



# Active IQ Unified Managerのドキュメント

## Active IQ Unified Manager 9.14

NetApp  
November 12, 2024

# 目次

Active IQ Unified Managerのドキュメント	1
リリースノート	2
開始する	3
クイックスタートガイド (VMwareのインストール)	3
クイックスタートガイド (Linuxのインストール)	4
クイックスタートガイド (Windowsのインストール)	5
VMware vSphereシステムへのUnified Managerのインストール	7
Active IQ Unified Managerの概要	7
Unified Managerのインストール要件	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	16
LinuxシステムへのUnified Managerのインストール	26
Active IQ Unified Managerの概要	26
Unified Managerのインストール要件	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	36
WindowsシステムへのUnified Managerのインストール	57
Active IQ Unified Managerの概要	57
Unified Managerのインストール要件	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	67
設定タスクと管理タスクの実行	78
Active IQ Unified Managerの設定	78
Unified Manager のバックアップを設定しています	98
機能設定の管理	98
メンテナンスコンソールの使用	102
ユーザアクセスの管理	116
SAML認証設定の管理	123
認証の管理	129
セキュリティ証明書の管理	137
ストレージの監視と管理	144
Active IQ Unified Managerの概要	144
ユーザインターフェイスの概要	147
ダッシュボードからのクラスタの監視と管理	154
クラスタの管理	165
VMware仮想インフラの監視	171
ワークロードのプロビジョニングと管理	180
MetroCluster設定の管理と監視	196
クォータの管理	204
トラブルシューティング	211
イベントとアラートの管理	219
イベントの管理	219

アラートの管理	316
スクリプトの管理	331
クラスタのパフォーマンスの監視と管理	343
Active IQ Unified Managerパフォーマンス監視の概要	343
Unified Manager の GUI で実行するパフォーマンスワークフロー	347
ダッシュボードからのクラスタパフォーマンスの監視	356
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	358
[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	361
[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	367
[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	377
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	398
パフォーマンス容量と使用可能なIOPSの情報を使用したパフォーマンスの管理	404
[Node Failover Planning]ページの概要と使用方法	412
データの収集とワークロードパフォーマンスの監視	416
パフォーマンスイベントとアラートの概要	423
パフォーマンスしきい値の管理	434
パフォーマンスイベントの分析	445
パフォーマンスイベントの解決	460
Unified Manager サーバと外部データプロバイダ間の接続の設定	475
クラスタの健全性の監視と管理	480
Active IQ Unified Managerの健全性監視の概要	480
クラスタとクラスタオブジェクトの健全性の管理と監視	483
Unified Managerの一般的な健全性ワークフローとタスク	497
データの保護とリストア	630
保護関係の作成、監視、およびトラブルシューティング	630
保護関係の管理と監視	643
カスタムレポートの生成	723
Unified Manager のレポート機能	723
レポートの操作	728
レポートのスケジュール設定	736
サンプルのカスタムレポート	741
Microsoft Excelレポートの例	759
REST APIを使用したストレージの管理	771
Active IQ Unified Manager REST APIでの作業の開始	771
Active IQ Unified ManagerでのREST APIアクセスと認証	775
Unified Manager REST API	785
ストレージ管理のための一般的なAPIワークフロー	819
法的通知	854
著作権	854
商標	854
特許	854

プライバシーポリシー .....	854
オープンソース .....	854

# Active IQ Unified Managerのドキュメント

# リリースノート

Active IQ Unified Manager 9.14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 ["Active IQ Unified Manager リリースノート"](#) ください。

# 開始する

## クイックスタートガイド (VMwareのインストール)

ルート証明書、ファイル、OVA`およびファイルが含まれているファイルを `README`ダウンロードし、Unified Managerを仮想アプライアンスとして導入できます`.tar。

### システム要件

- オペレーティングシステム：VMware ESXi 7.0および8.0
- 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）

詳細なシステム要件については、およびを参照して"[Unified Managerのインストール要件](#)"["Interoperability Matrix"](#)ください。

## Active IQ Unified Managerのインストール

### インストーラをダウンロードする

1. ルート証明書、ファイル、および `OVA`ファイルが含まれているファイルを `README`ダウンロードし`.tar`ます。
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. ファイルをダウンロードしたディレクトリ`.tar`で、コマンドを入力し`tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz`ます。+必要な `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。

### 整合性の検証

ファイルの整合性を検証する `OVA`には、ファイルに記載されている手順に従い `README`ます。

### Unified Managerをインストールする

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. [レビューの詳細]ページの[パブリッシャ]セクションで、ダウンロードしたファイルの整合性を確認する OVA`メッセージが表示され `Entrust Code Signing - OVCS2 (Trusted certificate)`ます。このメッセージが表示されたら `Entrust Code Signing - OVCS2 (Invalid certificate)`、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 (Customize Template) ]ページの[プロパティ (Properties) ]タブで、実行するインストールのタイプに応じてフィールドを入力します。

- 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の場合は、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]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. [Console]タブをクリックして、初期ブート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。

インストールが完了すると、Unified Manager Web UIに接続するための情報が表示されます。

## クイックスタートガイド (Linuxのインストール)

Unified Managerは、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8.9、またはx86\_64アーキテクチャをベースとする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
- RAM：12 GB、CPU：合計 9572MHz
- 空きディスクスペース：ディレクトリに100GB /opt/netapp/data、ルートパーティションに50GB。ディレクトリと /var/log`ディレクトリが個別にマウントされている場合は、`/opt、に15GB、/var/log`16GB、および `/tmp`10GBの空きスペースがあることを確認します ` /opt。

セキュリティで保護されたサイトへの製品のインストールに関する詳細なシステム要件については、およびを参照して"[Unified Managerのインストール要件](#)" "[Interoperability Matrix](#)" ください。

### Active IQ Unified Managerのインストール

インストーラをダウンロードする

1. インストールパッケージとコード(.pem`署名証明書をダウンロードし、`ActiveIQUnifiedManager-  
<version>.zip(.sig`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、次のコマンドを実行します。

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

### 整合性の検証

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 `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public\_key\_file\_name>` で、コード署名証明書から公開鍵を持つファイルを作成します。
- を実行し `openssl dgst -sha256 -verify <public\_key\_file\_name> -signature <signature\_file\_name> ActiveQUnifiedManager-<version>.zip` でインストーラパッケージの署名を確認します。

## リポジトリ設定を確認

Red Hat Enterprise LinuxまたはCentOSのリポジトリの設定手順はサイトによって異なります。インストールパッケージに含まれているスクリプトを使用して、オペレーティングシステムの設定を確認できます `pre_install_check.sh`。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 またはCentOSの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をインストールする

Unified Managerでは、ユーティリティを使用して `yum` ソフトウェアとそれに依存するソフトウェアをインストールします。Red Hat Enterprise LinuxまたはCentOSのイメージはさまざまであるため、インストールされ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` ユーティリティによって、インストールに必要な依存ソフトウェアパッケージが決定されます。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、インストールファイルを解凍したディレクトリからrootユーザまたははを使用して次のコマンドを実行し `sudo` ます。

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

または

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

インストールが完了すると、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、ソフトウェアに付属のファイルで、ポート443の制限事項の詳細を参照 `README` してください。

## クイックスタートガイド (Windowsのインストール)

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、64ビットのWindowsオペレーティングシステムで次の言語に対応しています。

- 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 : 100GB (インストールディレクトリ用) 、 50GB (MySQLデータディレクトリ用)

詳細なシステム要件については、およびを参照して"[Unified Managerのインストール要件](#)" "[Interoperability Matrix](#)" ください。

## Active IQ Unified Managerのインストール

インストーラをダウンロードする

1. インストールパッケージをダウンロードし `ActiveIQUnifiedManager-<version>.exe` ます。
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**をインストールする

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。Unified Managerのインストールプロセスでは、必要に応じて他のサードパーティパッケージがインストールされます。依存ソフトウェアパッケージの詳細については、を参照して"[Windowsソフトウェアとインストールの要件](#)" ください。

1. デフォルトのローカル管理者アカウントを使用して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の実行可能ファイル (.exe) を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システムへのUnified Managerのインストール

## 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で監視および管理できます。Unified Managerは、LinuxサーバやWindowsサーバに導入することも、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に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、監視対象の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"](#)

## Unified Managerサーバの機能

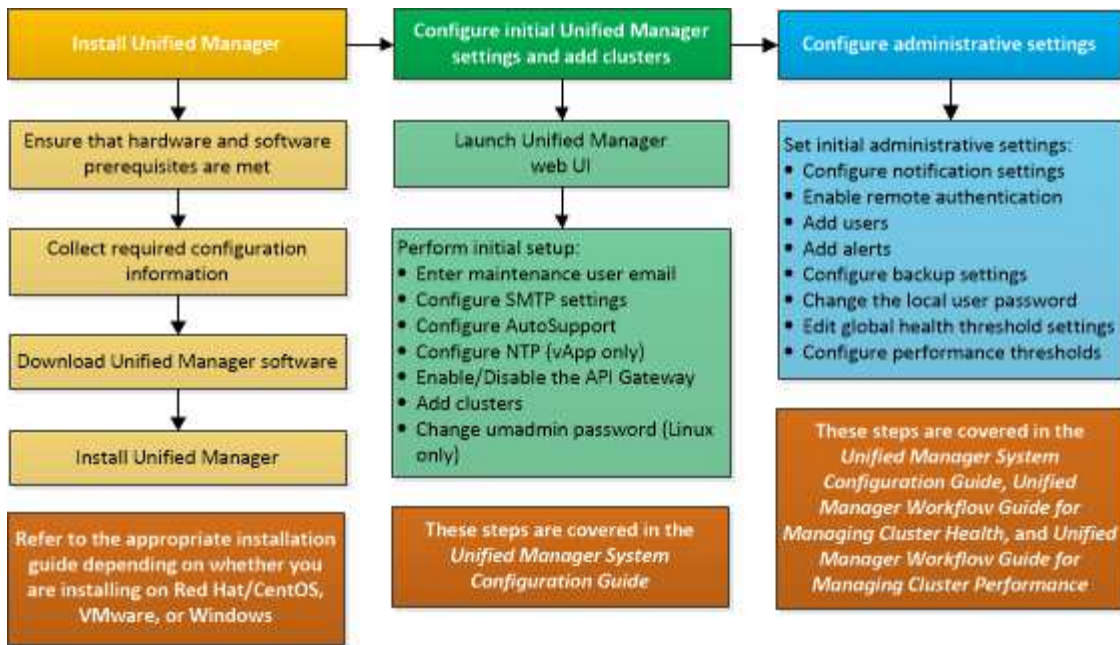
Unified Manager サーバインフラは、データ収集ユニット、データベース、アプリケーションサーバで構成され、検出、監視、ロールベースアクセス制御（RBAC）、監査、ロギングなどのインフラサービスを提供します。

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、以下のワークフローの各項目について説明します。



## Unified Managerのインストール要件

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。

NetAppでは、Unified Managerアプリケーションコードの変更はサポートされていません。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サーバにセキュリティ対策を適用する方法の詳細については、技術情報アートを参照してください。

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

- 関連情報 \*

詳細については、を参照してください。 ["NetApp Interoperability Matrix Tool"](#)

### 仮想インフラとハードウェアシステムの要件

Unified Managerを仮想インフラまたは物理システムにインストールするには、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推奨される値を示します。これらの値は、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9572MHz）
空きディスクスペース	<ul style="list-style-type: none"> <li>• 5GB（シンプロビジョニング）</li> <li>• 152GB（シックプロビジョニング）</li> </ul>

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します。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"。

メモリページスワッピングは、システムと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。ホスト全体の利用率が原因で使用できないCPUリソースを競合すると、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と、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、ホスト自体からホスト名を実行できるように設定する必要があります ping。IPv6構成の場合は、Unified Managerを正しくインストールするために、ホスト名への成功を確認する必要があります ping6。

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。導入時にネットワークに静的IPアドレスを設定した場合は、ネットワークホストの名前を指定します。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。

## 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

次のバージョンのVMware ESXiがサポートされています。

- ESXi 7.0および8.0



VMware vSphereシステム上のUnified Manager OVAは、内部でDebian OS 11 (bunseye) を実行します。サポートされるESXiサーバのバージョンでサポートでき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 7.0および8.0

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機能するためには、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、時刻エラーを回避できます。

### 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。

リソースが不足しているために導入環境でハイアベイラビリティが有効になっていない場合は、[Cluster Features]の[Virtual Machine Options]の変更が必要になることがあります。[VM Restart Priority]を無効にし、[Host Isolation Response]をオンのままにします。



