワークロードタイプのサービスも有効にすることを推奨します。

環境で SLO ベースのワークロードプロビジョニングを有効にしている場合、ストレージワークロードがプロビジョニングされている Storage VM は削除できません。CIFS または SMB サーバが設定されている Storage VM を削除すると、ローカルの Active Directory 設定に加えて CIFS サーバまたは SMB サーバも削除されます。ただし、CIFS サーバまたは SMB サーバの名前は Active Directory 設定に残っているため、Active Directory サーバから手動で削除する必要があります。

データセンター内のネットワーク要素用の API

データセンターカテゴリの次の API は、環境内のポートとネットワークインターフェイス、特に FC ポート、FC インターフェイス、イーサネットポート、および IP インターフェイスに関する情報を取得します。

HTTP 動詞	パス	説明
GET	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	データセンター環境内のすべてのイーサネットポートに関する情報を取得します。入力パラメータとしてポートキーを使用すると、そのポートの情報を表示できます。クラスタの詳細、ブロードキャストドメイン、状態、速度などのポートの詳細、と入力し、ポートが有効になっているかどうかを取得されます。
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	このメソッドを使用して、データセンター環境内の FC インターフェイスの詳細を表示できます。入力パラメータとしてインターフェイスキーを使用すると、そのインターフェイスの情報を表示できます。クラスタの詳細、ホームノードの詳細、ホームポートの詳細などの情報が取得されます。
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	データセンター環境のノードで使用されているすべての FC ポートに関する情報を取得します。入力パラメータとしてポートキーを使用すると、そのポートの情報を表示できます。クラスタの詳細、ポート概要、サポートされているプロトコル、ポートの状態などの情報が取得されます。
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	このメソッドを使用して、データセンター環境内の IP インターフェイスの詳細を表示できます。入力パラメータとしてインターフェイスキーを使用すると、そのインターフェイスの情報を表示できます。クラスタの詳細、IPspace の詳細、ホームノードの詳細、フェイルオーバーが有効かどうかなどの情報が取得されます。

プロキシアクセスを介して **ONTAP API** にアクセスする

ゲートウェイ API を使用すると、Active IQ Unified Manager クレデンシャルを使用して ONTAP REST API を実行し、ストレージオブジェクトを管理するという利点が得られます。これらの API は、Unified Manager Web UI から API ゲートウェイ機能を有効にすると使用できます。


Unified Manager REST API では、ONTAP クラスタである Unified Manager データソースで実行する一連の操作のみがサポートされます。その他の機能は、ONTAP API を使用して利用できます。ゲートウェイAPIを使用すると、Unified Managerをパススルーインターフェイスにして、管理対象のONTAP クラスタですべてのAPI要求をトンネリングできます。各データセンタークラスタに個別にログインする必要はありません。単一の管理ポイントとして機能し、Unified Manager インスタンスで管理される ONTAP クラスタ全体で API を実行できます。API ゲートウェイ機能を使用すると、個別にログインしなくても、複数の ONTAP クラスタを一元的に管理できます。ゲートウェイ API を使用すると、ONTAP REST API 処理を実行して Unified Manager にログインしたまま ONTAP クラスタを管理できます。



すべてのユーザは、GET 処理を使用してクエリを実行できます。アプリケーション管理者は、すべての ONTAP REST 処理を実行できます。

ゲートウェイは、ヘッダーと本文の形式を ONTAP API と同じにすることで、API 要求をトンネリングするプロキシとして機能します。Unified Manager のクレデンシャルを使用して特定の処理を実行することで、個々のクラスタのクレデンシャルを渡すことなく ONTAP クラスタにアクセスして管理することができます。クラスタ認証とクラスタ管理は引き続き管理されますが、API 要求は特定のクラスタで直接実行されます。API から返される応答は、対応する ONTAP REST API を ONTAP から直接実行した場合と同じです。

HTTP 動詞	パス（URL）	説明
GET	/gateways	<div><p>この取得メソッドは、ONTAP REST 呼び出しをサポートする Unified Manager で管理されているすべてのクラスタのリストを取得します。クラスタの詳細を確認し、クラスタ UUID または Universal Unique Identifier（UUID）に基づいて他の方法を実行するように選択できます。</p><div><p>ゲートウェイ API は、ONTAP 9.5 以降でサポートされているクラスタのみを取得し、HTTPS を使用して Unified Manager に追加します。</p></div></div>

HTTP 動詞	パス (URL)	説明
GET POST DELETE PATCH OPTIONS (Swaggerでは提供されていません) HEAD (Swaggerでは提供されていません)	<div> <div>/gateways/{uuid}/{path}</div> <div>  <p>「 {uuid} 」の値を、REST 処理を実行するクラスタ UUID に置き換える必要があります。また、UUID が ONTAP 9.5 以降でサポートされているクラスタのものであること、および Unified Manager に HTTPS 経由で追加されていることを確認してください。 \ {path} を ONTAP REST URL に置き換える必要があります。削除する必要があります /api/ URLから。</p> </div> </div>	<p>これは単一ポイントのプロキシ API で、POST、削除、パッチ処理がサポートされ、すべての ONTAP REST API に対応しています。ONTAP でサポートされている場合は、API に制限は適用されません。トンネリングまたはプロキシ機能をディセーブルにすることはできません。</p> <p>。OPTIONS メソッドは、ONTAP REST APIでサポートされているすべての処理を返します。たとえば、ONTAP APIでのみがサポートされている場合などです GET を実行します OPTIONS このゲートウェイAPIの戻り値を使用するメソッド GET をクリックします。Swagger ではサポートされていませんが、他の API ツールで実行することもできます。</p> <p>。OPTIONS メソッドは、リソースが使用可能かどうかを決定します。この処理を使用すると、HTTP 応答ヘッダー内のリソースに関するメタデータを表示できます。Swagger ではサポートされていませんが、他の API ツールで実行することもできます。</p>

API ゲートウェイトンネリングの概要

ゲートウェイ API を使用すると、Unified Manager を介して ONTAP オブジェクトを管理できます。Unified Manager はクラスタと認証の詳細を管理し、ONTAP REST エンドポイントに要求をリダイレクトします。ゲートウェイ API は、ヘッダーおよび応答本文内の Engine of Application State (HATEOAS) リンクとして、URL および Hypermedia を API ゲートウェイベース URL で変換します。ゲートウェイ API は、ONTAP REST URL を追加して必要な ONTAP REST エンドポイントを実行するプロキシのベース URL として機能します。



ONTAP APIをAPIゲートウェイ経由で正常に実行するには、APIが実行されているONTAP クラスタの同じバージョンでサポートされている必要があります。ONTAP クラスタでサポートされていないAPIを実行しても、結果は返されません。

この例では、ゲートウェイAPI（プロキシベースURL）は次のようになります。 /gateways/{uuid}/

取得されるONTAP APIは次のとおりです。 /storage/volumes。 path パラメータの値として、ONTAP API REST URL を追加する必要があります。



パスを追加する際には、「」が削除されていることを確認してください" symbol at the beginning of the URL. For the API `/storage/volumes`, 追加 (Add) `storage/volumes`.

追加されるURLは次のとおりです。 `/gateways/{uuid}/storage/volumes`

を実行している GET 処理の場合、生成されるURLは次のとおりです。

`GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes`

。 `/api` ONTAP REST URLのタグが付加されたURLから削除され、ゲートウェイAPIのタグは保持されます。

• cURL コマンドの例 *

```
curl -X GET "https://<hostname>/api/gateways/lcd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

API は、クラスタ内のストレージボリュームのリストを返します。応答形式は、ONTAP から同じ API を実行した場合と同じです。ONTAP REST ステータスコードが返されます。

API スコープを設定します

すべての API には、クラスタのスコープ内にコンテキストセットがあります。Storage VM ベースで動作する API のスコープはクラスタでもあります。つまり、API 処理は管理対象クラスタ内の特定の Storage VM に対して実行されます。を実行すると `/gateways/{uuid}/{path}` APIを使用して、処理を実行するクラスタのクラスタUUID (Unified ManagerデータソースUUID) を入力していることを確認してください。そのクラスタ内の特定の Storage VM にコンテキストを設定する場合は、その Storage VM キーを `X-Dot-svm-UUID` パラメータとして指定するか、Storage VM の名前を `X-Dot-SVM-name` パラメータとして入力します。パラメータが文字列ヘッダーのフィルタとして追加され、そのクラスタ内の Storage VM の範囲内で処理が実行されます。

• cURL コマンドの例 *

```
curl -X GET "https://<hostname>/api/gateways/e4f33f90-f75f-11e8-9ed9-00a098e3215f/storage/volume" -H "accept: application/hal+json" -H "X-Dot-SVM-UUID: d9c33ec0-5b61-11e9-8760-00a098e3215f" -H "Authorization: Basic <Base64EncodedCredentials>"
```

ONTAP REST APIの使用方法の詳細については、を参照してください<https://docs.netapp.com/us-en/ontap-automation/index.html>["ONTAP REST API の自動化"]

APIを使用した管理タスクの実行

のAPIを使用できます `administration` バックアップ設定を変更するカテゴリで、バックアップファイル情報とクラスタ証明書を確認し、ONTAP クラスタをActive IQ Unified Manager データソースとして管理する。



これらの処理を実行するには、アプリケーション管理者ロールが必要です。また、 Unified Manager Web UI を使用してこれらの設定を行うこともできます。

HTTP 動詞	パス	説明
GET PATCH	/admin/backup-settings /admin/backup-settings	<p>を使用できます GET デフォルトでUnified Managerで設定されているバックアップスケジュールの設定を表示する方法。次のことを確認できます。</p> <ul style="list-style-type: none">• スケジュールが有効か無効か• スケジュールされたバックアップの頻度（日単位または週単位）• バックアップの時刻• アプリケーションに保持するバックアップファイルの最大数 <p>バックアップの時刻はサーバのタイムゾーンにあります。</p> <p>データベースのバックアップ設定は、 Unified Manager ではデフォルトで有効になっており、バックアップスケジュールを作成することはできません。ただし、を使用することはできます PATCH メソッドを使用して、デフォルト設定を変更します。</p>
GET	/admin/backup-file-info	<p>バックアップダンプファイルは、 Unified Manager のバックアップスケジュールが変更されるたびに生成されます。このメソッドを使用すると、変更したバックアップ設定に従ってバックアップファイルが生成されているかどうか、およびファイルの情報が変更した設定と一致するかどうかを確認できます。</p>
GET	/admin/datasource-certificate	<p>このメソッドを使用して、信頼ストアからデータソース（クラスタ）証明書を表示できます。ONTAP クラスタを Unified Manager データソースとして追加する前に、証明書を検証する必要があります。</p>

HTTP 動詞	パス	説明
GET	/admin/datasources/clusters	使用できます GET Unified Managerで管理されているデータソース（ONTAP クラスタ）の詳細を取得する方法。 新しいクラスタを Unified Manager にデータソースとして追加することもできます。クラスタを追加するには、ホスト名、ユーザ名、パスワードが必要です。 Unified Manager のデータソースとして管理されるクラスタを変更および削除するには、 ONTAP クラスタキーを使用します。
POST	/admin/datasources/clusters/{key}	
PATCH		
DELETE		

APIを使用したユーザの管理

のAPIを使用できます security Active IQ Unified Manager で選択したクラスタオブジェクトへのユーザアクセスを制御するカテゴリ。ローカルユーザまたはデータベースユーザを追加できます。また、認証サーバに属するリモートユーザやリモートグループを追加することもできます。ユーザに割り当てたロールの権限に基づいて、ストレージオブジェクトを管理したり、Unified Manager でデータを表示したりできます。



これらの処理を実行するには、アプリケーション管理者ロールが必要です。また、Unified Manager Web UI を使用してこれらの設定を行うこともできます。

のAPI security カテゴリでは、ユーザエンティティの一意の識別子としてkeyパラメータではなく、ユーザ名のusersパラメータを使用します。

HTTP 動詞	パス	説明
GET	/security/users	<p>これらのメソッドを使用して、ユーザの詳細を取得したり、Unified Manager に新しいユーザを追加したりできます。</p> <p>ユーザのタイプに基づいて、ユーザに特定のロールを追加できます。ユーザを追加する際には、ローカルユーザ、メンテナンスユーザ、およびデータベースユーザのパスワードを指定する必要があります。</p>
POST	/security/users	

HTTP 動詞	パス	説明
GET	/security/users/{name}	GET メソッドを使用すると、名前、E メールアドレス、ロール、認証タイプなど、ユーザのすべての詳細を取得できます。PATCH メソッドで詳細を更新できます。削除メソッドを使用すると、ユーザを削除できます。
PATCH		
DELETE		

APIを使用したパフォーマンス指標の表示

Active IQ Unified Manager には、の一連のAPIが用意されています /datacenter データセンター内のクラスタおよびストレージオブジェクトのパフォーマンスデータを表示できるカテゴリ。これらのAPIは、クラスタ、ノード、LUN、ボリューム、アグリゲートなどのさまざまなストレージオブジェクトのパフォーマンスデータを取得します。Storage VM、FC インターフェイス、FC ポート、イーサネットポート、IP インターフェイス

。 /metrics および /analytics APIを使用すると、パフォーマンス指標をさまざまなビューで確認できます。データセンター内の次のストレージオブジェクトについて、さまざまなレベルの詳細にドリルダウンできます。

- クラスタ
- ノード
- Storage VMs
- アグリゲート
- 個のボリューム
- LUN
- FC インターフェイス
- FC ポート
- イーサネットポート
- IP インターフェイス

次の表は、間の比較を示しています /metrics および /analytics 取得したパフォーマンスデータのの詳細を示すAPI。

指標	分析
1つのオブジェクトのパフォーマンスの詳細。たとえば、などです /datacenter/cluster/clusters/{key}/metrics APIでは、特定のクラスタの指標を取得するためのパスパラメータとしてクラスタキーを入力する必要があります。	データセンター内の同じタイプの複数のオブジェクトのパフォーマンスの詳細。たとえば、などです /datacenter/cluster/clusters/analytics APIは、データセンター内のすべてのクラスタの集合的な指標を取得します。

指標	分析
読み出しの時間間隔パラメータに基づくストレージオブジェクトのパフォーマンス指標サンプル。	特定の期間（72 時間を超える）における特定のタイプのストレージオブジェクトのパフォーマンスの概要レベルの集計値。
ノードやクラスタの詳細など、オブジェクトの基本的な詳細が読み出されます。	具体的な詳細は取得されません。
1 つのオブジェクトについて、読み取り、書き込み、合計、その他のカウンタなど、一定期間の平均パフォーマンス値の最小値、最大値、95 パーセンタイル値などの累積カウンタが取得されます。	同じタイプのすべてのオブジェクトについて、集約された単一の値が表示されます。

指標	分析
<p>時間範囲とサンプルデータは、次のスケジュールに基づいています。データの時間範囲。例として、1h、12h、1d、2d、3d があります。15D、1w、1m、2m、3m、6M。範囲が3日（72時間）を超える場合は1時間のサンプルを取得し、それ以外の場合は5分のサンプルを取得します。各期間は次のとおりです。</p> <ul style="list-style-type: none"> • 1H：直近1時間の測定値が5分以上にわたってサンプリングされます。 • 12時間：5分以上にわたってサンプリングされた最新の12時間のメトリック。 • 1D：直近の1日の測定値が5分以上にわたってサンプリングされます。 • 2D：直近2日間の測定値が5分を超えてサンプリングされます。 • 3D：直近3日間の測定値が5分を超えてサンプリングされます。 • 15D：1時間にわたってサンプリングされた最新の15日間のメトリック。 • 1W：1時間以上サンプリングされた最新の週のメトリック。 • 1M：最近1時間でサンプリングされた月のメトリックス。 • 2M：直近2カ月間の測定値が1時間以上にわたってサンプリングされます。 • 3M：最近3カ月間の測定値が1時間以上サンプリングされています。 • 6M：直近6カ月間の測定値が1時間以上にわたってサンプリングされます。 <p>使用可能な値は、1h、12h、1d、2d、3d です。15D、1w、1m、2m、3m、6M</p> <p>デフォルト値：1h</p>	<p>72時間以上。このサンプルを計算する期間は、ISO-8601 標準形式で表されます。</p>

指標APIの出力例

たとえば、などです `/datacenter/cluster/nodes/{key}/metrics` APIがノードについて次の詳細を取得する（特にその他）。



サマリ値の95パーセンタイルは、期間について収集されたサンプルの95%が、95パーセンタイルで指定された値よりも小さいカウンタ値を持っていることを示しています。