Unified Managerのインストールまたはアップグレード中に、必要なサードパーティ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、スタンドアロンのサードパーティコンポーネントの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の一覧については、Interoperability Matrixを参照してください。



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

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と、ソフトウェア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にSAML認証を設定する場合は、IdPでサポートされているブラウザの一覧も確認してください。

## プロトコルとポートの要件

必要なポートとプロトコルを使用して、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で通信できます。

### Unified Managerサーバへの接続

一般的な環境では、Unified Manager Web UIへの接続時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、の代わりに `https://<host>:443` と入力できます `https://<host>`。

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

インターフェイス	プロトコル	ポート	製品説明
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やAPI呼び出しに使用されます。API呼び出しはHTTPSでのみ実行できます。
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へのアクセスとサポートバンドルの取得に使用されます。
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	製品説明
syslog	UDP	514	ONTAPシステムから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場合に使用されます。
REST	HTTPS	9443	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EMSイベントにアクセスするために使用されます。



MySQLのデフォルトポート3306は、VMware vSphereシステムにUnified Managerをインストールする際のlocalhostのみに制限されます。これは、以前の設定が維持されているアップグレードシナリオには影響しません。この設定を変更したり、メンテナンスコンソールのオプションを使用して他のホストに接続を許可したりすることができ、`Control access to MySQL port 3306`ます。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通信に使用するポート（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いておく必要があります。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。



デスティネーション	プロトコル	ポート	製品説明
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> <p> このポートまたはその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、ポートが使用可能で、セキュアなサイトで接続できることを確認してください。</p>
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メールの送信に使用されます。	SNMPトラップの送信者
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サーバ

デスティネーション	プロトコル	ポート	製品説明
TCP	2003	外部のデータプロバイダ（Graphiteなど）にパフォーマンスデータを送信するために使用されま 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。ワークシートに情報を記録できます。

### 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名前	
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。構成に応じて、一部の値はオプションです。

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のユーザ名	
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	
認証サーバのホスト名またはIPアドレス	
Active Directory管理者名またはLDAPのバインド識別名	
Active DirectoryパスワードまたはLDAP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) 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詳細を記入します。

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	

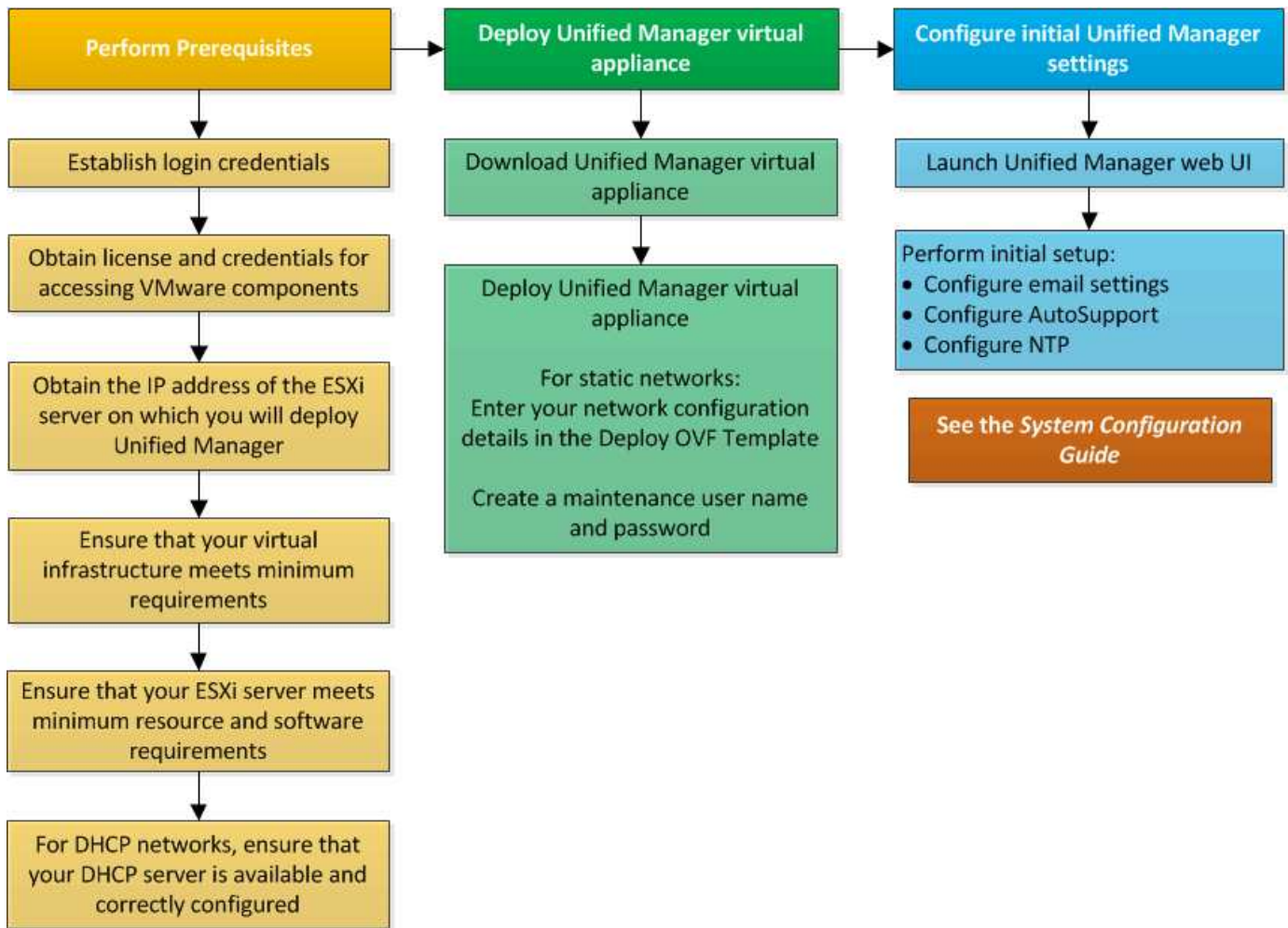
クラスタ 1 / N	あなたの価値
ONTAP管理者のユーザ名  管理者には「admin」ロールが割り当てられている必要があります。	
ONTAP管理者のパスワード	
プロトコル	HTTPS

## Unified Managerソフトウェアのインストール、アップグレード、削除

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の導入

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て完了する必要があります。

を参照して ["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
  - データセンターの詳細（データストアのストレージスペースやメモリの要件など）
  - 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 open-vm-tools`います)。はUnified Managerのインストールパッケージに含まれているため、インストール時にVMware Toolsをインストールする必要はありません `open-vm-tools。

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、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. さらに、 の手順に従います ["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のダウンロード

NetAppサポートサイトからUnified Managerのインストールファイルをダウンロードして、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サポートサイト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、ルート証明書、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 `README`です `tar。

手順

1. NetAppサポートサイトにログインし、Unified Managerのダウンロードページに移動します。

["NetAppサポートサイト"](#)

2. 必要なUnified Managerのバージョンを選択し、エンドユーザライセンス契約（EULA）に同意します。
3. VMware vSphereのインストール用ファイルをダウンロードし、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 .tar。
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. ファイルをダウンロードしたディレクトリに移動 `tar`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バンドルを展開します。

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

必要な `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. ファイルに記載されている手順に従って、ファイルの `README`整合性を検証し `OVA`ます。

## 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 "[仮想インフラの要件](#)"

を参照して "[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ること、およびDHCPと仮想マシン (VM) 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。

静的な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
- データセンターの詳細 (使用可能なストレージスペースなど)
- DHCPを使用していない場合は、接続するネットワークデバイスのIPv4アドレスまたは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 `open-vm-tools` います)。はUnified Managerのインストールパッケージに含まれているため、インストールプロセスでVMware Toolsをインストールする必要はありません `open-vm-tools`。

仮想アプライアンスを導入すると、HTTPSアクセス用の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。

[Review Details]ページで、

- Publisherセクションの詳細を確認します。「\* Entrust Code Signing - OVCS2 (Trusted certificate) \*」というメッセージは、ダウンロードしたファイルの整合性を確認します OVA。 + 「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、次の操作を行います。

- DHCPおよび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、このページの各フィールドに値を入力すると、それらの設定が導入時に適用されます。IPアドレスが導入先のホストで一意であること、まだ使用されていないこと、および有効なDNSエントリが設定されてい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。

初期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が同じNTPサーバを使用して設定されている場合は、表示方法が異なっていても、同じインスタントインタイムを参照しています。たとえば、管理サーバとは異なるタイムゾーンを使用して設定されたデバイスを使用してSnapshotコピーを作成した場合、タイムスタンプは管理サーバの時刻になります。

6. 使用可能なDHCPサービスがない場合、または静的なネットワーク設定の詳細に誤りがある場合は、次のいずれかのオプションを選択します。



状況	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する必要があります。</p> <p>DHCP対応のネットワークを使用する場合は、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、1文字目はa～z、続けて-、a～z、または0～9を任意に組み合わせて指定する必要があります。

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["Active IQ Unified Managerの設定"](#)ください。

## Unified Managerのアップグレード

Active IQ Unified Managerをリリース9.12または9.13からリリース9.14にアップグレードできるのは、リリース9.12または9.13からのみです。

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ください。

Unified ManagerをOnCommand Workflow Automationのインスタンスとペアにしている、両方の製品で新しいバージョンのソフトウェアを使用できる場合は、2つの製品の接続を解除し、アップグレードの実行後に新しいWorkflow Automation接続を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、で説明されている手順を実行し ["Unified Manager をアップグレードします"](#)ます。

サポートされる**Unified Manager**のバージョンの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。

Unified Managerの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モデルに制限されているため、アップグレードはすべてのプラットフォームで次の2リリースまで実行できません。たとえば、Unified Manager 9.12および9.13からUnified Manager 9.14へのアップグレードのみを実行できます。

サポート対象のバージョンよりも前のバージョンを実行している場合は、Unified Managerインスタンスをサポート対象のいずれかの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Unified Manager 9.9でUnified Manager 9.14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. 9.9から9.11へのアップグレード
2. 9.11から9.13へのアップグレード
3. 9.13→9.14にアップグレード

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のダウンロード

Unified Managerをアップグレードする前に、NetAppサポートサイトからUnified Managerのアップグレードファイルをダウンロードします。

- 必要なもの \*

NetAppサポートサイトのログインクレデンシャルが必要です。

手順

1. NetAppサポートサイトにログインします。

["NetAppサポートサイト"](#)

2. VMware vSphereでUnified Managerをアップグレードするためのダウンロードページに移動します。
3. アップグレード用のイメージをダウンロードし .iso、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のアップグレード

Active IQ Unified Manager仮想アプライアンスをリリース9.12または9.13から9.14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。

- アップグレードファイル（ISOイメージ）をNetAppサポートサイトから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。

を参照して ["仮想インフラの要件"](#)

を参照して ["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、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か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。確認すると、6か月後に履歴パフォーマンスデータがパージされます。
- 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ください。

Workflow AutomationとUnified Managerを連携させて使用している場合は、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. Unified Manager VMのバックアップコピー（Snapshotやクローンなど）を作成して、アプリケーションと整合性のあるバックアップを作成します。
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. ファイルを選択し ActiveIQUnifiedManager-<version>-virtual-update.iso、 \*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. と入力 `y` して続行します。

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せん。

13. と入力 `y` して続行します。

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. いずれか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してからUIでのタスクを実行する必要があります。

## Unified Manager仮想マシンの再起動

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あと、またはVMで問題が発生した場合は、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する必要があります。
- 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の削除

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および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システムへのUnified Managerのインストール

## 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で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に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、監視対象の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"](#)

## Unified Managerサーバの機能

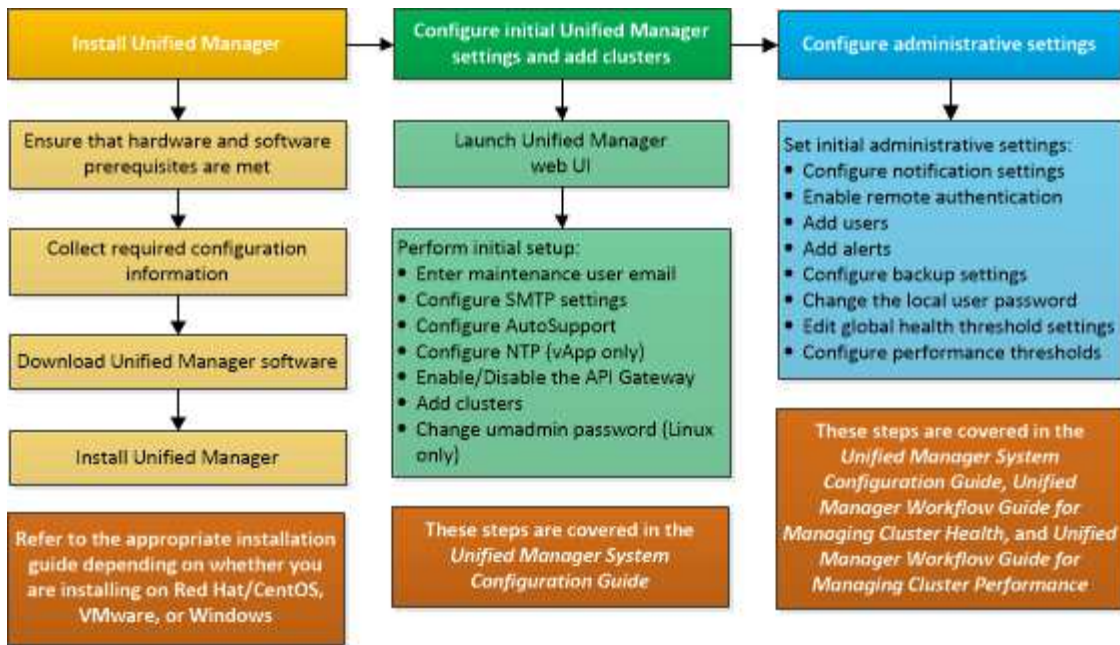
Unified Manager サーバインフラは、データ収集ユニット、データベース、アプリケーションサーバで構成され、検出、監視、ロールベースアクセス制御（RBAC）、監査、ロギングなどのインフラサービスを提供します。

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、以下のワークフローの各項目について説明します。



## Unified Managerのインストール要件

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。

NetAppでは、Unified Managerアプリケーションコードの変更はサポートされていません。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サーバにセキュリティ対策を適用する方法の詳細については、技術情報アートを参照してください。

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

- 関連情報 \*

["NetApp Interoperability Matrix Tool"](#)

### 仮想インフラとハードウェアシステムの要件

Unified Managerを仮想インフラまたは物理システムにインストールするには、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推奨される値を示します。これらの値は、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9572MHz）
空きディスクスペース	<p>150GB。割り当ては次のとおりです。</p> <ul style="list-style-type: none"> <li>• 50GBをルートパーティションに割り当て</li> <li>• 100GBの空きディスクスペースをディレクトリに割り当て（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） /opt/netapp/data</li> </ul> <p> ディレクトリと /var/log`ディレクトリが個別にマウントされている場合は、`/opt、に15GB、 /var/log`に16GBの空きスペースがあることを確認します。`/opt。`tmp`ディレクトリに10GB以上の空きスペースが必要です。</p>

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します。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 』 "

メモリページスワッピングは、システムと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。ホスト全体の利用率が原因で使用できないCPUリソースを競合すると、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と、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、ホスト自体からホスト名に実行できるように設定する必要があります ping。IPv6構成の場合は、Unified Managerを正しくインストールするために、ホスト名へのが成功することを確認する必要があります ping6。

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。導入時にネットワークに静的IPアドレスを設定した場合は、ネットワークホストの名前を指定します。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。

## 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システムには、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8.9（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 Stream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)

Unified Manager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。会社の規制により、Qualysのような脆弱性スキャナがLinux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するには、Unified Managerをインストールする前に脆弱性スキャナを無効にする必要があります。



脆弱性スキャナ（Qualysなど）を使用すると、内部（Unified Managerと脆弱性スキャナが同じVMにインストールされている場合）または外部で仮想マシン（VM）をスキャンする際にCPU使用率が高くなる場合があります。（Unified Managerと脆弱性スキャナが2つの異なるサーバにインストールされ、脆弱性スキャナがUnified ManagerがインストールされているVMをスキャンします）。この問題を実行すると、VMが応答しなくなり、Unified Managerサービスに影響することがよくあります。そのため、NetAppでは、Unified ManagerがインストールされているVMで脆弱性スキャナを無効にすることを推奨しています。スキャナを無効にできない場合は、営業時間外にVMをスキャンし、スキャンの完了後にサービスを再起動してください。

### 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 26.1.3はUnified Managerにバンドルされ、設定されています。

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、インストール時にインストーラによって自動的にインストールされ `yum` ます。ただし、次のセクションで説明するようにリポジトリを設定している場合に限りです。

- MySQL Community Editionバージョン8.0.34（MySQLリポジトリから入手）。
- OpenJDKバージョン11.0.21（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ユーザまたはroot以外のユーザがコマンドを使用して実行できます `sudo`。

## 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を次に示します。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、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、システムには適切なリポジトリへのアクセスが必要です。
- インストーラがRed Hat Enterprise Linuxリポジトリから依存するソフトウェアを検索するには `yum`、Red Hat Enterprise Linuxのインストール時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の詳細については、Red Hatのマニュアル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をシステムに正しくインストールするには、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 ["EPELリポジトリの手動設定"](#)

- 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、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 "[MySQLリポジトリの手動設定](#)"

システムがインターネットに接続されておらず、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ダウンロードしたら、インターネットに接続されたシステムにそのソフトウェアをダウンロードし、Unified Managerをインストールするシステムにファイルをコピーし、`.rpm`を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、コマンドを使用する必要があります `yum install`。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またはCentOSの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する必要があります。



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専用に設計されたもので、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これらのガイドラインに従っていないため、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の汎用イメージでは、ポート443への外部アクセスがブロックされることがあります。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。Unified Managerのインストール手順で使用す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。システムにがない場合は `firewall-cmd`、次のコマンドを実行して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部門に連絡して、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、THP（Transparent Huge Pages）を無効にする必要があります。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ときにUnified Managerがシャットダウンすることがあります。

### サポートされるブラウザ

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の一覧については、Interoperability Matrixを参照してください。

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

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と、ソフトウェア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にSAML認証を設定する場合は、IdPでサポートされているブラウザの一覧も確認してください。

## プロトコルとポートの要件

必要なポートとプロトコルを使用して、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で通信できます。

### Unified Managerサーバへの接続

一般的な環境では、Unified Manager Web UIへの接続時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、の代わりに `https://<host>:443` と入力できます `https://<host>`。

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

インターフェイス	プロトコル	ポート	製品説明
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やAPI呼び出しに使用されます。API呼び出しはHTTPSでのみ実行できます。
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へのアクセスとサポートバンドルの取得に使用されます。
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 Workflow AutomationおよびOnCommand APIサービスからUnified Managerへのアクセスで使用されます。

インターフェイス	プロトコル	ポート	製品説明
syslog	UDP	514	ONTAPシステムから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場合に使用されます。
REST	HTTPS	9443	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EMSイベントにアクセスするために使用されます。



MySQLのデフォルトポート3306は、LinuxシステムへのUnified Managerのインストール時にlocalhostに制限されます。これは、以前の設定が維持されているアップグレードシナリオには影響しません。この設定を変更したり、メンテナンスコンソールのオプションを使用して他のホストに接続を許可したりすることができ`Control access to MySQL port 3306`ます。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通信に使用するポート（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いておく必要があります。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。

デスティネーション	プロトコル	ポート	製品説明
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。

デスティネーション	プロトコル	ポート	製品説明
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メールの送信に使用されます。	SNMPトラップの送信者
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せん。	外部データプロバイダサーバ
TCP	2003	外部のデータプロバイダ（Graphiteなど）にパフォーマンスデータを送信するために使用されません。	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。ワークシートに情報を記録できます。

### 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	

ソフトウェアが導入されているシステム	あなたの価値
メンテナンスユーザの名前	
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。構成に応じて、一部の値はオプションです。

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のユーザ名	
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	
認証サーバのホスト名またはIPアドレス	
Active Directory管理者名またはLDAPのバインド識別名	
Active DirectoryパスワードまたはLDAP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) 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詳細を記入します。

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

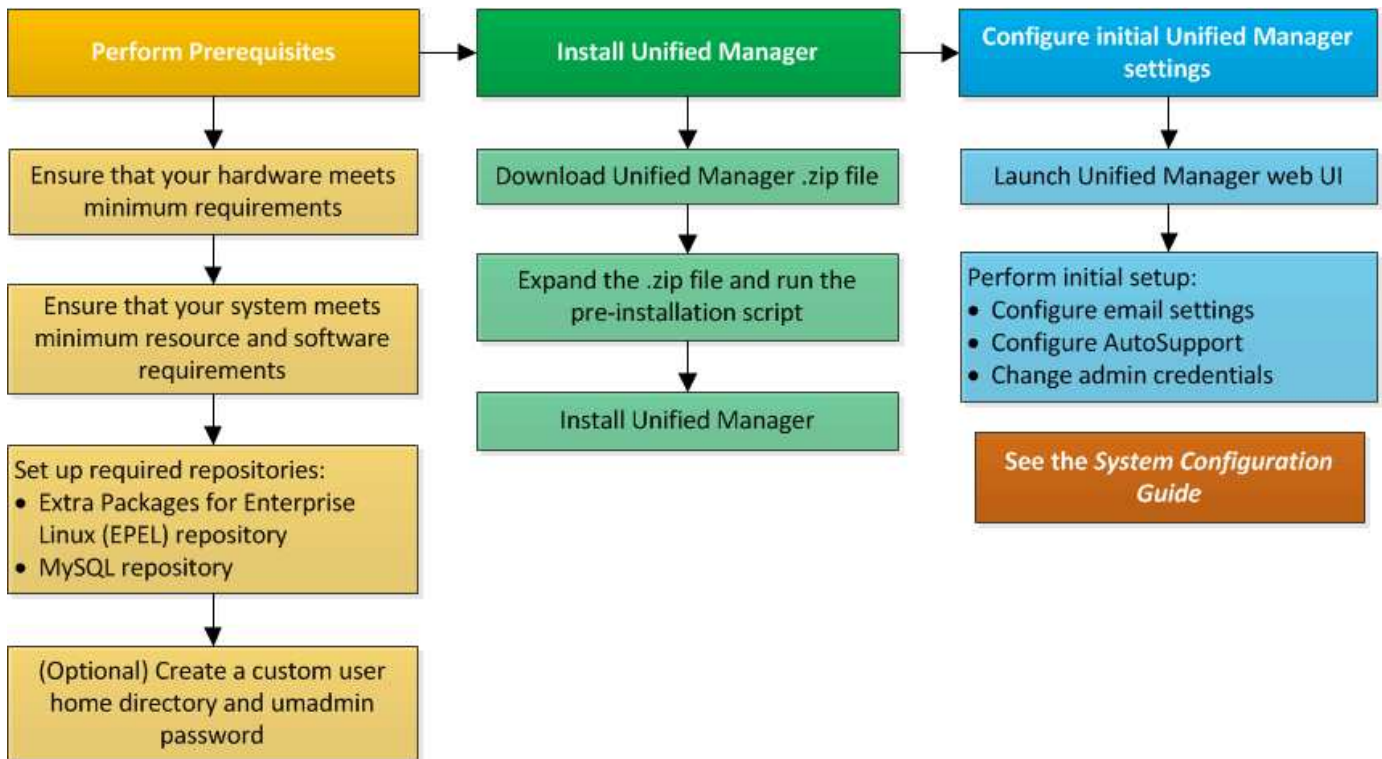
Linux システムで、Unified Manager ソフトウェアのインストール、新しいバージョンへのアップグレード、または Unified Manager の削除を実行できます。

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のセットアップ

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、システムには特定のリポジトリへのアクセスが必要です。

### EPELリポジトリの手動設定

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ます。

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

バージョン8の場合は、次のサイトからダウンロードします。

```
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システムで、モジュラRPMパッケージ（など）を含む内部リポジトリがある場合は `javapackages-filesystem-<version>.module.rpm`、モジュラパッケージのメタデータも同じリポジトリにあることを確認してください。

## MySQLリポジトリの手動設定

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。



システムがインターネットに接続されていない場合、このタスクは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ます。

```
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の場合は、次のサイトからダウンロードします。

```
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システムで、AppStreamリポジトリが提供する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は、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
```

キーの欠落またはキーの不一致に関するエラーが表示され、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、をマークして `gpgcheck=0` 無効にします `gpgcheck`。

## NFS共有とCIFS共有でのSELinuxの要件

SELinuxを有効にしている環境でNASデバイスまたはSANデバイスにまたはを `/opt/netapp/data` マウントする場合は `/opt/netapp`、いくつかの考慮事項について確認しておく必要があります。