```

{
  "iops": {
    "local": {
      "other": 100.53,
      "read": 100.53,
      "total": 100.53,
      "write": 100.53
    },
    "other": 100.53,
    "read": 100.53,
    "total": 100.53,
    "write": 100.53
  },
  "latency": {
    "other": 100.53,
    "read": 100.53,
    "total": 100.53,
    "write": 100.53
  },
  "performance_capacity": {
    "available_iops_percent": 0,
    "free_percent": 0,
    "system_workload_percent": 0,
    "used_percent": 0,
    "user_workload_percent": 0
  },
  "throughput": {
    "other": 100.53,
    "read": 100.53,
    "total": 100.53,
    "write": 100.53
  },
  "timestamp": "2018-01-01T12:00:00-04:00",
  "utilization_percent": 0
}
],
"start_time": "2018-01-01T12:00:00-04:00",
"summary": {
  "iops": {
    "local_iops": {
      "other": {
        "95th_percentile": 28,
        "avg": 28,
        "max": 28,
        "min": 5
      }
    }
  },

```



```
"read": {
  "95th_percentile": 28,
  "avg": 28,
  "max": 28,
  "min": 5
},
"total": {
  "95th_percentile": 28,
  "avg": 28,
  "max": 28,
  "min": 5
},
"write": {
  "95th_percentile": 28,
  "avg": 28,
  "max": 28,
  "min": 5
}
},
```

分析**API**の出力例を示します

たとえば、などです /datacenter/cluster/nodes/analytics APIがすべてのノードに対して次の値を（特に）取得する。

```
{
  "iops": 1.7471,
  "latency": 60.0933,
  "throughput": 5548.4678,
  "utilization_percent": 4.8569,
  "period": 72,
  "performance_capacity": {
    "used_percent": 5.475,
    "available_iops_percent": 168350
  },
  "node": {
    "key": "37387241-8b57-11e9-8974-00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a",
    "uuid": "95f94e8d-8b4e-11e9-8974-00a098e0219a",
    "name": "ocum-infinity-01",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/nodes/37387241-8b57-11e9-8974-00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a"
      }
    }
  },
  "cluster": {
    "key": "37387241-8b57-11e9-8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a",
    "uuid": "37387241-8b57-11e9-8974-00a098e0219a",
    "name": "ocum-infinity",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/37387241-8b57-11e9-8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a"
      }
    }
  },
  "_links": {
    "self": {
      "href": "/api/datacenter/cluster/nodes/analytics"
    }
  }
},
```

使用可能なAPIのリスト

次の表で、について説明します /metrics および /analytics APIの詳細をご覧ください。



これらのAPIから返されるIOPSとパフォーマンスの指標には、たとえば2倍の値があります 100.53。これらの浮動小数点値をパイプ（|）およびワイルドカード（*）文字でフィルタリングすることはできません。

HTTP 動詞	パス	説明
GET	/datacenter/cluster/clusters/{key}/metrics	クラスタキーの入力パラメータで指定したクラスタのパフォーマンスデータ（サンプルと概要）を取得します。クラスタキーと UUID、時間範囲、IOPS、スループット、サンプル数などの情報が返されます。
GET	/datacenter/cluster/clusters/analytics	は、データセンター内のすべてのクラスタのパフォーマンス指標の概要を取得します。必要な条件に基づいて結果をフィルタできます。集計 IOPS、スループット、収集期間（時間数）などの値が返されます。
GET	/datacenter/cluster/nodes/{key}/metrics	ノードキーの入力パラメータで指定したノードのパフォーマンスデータ（サンプルとサマリ）を取得します。ノード UUID、時間範囲、IOPS、スループット、レイテンシ、パフォーマンスの概要、収集されたサンプル数、利用率などの情報が返されます。
GET	/datacenter/cluster/nodes/analytics	は、データセンター内のすべてのノードのパフォーマンス指標の概要を取得します。必要な条件に基づいて結果をフィルタできます。ノードキーやクラスタキーなどの情報、および集計 IOPS、スループット、収集期間（時間数）などの値が返されます。
GET	/datacenter/storage/aggregates/{key}/metrics	aggregate キーの入力パラメータで指定したアグリゲートのパフォーマンスデータ（サンプルとサマリ）を取得します。時間範囲、IOPS、レイテンシ、スループット、パフォーマンス容量の概要、各カウンタで収集されたサンプル数、使用率などの情報が返されます。

HTTP 動詞	パス	説明
GET	/datacenter/storage/aggregates/analytics	データセンター内のすべてのアグリゲートのパフォーマンス指標の概要が取得されます。必要な条件に基づいて結果をフィルタできます。アグリゲートキーやクラスタキーなどの情報、および集計 IOPS、スループット、収集期間（時間数）などの値が返されます。
GET	/datacenter/storage/luns/{key}/metrics /datacenter/storage/volumes/{key}/metrics	LUN またはボリュームキーの入力パラメータで指定された LUN またはファイル共有（ボリューム）のパフォーマンスデータ（サンプルとサマリ）を取得します。読み取り、書き込み、合計 IOPS、レイテンシ、スループットの最小値、最大値、平均値の概要などの情報。各カウンタについて収集されたサンプル数が返されます。
GET	/datacenter/storage/luns/analytics /datacenter/storage/volumes/analytics	データセンター内のすべての LUN またはボリュームのパフォーマンス指標の概要を取得します。必要な条件に基づいて結果をフィルタできます。Storage VM やクラスタキーなどの情報、および集計 IOPS、スループット、収集期間（時間数）などの値が返されます。
GET	/datacenter/svm/svms/{key}/metrics	Storage VM キーの入力パラメータで指定した Storage VM のパフォーマンスデータ（サンプルと概要）を取得します。など、サポートされている各プロトコルに基づく IOPS の概要 <code>nvmf</code> 、 <code>fcp</code> 、 <code>iscsi</code> 、および <code>nfs</code> 、スループット、レイテンシ、収集されたサンプル数が返されます。
GET	/datacenter/svm/svms/analytics	は、データセンター内のすべての Storage VM のパフォーマンス指標の概要を取得します。必要な条件に基づいて結果をフィルタできます。Storage VM の UUID、アグリゲート IOPS、レイテンシ、スループット、収集期間（時間数）などの情報が返されます。

HTTP 動詞	パス	説明
GET	/datacenter/network/ethernet/ports/{key}/metrics	ポートキーの入力パラメータで指定された特定のイーサネットポートのパフォーマンス指標を取得します。サポートされている範囲から間隔（時間範囲）を指定すると、API はその期間における最小、最大、平均パフォーマンス値などの累積カウンタを返します。
GET	/datacenter/network/ethernet/ports/analytics	データセンター環境内のすべてのイーサネットポートのパフォーマンス指標の概要を取得します。クラスタとノードキー、UUID、スループット、収集期間、ポートの利用率などの情報が返されます。ポートキー、利用率、クラスタとノードの名前と UUID など、使用可能なパラメータで結果をフィルタリングできます。
GET	/datacenter/network/fc/interfaces/{key}/metrics	インターフェイスキーの入力パラメータで指定した特定のネットワーク FC インターフェイスのパフォーマンス指標を取得します。サポートされている範囲から間隔（時間範囲）を指定すると、API はその期間における最小、最大、平均パフォーマンス値などの累積カウンタを返します。
GET	/datacenter/network/fc/interfaces/analytics	データセンター環境内のすべてのイーサネットポートのパフォーマンス指標の概要を取得します。クラスタと FC インターフェイスキーと UUID、スループット、IOPS、レイテンシ、Storage VM などの情報が返されます。クラスタと FC インターフェイスの名前と UUID、Storage VM、スループットなど、使用可能なパラメータで結果をフィルタリングできます。

HTTP 動詞	パス	説明
GET	/datacenter/network/fc/ports/{key}/metrics	ポートキーの入力パラメータで指定した特定の FC ポートのパフォーマンス指標を取得します。サポートされている範囲から間隔（時間範囲）を指定すると、API はその期間における最小、最大、平均パフォーマンス値などの累積カウンタを返します。
GET	/datacenter/network/fc/ports/analytics	データセンター環境内のすべての FC ポートのパフォーマンス指標の概要を取得します。クラスタとノードキー、UUID、スループット、収集期間、ポートの利用率などの情報が返されます。ポートキー、利用率、クラスタとノードの名前と UUID など、使用可能なパラメータで結果をフィルタリングできます。
GET	/datacenter/network/ip/interfaces/{key}/metrics	インターフェイスキーの入力パラメータで指定されたネットワーク IP インターフェイスのパフォーマンス指標を取得します。サポートされている範囲から間隔（時間範囲）を指定すると、サンプル数、累積カウンタ、スループット、送受信パケット数などの情報が返されます。
GET	/datacenter/network/ip/interfaces/analytics	データセンター環境内のすべてのネットワーク IP インターフェイスのパフォーマンス指標の概要を取得します。クラスタと IP インターフェイスキー、UUID、スループット、IOPS、レイテンシなどの情報が返されます。クラスタと IP インターフェイスの名前と UUID、IOPS、レイテンシ、スループットなど、使用可能なパラメータで結果をフィルタリングできます。

ジョブおよびシステムの詳細を表示しています

を使用できます jobs のAPI management-server 非同期操作の実行の詳細を表示するカテゴリ。。 system のAPI management-server カテゴリを使用すると、Active IQ Unified Manager 環境内のインスタンの詳細を表示できます。

ジョブの表示

Active IQ Unified Manager では、リソースの追加や変更などの処理は、同期および非同期の API 呼び出しによって実行されます。非同期で実行されるようにスケジュールされている呼び出しは、その呼び出しに対して作成されたジョブオブジェクトによって追跡できます。各ジョブオブジェクトには、識別用の一意のキーがあります。各ジョブオブジェクトはジョブオブジェクト URI を返し、ジョブの進捗状況を確認および追跡できます。この API を使用して、各実行の詳細を取得できます。

この API を使用して、履歴データを含む、データセンターのすべてのジョブオブジェクトを照会できます。デフォルトですべてのジョブを照会すると、Web UI および API インターフェイスからトリガーされた最新 20 件のジョブの詳細が返されます。組み込みのフィルタを使用して、特定のジョブを表示します。ジョブキーを使用して特定のジョブの詳細を照会し、リソースに対して次の処理セットを実行することもできます。

カテゴリ	HTTP 動詞	パス	説明
management-server	取得	/management-server/jobs	すべてのジョブのジョブ詳細を返します。ソート順が指定されていない場合は、最後に送信されたジョブオブジェクトが先頭に返されます。
management-server	取得	/management-server/jobs/{key} ジョブオブジェクトのジョブキーを入力して、そのジョブの具体的な詳細を表示します。	特定のジョブオブジェクトの詳細を返します。

システムの詳細の表示

を使用します /management-server/system APIを使用して、インスタンス固有の詳細情報をUnified Manager環境で照会できます。API から返される製品とサービスに関する情報には、システムにインストールされている Unified Manager のバージョン、UUID、ベンダー名、ホスト OS、名前、概要、および Unified Manager インスタンスで実行されているサービスのステータス。

カテゴリ	HTTP 動詞	パス	説明
management-server	取得	/management-server/system	この API を実行するために入力パラメータは必要ありません。デフォルトでは、現在の Unified Manager インスタンスのシステムの詳細が返されます。

APIを使用してイベントとアラートを管理する

。 events、 alerts、および scripts のAPI management-server カテゴリを使用

すると、Active IQ Unified Manager 環境のアラートに関連付けられているイベント、アラート、およびスクリプトを管理できます。

イベントを表示および変更する

Unified Manager は、Unified Manager で監視および管理されているクラスタについて ONTAP で生成されたイベントを受信します。これらの API を使用して、クラスタに対して生成されたイベントを表示し、解決および更新することができます。

を実行します GET のメソッド `/management-server/events` APIを使用して、履歴データなど、データセンター内のイベントを照会できます。名前、インパクトレベル、インパクトエリア、重大度などの組み込みフィルタを使用します。特定のイベントを表示するには、状態、リソース名、およびリソースタイプを指定します。リソースタイプと領域パラメータは、イベントが発生したストレージオブジェクトに関する情報を返し、影響領域は、可用性、容量、構成、セキュリティなど、イベントが発生した問題に関する情報を返します。保護とパフォーマンス：

この API の PATCH 処理を実行すると、イベントの解決ワークフローを有効にすることができます。イベントを自分または別のユーザーに割り当てて、イベントの受信を確認することができます。リソースに対して手順を実行してイベントをトリガーした問題を解決すると、この API を使用してイベントを解決済みとしてマークできます。

イベントの詳細については、を参照してください ["イベントの管理"](#)。

カテゴリ	HTTP 動詞	パス	説明
management-server	取得	<code>/management-server/events</code> <code>/management-server/events/{key}</code>	GET All メソッドを実行すると、応答の本文にはデータセンター内のすべてのイベントの詳細が含まれます。特定のキーを使用してイベントの詳細を取得すると、特定のイベントの詳細を表示し、リソースに対して次の処理を実行できます。応答の本文は、そのイベントの詳細で構成されます。
management-server	パッチ	<code>management-server/events/{key}</code>	この API を実行してイベントを割り当てるか、または状態を <code>acknowledged</code> または <code>Resolved</code> に変更します。このメソッドを使用して、自分または別のユーザーにイベントを割り当てることもできます。これは同期操作です。

アラートの管理

イベントは自動的かつ継続的に生成されます。Unified Manager では、イベントが特定のフィルタ条件を満た

している場合にのみアラートが生成されます。アラートを生成するイベントを選択できます。を使用します
/management-server/alerts APIでは、特定のイベントまたは特定の重大度タイプイベントが発生したときに自動的に通知を送信するアラートを設定できます。

アラートの詳細については、を参照してください ["アラートの管理"](#)。

カテゴリ	HTTP 動詞	パス	説明
management-server	取得	/management-server/alerts /management-server/alerts/{key}	アラートキーを使用して、環境内の既存のすべてのアラートまたは特定のアラートを照会します。環境で生成されたアラートについて、アラート概要、アクション、通知の送信先 E メール ID、イベント、重大度などの情報を確認することができます。
management-server	投稿（Post）	/management-server/alerts	このメソッドを使用すると、特定のイベントに対するアラートを追加できます。アラート名、アラートが適用される物理リソースまたは論理リソース、アラートが有効かどうか、および SNMP トラップを発行するかどうかを追加する必要があります。アラートを生成する追加の詳細を追加できます。これには、アラートスクリプトを追加する場合に備えて、アクション、通知 E メール ID、スクリプトの詳細などの情報が含まれます。
management-server	パッチと削除	management-server/events/{key}	これらのメソッドを使用して、特定のアラートを変更および削除できます。概要、名前、アラートの有効化 / 無効化など、さまざまな属性を変更できます。不要になったアラートを削除できます。



アラートを追加するリソースを選択する際に、リソースとしてクラスタを選択しても、そのクラスタ内のストレージオブジェクトは自動的に選択されないことに注意してください。たとえば、すべてのクラスタのすべての重大イベントに対するアラートを作成した場合、受信するアラートの対象はクラスタの重大イベントのみです。ノードやアグリゲートなどの重大イベントに対するアラートは受信しません。

スクリプトの管理

を使用します `/management-server/scripts` APIでは、アラートがトリガーされたときに実行されるスクリプトにアラートを関連付けることもできます。Unified Manager で複数のストレージオブジェクトを自動的に変更または更新するスクリプトを作成することができます。スクリプトはアラートに関連付けられます。イベントによってアラートがトリガーされるとスクリプトが実行されます。カスタムスクリプトをアップロードし、アラートが生成されたときの動作をテストすることができます。Unified Manager でイベントに対するアラートが発生したときにスクリプトが実行されるように、スクリプトにアラートを関連付けることができます。

スクリプトの詳細については、を参照してください ["スクリプトの管理"](#)。

カテゴリ	HTTP 動詞	パス	説明
management-server	取得	<code>/management-server/scripts</code>	この API を使用して、環境内の既存のすべてのスクリプトを照会します。特定のスクリプトのみを表示するには、標準のフィルタと処理順を使用します。
management-server	投稿（Post）	<code>/management-server/scripts</code>	この API を使用して、スクリプトの概要を追加し、アラートに関連付けられたスクリプトファイルをアップロードします。

APIを使用してワークロードを管理する

ここで説明する API は、ストレージワークロードの表示、LUN とファイル共有の作成、パフォーマンスサービスレベルとストレージ効率化ポリシーの管理、ストレージワークロードに対するポリシーの割り当てなど、ストレージ管理のさまざまな機能に対応しています。

APIを使用したストレージワークロードの表示

ここに記載されている API を使用すると、データセンター内のすべての ONTAP クラスタのストレージワークロードをまとめて表示できます。また、Active IQ Unified Manager 環境でプロビジョニングされているストレージワークロードの数と、その容量とパフォーマンス（IOPS）の統計情報も表示されます。

ストレージワークロードを表示します

データセンター内のすべてのクラスタのすべてのストレージワークロードを表示するには、次のメソッドを使用します。特定の列で応答をフィルタリングする方法については、Unified Manager インスタンスで使用可能な API のリファレンスドキュメントを参照してください。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/workloads

ストレージワークロードの概要を表示します

使用済み容量、使用可能容量、使用済み IOPS、使用可能 IOPS、各パフォーマンスサービスレベルで管理されているストレージワークロードの数を評価するには、次のメソッドを使用します。任意の LUN、NFS ファイル共有、または CIFS 共有のストレージワークロードを表示できます。この API は、ストレージワークロードの概要、Unified Manager でプロビジョニングされたストレージワークロードの概要、データセンターの概要、データセンターの合計、使用済み、使用可能なスペースと IOPS の概要を、割り当てられたパフォーマンスサービスレベル別に表示します。この API の応答として受信した情報を使用して、Unified Manager UI のダッシュボードにデータが表示されます。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/workloads-summary

APIを使用したアクセスエンドポイントの管理

Storage Virtual Machine（SVM）、LUN、およびファイル共有のプロビジョニングに必要なアクセスエンドポイントまたは論理インターフェイス（LIF）を作成する必要があります。Active IQ Unified Manager 環境内の SVM、LUN、またはファイル共有のアクセスエンドポイントを表示、作成、変更、および削除できます。

アクセスエンドポイントを表示します

Unified Manager 環境のアクセスエンドポイントのリストを表示するには、次のメソッドを使用します。特定の SVM、LUN、またはファイル共有のアクセスエンドポイントのリストを照会するには、SVM、LUN、またはファイル共有の一意の識別子を入力する必要があります。一意のアクセスエンドポイントキーを入力して、特定のアクセスエンドポイントの詳細を取得することもできます。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

アクセスエンドポイントを追加する

カスタムのアクセスエンドポイントを作成して、必要なプロパティを割り当てることができます。作成するアクセスエンドポイントの詳細を、入力パラメータとして指定する必要があります。この API、または System Manager または ONTAP CLI を使用して、各ノードにアクセスエンドポイントを作成できます。アクセスエンドポイントの作成では、IPv4 アドレスと IPv6 アドレスの両方がサポートされます。



LUN とファイル共有をプロビジョニングするためには、SVM にノードあたりの最小アクセスエンドポイント数を設定する必要があります。SVM には、ノードごとに少なくとも 2 つのアクセスエンドポイントを設定する必要があります。1 つは CIFS プロトコルおよび / または NFS プロトコルをサポートし、もう 1 つは iSCSI プロトコルまたは FCP プロトコルをサポートします。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	投稿 (Post)	/storage-provider/access-endpoints

アクセスエンドポイントを削除する

特定のアクセスエンドポイントを削除するには、次のメソッドを使用します。特定のアクセスエンドポイントを削除するには、入力パラメータとしてアクセスエンドポイントキーを指定する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	削除	/storage-provider/access-endpoints/{key}

アクセスエンドポイントを変更します

アクセスエンドポイントを変更し、そのプロパティを更新するには、次のメソッドを使用します。特定のアクセスエンドポイントを変更するには、アクセスエンドポイントキーを指定する必要があります。また、更新するプロパティとその値を入力する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	パッチ	/storage-provider/access-endpoints/{key}

APIを使用したActive Directoryマッピングの管理

ここに記載された API を使用して、SVM 上の CIFS 共有のプロビジョニングに必要な SVM の Active Directory マッピングを管理できます。ONTAP を備えた SVM をマッピングするには、Active Directory マッピングを設定する必要があります。

Active Directory マッピングを表示します

SVM の Active Directory マッピングの設定の詳細を表示するには、次のメソッドを使用します。SVM の Active Directory マッピングを表示するには、SVM キーを入力する必要があります。特定のマッピングの詳細

を照会するには、マッピングキーを入力する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/active-directories-mappings /storage-provider/active-directories-mappings/{key}

Active Directory マッピングを追加します

SVM に Active Directory マッピングを作成するには、次のメソッドを使用します。マッピングの詳細を入力パラメータとして指定する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	投稿（Post）	/storage-provider/active-directories-mappings

APIを使用したファイル共有の管理

を使用できます /storage-provider/file-shares データセンター環境内のCIFSおよびNFSファイル共有ボリュームを表示、追加、変更、削除するためのAPI。

ファイル共有ボリュームをプロビジョニングする前に、SVM が作成され、サポートされるプロトコルでプロビジョニングされていることを確認します。プロビジョニング中にパフォーマンスサービスレベル（PSL）またはストレージ効率化ポリシー（SEP）を割り当てる場合は、ファイル共有を作成する前に PSL または SEP を作成する必要があります。

ファイル共有を表示します

Unified Manager 環境で使用可能なファイル共有ボリュームを表示するには、次のメソッドを使用します。Active IQ Unified Manager のデータソースとして ONTAP クラスタを追加すると、それらのクラスタのストレージワークロードが Unified Manager インスタンスに自動的に追加されます。この API は、Unified Manager インスタンスに自動および手動で追加されたファイル共有を取得します。特定のファイル共有の詳細を表示するには、ファイル共有キーを指定してこの API を実行します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/file-shares /storage-provider/file-shares/{key}

ファイル共有を追加

SVM に CIFS および NFS ファイル共有を追加するには、次のメソッドを使用します。作成するファイル共有の詳細を入力パラメータとして指定する必要があります。この API を使用して FlexGroup ボリュームを追加

することはできません。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	投稿（Post）	/storage-provider/file-shares



アクセス制御リスト（ACL）パラメータまたはエクスポートポリシーパラメータのどちらを指定するかに応じて、CIFS 共有または NFS ファイル共有が作成されます。ACL パラメータの値を指定しない場合、CIFS 共有は作成されず、デフォルトで NFS 共有が作成され、すべてのアクセスが提供されます。

データ保護ボリュームの作成：SVMにファイル共有を追加する場合、デフォルトでマウントされるボリュームのタイプは `rw`（読み取り/書き込み）。データ保護（DP）ボリュームを作成する場合は、`dp` を指定します `dp` の値として指定します `type` パラメータ

ファイル共有を削除します

特定のファイル共有を削除するには、次のメソッドを使用します。特定のファイル共有を削除するには、入力パラメータとしてファイル共有キーを入力する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	削除	/storage-provider/file-shares/{key}

ファイル共有を変更する

ファイル共有を変更し、そのプロパティを更新するには、次のメソッドを使用します。

特定のファイル共有を変更するには、ファイル共有キーを指定する必要があります。また、更新するプロパティとその値を入力する必要があります。



この API の 1 回の呼び出しで更新できるプロパティは 1 つだけです。更新が複数ある場合は、この API を何度でも実行する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	パッチ	/storage-provider/file-shares/{key}

APIを使用したLUNの管理

を使用できます `/storage-provider/luns` データセンター環境内のLUNを表示、追加、変更、削除するためのAPI。

LUN をプロビジョニングする前に、SVM が作成され、サポートされるプロトコルでプロビジョニングされていることを確認してください。プロビジョニング中にパフォーマンスサービスレベル（PSL）またはストレージ効率化ポリシー（SEP）を割り当てる場合は、LUN を作成する前に PSL または SEP を作成する必要

があります。

LUN を表示します

Unified Manager 環境の LUN を表示するには、次のメソッドを使用します。Active IQ Unified Manager のデータソースとして ONTAP クラスタを追加すると、それらのクラスタのストレージワークロードが Unified Manager インスタンスに自動的に追加されます。この API は、Unified Manager インスタンスに自動および手動で追加されたすべての LUN を取得します。特定の LUN の詳細を表示するには、LUN キーを指定してこの API を実行します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/luns /storage-provider/luns/{key}

LUN を追加します

SVM に LUN を追加するには、次のメソッドを使用します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	投稿（Post）	/storage-provider/luns



cURL 要求で、入力にオプションのパラメータ `volume_name_tag` の値を指定すると、LUN の作成でボリュームの名前を指定する際にその値が使用されます。このタグにより、ボリュームを簡単に検索できます。要求にボリュームキーを指定した場合、このタギングはスキップされます。

LUN を削除します

特定の LUN を削除するには、次のメソッドを使用します。特定の LUN を削除するには、LUN キーを指定する必要があります。



ONTAP でボリュームを作成し、そのボリュームで Unified Manager を使用して LUN をプロビジョニングした場合、この API を使用してすべての LUN を削除すると、ボリュームも ONTAP クラスタから削除されます。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	削除	/storage-provider/luns/{key}

LUNs を変更する

LUN を変更してそのプロパティを更新するには、次のメソッドを使用します。特定の LUN を変更するには、LUN キーを指定する必要があります。また、更新する LUN プロパティとその値を入力する必要があります。この API を使用して LUN アレイを更新する場合は 'API の使用に関する推奨事項を確認する必要があります



この API の 1 回の呼び出しで更新できるプロパティは 1 つだけです。更新が複数ある場合は、この API を何度でも実行する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	パッチ	/storage-provider/luns/{key}

APIを使用したパフォーマンスサービスレベルの管理

Active IQ Unified Manager でストレージプロバイダ API を使用して、パフォーマンスサービスレベルを表示、作成、変更、および削除できます。

パフォーマンスサービスレベルを表示します

ストレージワークロードに割り当てる際にパフォーマンスサービスレベルを表示するには、次のメソッドを使用します。この API は、システム定義およびユーザ作成のすべてのパフォーマンスサービスレベルを表示し、すべてのパフォーマンスサービスレベルの属性を取得します。特定のパフォーマンスサービスレベルを照会する場合は、パフォーマンスサービスレベルの一意の ID を入力して詳細を取得する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/performance-service-levels /storage-provider/performance-service-levels/{key}

パフォーマンスサービスレベルを追加

システム定義のパフォーマンスサービスレベルがストレージワークロードに必要なサービスレベル目標（SLO）を満たしていない場合は、次のメソッドでカスタムパフォーマンスサービスレベルを作成し、ストレージワークロードに割り当てることができます。作成するパフォーマンスサービスレベルの詳細を入力します。IOPS プロパティには、有効な値の範囲を入力してください。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	投稿（Post）	/storage-provider/performance-service-levels

パフォーマンスサービスレベルを削除します

特定のパフォーマンスサービスレベルを削除するには、次のメソッドを使用します。ワークロードに割り当てられている場合、または他に使用可能なパフォーマンスサービスレベルがない場合、そのパフォーマンスサービスレベルは削除できません。特定のパフォーマンスサービスレベルを削除するには、パフォーマンスサービスレベルの一意の ID を入力パラメータとして指定する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	削除	/storage-provider/performance-service-levels/{key}

パフォーマンスサービスレベルの変更

パフォーマンスサービスレベルを変更してそのプロパティを更新するには、次のメソッドを使用します。システム定義のパフォーマンスサービスレベル、またはワークロードに割り当てられているパフォーマンスサービスレベルは変更できません。特定のパフォーマンスサービスレベルを変更するには、の一意の ID を指定する必要があります。また、更新する IOPS プロパティと有効な値も入力する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	パッチ	/storage-provider/performance-service-levels/{key}

パフォーマンスサービスレベルに基づくアグリゲート機能の表示

パフォーマンスサービスレベルに基づいてアグリゲート機能を照会するには、次のメソッドを使用します。この API は、データセンターで使用可能なアグリゲートのリストを返し、それらのアグリゲートでサポート可能なパフォーマンスサービスレベルに関する機能を示します。ボリュームでワークロードをプロビジョニングする際に、特定のパフォーマンスサービスレベルをサポートするアグリゲートの機能を表示し、その機能に基づいてワークロードをプロビジョニングできます。アグリゲートを指定できるのは、API を使用してワークロードをプロビジョニングする場合のみです。この機能は Unified Manager Web UI では使用できません。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/aggregate-capabilities /storage-provider/aggregate-capabilities/{key}

APIを使用したストレージ効率化ポリシーの管理

ストレージプロバイダ API を使用して、ストレージ効率化ポリシーを表示、作成、変更、および削除できます。

次の点に注意してください。



- Unified Manager でワークロードを作成する場合、ストレージ効率化ポリシーの割り当ては必須ではありません。
- ポリシーが割り当てられたあとで、ワークロードからストレージ効率化ポリシーの割り当てを解除することはできません。
- 重複排除や圧縮など、ONTAP で指定されたストレージ設定がワークロードに含まれている場合、Unified Manager でストレージワークロードを追加するときに適用するストレージ効率化ポリシーの設定で、その設定を上書きすることができます。

ストレージ効率化ポリシーを表示します

ストレージワークロードに割り当てる前にストレージ効率化ポリシーを表示するには、次のメソッドを使用します。この API は、システム定義およびユーザ作成のすべてのストレージ効率化ポリシーを表示し、すべてのストレージ効率化ポリシーの属性を取得します。特定のストレージ効率化ポリシーを照会するには、ポリシーの一意の ID を入力して詳細を取得する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/storage-efficiency-policies /storage-provider/storage-efficiency-policies/{key}

ストレージ効率化ポリシーを追加します

システム定義のポリシーがストレージワークロードのプロビジョニング要件を満たしていない場合は、次のメソッドでカスタムのストレージ効率化ポリシーを作成し、ストレージワークロードに割り当てることができます。作成するストレージ効率化ポリシーの詳細を入力パラメータとして指定します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	投稿（Post）	/storage-provider/storage-efficiency-policies

ストレージ効率化ポリシーを削除します

特定のストレージ効率化ポリシーを削除するには、次のメソッドを使用します。ワークロードに割り当てられている場合、または他に使用可能なストレージ効率化ポリシーがない場合、そのストレージ効率化ポリシーは削除できません。特定のストレージ効率化ポリシーを削除するには、ストレージ効率化ポリシーの一意の ID を入力パラメータとして指定する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	削除	/storage-provider/storage-efficiency-policies/{key}

ストレージ効率化ポリシーを変更し、そのプロパティを更新するには、次のメソッドを使用します。システム定義のストレージ効率化ポリシー、またはワークロードに割り当てられているストレージ効率化ポリシーは変更できません。特定のストレージ効率化ポリシーを変更するには、ストレージ効率化ポリシーの一意の ID を指定する必要があります。また、更新するプロパティとその値を指定する必要があります。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	パッチ	/storage-provider/storage-efficiency-policies/{key}

ストレージ管理のための一般的なAPIワークフロー

この一般的なワークフローは、クライアントアプリケーション開発者向けに、クライアントアプリケーションから Active IQ Unified Manager API を呼び出して一般的なストレージ管理機能を実行する方法を示します。ここでは、これらのサンプルワークフローの一部を紹介します。

ワークフローごとに、代表的なストレージ管理のユースケースと、使用するサンプルコードを記載します。各タスクについて、1 つ以上の API 呼び出しで構成されるワークフロープロセスを使用して説明します。

ワークフローで使用する API 呼び出しについて

Unified Manager インスタンスから、すべての REST API 呼び出しの詳細を含むオンラインドキュメントページを表示できます。このドキュメントでは、オンラインドキュメントの詳細については説明しません。このドキュメントのワークフローサンプルで使用されている各 API 呼び出しには、ドキュメントページで呼び出しを検索するために必要な情報だけが含まれています。特定の API 呼び出しを検索すると、入力パラメータ、出力形式、HTTP ステータスコード、要求処理タイプなど、呼び出しのすべての詳細を確認できます。

ワークフロー内の各 API 呼び出しについて、ドキュメントページで検索するのに役立つ次の情報が含まれています。

- カテゴリ：ドキュメントページでは、機能的な関連領域またはカテゴリ別に API 呼び出しが分類されています。特定の API 呼び出しを検索するには、ページの一番下までスクロールして、該当する API カテゴリをクリックします。
- HTTP 動詞（呼び出し）：HTTP 動詞は、リソースに対して実行する操作を示します。各 API 呼び出しは、単一の HTTP 動詞を使用して実行されます。
- パス：このパスは、呼び出しの実行中に環境が処理する特定のリソースを指定します。パス文字列がコア URL に追加され、リソースを識別する完全な URL が形成されます。

APIを使用したアグリゲートのスペースの問題の特定

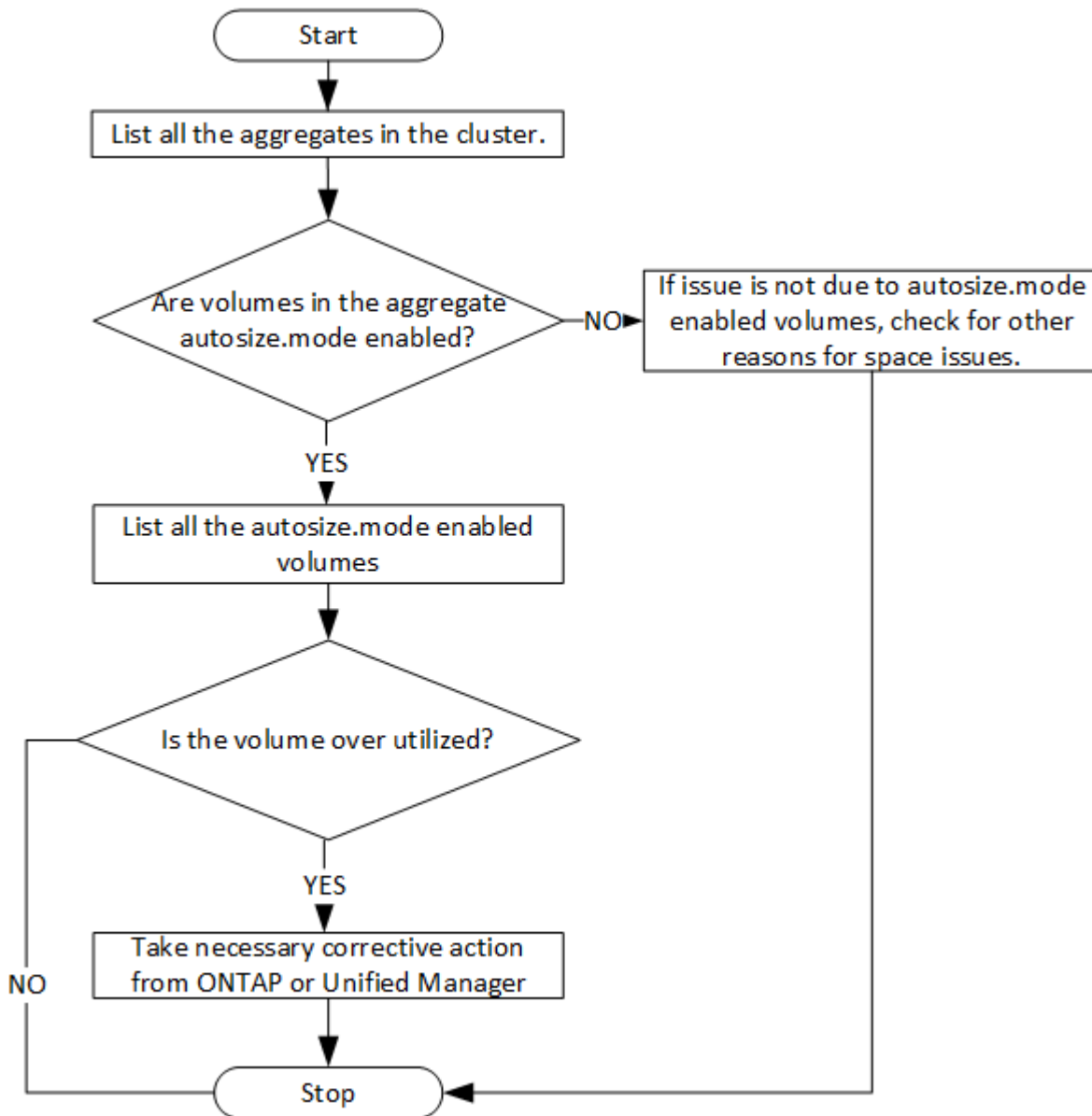
Active IQ Unified Manager のデータセンター API を使用して、ボリューム内のスペースの可用性と使用率を監視できます。ボリューム内のスペースの問題を特定し、使用率が高すぎる、または十分に活用されていないストレージリソースを特定できます。

アグリゲート用のデータセンター API は、使用可能スペースと使用済みスペース、およびスペース削減の効

率化設定に関する関連情報を取得します。また、指定した属性に基づいて取得した情報をフィルタすることもできます。

アグリゲートにスペースが不足しているかどうかを確認する方法の 1 つは、オートサイズモードを有効にした環境内にボリュームがあるかどうかを確認することです。次に、過剰に利用されているボリュームを特定し、対処を行う必要があります。

次のフローチャートは、オートサイズモードが有効になっているボリュームに関する情報を取得するプロセスを示しています。



このフローは、クラスタがすでに ONTAP に作成され、Unified Manager に追加されていることを前提としています。

1. 値がわからないかぎりクラスタキーを取得します。

カテゴリ	HTTP 動詞	パス
データセンター	取得	/datacenter/cluster/clusters

2. クラスターキーをフィルタパラメータとして使用して、そのクラスターのアグリゲートを照会します。

カテゴリ	HTTP 動詞	パス
データセンター	取得	/datacenter/storage/aggregates

3. 応答から、アグリゲートのスペース使用量を分析し、スペースに問題があるアグリゲートを特定します。スペース問題を使用する各アグリゲートについて、同じ JSON 出力からアグリゲートキーを取得します。
4. 各アグリゲートキーを使用して、autosize-modeパラメータの値がになっているすべてのボリュームをフィルタリングします grow.

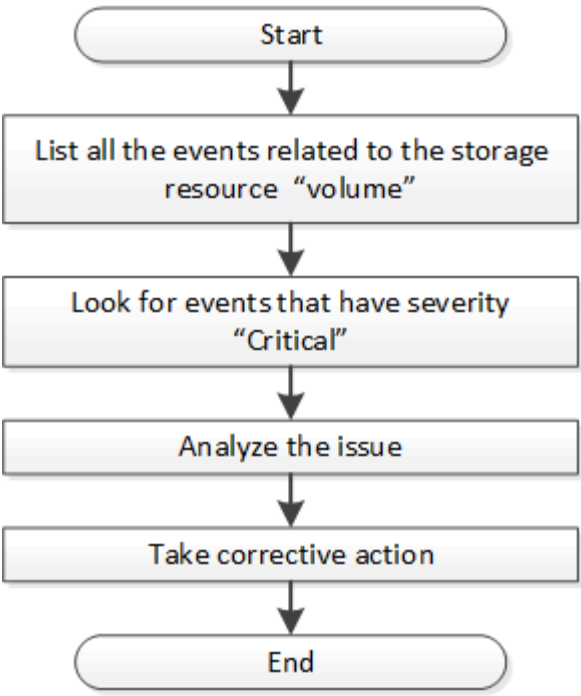
カテゴリ	HTTP 動詞	パス
データセンター	取得	/datacenter/storage/volumes

5. 利用率が高いボリュームを分析します。
6. ボリュームのスペースに関する問題に対処するために、アグリゲート間でのボリュームの移動などの必要な対処策を実行します。これらの操作は、ONTAP または Unified Manager Web UI から実行できます。

イベントAPIを使用してストレージオブジェクトの問題を特定する

データセンターのストレージオブジェクトがしきい値を超えると、そのイベントに関する通知が表示されます。この通知を使用すると、問題を分析し、を使用して対処することができます events API :

このワークフローでは、リソースオブジェクトとしてボリュームの例を使用します。を使用できます events APIを使用してボリュームに関連するイベントのリストを取得し、そのボリュームの重大な問題を分析してから、問題を修正します。



修復手順を実行する前に、次の手順に従ってボリュームの問題を特定します。

手順

- 1. データセンター内のボリュームに関する重要な Active IQ Unified Manager イベント通知を分析できます。
- 2. /management-server/events APIで次のパラメータを使用して、ボリュームに対するすべてのイベントを照会します。