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またはを `/opt/netapp/data` マウントする場合は `/opt/netapp`、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。使用環境の該当するシナリオに応じて、次の手順に従って、正しいSELinuxコンテキストを設定および確認します。

をマウントしている場合のSELinuxコンテキストの設定 `/opt/netapp/data`

システムにをマウントし、SELinuxがに設定されている `Enforcing` 場合は `/opt/netapp/data`、のSELinuxコンテキストタイプがに設定されている `mysql_d_db_t` ことを確認します `/opt/netapp/data`。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_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 `/opt/netapp/data` ます。
  - a. 次のコマンドを実行してコンテキストをに設定し `mysql_d_db_t` ます。

```
`semanage fcontext -a -t mysql_d_db_t "/opt/netapp/data"
`restorecon -R -v /opt/netapp/data
```
  - b. で `/etc/fstab` を設定した場合は `/opt/netapp/data`、ファイルを編集する必要があります `/etc/fstab`。マウントオプションに `/opt/netapp/data/`、MySQLラベルを次のように追加します。

```
context=system_u:object_r:mysql_d_db_t:s0
```

- c. コンテキストを有効にするためにアンマウントして再マウントし `/opt/netapp/data/` 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 `'mysql_d_db_t'` ます。

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

出力例を次に示します。

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

をマウントし、を `/opt/netapp/data/` 個別にマウントした場合のSELinuxコンテキストの設定 `'/opt/netapp'`

このシナリオでは、最初に、前のセクションで説明したようにのコンテキストを設定する必要があります `/opt/netapp/data/`。のコンテキストを正しく設定したら `/opt/netapp/data/`、親ディレクトリのSELinuxコンテキストがに設定されていない `'file_t'` ことを確認し `'/opt/netapp'` ます。

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:file_t:s0 /opt/netapp
```

この出力では、コンテキストを `file_t` 変更する必要があります。次のコマンドは、コンテキストをに設定し `'usr_t'` ます。コンテキストは、セキュリティ要件に応じて以外の任意の値に設定できます `'file_t'`。

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 `'/opt/netapp'` ます。
  - 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. で `/etc/fstab` を設定した場合は `'/opt/netapp'`、ファイルを編集する必要があります `/etc/fstab`。マウントオプションに `/opt/netapp`、MySQLラベルを次のように追加します。

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

2. コンテキストを有効にするために、アンマウントしてから再度マウントし ` /opt/netapp` 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

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

をマウントして個別にマウントし ` /opt/netapp/data/` ない場合のSELinuxコンテキストの設定  
` /opt/netapp

システムにをマウントし、SELinuxがに設定されている Enforcing`場合は ` /opt/netapp、のSELinuxコ  
ンテキストタイプがに設定されている mysql\_d\_db\_t`ことを確認します ` /opt/netapp。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  
mysql\_d\_db\_t。

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 ` /opt/netapp` ます。
  - a. 次のコマンドを実行してコンテキストをに設定し mysql\_d\_db\_t` ます。

```
` semanage fcontext -a -t mysql_d_db_t "/opt/netapp"  
` restorecon -R -v /opt/netapp
```
  - b. で /etc/fstab`を設定した場合は ` /opt/netapp、ファイルを編集し /etc/fstab` ます。マウン  
トオプションに ` /opt/netapp/、MySQLラベルを次のように追加します。

```
context=system_u:object_r:mysql_d_db_t:s0
```
  - c. コンテキストを有効にするために、アンマウントしてから再度マウントし ` /opt/netapp/` 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 mysql\_d\_db\_t` ま  
す。

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

インストール前のカスタムユーザのホームディレクトリと **umadmin** パスワードの作成

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 \*
- システムがに記載されている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。

- umadminユーザが作成され、が `/home/umadmin` ホームディレクトリになります。
- umadmin ユーザにデフォルトのパスワード「admin」を割り当てます。

一部のインストール環境ではへのアクセスが制限されているため、`/home` 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、一部のサイトでは、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管理者によるパスワードの設定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すると、インストールスクリプトによってこれらの設定が検出され、インストールのデフォルト設定ではなく定義された値が使用されます。

また、Unified Managerのデフォルトのインストールでは、`sudoers`ファイルおよび `ocie_sudoers`) `/etc/sudoers.d/` ディレクトリにumadminユーザが含まれてい( `ocum_sudoers` )ます。セキュリティポリシーまたは一部のセキュリティ監視ツールが原因で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。

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、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
```

このコマンドを実行すると、ocieサービスの適切なステータスがエラーなしで返されます。

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のダウンロード

Unified Managerをインストールするには、NetAppサポートサイトからUnified Managerのファイルをダウンロードする必要があります .zip。

- 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サポートサイトにログインし、Unified Managerのダウンロードページに移動します。

["NetAppサポートサイト"](#)

2. 必要なUnified Managerのバージョンを選択し、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、ファイルをターゲットシステムのディレクトリに保存します .zip。





- お使いの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ください。インストールされているRed Hat Enterprise Linux 7または8に基づいて、適切なバージョンのUnified Managerファイルをダウンロードして`.zip`ください。
- NetAppでは、ファイル(`.sig`と一緒に`.pem`、コード署名証明書とデジタル署名をダウンロードすることを推奨しています`.zip`。

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検証できます。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。
  - 次のコマンドは、コード署名証明書から公開鍵を持つ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。
- 次のコマンドは、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は 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のインストール

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 "[ハードウェアシステムの要件](#)"

を参照して "[Linuxソフトウェアとインストールの要件](#)"

- Unified ManagerのファイルをNetAppサポートサイトからターゲットシステムにダウンロードしておく必要があります`.zip`。
- ダウンロードしたファイルの整合性を確認しておく必要があります`.zip`。
- 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は、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システムに、必要なサポートソフトウェア（Java、MySQL、その他のユーティリティ）の必要なバージョンがすべてインストールされているか、一部の必要なソフトウェアのみがインストールされているか、または新しくインストールしたシステムに必要なソフトウェアがまったくインストールされていない場合があります。

## 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て、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のインストールやアップグレードが必要なソフトウェアを評価します。

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11.0.21	<code>java -version</code>
MySQL 8.0.34 Community Edition	<code>`rpm -qa</code>
<code>grep -i mysql`</code>	<code>p7zip 16.02</code>
<code>`rpm -qa</code>	<code>grep p7zip`</code>

3. インストールされているMySQLのバージョンがMySQL 8.0.34 Community Editionより前の場合は、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>
```

依存関係エラーが発生した場合は、コンポーネントをアンインストールするオプションを追加する必要があります `--nodeps`。

4. 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に移動 ``zip`` 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。

5. 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
```

6. 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こと、および必要なソフトウェアリポジトリにアクセスできることを確認します。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システムで、AppStreamリポジトリが提供するJDK 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は、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
```

7. \* 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。システムがインターネットに接続されていて、必要なパッケージがすべて揃っている場合は、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、不足しているパッケージをダウンロードします。

- a. 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確認します。+

```
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 --downloaddir=.
```



Red Hat Enterprise Linuxシステムではプラグイン「yum-plugin-downloadonly」が常に有効になっているわけではないため、インストールせずにパッケージをダウンロードする機能を有効にしなければならない場合があります。

```
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インストールシステムに不足しているパッケージをコピーします。
8. rootユーザとして、またはを使用して sudo、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、必要なその他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。

インストールがGPG NOKEYエラーで失敗した場合は、を使用して `rpm --import` でURLからキーをインポートします。

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



他のコマンド（など）を使用してインストールを実行しないでください 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。そのためにはコマンドを使用する必要があります。 yum install netapp-um<version>.x86\_64.rpm

- 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メールでは、最初のcronジョブが失敗したことがrootユーザに通知されますが、インストールには影響しません。

- インストールメッセージが完了したら、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 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
```

- IPアドレスまたはURL、割り当てられているユーザ名 (umadmin) 、および現在のパスワードを記録します。
- 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
```

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 (を参照) "[Active IQ Unified Managerの設定](#)". umadminユーザのデフォルトのパスワードは必ず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用します。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用します。このユーザは Unified Manager によって作成されます。

## • \* MySQL \*

Unified Manager の MySQL データベーススキエリの実行に使用します。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パスワードの変更

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せん。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へのアクセスにJBossが使用するパスワードも変更されます。

- 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。
- ディレクトリにあるNetAppが提供するスクリプト `/opt/netapp/essentials/bin`` にアクセスできる必要があります ``password.sh`。

## 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を少なくとも1文字使用する必要があります。

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

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ら、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いる、両方の製品で新しいバージョンのソフトウェアを使用できる場合は、2つの製品の接続を解除し、アップグレードの実行後に新しいWorkflow Automation接続を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。

サポートされる**Unified Manager**のバージョンの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。

Unified Managerの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モデルに制限されているため、アップグレードはすべてのプラットフォームで次の2リリースまで実行できません。たとえば、Unified Manager 9.12および9.13からUnified Manager 9.14へのアップグレードのみを実行できます。

サポート対象のバージョンよりも前のバージョンを実行している場合は、Unified Managerインスタンスをサポート対象のいずれかの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Unified Manager 9.9でUnified Manager 9.14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. 9.9から9.11へのアップグレード
2. 9.11から9.13へのアップグレード
3. 9.13→9.14にアップグレード

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

LinuxプラットフォームでUnified Manager 9.12または9.13から9.14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 "[ハードウェアシステムの要件](#)"

を参照して "[Linuxソフトウェアとインストールの要件](#)"

- Red Hat Enterprise Linux Subscription Managerのサブスクリプションが必要です。
- 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、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 "[LinuxでのJREのアップグレード](#)"

- アップグレードで問題が発生した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。NetAppでは、バックアップファイルをディレクトリから外部の場所に移動することを推奨して `'/opt/netapp/data` ます。
- アップグレードの実行中、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か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。確認すると、6か月後に履歴パフォーマンスデータがパージされます。
- 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く必要があります。
- 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8.0.34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8.0.34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. Unified Managerのバンドルをサーバにダウンロードします。

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

3. 目的の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こと、および必要なソフトウェアリポジトリにアクセスできることを確認します。問題が検出された場合

は、問題を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"[不足しているパッケージに対して実行する追加手順](#)"ます。不足している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のかも確認されます。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/
```

サポート対象のWebブラウザの新しいウィンドウに指定した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、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不足し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。この手順ではUnified Managerをアップグレードするため、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。



- 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 --downloaddir=.
```

パッケージは、で指定したディレクトリにダウンロードされ`--downloaddir=`ます。

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
```

- ダウンロードしたパッケージを、インストールシステムでUnified Managerバンドルを解凍したディレクトリにコピーします。
- 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、不足している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
```

- 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。サポート対象のWebブラウザの新しいウィンドウに指定した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。

## 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で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8.9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システムが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。

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かどうかは、を参照してください"[バックアップ処理とリストア処理の管理](#)"。



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り、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場合は、次の手順を実行します。

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 "[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、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 "[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、認証設定を設定したりしないでください。バックアップファイルには、リストアップロセス中にこの情報が入力されます。

3. Red Hat Enterprise Linux 7.xシステムで、Web UIの[管理]メニューを使用してUnified Managerのバックアップを作成し、バックアップファイルファイル) とデータベースリポジトリディレクトリのサブディレクトリの内容を(/database-dumps-repo`外部の場所にコピーし(.7z`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ファイル) を外部の場所からに /opt/netapp/data/ocum-backup/`コピーし、データベースリポジトリファイルを ` /database-dumps-repo`ディレクトリの下サブディレクトリに ` /ocum-backup`コピーします(.7z`。
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ップします。

```
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、次の手順を実行します。

1. Web UIの[管理]メニューを使用して、Unified Managerのバックアップを作成し、バックアップファイルファイルとデータベースリポジトリディレクトリのサブディレクトリの内容を(/database-dumps-repo`外部の場所にコピーし(.7z`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 "[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、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 "[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、認証設定を設定したりしないでください。バックアップファイルには、リストアッププロセス中にこの情報が入力されます。

5. バックアップファイル(ファイル) を外部の場所からに `/opt/netapp/data/ocum-backup/`` コピーし、データベースリポジトリファイルを ``/database-dumps-repo`` ディレクトリの下の子ディレクトリに ``/ocum-backup`` コピーします (.7z)。
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ップします。

```
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のインストール後の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Linuxシステムにインストールされている場合は、Unified Manager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している企業は、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へのアップグレードは、ご自身のスケジュールで行うことができます。

### 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の再起動

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またはCentOSのサーバへのrootユーザ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ユーザとしてログインします。
2. Unified Managerサービスと関連するMySQLサービスを次の順序で停止します。