```
"resource_type": "volume"
"severity": "critical"
```

カテゴリ	HTTP 動詞	パス
management-server	取得	/management-server / イベント

- 3. の出力を確認し、特定のボリュームの問題を分析します。
- 4. Unified Manager REST API または Web UI を使用して必要な操作を実行し、問題を解決します。

ゲートウェイ **API** を使用した **ONTAP** ボリュームのトラブルシューティング

ゲートウェイ API はゲートウェイとして機能し、ONTAP API を呼び出して ONTAP ストレージオブジェクトに関する情報を照会し、報告された問題に対処するための修復方法を実行します。

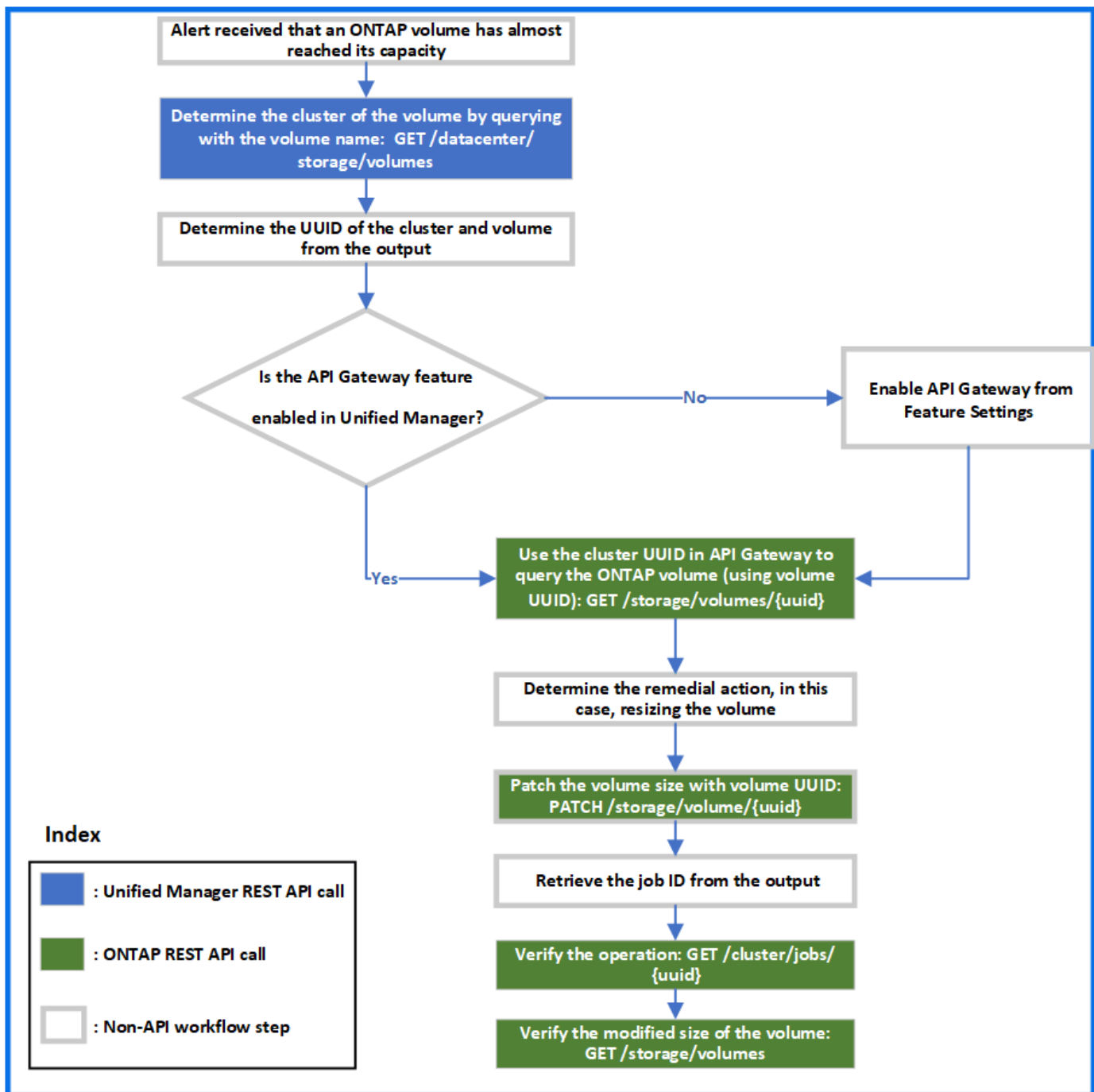
このワークフローでは、ONTAP ボリュームの容量がほぼフルに達したときにイベントが生成されるユースケースの例を示します。また、Active IQ Unified Manager と ONTAP の REST API を組み合わせて呼び出すことで、この問題に対処する方法についても説明します。

ワークフローの手順を実行する前に、次の点を確認してください。



- ゲートウェイの API とその使用方法を理解しておきます。詳細については、を参照してください ["プロキシアクセスを介して ONTAP API にアクセスする"](#)。
- ONTAP REST API の使用について理解しておく必要があります。ONTAP REST APIの使用については、を参照してください<https://docs.netapp.com/us-en/ontap-automation/index.html>["ONTAP 自動化に関するドキュメント"]。
- あなたはアプリケーション管理者です。
- REST API 処理を実行するクラスタは ONTAP 9.5 以降でサポートされており、クラスタは HTTPS 経由で Unified Manager に追加されます。

次の図は、ONTAP of 問題ボリュームの容量使用に関するトラブルシューティングワークフローの各手順を示しています。



このワークフローでは、Unified Manager と ONTAP REST API の呼び出しポイントを取り上げます。

1. ボリュームの容量利用率を通知するイベントからボリューム名をメモします。
2. name パラメータにボリューム名を指定し、次の Unified Manager API を実行してボリュームを照会します。

カテゴリ	HTTP 動詞	パス
データセンター	取得	/datacenter/storage/volumes

3. 出力からクラスタ UUID とボリューム UUID を取得します。

4. Unified Manager Web UI で、 * 一般 * > * 機能設定 * > * API ゲートウェイ * と移動して、API ゲートウェイ機能が有効になっているかどうかを確認します。有効になっていないかぎり、ゲートウェイカテゴリの API を呼び出すことはできません。機能が無効になっている場合は、有効にします。
5. クラスタUUIDを使用してONTAP APIを実行します /storage/volumes/{uuid} APIゲートウェイを使用 : API パラメータとしてボリューム UUID を指定した場合、クエリはボリュームの詳細を返します。

ONTAP API を API ゲートウェイ経由で実行する場合、Unified Manager のクレデンシャルは認証のために内部で渡されます。このため、個々のクラスタアクセスに対して追加の認証手順を実行する必要はありません。

カテゴリ	HTTP 動詞	パス
Unified Manager : ゲートウェイ ONTAP ストレージ	取得	ゲートウェイAPI : /gateways/{uuid}/{path} ONTAP API : /storage/volumes/{uuid}



/gateways / { uuid } / { path } の値は、REST 処理を実行するクラスタ UUID に置き換える必要があります。 \ { path } を ONTAP REST URL / ストレージ / ボリューム / { uuid } に置き換える必要があります。

追加されるURLは次のとおりです。

/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}

GET処理の実行時に生成されるURLは次のとおりです。

GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes/{volume_uuid}

◦ cURL コマンドの例 *

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

6. 出力から、取得するサイズ、使用状況、および修復方法を確認します。このワークフローで実施する修復方法は、ボリュームのサイズを変更することです。
7. ボリュームのサイズを変更するには、クラスタ UUID を使用し、API ゲートウェイから次の ONTAP API を実行してください。ゲートウェイと ONTAP API の入力パラメータについては、ステップ 5 を参照してください。

カテゴリ	HTTP 動詞	パス
Unified Manager : ゲートウェイ ONTAP ストレージ	パッチ	ゲートウェイAPI : /gateways/{uuid}/{path} ONTAP API : /storage/volumes/{uuid}



クラスタ UUID とボリューム UUID に加え、ボリュームのサイズ変更用の size パラメータの値を入力する必要があります。値をバイト単位で入力してください。たとえば、ボリュームのサイズを100GBから120GBに拡張する場合は、クエリの最後にパラメータサイズの値を入力します。-d {"size\": 128849018880}"

° cURL コマンドの例 *

```
curl -X PATCH "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>" -d {"size\": 128849018880}"
```

+

JSON 出力でジョブ UUID が返されます。

- ジョブ UUID を使用して、ジョブが正常に実行されたかどうかを確認します。クラスタ UUID とジョブ UUID を使用して、API ゲートウェイ経由で次の ONTAP API を実行します。ゲートウェイと ONTAP API の入力パラメータについては、ステップ 5 を参照してください。

カテゴリ	HTTP 動詞	パス
Unified Manager : ゲートウェイ ONTAP クラスタ	取得	ゲートウェイAPI : /gateways/{uuid}/{path} ONTAP API : /cluster/jobs/{uuid}

返される HTTP コードは、ONTAP REST API の HTTP ステータスコードと同じです。

- 次の ONTAP API を実行して、サイズ変更されたボリュームの詳細を照会します。ゲートウェイと ONTAP API の入力パラメータについては、ステップ 5 を参照してください。

カテゴリ	HTTP 動詞	パス
Unified Manager : ゲートウェイ ONTAP ストレージ	取得	ゲートウェイAPI : /gateways/{uuid}/{path} ONTAP API : /storage/volumes/{uuid}

出力には、拡張後のボリュームサイズとして 120GB が表示されます。

ワークロード管理用のAPIワークフロー

Active IQ Unified Manager を使用して、ストレージワークロード（LUN、NFS ファイル共有、CIFS 共有）をプロビジョニングおよび変更できます。プロビジョニングは、Storage Virtual Machine（SVM）の作成から、ストレージワークロードへのパフォーマンスサービスレベルポリシーとストレージ効率化ポリシーの適用まで、複数の手順で構成されます。ワークロードの変更は、特定のパラメータの変更と、パラメータでの追加機能の有効化で構成されます。

次のワークフローについて説明します。

- Unified Manager で Storage Virtual Machine（SVM）をプロビジョニングするためのワークフロー



このワークフローは、Unified Manager で LUN またはファイル共有をプロビジョニングする前に実行する必要があります。

- ファイル共有のプロビジョニング
- LUN のプロビジョニング
- LUN とファイル共有の変更（ストレージワークロードのパフォーマンスサービスレベルパラメータの更新例を使用）
- CIFS プロトコルをサポートするための NFS ファイル共有の変更
- QoS を AQoS にアップグレードするためのワークロードの変更



各プロビジョニングワークフロー（LUN およびファイル共有）では、クラスタの SVM を確認するワークフローを完了しておく必要があります。

また、ワークフローで各 API を使用する前に、推奨事項と制限事項を確認しておく必要があります。API の詳細については、関連する概念および資料に記載されている個々のセクションを参照してください。

APIを使用したクラスタのSVMの確認

ファイル共有または LUN をプロビジョニングする前に、クラスタに Storage Virtual Machine（SVM）が作成されているかどうかを確認する必要があります。



このワークフローは、ONTAP クラスタが Unified Manager に追加され、クラスタキーが取得されていることを前提としています。クラスタには、LUN とファイル共有をプロビジョニングするためのライセンスが必要です。

1. クラスタに SVM が作成されているかどうかを確認します。

カテゴリ	HTTP 動詞	パス
データセンター	取得	/datacenter/svm/svms /datacenter/svm/svms/{key}

◦ cURL の例 *

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. SVM キーが返されない場合は、SVM を作成します。SVM を作成するには、SVM をプロビジョニングするクラスタキーが必要です。SVM 名も指定する必要があります。次の手順を実行します。

カテゴリ	HTTP 動詞	パス
データセンター	取得	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}

クラスタキーを取得します。

◦ cURL の例 *

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

3. 出力からクラスタキーを取得し、SVM を作成するための入力として使用します。



SVM を作成するには、LUN およびファイル共有のプロビジョニングに必要なすべてのプロトコル（CIFS、NFS、FCP など）をサポートしていることを確認してください。および iSCSI などです。SVM が必要なサービスをサポートしていないと、プロビジョニングワークフローが失敗することがあります。対応するワークロードタイプのサービスも有効にすることを推奨します。

カテゴリ	HTTP 動詞	パス
データセンター	投稿（Post）	/datacenter/svm/svms

◦ cURL の例 *

SVM オブジェクトの詳細を入力パラメータとして指定します。