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

```
systemctl stop mysqld
```

3. MySQLサービスとUnified Managerサービス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の削除

Unified Managerは、Red Hat Enterprise LinuxホストまたはCentOSホストから1つのコマンドで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。コマンドを使用して、SELinuxランタイムモードを「permissive」に変更します `setenforce 0`。
- 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よう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
```

この手順では、関連付けられているすべてのNetApp RPMパッケージが削除されます。Java、MySQL、p7zipなどの前提条件となる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。アンインストール後、ディレクトリのすべてのデータ`/opt/netapp/data`がフォルダに移動され`/opt/netapp/data/BACKUP`ます。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（必要なパッケージでシステムの他のアプリケーションで使用されている場合を除く）。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グループの削除

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システムへのUnified Managerのインストール

## 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で監視および管理できます。Unified Managerは、LinuxサーバやWindowsサーバに導入することも、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に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、監視対象の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"](#)

## Unified Managerサーバの機能

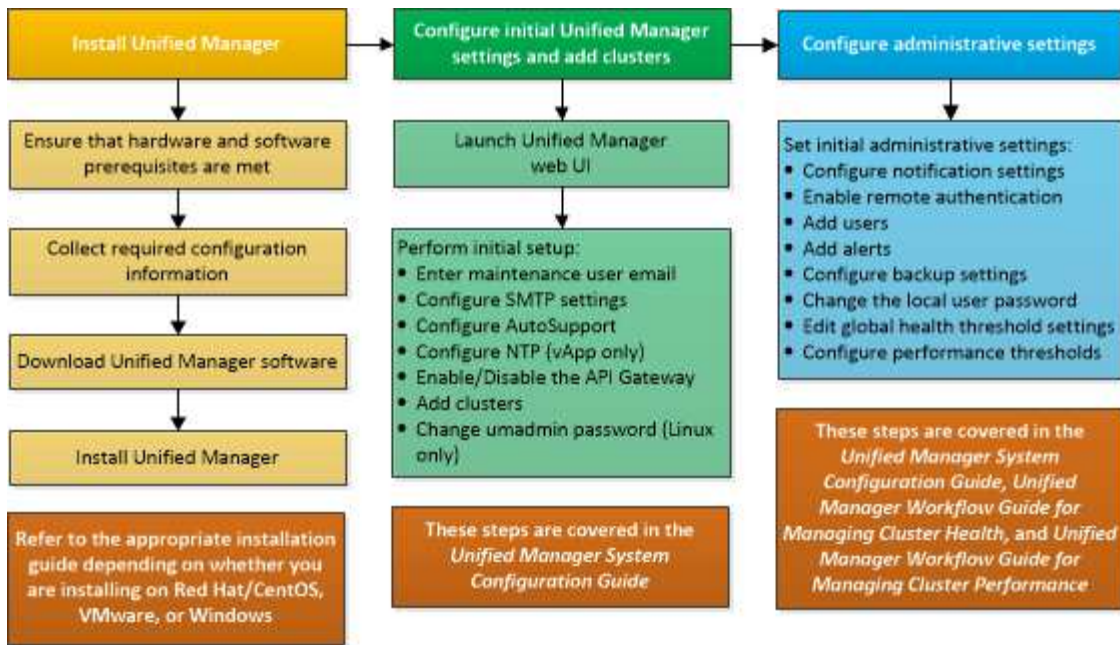
Unified Manager サーバインフラは、データ収集ユニット、データベース、アプリケーションサーバで構成され、検出、監視、ロールベースアクセス制御（RBAC）、監査、ロギングなどのインフラサービスを提供します。

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、以下のワークフローの各項目について説明します。



## Unified Managerのインストール要件

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。

NetAppでは、Unified Managerアプリケーションコードの変更はサポートされていません。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サーバにセキュリティ対策を適用する方法の詳細については、技術情報アートを参照してください。

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

- 関連情報 \*

["NetApp Interoperability Matrix Tool"](#)

### 仮想インフラとハードウェアシステムの要件

Unified Managerを仮想インフラまたは物理システムにインストールするには、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推奨される値を示します。これらの値は、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9572MHz）
空きディスクスペース	150GB。割り当ては次のとおりです。 <ul style="list-style-type: none"> <li>• 100GB（インストールディレクトリ用）</li> <li>• 50GB - MySQLのデータディレクトリ用</li> </ul>

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します。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』"

メモリページスワッピングは、システムと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。ホスト全体の利用率が原因で使用できないCPUリソースを競合すると、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と、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、ホスト自体からホスト名に実行できるように設定する必要があります ping。IPv6構成の場合は、Unified Managerを正しくインストールするために、ホスト名へのアクセスが成功することを確認する必要があります ping6。

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。導入時にネットワークに静的IPアドレスを設定した場合は、ネットワークホストの名前を指定します。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。

## 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Windowsエディション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、64ビットのWindowsオペレーティングシステムで次の言語に対応しています。

- 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)



NetAppでは、Microsoft System Center Configuration Manager (SCCM) などのサードパーティ製ツールを使用したUnified Managerのインストールはサポートされていません。

Unified Manager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。会社の規制により、アクティブなウイルス対策ソフトウェアが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イ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には次のサードパーティパッケージがバンドルされています。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8.0.34
- Python 3.11.6
- OpenJDKバージョン11.0.20
- p7zipバージョン23.01以降





Unified Manager 9.5以降では、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がサポートされません。

MySQLが事前に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ます。
- 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 26.1.3はUnified Managerにバンドルされ、設定されています。



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2GBのディスクスペースが設定されている必要があります。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、ホスト名およびFQDNへののが正常に応答するように設定する必要があります ping。
- Microsoft IIS World Wide Web Publishing Serviceを無効にして、ポート80と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を空けておき、他のサービスで使用されないようにしてください。
- Unified Managerをインストールする前に、システムのウイルス対策ソフトウェアをすべて無効にする必要があります。インストールが完了したら、次のパスをアンチウイルス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の一覧については、Interoperability Matrixを参照してください。

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

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と、ソフトウェア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にSAML認証を設定する場合は、IdPでサポートされているブラウザの一覧も確認してください。

## プロトコルとポートの要件

必要なポートとプロトコルを使用して、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で通信できます。

### Unified Managerサーバへの接続

一般的な環境では、Unified Manager Web UIへの接続時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、の代わりに `https://<host>:443`と入力できます `https://<host>`。`

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

インターフェイス	プロトコル	ポート	製品説明
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やAPI呼び出しに使用されます。API呼び出しはHTTPSでのみ実行できます。
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へのアクセスとサポートバンドルの取得に使用されます。
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	製品説明
syslog	UDP	514	ONTAPシステムから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場合に使用されます。
REST	HTTPS	9443	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EMSイベントにアクセスするために使用されます。
MySQLデータベース	MySQL	3306	OnCommand Workflow AutomationおよびOnCommand APIサービスからUnified Managerへのアクセスで使用されます。
AMQP QPIDブローカー	TCP/IP	56072	内部メッセージ通信に使用されます。
AMQP QPIDブローカー	TCP経由のWebSocket	56080	ONTAP（クラウドエージェント）から受信したメッセージをこのポートでリッスンするために使用されます。
AMQP QPIDブローカー	TCP経由のWebSocket	56443	ONTAP（クラウドエージェント）から受信したメッセージをこのポートでリッスンするために使用されます。このポートを介した通信では、TLSまたはSSLによる暗号化がサポートされます。
AMQP QPIDブローカー	HTTP	9000	このページでAMQP管理UIインターフェイスを起動するために使用します。



WindowsシステムにUnified Managerをインストールする場合、MySQLのデフォルトポート3306はlocalhostに制限されます。インストールが完了したら、ファイアウォールを有効にしてポートmysql (3306) へのアクセスを制限します。これは、以前の設定が維持されているアップグレードシナリオには影響しません。この設定を変更したり、メンテナンスコンソールのオプションを使用して他のホストに接続を許可したりすることができ、`Control access to MySQL port 3306`ます。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通信に使用するポート (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の設定](#)"。

## 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いておく必要があります。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。

デスティネーション	プロトコル	ポート	製品説明
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。
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メールの送信に使用されます。	SNMPトラップの送信者

デスティネーション	プロトコル	ポート	製品説明
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サ ーバ
TCP	2003	外部のデータプロバイダ (Graphiteなど)にパフ ォーマンスデータを送信 するために使用されま す。	NTPサーバ
NTP	123 / UDP	Unified Managerサーバの 時刻を外部のNTPタイム サーバと同期するために 使用されます。(VMware システムのみ)	AMQP QPIDブローカー
TCP/IP	56072	内部メッセージ通信に使 用されます。	AMQP QPIDブローカー
TCP経由のWebSocket	56080	ONTAP (クラウドエー ジェント) から受信したメ ッセージをこのポートで リッスンするために使用 されます。	AMQP QPIDブローカー

## 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。ワークシートに情報を記録できます。

### 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	

ソフトウェアが導入されているシステム	あなたの価値
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名前	
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。構成に応じて、一部の値はオプションです。

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のユーザ名	
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	
認証サーバのホスト名またはIPアドレス	
Active Directory管理者名またはLDAPのバインド識別名	
Active DirectoryパスワードまたはLDAP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) メタデータ	
SNMPトラップの送信先ホストのIPアドレス	

設定	あなたの価値
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詳細を記入します。

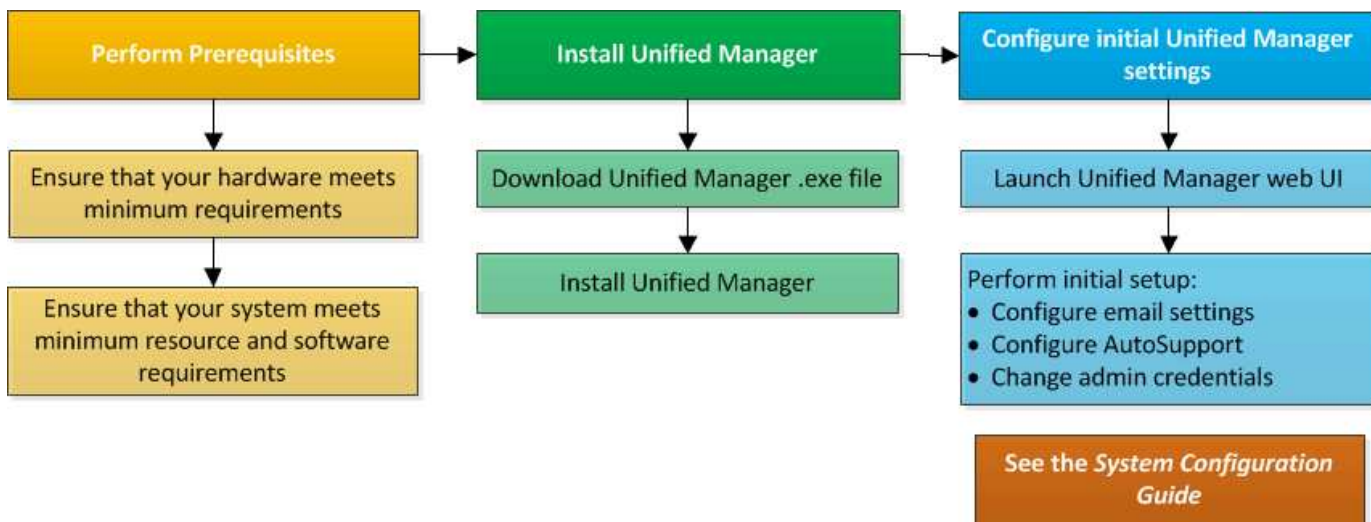
クラスタ 1 / N	あなたの価値
ホスト名またはクラスタ管理IPアドレス	
ONTAP管理者のユーザ名	
 管理者には「admin」ロールが割り当てられている必要があります。	
ONTAP管理者のパスワード	
プロトコル	HTTPS

## Unified Managerソフトウェアのインストール、アップグレード、削除

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のインストール

Unified Managerをインストールすると、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 "[ハードウェアシステムの要件](#)"

を参照して "[Windowsソフトウェアとインストールの要件](#)"



Unified Manager 9.5以降では、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がサポートされません。

- Windows管理者Privileges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ブラウザが必要です。
- 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、および特殊文字を使用する必要があります。
- 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。""%、=<>|^V () [];

使用できる特殊文字は次のとおりです。~!@#\*\$-?です。+ {}

### 手順

1. デフォルトのローカル管理者アカウントを使用してWindowsにログインします。
2. NetAppサポートサイトにログインし、Unified Managerのダウンロードページに移動します。

["NetAppサポートサイト"](#)

3. 必要なUnified Managerのバージョンを選択し、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可能ファイル (.exe) を右クリックし、管理者として実行します。

Unified Managerで不足しているサードパーティパッケージやプリインストールされているパッケージが検





## Unified Managerの無人インストールの実行

コマンドラインインターフェイスを使用すると、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を使用して、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_password MAINTENANCE_USERNAME=maintenance_username /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` オプションを使用すると、ユーザインターフェイスを縮小したクワイエットモードが有効になります。基本的なユーザインターフェイスが表示され、インストールの進行状況が示されます。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、オプションを使用し`/qr` ます。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オプションを使用すると、インストールが失敗します `/qn`。

この `/qn` オプションを使用すると、ユーザインターフェイスを使用せずにクワイエットモードが有効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。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場合は使用しない `/qn` でください。

- 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パスワードの変更

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せん。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へのアクセスにJBossが使用するパスワードも変更されます。

- 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。
- ディレクトリにあるNetAppが提供するスクリプトにアクセスできる必要があります。 password.bat  
`C:\Program Files\NetApp\essentials\bin`です。

#### 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の[サービス]コンソールを使用して、Unified Managerの次の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. スクリプトを起動し `password.bat` で、パスワードの変更プロセスを開始します。