```
curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": { }, \"key\": \"1cd8a442-86d1,type=objecttype,uuid=1cd8a442-86d1-11e0-ae1c-9876567890123\", \"name\": \"cluster2\", \"uuid\": \"02c9e252-41be-11e9-81d5-00a0986138f7\" } ], \"cifs\": { \"ad_domain\": { \"fqdn\": \"string\", \"password\": \"string\", \"user\": \"string\" }, \"enabled\": true, \"name\": \"CIFS1\" }, \"cluster\": { \"key\": \"1cd8a442-86d1-11e0-ae1c-123478563412,type=object type,uuid=1cd8a442-86d1-11e0-ae1c-9876567890123\" }, \"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ], \"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] }, \"fc\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true, \"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" } }, \"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\": \"dataLif1\" }, \"ipspace\": { \"name\": \"exchange\" }, \"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\", \"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\", \"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ] }, \"name\": \"svm1\", \"nfs\": { \"enabled\": true }, \"nis\": { \"domain\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true }, \"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" }, \"gateway\": \"string\" } ], \"snapshot_policy\": { \"name\": \"default\" }, \"state\": \"running\", \"subtype\": \"default\" } }
```

+

JSON 出力にジョブオブジェクトキーが表示され、作成した SVM の検証に使用できます。

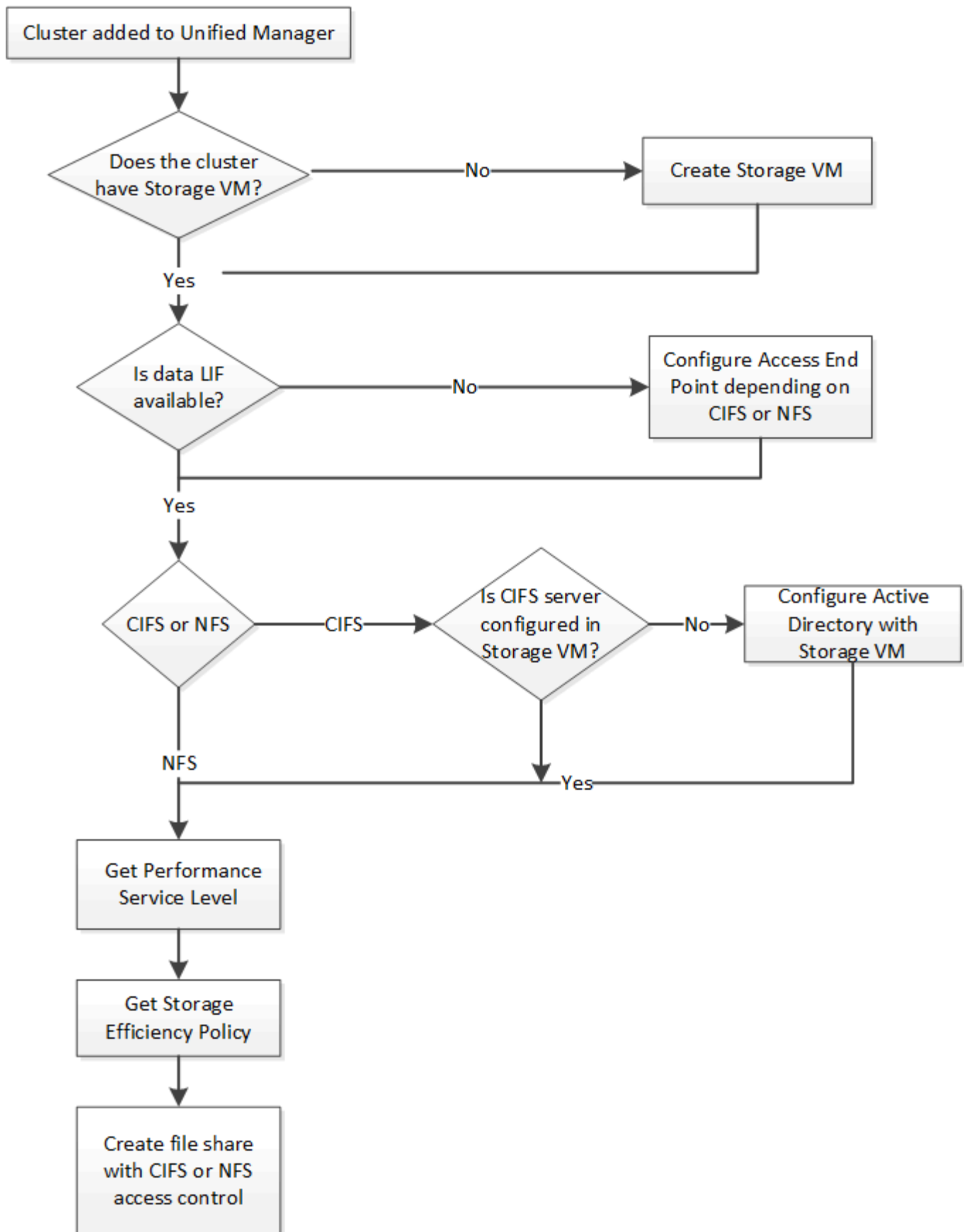
4. ジョブオブジェクトキーを使用して照会し、SVM の作成を確認します。SVM が正常に作成されると、SVM キーが応答に返されます。

カテゴリ	HTTP 動詞	パス
management-server	取得	/management-server/jobs/{key}

APIを使用したCIFSおよびNFSファイル共有のプロビジョニング

Active IQ Unified Manager に付属のプロビジョニング API を使用して、Storage Virtual Machine （ SVM ） に CIFS 共有と NFS ファイル共有をプロビジョニングできます。このプロビジョニングワークフローでは、ファイル共有を作成する前に SVM、パフォーマンスサービスレベル、およびストレージ効率化ポリシーのキーを取得する手順について詳しく説明します。

次の図は、ファイル共有のプロビジョニングワークフローの各手順を示しています。ワークフローには、CIFS 共有と NFS ファイル共有の両方のプロビジョニングが含まれています。



次の点を確認します。



- ONTAP クラスタが Unified Manager に追加され、クラスタキーが取得されている必要があります。
- クラスタに SVM が作成されている必要があります。
- SVM で CIFS サービスと NFS サービスがサポートされている。SVM が必要なサービスをサポートしていないと、ファイル共有のプロビジョニングが失敗することがあります。
- FCP ポートがポートプロビジョニング用にオンラインになっている必要があります。

1. CIFS 共有を作成する SVM で、データ LIF またはアクセスエンドポイントを使用できるかどうかを確認します。SVM で使用可能なアクセスエンドポイントのリストを取得します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

◦ cURL の例 *

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. 使用するアクセスエンドポイントがリストに表示されている場合は、アクセスエンドポイントキーを取得します。表示されていない場合は、アクセスエンドポイントを作成します。



CIFS プロトコルを有効にしてアクセスエンドポイントを作成してください。CIFS プロトコルを有効にしたアクセスエンドポイントを作成しないと、CIFS 共有のプロビジョニングは失敗します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	投稿 (Post)	/storage-provider/access-endpoints

◦ cURL の例 *

作成するアクセスエンドポイントの詳細を、入力パラメータとして指定する必要があります。


```
curl -X POST "https://<hostname>/api/storage-provider/access-endpoints"
-H "accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
{ \"data_protocols\": \"nfs\",
\"fileshare\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=volume,uuid=f3063d27-2c71-44e5-9a69-a3927c19c8fc\" },
\"gateway\": \"10.132.72.12\",
\"ip\": { \"address\": \"10.162.83.26\",
\"ha_address\": \"10.142.83.26\",
\"netmask\": \"255.255.0.0\" },
\"lun\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=lun,uuid=d208cc7d-80a3-4755-93d4-5db2c38f55a6\" },
\"mtu\": 15000, \"name\": \"aep1\",
\"svm\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a178d39e12:type=vserver,uuid=1d1c3198-fc57-11e8-99ca-00a098d38e12\" },
\"vlan\": 10}"
```

+

JSON 出力にジョブオブジェクトキーが表示され、作成したアクセスエンドポイントの検証に使用できません。

3. アクセスエンドポイントを検証します。

カテゴリ	HTTP 動詞	パス
management-server	取得	/management-server/jobs/{key}

4. CIFS 共有と NFS ファイル共有のどちらを作成する必要があるかを判断します。CIFS 共有を作成するには、次の手順を実行します。

- a. SVM に CIFS サーバが設定されているかどうかを確認します。そのためには、SVM に Active Directory マッピングが作成されているかどうかを特定します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/active-directories-mappings

- b. Active Directory マッピングが作成されている場合は、キーを取得します。作成されていない場合は、SVM に Active Directory マッピングを作成します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	投稿（Post）	/storage-provider/active-directories-mappings

▪ cURL の例 *

Active Directory マッピングを作成するための詳細を、入力パラメータとして指定する必要があります。

```
curl -X POST "https://<hostname>/api/storage-provider/active-directories-mappings" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
{ \"_links\": {},
  \"dns\": \"10.000.000.000\",
  \"domain\": \"example.com\",
  \"password\": \"string\",
  \"svm\": { \"key\": \"9f4ddea-e395-11e9-b660-005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },
  \"username\": \"string\"}
```

+

これは同期呼び出しであり、Active Directory マッピングの作成を出力で確認できます。エラーが発生した場合はエラーメッセージが表示されるため、トラブルシューティングして要求を再実行します。

5. CIFS 共有または NFS ファイル共有を作成する SVM の SVM キーを取得します。詳細については、「クラスタの SVM の確認」ワークフローのトピックを参照してください。
6. 次の API を実行し、応答からパフォーマンスサービスレベルのキーを取得します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/performance-service-levels



システム定義のパフォーマンスサービスレベルの詳細を取得するには、を設定します `system_defined` パラメータをに入力します `true`。出力から、ファイル共有に適用するパフォーマンスサービスレベルのキーを取得します。

7. 必要に応じて、次の API を実行し、応答からファイル共有に適用するストレージ効率化ポリシーのキーを取得します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/storage-efficiency-policies

8. ファイル共有を作成します。アクセス制御リストとエクスポートポリシーを指定すると、CIFS と NFS の両方をサポートするファイル共有を作成できます。次の手順は、ボリュームのどちらか一方のプロトコルのみをサポートするファイル共有を作成する場合の情報を示しています。作成後に NFS ファイル共有を更新し、アクセス制御リストを追加することもできます。詳細については、「ストレージワークロードの変更」を参照してください。

- a. CIFS 共有のみを作成する場合は、アクセス制御リスト（ACL）に関する情報を収集します。CIFS 共有を作成するには、次の入力パラメータに有効な値を指定します。割り当てたユーザグループごとに、CIFS 共有または SMB 共有のプロビジョニング時に ACL が作成されます。ACL および Active Directory マッピングに入力した値に基づいて、CIFS 共有の作成時にアクセス制御とマッピングが決定されます。

▪ サンプル値 * を指定した cURL コマンド

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
  },
}
```

- b. NFS ファイル共有のみを作成する場合は、エクスポートポリシーに関する情報を収集します。NFS ファイル共有を作成するには、次の入力パラメータに有効な値を指定します。この値に基づいて、NFS ファイル共有の作成時にエクスポートポリシーが適用されます。



NFS 共有のプロビジョニングする際には、必要なすべての値を指定してエクスポートポリシーを作成するか、エクスポートポリシーキーを指定して既存のエクスポートポリシーを再利用できます。Storage VM のエクスポートポリシーを再利用する場合は、エクスポートポリシーキーを追加する必要があります。キーが不明な場合は、を使用してエクスポートポリシーキーを取得できます /datacenter/protocols/nfs/export-policies API新しいポリシーを作成する場合は、次の例に示すようにルールを入力する必要があります。入力されたルールに対して、API はホスト、Storage VM、およびルールを照合して既存のエクスポートポリシーを検索します。既存のエクスポートポリシーがある場合は、そのポリシーが使用されます。それ以外の場合は、新しいエクスポートポリシーが作成されます。

▪ サンプル値 * を指定した cURL コマンド

```
"export_policy": {
  "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
  "name_tag": "ExportPolicyNameTag",
  "rules": [
    {
      "clients": [
        {
          "match": "0.0.0.0/0"
        }
      ]
    }
  ]
}
```

アクセス制御リストとエクスポートポリシーを設定したら、CIFS と NFS ファイル共有の両方に必須のパラメータに有効な値を指定します。



ストレージ効率化ポリシーは、ファイル共有の作成ではオプションのパラメータです。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	投稿（Post）	/storage-provider/file-shares

JSON 出力にジョブオブジェクトキーが表示され、作成したファイル共有の検証に使用できます。。ジョブの照会で返されたジョブオブジェクトキーを使用して、ファイル共有の作成を確認します。

カテゴリ	HTTP 動詞	パス
management-server	取得	/management-server/jobs/{key}

応答の末尾に、作成されたファイル共有のキーが表示されます。

```

],
"job_results": [
  {
    "name": "fileshareKey",
    "value": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
  }
],
"_links": {
  "self": {
    "href": "/api/management-server/jobs/06a6148bf9e862df:-2611856e:16e8d47e722:-7f87"
  }
}
}

```

1. 返されたキーを指定して次の API を実行し、ファイル共有の作成を確認します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/file-shares/{key}

◦ JSON 出力の例 *

のPOSTメソッドが表示されます /storage-provider/file-shares 各関数に必要なすべてのAPIを内部的に呼び出し、オブジェクトを作成します。たとえば、を呼び出します /storage-provider/performance-service-levels/ ファイル共有にパフォーマンスサービスレベルを割り当てるためのAPI。

```

{
  "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
  "name": "FileShare_377",
  "cluster": {
    "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
    "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
    "name": "AFFA300-206-68-70-72-74",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959"
      }
    }
  }
}

```

```

    },
    "svm": {
      "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
      "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
      "name": "RRT_ritu_vs1",
      "_links": {
        "self": {
          "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959"
        }
      }
    },
    "assigned_performance_service_level": {
      "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
      "name": "Value",
      "peak_iops": 75,
      "expected_iops": 75,
      "_links": {
        "self": {
          "href": "/api/storage-provider/performance-service-levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
        }
      }
    },
    "recommended_performance_service_level": {
      "key": null,
      "name": "Idle",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
    "space": {
      "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
      "key": null,
      "name": "Unassigned",
      "_links": {}
    },
    "access_control": {
      "acl": [
        {
          "user_or_group": "everyone",

```

```

        "permission": "read"
    }
],
"export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
        {
            "anonymous_user": "65534",
            "clients": [
                {
                    "match": "0.0.0.0/0"
                }
            ],
            "index": 1,
            "protocols": [
                "nfs3",
                "nfs4"
            ],
            "ro_rule": [
                "sys"
            ],
            "rw_rule": [
                "sys"
            ],
            "superuser": [
                "none"
            ]
        },
        {
            "anonymous_user": "65534",
            "clients": [
                {
                    "match": "0.0.0.0/0"
                }
            ],
            "index": 2,
            "protocols": [
                "cifs"
            ],
            "ro_rule": [
                "ntlm"
            ],
            "rw_rule": [

```

```

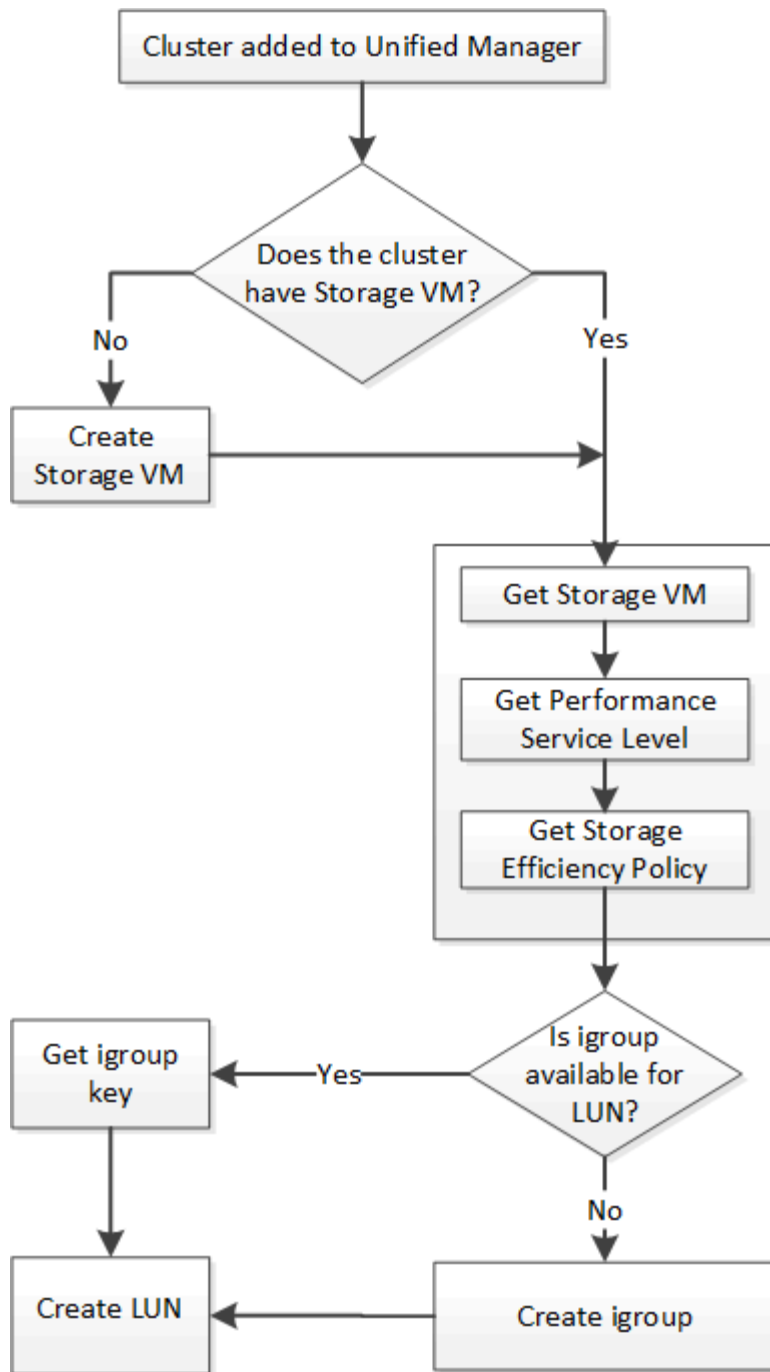
        "ntlm"
    ],
    "superuser": [
        "none"
    ]
}
],
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
}
},
"_links": {
    "self": {
        "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
    }
}
}
}

```

APIを使用したLUNのプロビジョニング

Active IQ Unified Manager に付属のプロビジョニング API を使用して、Storage Virtual Machine（SVM）に LUN をプロビジョニングできます。このプロビジョニングワークフローでは、LUN を作成する前に SVM、パフォーマンスサービスレベル、およびストレージ効率化ポリシーのキーを取得する手順について詳しく説明します。

次の図は、LUN のプロビジョニングワークフローの手順を示しています。



このワークフローは、ONTAP クラスタが Unified Manager に追加され、クラスタキーが取得されていることを前提としています。また、SVM がすでにクラスタに作成されていることも前提としています。

1. LUN を作成する SVM の SVM キーを取得します。詳細については、「クラスタテノ SVM ノサクショ _ ワークフロー」のトピックを参照してください。
2. 次の API を実行し、応答からパフォーマンスサービスレベルのキーを取得します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/performance-service-levels



システム定義のパフォーマンスサービスレベルの詳細を取得するには、を設定します `system_defined` パラメータをに☐true。出力から、LUN に適用するパフォーマンスサービスレベルのキーを取得します。

- 必要に応じて、次の API を実行し、応答から LUN に適用するストレージ効率化ポリシーのキーを取得します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/storage-efficiency-policies

- 作成する LUN ターゲットへのアクセスを許可するイニシエータグループ（igroup）が作成されているかどうかを確認します。

カテゴリ	HTTP 動詞	パス
データセンター	取得	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}

igroup がアクセス権を持つ SVM をパラメータ値として入力する必要があります。また、特定の igroup を照会する場合は、入力パラメータとして igroup 名（キー）を入力します。

- アクセスを許可する igroup が出力に見つかった場合は、そのキーを取得します。見つからない場合は igroup を作成します。

カテゴリ	HTTP 動詞	パス
データセンター	投稿（Post）	/datacenter/protocols/san/igroups

作成する igroup の詳細を、入力パラメータとして指定する必要があります。これは同期呼び出しであり、igroup の作成を出力で確認できます。エラーが発生した場合はメッセージが表示されるため、トラブルシューティングして API を再実行します。