```
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を少なくとも1文字使用する必要があります。

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

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。

## サポートされるUnified Managerのバージョンの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。

Unified Managerの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モデルに制限されているため、アップグレードはすべてのプラットフォームで次の2リリースまで実行できません。たとえば、Unified Manager 9.12および9.13からUnified Manager 9.14へのアップグレードのみを実行できます。

サポート対象のバージョンよりも前のバージョンを実行している場合は、Unified Managerインスタンスをサポート対象のいずれかの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Unified Manager 9.9でUnified Manager 9.14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. 9.9から9.11へのアップグレード
2. 9.11から9.13へのアップグレード
3. 9.13→9.14にアップグレード

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

WindowsプラットフォームでUnified Manager 9.12または9.13から9.14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 ["ハードウェアシステムの要件"](#)

を参照して ["Windowsソフトウェアとインストールの要件"](#)



Unified Manager 9.5以降では、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がサポートされません。



アップグレードを開始する前に、Microsoft .NET 4.5.2以降がシステムに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8.0.34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8.0.34に自動的にアップグレードされます。MySQLの旧バージョンから8.0.34へのスタンドアロンアップグレードを実行しないでください。
- Windows管理者Privileges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サポートサイト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。
- アップグレードで問題が発生した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は、データディレクトリのサイズよりも2.5GB大きくする必要があります。十分な空きスペースがないと、アップグレードが停止し、追加するスペースの量を示すエラーメッセージが表示されます。

- アップグレードの実行中、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。確認すると、6カ月を経過した過去のパフォーマンスデータがパージされます。
- 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

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イルス対策ソフトウェアがインストールされていると、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、システムのウイ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ください。

Unified ManagerをOnCommand Workflow Automationのインスタンスとペアにしている、両方の製品で新しいバージョンのソフトウェアを使用できる場合は、2つの製品の接続を解除し、アップグレードの実行後に新しいWorkflow Automation接続を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サポートサイトにログインし、Unified Managerのダウンロードページに移動します。

"NetAppサポートサイト"です。

2. 必要なUnified Managerのバージョンを選択し、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可能ファイル（.exe）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ブラウザの新しいウィンドウでWeb UIを起動し、アップグレード後のバージョンのUnified Managerを使用するにはログインします。
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、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実行するには、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している企業は、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へのアップグレードは、ご自身のスケジュールで行うことができます。

### 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システムのWindows管理Privilegesが必要です。

OpenJDK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 11.0.16からOpenJDK 11.0.18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. 適切なバージョンのOpenJDK（64ビット）をOpenJDKのサイトからターゲットシステムにダウンロードします。

たとえば、ダウンロードし `jdk-11.0.18\_windows-x64\_bin.zip` from <https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html> ます。



ファイルをダウンロードするにはOracleアカウントが必要です。Oracleアカウントをお持ちでない場合は、ページに移動してアカウント"[Oracleアカウントのサインイン](#)"を作成してください。

3. Windowsの[サービス]コンソールを使用して、Unified Managerの次の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. ファイルを展開し `zip` ます。
5. 作成されたディレクトリ（など）のディレクトリとファイルを、`jdk-11.0.18` Javaがインストールされている場所にコピーします `jdk`。例：`C:\Program Files\NetApp\JDK\`
6. Windowsの[サービス]コンソールを使用して、Unified Managerの次の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の再起動

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管理者Privileges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を使用してWindowsにログインします。
2. Unified Manager のサービスを停止します。

アクセス元	サービスを停止する順序
コマンドライン	<ol style="list-style-type: none"> <li>a. <code>sc stop ocie-au</code></li> <li>b. <code>sc stop Oncommandsvc</code></li> </ol>
Microsoftサービスマネージャ	<ol style="list-style-type: none"> <li>a. NetApp Active IQ取得サービス (Ocie-au)</li> <li>b. NetApp Active IQ管理サーバサービス (Oncommandsvc)</li> </ol>

3. Unified Manager のサービスを開始します。

アクセス元	サービスを開始する順序
コマンドライン	<ol style="list-style-type: none"> <li>a. <code>sc start Oncommandsvc</code></li> <li>b. <code>sc start ocie-au</code></li> </ol>
Microsoftサービスマネージャ	<ol style="list-style-type: none"> <li>a. NetApp Active IQ管理サーバサービス (Oncommandsvc)</li> <li>b. NetApp Active IQ取得サービス (Ocie-au)</li> </ol>

## Unified Managerのアンインストール

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管理者Privileges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よう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-E4A89CDDFF4E1} /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、コマンドラインのアンインストール方法を使用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の実行

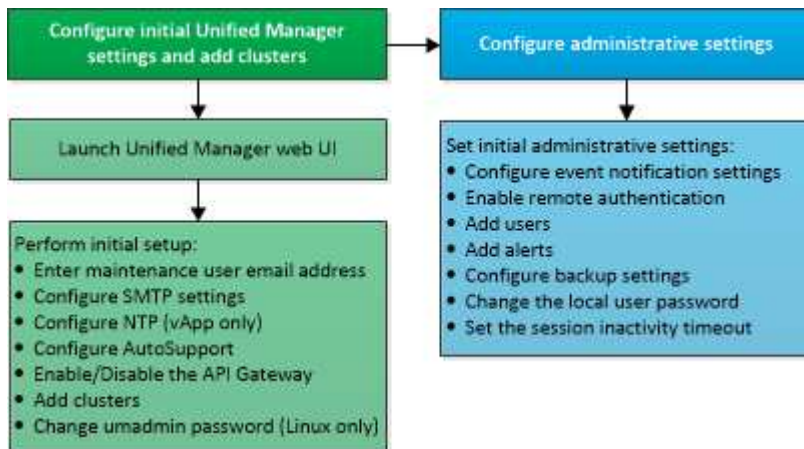
## Active IQ Unified Managerの設定

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の初期セットアップ (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、追加の設定タスクを実行できます。

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や、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を推奨します。

### 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。
- サーバで自己署名デジタル証明書が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) が署名したサーバ認証用のデジタル証明書をインストールします。

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へのログインを3回連続して失敗すると、システムがロックアウトされ、システム管理者に問い合わせる必要があります。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の実行

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。

- インストール後に表示された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[はじめに]ページは、Web UIへの初回アクセス時にのみ表示されます。次のページは、VMwareへのインストールからのものです。

## Getting Started



### Notifications

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

### Maintenance User Email

Email

### SMTP Server

Host Name or IP Address

Port

User Name

Password

Use STARTTLS ⓘ  Use SSL ⓘ

**Continue**

これらのオプションをあとで変更する場合は、Unified Managerの左側のナビゲーションペインの[全般]オプションから選択できます。NTP設定はVMware環境専用で、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サーバを入力します（VMwareの場合のみ）。[\* 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に進みます。

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、監視対象のONTAPクラスタをONTAP REST APIを使用してUnified Managerで管理できるように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せん。APIの詳細については、を参照してください"[Active IQ Unified Manager REST APIでの作業の開始](#)"。

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。

[はじめに] ページが閉じ、Unified Managerの[ダッシュボード]ページが表示されます。

## クラスタノツイカ

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、発生する可能性のある問題を見つけて解決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。
  - Unified Managerは、オンプレミスのONTAP クラスタ、ONTAP Select、Cloud Volumes ONTAP をサポートしています。
  - 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がクラスタに接続するために使用するFQDNまたは短縮名です。ホスト名は、クラスタ管理IPアドレスに解決される必要があります。

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ためのポート番号（通常はポート443）
- 必要な証明書を用意しておきます。
- SSL（HTTPS）証明書\*：この証明書の所有者はUnified Managerです。Unified Managerを新規にインストールすると、デフォルトの自己署名SSL（HTTPS）証明書が生成されます。セキュリティを強化するために、NetAppではCA署名証明書にアップグレードすることを推奨しています。サーバ証明書の有効期限が切れた場合は、証明書を再生成し、Unified Managerを再起動して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"](#)。
- EMS証明書\*：この証明書はUnified Managerが所有しています。ONTAPから受信したEMS通知の認証時に使用されます。

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がONTAPのバージョンに基づいてクラスタに対して有効になっている。ONTAPバージョンが9.5よりも前のクラスタでは、証明書ベースの認証は有効になりません。

Unified Managerの古いバージョンを更新する場合、クラスタで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することができます。証明書の有効期限が切れた場合は、新しい証明書を組み込むために証明書を再生成する必要があります。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"クラスタの編集"](#)。



- Web UIからクラスタを追加すると、証明書ベースの認証が自動的に有効になります。
- Unified ManagerのCLIを使用してクラスタを追加できますが、証明書ベースの認証はデフォルトでは有効になっていません。Unified Manager CLIを使用してクラスタを追加する場合は、Unified Manager UIを使用してクラスタを編集する必要があります。クラスタを追加するには、["サポートされるUnified ManagerのCLIコマンド"](#) Unified Manager CLIを使用します。
- 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。この問題を回避するには、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"クラスタの編集"](#)。

クラスタ証明書：この証明書の所有者はONTAP です。証明書の有効期限が切れているクラスタをUnified Managerに追加することはできません。証明書の有効期限が切れている場合は、クラスタを追加する前に証明書を再生成する必要があります。証明書の生成の詳細については、ナレッジベース（KB）の記事を参照して ["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"](#) ください。

- 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構成の場合は、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、新しいIPアドレスがクラスタグリッドとクラスタ設定ページに反映されます。

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。

クラスタの詳細を保存すると、クラスタの相互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はクラスタを最初に追加したときにのみ証明書をチェックします。Unified Managerでは、ONTAPに対するAPI呼び出しのたびに証明書は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は過去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。この機能を使用すると、クラスタを追加した直後に2週間分のパフォーマンス情報を取得できます。データの継続性収集サイクルの完了後、リアルタイムのクラスタパフォーマンスデータが収集されます（デフォルトは5分間隔）。



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、時間をずらして追加することを推奨します。また、データの継続性収集期間中にUnified Managerを再起動すると収集が停止し、その間の期間がパフォーマンスチャートに表示されません。



クラスタを追加できないというエラーメッセージが表示された場合は、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になっていないかどうかを確認してください。NTPまたは同様のサービスを使用してクロックが同期されていることを確認する必要があります。

- 関連情報 \*

["CA署名済みおよび返されたHTTPS証明書のインストール"](#)

## アラート通知を送信するためのUnified Manager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"です。

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、そのオプションを選択して必要な情報を指定できます。

### 2. "リモート認証を有効にする"です。

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. "認証サーバを追加する"です。

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することができます。

### 4. "ユーザの追加"です。

さまざまな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て、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ときに、アラート通知を受信するユーザを割り当てます。

### 5. "アラートの追加"です。

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。

## イベント通知の設定

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メールを配信できない場合、このメールアドレスは配信できない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

トラップ送信先を複数指定するには、各ホストをカンマで区切ります。この場合、他のすべてのSNMP設定（バージョンやアウトバウンドトラップポートなど）がリスト内のすべてのホストで同じである必要があります。

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、\* 一般 \* > \* 通知 \* をクリックします。
2. [Notifications] ページで、適切な設定を行います。