- LUN を作成します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	投稿（Post）	/storage-provider/luns

LUN を作成するには、取得した値を必須パラメータとして指定する必要があります。



ストレージ効率化ポリシーは、LUN の作成ではオプションのパラメータです。

◦ cURL の例 *

作成する LUN のすべての詳細を入力パラメータとして指定する必要があります。

JSON 出力にジョブオブジェクトキーが表示され、作成した LUN の検証に使用できます。

7. ジョブの照会で返されたジョブオブジェクトキーを使用して、LUN の作成を確認します。

カテゴリ	HTTP 動詞	パス
management-server	取得	/management-server/jobs/{key}

応答の末尾に、作成された LUN のキーが表示されます。

8. 返されたキーを指定して次の API を実行し、LUN の作成を確認します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/luns/{key}

◦ JSON 出力の例 *

のPOSTメソッドが表示されます /storage-provider/luns 各関数に必要なすべてのAPIを内部的に呼び出し、オブジェクトを作成します。たとえば、を呼び出します /storage-provider/performance-service-levels/ LUNにパフォーマンスサービスレベルを割り当てるためのAPI。

= LUNの作成またはマッピングに失敗した場合のトラブルシューティング手順

このワークフローを完了しても、LUN の作成に失敗することがあります。LUN の作成に成功しても、LUN を作成したノードに SAN LIF またはアクセスエンドポイントがないために igroup との LUN マッピングが失敗することがあります。障害が発生すると、次のメッセージが表示されます。

```
The nodes <node_name> and <partner_node_name> have no LIFs configured with the iSCSI or FCP protocol for Vserver <server_name>. Use the access-endpoints API to create a LIF for the LUN.
```

この問題を回避するには、次のトラブルシューティング手順を実行します。

1. LUN を作成しようとした SVM に、iSCSI/FCP プロトコルをサポートするアクセスエンドポイントを作成します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	投稿（Post）	/storage-provider/access-endpoints

◦ cURL の例 *

作成するアクセスエンドポイントの詳細を、入力パラメータとして指定する必要があります。



入力パラメータに、LUN のホームノードを示すアドレスと、ホームノードのパートナーノードを示す ha_address を追加したことを確認します。この処理を実行すると、ホームノードとパートナーノードの両方にアクセスエンドポイントが作成されます。

2. JSON 出力で返されたジョブオブジェクトキーを使用してジョブを照会し、SVM にアクセスエンドポイントを追加するジョブが正常に実行されたこと、および SVM で iSCSI/FCP サービスが有効になっていることを確認します。

カテゴリ	HTTP 動詞	パス
management-server	取得	/management-server/jobs/{key}

◦ JSON 出力の例 *

出力の末尾に、作成されたアクセスエンドポイントのキーが表示されます。次の出力では、「name」：「accessEndpointKey」値は LUN のホームノードに作成されたアクセスエンドポイントを示します。このキーは 9c964258-14ef-11ea95e2-00a098e32c28 です。「name」：「accessEndpointHAKey」値は、ホームノードのパートナーノードに作成されたアクセスエンドポイントを示します。このキーは 9d347006-14ef-11ea-8760-00a098e3215f です。

3. LUN を変更して igroup マッピングを更新します。ワークフローの変更の詳細については、「ストレージワークロードの変更」を参照してください。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	パッチ	/storage-provider/lun/{key}

入力で、LUN マッピングの更新に使用する igroup キーと LUN キーを指定します。

◦ cURL の例 *

JSON 出力にジョブオブジェクトキーが表示され、マッピングが成功したかどうかの検証に使用できます。

4. LUN キーを指定して照会することで、LUN マッピングを確認します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/luns/{key}

◦ JSON 出力の例 *

この出力から、LUN のプロビジョニング時に使用された igroup (d19ec2fa -fec7-11E8-b23d -00a098e32c28 キー) に LUN が正常にマッピングされていることがわかります。

APIを使用したストレージワークロードの変更

ストレージワークロードを変更するには、パラメータが不足している LUN またはファイル共有を更新するか、既存のパラメータを変更します。

このワークフローは、LUN とファイル共有のパフォーマンスサービスレベルを更新する例を示しています。



ワークフローは、LUN またはファイル共有がパフォーマンスサービスレベルでプロビジョニングされていることを前提としています。

ファイル共有の変更

ファイル共有の変更では、次のパラメータを更新できます。

- 容量またはサイズ。
- オンラインまたはオフラインの設定
- ストレージ効率化ポリシー
- パフォーマンスサービスレベル
- アクセス制御リスト (ACL) の設定
- エクスポートポリシーの設定。エクスポートポリシーパラメータを削除して、ファイル共有のデフォルト (空) のエクスポートポリシールールに戻すこともできます。



1 回の API の実行で更新できるパラメータは 1 つだけです。

この手順では、パフォーマンスサービスレベルをファイル共有に追加する方法について説明します。その他のファイル共有プロパティを更新する場合にも、同じ手順を使用できます。

1. 更新するファイル共有の CIFS 共有キーまたは NFS ファイル共有キーを取得します。この API は、データセンター上のすべてのファイル共有を照会します。ファイル共有キーがすでにわかっている場合は、この手順を省略してください。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/file-shares

2. 取得したファイル共有キーを指定して次の API を実行し、ファイル共有の詳細を表示します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/file-shares/{key}

出力内のファイル共有の詳細を確認します。

```
"assigned_performance_service_level": {
  "key": null,
  "name": "Unassigned",
  "peak_iops": null,
  "expected_iops": null,
  "_links": {}
},
```

3. このファイル共有に割り当てるパフォーマンスサービスレベルのキーを取得します。現在、ポリシーは割り当てられていません。

カテゴリ	HTTP 動詞	パス
パフォーマンスサービスレベル	取得	/storage-provider/performance-service-levels



システム定義のパフォーマンスサービスレベルの詳細を取得するには、を設定します `system_defined` パラメータをに入力します `true`。出力から、ファイル共有に適用するパフォーマンスサービスレベルのキーを取得します。

4. ファイル共有にパフォーマンスサービスレベルを適用します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	パッチ	/storage-provider/file-shares/{key}

入力では、更新するパラメータのみをファイル共有キーとともに指定する必要があります。ここでは、パフォーマンスサービスレベルのキーを指定します。

◦ cURL の例 *

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{
  \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" },
}"
```

+

JSON 出力にジョブオブジェクトが表示されます。このジョブオブジェクトを使用して、ホームノードとパートナーノードのアクセスエンドポイントが正常に作成されたかどうかを確認できます。

- 出力に表示されたジョブオブジェクトキーを使用して、パフォーマンスサービスレベルがファイル共有に追加されているかどうかを確認します。

カテゴリ	HTTP 動詞	パス
管理サーバ	取得	/management-server/jobs/{key}

ジョブオブジェクトの ID で照会すると、ファイル共有が更新されたかどうかを確認できます。障害が発生した場合は、問題を解決してから API を再度実行します。作成が完了したら、ファイル共有を照会して、変更されたオブジェクトを確認します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/file-shares/{key}

出力内のファイル共有の詳細を確認します。

```
"assigned_performance_service_level": {
  "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
  "name": "Value",
  "peak_iops": 75,
  "expected_iops": 75,
  "_links": {
    "self": {
      "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
    }
  }
}
```

LUN を更新しています

LUN の更新では、次のパラメータを変更できます。

- 容量またはサイズ
- オンラインまたはオフラインの設定
- ストレージ効率化ポリシー
- パフォーマンスサービスレベル
- LUN マップ

 1 回の API の実行で更新できるパラメータは 1 つだけです。

この手順では、パフォーマンスサービスレベルを LUN に追加する方法について説明します。その他の LUN プロパティを更新する場合にも、同じ手順を使用できます。

1. 更新する LUN の LUN キーを取得します。この API は、データセンター内のすべての LUN の詳細を返します。LUN キーがすでにわかっている場合は、この手順を省略してください。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/luns

2. 取得した LUN キーを指定して次の API を実行し、LUN の詳細を表示します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/luns/{key}

出力内の LUN の詳細を確認します。この LUN にはパフォーマンスサービスレベルが割り当てられていないことがわかります。

◦ JSON 出力の例 *

```
"assigned_performance_service_level": {
  "key": null,
  "name": "Unassigned",
  "peak_iops": null,
  "expected_iops": null,
  "_links": {}
},
```

3. LUN に割り当てるパフォーマンスサービスレベルのキーを取得します。

カテゴリ	HTTP 動詞	パス
パフォーマンスサービスレベル	取得	/storage-provider/performance-service-levels



システム定義のパフォーマンスサービスレベルの詳細を取得するには、を設定します `system_defined` パラメータをに入力します `true`。出力から、LUN に適用するパフォーマンスサービスレベルのキーを取得します。

4. LUN にパフォーマンスサービスレベルを適用します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	パッチ	/storage-provider/lun/{key}

入力では、更新するパラメータのみを LUN キーとともに指定する必要があります。ここでは、パフォーマンスサービスレベルのキーを指定します。

◦ cURL の例 *

```
curl -X PATCH "https://<hostname>/api/storage-provider/luns/7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" -d "{ \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-fa163e82bbf2\" } }"
```

+

JSON 出力にジョブオブジェクトキーが表示され、更新した LUN の検証に使用できます。

5. 取得した LUN キーを指定して次の API を実行し、LUN の詳細を表示します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/luns/{key}

出力内の LUN の詳細を確認します。この LUN にパフォーマンスサービスレベルが割り当てられていることがわかります。

◦ JSON 出力の例 *

```

"assigned_performance_service_level": {
  "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
  "name": "Value",
  "peak_iops": 75,
  "expected_iops": 75,
  "_links": {
    "self": {
      "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
    }
  }
}

```

CIFSをサポートするためのAPIを使用したNFSファイル共有の変更

CIFS プロトコルをサポートするように NFS ファイル共有を変更できます。ファイル共有を作成するときに、アクセス制御リスト（ACL）パラメータとエクスポートポリシーの両方を同じファイル共有に対して指定できます。ただし、NFS ファイル共有を作成したボリュームで CIFS を有効にする場合は、CIFS をサポートするようにファイル共有の ACL パラメータを更新できます。

• 必要なもの *

1. エクスポートポリシーの詳細のみを指定して、NFS ファイル共有を作成しておく必要があります。詳細については、「ファイル共有の管理」および「ストレージワークロードの変更」を参照してください。
2. この処理を実行するには、ファイル共有キーが必要です。ファイル共有の詳細の表示とジョブ ID を使用したファイル共有キーの取得については、`_CIFS` および `NFS` ファイル共有のプロビジョニング `_` を参照してください。

この処理は、ACL パラメータは指定せずに、エクスポートポリシーのみを指定して作成した NFS ファイル共有が対象です。NFS ファイル共有を変更して ACL パラメータを追加します。

手順

1. NFSファイル共有で、を実行します `PATCH` CIFSアクセスを許可するためのACLの詳細を含む処理。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	パッチ	/storage-provider/file-shares

◦ cURL の例 *

次の例に示すように、ユーザグループに割り当てたアクセス権限に基づいて ACL が作成され、ファイル共有に割り当てられます。

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
  }
}
```

◦ JSON 出力の例 *

更新を実行するジョブのジョブ ID が返されます。

2. 同じファイル共有に対して詳細を照会し、パラメータが正しく追加されているかどうかを確認します。

カテゴリ	HTTP 動詞	パス
ストレージプロバイダ	取得	/storage-provider/file-shares/{key}

◦ JSON 出力の例 *

```
"access_control": {
  "acl": [
    {
      "user_or_group": "everyone",
      "permission": "read"
    }
  ],
  "export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
      {
        "anonymous_user": "65534",
        "clients": [
          {
            "match": "0.0.0.0/0"
          }
        ],
        "index": 1,

```

```

        "protocols": [
            "nfs3",
            "nfs4"
        ],
        "ro_rule": [
            "sys"
        ],
        "rw_rule": [
            "sys"
        ],
        "superuser": [
            "none"
        ]
    },
    {
        "anonymous_user": "65534",
        "clients": [
            {
                "match": "0.0.0.0/0"
            }
        ],
        "index": 2,
        "protocols": [
            "cifs"
        ],
        "ro_rule": [
            "ntlm"
        ],
        "rw_rule": [
            "ntlm"
        ],
        "superuser": [
            "none"
        ]
    }
],
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
}
},
"_links": {

```

```
    "self": {  
      "href": "/api/storage-provider/file-shares/7d5a59b3-953a-  
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-  
00a098dcc6b6"  
    }  
  }  
}
```

+

同じファイル共有に対して、エクスポートポリシーに加えて ACL が割り当てられていることがわかります。

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NetApp、NetApp のロゴ、および NetApp の商標ページに記載されているマークは、NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

プライバシーポリシー

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

オープンソース

本製品で使用されているサードパーティの著作権およびライセンスに関する情報。

["Active IQ Unified Manager 9.12に関する注意事項"](#)

著作権に関する情報

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。