◦ 注： \*

- 送信元アドレスに「 + ActiveQUnifiedManager@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、ホスト名の代わりにSMTPサーバの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を使用して有効にできます。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およびLDAPS (Secure LDAP) 経由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"> <li>• 認証サーバの管理者名を次のいずれかの形式で指定します。 <ul style="list-style-type: none"> <li>◦ domainname\username</li> <li>◦ username@domainname</li> <li>◦ Bind Distinguished Name (適切なLDAP表記を使用)</li> </ul> </li> <li>• 管理者パスワード</li> <li>• ベース識別名 (適切なLDAP表記を使用)</li> </ul>
LDAPを開く	<ul style="list-style-type: none"> <li>• バインド識別名 (適切なLDAP表記)</li> <li>• バインドパスワード</li> <li>• ベース識別名</li> </ul>

Active Directoryユーザの認証に時間がかかる場合やタイムアウトになる場合は、認証サーバの応答に時間がかか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。

認証サーバで[セキュアな接続を使用]オプションを選択すると、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適用されます。

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。

#### 認証サービスのセットアップ

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、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 + <a href="#">ou@domain.com</a> + 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 + <a href="#">ou@domain.com</a> + 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 + <code>ou@domain.com</code> + である場合、ベース識別名は * <code>cn=ou</code>、<code>dc=domain</code>、<code>dc=com</code> * 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。

#### 認証サーバの追加


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
- リモート認証を有効にし、認証サーバ内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) ペアの一部である (同じデータベースを使用) 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到達できない場合でも、管理サーバがパートナーと通信できるようになります。

#### 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. [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
有効にする	<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. [Authorize Host]ダイアログボックスで、 [View Certificate]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 gray; padding: 5px; 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>
無効にする	<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. [認証サーバの追加]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]*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. テスト認証を実行して、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。

#### 認証サーバの設定のテスト

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ことを確認できます。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、設定された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。
- 管理サーバがこれらの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を検証すると、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は、パスワードを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、[スクリプト] 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。

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あとに [Event Details] ページから直接アラートを作成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 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。



ユーザに指定したEメールアドレスを変更し、アラートを編集用に再度開くと、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なくなるため、[Name]フィールドには何も表示されません。また、[ユーザ]ページで選択したユーザのEメールアドレスを変更しても、変更したEメールアドレスは更新されません。

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

次の例は、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イベントを含む
- アクション：「 + [sample@domain.com](mailto: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. [Available Resources]領域で\*\*を選択し[All Volumes whose name contains 'abc']、[Selected Resources]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](mailto: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の変更

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。

メンテナンスユーザとリモートユーザのパスワードは、次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には、[を参照してください"メンテナンスコンソールの使用"](#)。

### 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. [パスワードの変更]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。両方のインスタンスのパスワードが同じである必要があります。

## アクティブでないセッションのタイムアウトの設定

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られ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分数を設定する	[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 ホスト名の変更

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 サーバのいずれか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。ホスト名を変更した場合は、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。導入時にネットワークに静的 IP アドレスを設定した場合は、ネットワークホストの名前を指定します。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する必要があります。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、ホスト名を変更しても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の生成

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する

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、デフォルトのHTTPS証明書がインストールされます。新しいHTTPSセキュリティ証明書を生成して、既存の証明書と置き換えることができます。

- 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。

証明書を再生成する理由は複数あります。たとえば、識別名 (DN) の値をより適切に設定する場合、キーサイズを大きくする場合、有効期限を長くする場合、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、キーのサイズと有効期間を定義できます。メンテナンスコンソールのオプションを使用すると、`Reset Server Certificate`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. 証明書の生成方法に応じて、次のいずれかのオプションを選択します。

状況	操作
現在の値で証明書を再生成する	[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する	<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> <ul style="list-style-type: none"> <li>• キーサイズに指定できる値は 2048、`3072` および `4096` です。</li> <li>• 有効期間は最低1日から最高36500日です。</li> </ul> <p>36500日の有効期間が許可されていますが、397日または13カ月以内の有効期間を使用することをお勧めします。397日を超える有効期間を選択し、この証明書のCSRをエクスポートして既知のCAによる署名を取得する場合、CAから返される署名済み証明書の有効期間は397日に短縮されます。</p> <p> 証明書の[Alternative Names]フィールドからローカルの識別情報を削除する場合は、[Exclude local identifying information (e.g. localhost)]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、生成される証明書に[別名]フィールドは表示されません。</p>

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仮想マシンの再起動

Unified Managerのメンテナンスコンソールから仮想マシンを再起動できます。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。導入時にネットワークに静的IPアドレスを設定した場合は、ネットワークホストの名前を指定します。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する必要があります。

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、ホスト名を変更しても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
```

- Linuxのコマンドを使用してホスト名を変更し `hostnamectl` します。

```
hostnamectl set-hostname new_FQDN
```

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

- サーバのHTTPS証明書を再生成します。

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

- ネットワークサービスを再起動します。

```
systemctl restart NetworkManager.service
```

- サービスが再起動されたら、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
```

このコマンドは、元のホスト名に対して以前に設定したIPアドレスと同じIPアドレスを返す必要があります。

- 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の有効化と無効化

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次のような新しい項目が追加されます。

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

新しいコンテンツ	場所
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	タツシユホトカラシヨウ

これらのページおよび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"[バックアップ処理とリストア処理の管理](#)"。

## 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することができます。これには、ポリシーに基づく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、アラートを管理する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の無効化が含まれます。



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

スクリプトアップロードの詳細については、を参照してください"[スクリプトアップロードの有効化と無効化](#)"。

## 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クラスタでストレージワークロードをプロビジョニングし、割り当てられている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、次のページを操作および監視に使用できます。

- 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 \*

各画面を使用して、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、ストレージワークロードをプロビジョニングできます。また、割り当てられているパフォーマンスサービスレベルに準拠している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。または、ホスト名またはIPアドレスと <hostname> API ページにアクセスするための URL を +https://rest/docs/api/+ の形式で入力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での作業の開始](#)"。

## APIゲートウェイの有効化

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、ヘッダーと本文の要求を ONTAP API と同じ形式で維持することで、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、ONTAPから直接実行された対応するONTAP REST APIから返される応答と同じです。

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。または、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での作業の開始](#)"。

## 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。指定した時間が経過すると、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。これらのイベントは、監視対象の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。この機能を無効にして有効にすると、Unified Managerは、クラスタに対するActive IQイベントを00：15（クラスタのタイムゾーン）に受信することができます。

## 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する設定によって、Unified ManagerのクラスタおよびStorage VMの全体的な準拠ステータスが決まります。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



り」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が、に定義されている推奨事項に照らして評価され、『[Security Hardening Guide for NetApp ONTAP 9](#)』です。ダッシュボードの[セキュリティ]パネルと[セキュリティ]ページには、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準拠ステータスが表示されます。セキュリティイベントも生成され、セキュリティ違反が発生したクラスタと Storage VM に対して管理操作が有効になります。

## セキュリティ設定のカスタマイズ

ONTAP 環境に応じてコンプライアンス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。



有効または無効にするセキュリティコンプライアンスパラメータは、[Clusters]画面と[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済みレポートに直接影響する可能性があります。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は、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 の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と無効化

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 \* > \* 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する	• 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する	• 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。

## ログインハナアノツイカ

ログインバナーを追加すると、システムへのアクセスが許可されているユーザや、ログインおよびログアウト時の利用条件などの情報を組織で表示できます。

ストレージオペレータや管理者などのユーザは、ログイン、ログアウト、セッションタイムアウトの際にこのログインバナーのポップアップを表示できます。

## メンテナンスコンソールの使用

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の生成
- ネットワークの設定
- メンテナンスユーザのパスワードの変更
- 外部データプロバイダに接続してパフォーマンス統計を送信する
- パフォーマンスデータ収集の内部変更

- 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機能

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がトラブルシューティングを支援できるようにすることです。テクニカルサポートから指示があった場合にのみ使用してください。

診断ユーザは、トラブルシューティングのために、テクニカルサポートから指示があったときに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。

操作を行わないまま15分が経過すると、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、Secure Shellを使用して同時にログインすることはできません。

## 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"><li>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。</li><li>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。</li></ol>

オペレーティングシステム	実行する手順
Linux	<ol style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>コマンドを入力し maintenance_console、Enterキーを押します。</li> </ol>
ウィンドウ	<ol style="list-style-type: none"> <li>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。</li> <li>Windows管理者としてPowerShellを起動します。</li> <li>コマンドを入力し maintenance_console、Enterキーを押します。</li> </ol>

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た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。

操作を行わないまま15分が経過すると、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)
- ネットワーク構成 (VMwareのみ)
- システム構成 (VMwareのみ)
  - a. サポート/診断
  - b. サーバ証明書のリセット
  - c. 外部データプロバイダ
  - d. バックアップ/リストア
  - e. パフォーマンスポーリング間隔の設定
  - f. SAML認証の無効化
  - g. アプリケーションポートの表示/変更
  - h. デバッグログ設定
  - i. MySQLポート3306へのアクセスを制御
  - j. 終了

リストから番号を選択して、特定のメニューオプションにアクセスします。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]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 ユーザー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使用できます。

- \* 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 (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、DNSサーバなど) が表示されます。

- \* IP アドレス設定の変更 \*

仮想アプライアンスのネットワーク設定 (IPアドレス、ネットマスク、ゲートウェイ、DNSサーバなど) を変更できます。メンテナンスコンソールを使用して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、ホスト名を編集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。

- \* 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とき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を表示します。

- \* 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、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 \*

使用できる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 \*

ターゲットホストにpingを実行して、IPアドレスの変更またはDNS設定を確認します。

- \* 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]メニュー

[System Configuration]メニューでは、サーバステータスの表示、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使用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。

次のメニューオプションを使用できます。

- \* サーバステータスを表示 \*

現在のサーバステータスを表示します。ステータスオプションには、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への連絡が必要になることがあります。

- \* 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 \*

仮想マシンをシャットダウンし、すべてのサービスを停止します。

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（メンテナンスユーザのみ）のパスワードを変更します。

- \* 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 \*

タイムゾーンを現在地に変更します。

- \* NTP サーバーを変更 \*

IPアドレスや完全修飾ドメイン名 (FQDN) など、NTPサーバの設定を変更します。

- \* NTP サービスの変更 \*

サービスと `systemd-timesyncd` サービスを切り替えます ``ntp`。

- \* 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]メニューを終了し、[Main Menu]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]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な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

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 メッセージや軽量な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。

次のメニューオプションを使用できます。

- \* サーバー証明書をリセット \*

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、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の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
- \* サーバー接続の追加 / 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 から外部サーバへの接続が失われます。

- 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"[バックアップ処理とリストア処理の管理](#)"。

- \* 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 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を

提供します（セキュリティ上必要な場合）。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に制限されます。このオプションを使用すると、このポートの表示をローカルホストとリモートホストの間で切り替えることができます。つまり、環境内でlocalhostに対してのみ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。以前にリモートホストでアクセスが有効になっていた場合、設定はアップグレードシナリオで保持されます。ポートの可視性を切り替えたあとにWindowsシステムのファイアウォールの設定を確認し、MySQLポート3306へのアクセスを制限するように設定されている場合はファイアウォールの設定を無効にする必要があります。

- \* 終了 \*

メンテナンスコンソールメニューを終了します。

## Windowsでのメンテナンスユーザのパスワードの変更

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の入力を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ている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。必要に応じて、後でいつでもパスワードを変更できます。

- 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ブラウザを使用する場合、安全でないとみなされるポートがいくつかあります。HTTPおよび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。その場合は、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。

変更後は、Unified Manager Web UIにアクセスするためのURLに新しいポート番号を含める必要があります（例：+ <https://host.company.com:1234+>、+ <https://12.13.14.15:1122+>、+ [https://\[2001:db8:0:1\]:2123+](https://[2001:db8:0:1]:2123+)）。

## 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、新しく追加したネットワークインターフェイスがメンテナンスコンソールで検出されます。

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へのディスクスペースの追加

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格納されています。状況によっては、データベースディレクトリのサイズを拡張しなければならない場合があります。

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が90%フルになると警告イベントが表示され、95%フルになると重大イベントが表示されます。



ディレクトリの使用率が95%に達すると、クラスタから追加データが収集されません。

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へのスペースの追加

Linuxホストの最初のセットアップ時にUnified Managerをサポートするための十分なディスクスペースを割り当てていなかった場合は /opt/netapp/data、Unified Managerのインストール後にディレクトリのディスクスペースを増やしてディスクスペースを追加できます。 /opt/netapp/data

- 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 ユーザー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. 現在のディレクトリのデータを格納するのに十分なディスクスペースがある一時バックアップフォルダ（など）を /opt/netapp/data`作成します` /backup-data。
4. 既存のディレクトリの内容と権限の設定をバックアップデータディレクトリにコピーし`/opt/netapp/data` ます。

```
cp -arp /opt/netapp/data/* /backup-data
```

5. SE Linuxが有効な場合：

- a. 既存のフォルダのフォルダのSE Linuxタイプを取得し`/opt/netapp/data` ます。

```
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
mysqld_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=mysqld_db_t /backup-data
```

6. ディレクトリの内容を削除し `/opt/netapp/data` ます。

a. `cd /opt/netapp/data`

b. `rm -rf *`

7. LVM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以上に拡張します  
/opt/netapp/data。



をディスクから作成した場合は /opt/netapp/data、をNFS共有またはCIFS共有としてマウントしないで /opt/netapp/data` ください。この場合、ディスクスペースを拡張しようとする、や `extend` などの一部のLVMコマンドが想定どおりに動作しない可能性があるためです `resize`。

8. ディレクトリの所有者 (mysql) とグループ (root) が変更されていないことを確認し `/opt/netapp/data` ます。

```
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、ディレクトリのコンテキストが引き続きmysql\_d\_b\_tに設定されていることを確認し `/opt/netapp/data` ます。

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_b_t:s0  
/opt/netapp/data/abc
```

10. この無関係なファイルが将来データベースエラーの原因にならないように、ファイルabcを削除します。

11. backup-dataから展開したディレクトリに内容をコピーし `/opt/netapp/data` ます。

```
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=mysql_d_b_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ocieu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`/backup-data`ます。

```
rm -rf /backup-data
```

### VMware仮想マシンのデータディスクへのスペースの追加

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へのアクセスが必要です。
- 仮想マシンには、スナップショットがローカルに保存されていない必要があります。
- 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増やす前に、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、どちらか大きい方のディスクのスペースを増やしてください。データディスクには、常に他のディスクよりも多くのスペースがあります。

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へのスペースの追加

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管理者Privileges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	製品説明
物理サーバで、Unified Managerサーバがインストールされている論理ドライブに容量を追加します。	Microsoftの次のトピックの手順に従います。 <a href="#">"基本ボリュームの拡張"</a>
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。 <a href="#">"ハードディスクドライブの追加"</a>
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のトピックに記載されている手順に従います。 <a href="#">"ディスクパーティションのサイズの拡張"</a>

## ユーザアクセスの管理

ロールを作成し、Active IQ Unified Managerへのユーザアクセスを制御する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だけが、Unified Managerでオブジェクトを管理できます。

### ユーザの追加

[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。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には、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. [ユーザの追加] ダイアログボックスで、追加するユーザのタイプを選択し、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。複数のユーザが共有するEメールアドレスは指定しないでください。

4. [追加]\* をクリックします。

データベースユーザの作成

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ー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。

状況	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へのアクセス	レポートスキーマ

6. [追加]\* をクリックします。

## ユーザ設定の編集

ユーザごとに指定されたユーザ設定（Eメールアドレスやロールなど）を編集できます。たとえば、ストレージオペレータであるユーザのロールを変更し、そのユーザにストレージ管理者のPrivileges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、次のいずれかの処理が実行されたときに変更が適用されません。

- 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
- 24時間のセッションタイムアウトに達しました。

### 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. [Edit User]ダイアログボックスで、ユーザ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

[Users]ページでは、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確認できます。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、ユーザに関する詳細を確認できます。

- 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。

### 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の削除

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、それらのユーザに割り当てられていたイベントの

割り当ては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

ロールベースアクセス制御 (RBAC) 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す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。特定の機能に対するアクセスを選択した管理者だけに制限する必要がある場合は、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実行できる操作を制限する場合は、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RBACを使用します。管理サーバの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が求められます。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

ユーザタイプは、ユーザが保持するアカウントの種類を指定します。このタイプには、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、メンテナンスユーザが含まれます。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ー \*

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、追加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。

- \* ローカルユーザー \*

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する必要があります。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従って機能を実行できます。

- \* リモートユーザー \*

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ー \*

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Privilegesが含まれます。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。このロールでは、ストレージオペレータはイベントの表示、割り当て、確認応答、解決、メモの追加を行うことができます。

- \* 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、SMTP、ネットワーク、AutoSupportなどの管理オプションを管理できます。



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モデルビュー
- NetAppパフォーマンス
- ocum
- ocum\_report
- ocum\_report\_birt
- OPM
- スキャレモニタ

## Unified Managerのユーザロールと機能

Unified Managerで実行できる処理は、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	運用者	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情報の表示	•	•	•	•	•
履歴や容量のトレンドなど、その他のデータを表示する	•	•	•	•	•
イベントの表示、割り当て、解決	•	•	•		
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	•	•	•		
しきい値ポリシーの表示	•	•	•		

機能	運用者	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
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		•	•		
アラートの定義		•	•		
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します。		•	•		
ユーザの管理			•		
管理オプションの管理			•		
しきい値ポリシーの定義			•		
データベースアクセスの管理			•		
WFAとの統合を管理し、データベースビューへのアクセスを提供				•	
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		•	•		

機能	運用者	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
データベースビューへの読み取り専用アクセスの提供					•

## SAML認証設定の管理

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 Web UIにアクセスするリモートユーザがセキュアなアイデンティティプロバイダ (IdP) で認証されるようにすることができます。

SAML認証を有効にしたあとに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だけです。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 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。

### サポートされる暗号化標準

- Advanced Encryption Standard (AES) : AES-128およびAES-256
- Secure Hash Algorithm (SHA;セキュアハッシュアルゴリズム) : 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	値
sam-account-name	名前ID

要求規則	値
sam-account-name	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. 右側の[Actions]で、[Edit Global Primary Authentication Policy]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には、次の2つの回避策があります。
  - リンクに示されている手順に従って、チェーンCA証明書に関連付けられている証明書利用者についてADFSサーバで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ニンシヨウノユウコウカ

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、成功す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、両方の接続を完了する準備を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せん。

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、次回Unified ManagerのログインページではなくIdPのログインページでクレデンシャルを入力します。

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。



ADFSをアイデンティティプロバイダとして使用している場合、Unified Manager GUIではADFS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機能し続けます。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の変更

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。

設定の変更を確認す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。

許可されたりリモートユーザが 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	<ol style="list-style-type: none"><li>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。</li><li>を使用して、更新されたUnified Managerサーバから新しい証明書利用者信頼エントリを追加します <code>saml_sp_metadata.xml</code>。</li><li>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。</li><li>ADFS Windowsサービスを再起動します。</li></ol>
Shibboleth	<ol style="list-style-type: none"><li>Unified Managerサーバの新しいFQDNをファイルと <code>relying-party.xml</code>、ファイルに更新します <code>attribute-filter.xml</code>。</li><li>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。</li></ol>

9. Unified Managerにログインし、IdPでSAML認証が想定どおりに動作することを確認します。

## SAMLニンシヨウノムコウカ

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て、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。

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SAML認証を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

- 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。
- [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の SAML 認証の無効化

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。これは、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て、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ます。

SAML 認証は、 UI の [Setup/Authentication] 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] ページでは、 Unified Manager 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選択して、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 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。

## 認証サーバの編集

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。

## 認証サーバの削除

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



Microsoft Lightweight Directory Services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。管理サーバは、Lightweight Directory Access Protocol (LDAP) を使用して、設定した認証サーバ内のリモートユーザを認証します。

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。管理サーバは認証を実行し、認証にActive DirectoryまたはOpenLDAPを使用しません。

## 監査ログ

監査ログを使用すると、監査ログが侵害されていないかどうかを検出できます。ユーザが実行した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、インストールまたはアップグレードからシステムに存在するまで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で操作を実行すると、情報が更新されて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。監査ログがシステムで利用可能になると、次のいずれかの状態になります。

都道府県	製品説明
アクティブ	ログが現在ログに記録されているファイル。
標準	非アクティブで、圧縮され、システムに保存されているファイル。
改ざん	ファイルを手動で編集したユーザーによって侵害されたファイル。
手動削除	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ローリングオフされたために削除されたファイル。
予期しない削除	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、必要に応じてファイルを削除する理由を指定したりできます。これは、あとで有効な削除を判断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ーの名前とともに理由が一覧表示されます。



ログファイルを削除するとシステムからファイルが削除されますが、DBテーブル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。「正常」または「改ざん」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、.gzip します。

監査ログファイルは定期的にはアーカイブされ、参照用にデータベースに保存されます。セキュリティと整合性を維持するために、アーカイブの前に監査ログがデジタル署名されます。

フルAutoSupportバンドルが生成されると、アーカイブ済みとアクティブの両方の監査ログファイルがサポートバンドルに含まれます。ただし、簡易サポートバンドルが生成された場合は、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。

## 監査ログの設定

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すべて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の有効化

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。この機能を使用して、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グを使用すると、Active IQ Unified Managerサーバ上の監査ログファイルが改ざんされてもバックアップが改ざんされないようにすることができます。



## 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。

証明書は形式でアップロードする必要があります .pem。この証明書はターゲットのsyslogサーバから取得する必要があります、有効期限が切れていない必要があります。証明書には、(SAN) 属性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。

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 サーバー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では、コマンドを使用して証明書の<hash>を作成する必要があります。次に、クライアント認証証明書を<hash>.0にちなんだ名前のファイルにシンボリックリンクする必要があり `openssl x509 -noout -hash -in cert.pem` 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]ページにリダイレクトされます。



この値は、設定に影響する可能性があります。設定が定義された値よりも応答に時間がかかると、接続エラーが原因で設定に失敗する可能性があります。正常な接続を確立するには、[接続タイムアウト]\*の値を増やして、設定をやり直してください。

## [Remote Authentication]ページ

[リモート認証]ページでは、Unified Managerが認証サーバと通信してUnified Manager Web UIにログインするリモートユーザを認証するように設定できます。

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た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したり、独自の認証メカニズムを指定したりできます。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 \*

▪ 管理者名

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

認証サーバ内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

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索するため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

認証サーバ内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

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索するため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

認証サーバ内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。プロトコルバージョンを自動的に検出するか、バージョンを2または3に設定するかを指定できます。

- ユーザ名属性

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た属性と値に基づいて、管理サーバ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

リモートユーザが認証サーバのGroupOfUniqueNamesオブジェクトのメンバーとして含まれている場合、このオプションを使用すると、そのGroupOfUniqueNamesオブジェクト内の指定された属性に基づいて、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

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、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を検索して認証する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、削除できます。

#### ◦ 追加

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（同じデータベースを使用）の一部である場合は、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到達できない場合でも、管理サーバがパートナーと通信できるようになります。

#### ◦ 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。

テスト時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の両方を指定すると、管理サーバはリモートユーザを検索して認証します。

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確認したり、Unified Manager へのアクセスに使用できる Subject Alt Name (SAN ; 件名代替名) を確認したりできます。

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。

セキュリティ証明書に関する情報を[HTTPS Certificate]ページに表示される情報よりも詳細に表示する必要がある場合は、ブラウザで接続証明書を確認できます。

### HTTPS証明書署名要求のダウンロード

認証局にファイルを提供して署名するために、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、中間者攻撃を防止し、自己署名証明書よりもセキュリティ保護を強化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. ファイルを保存し `<hostname>.csr` ます。

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署名済みおよび返されたHTTPS証明書のインストール

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。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、中間者攻撃を防止し、自己署名証明書よりもセキュリティ保護を強化するのに役立ちます。

- 必要なもの \*

次の操作を完了しておく必要があります。

- 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た
- 証明書チェーンをPEM形式で保存しました
- 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が作成された証明書の有効期間が397日を超える場合は、CAによって証明書に署名して返送される前に、証明書の有効期間が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

次に、証明書チェーンファイルの表示例を示します。

```

-----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

自己署名証明書またはCA署名証明書をインストールし、OpenSSL、BoringSSL、LetsEncryptなどの外部ツールを使用して生成することができます。

証明書チェーンと一緒に秘密鍵をロードする必要があります。これらの証明書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. ルートまで逆方向のCAの証明書。上記の証明書を署名するために使用されます。

## ECキー ペアを含む証明書のロード形式

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キーペアを使用して証明書をロードする形式

ホスト証明書に属するRSAキーペアに許可されるキーサイズは、2048、3072、および4096です。外部で生成された\* RSAキーペアを持つ証明書\*：

```
-----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のチェック

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とき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と、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ています。

- 入力の秘密鍵は、入力のホスト証明書と照合して検証されます。
- ホスト証明書のCommon Name (CN；共通名) がホストのFQDNに照らしてチェックされます。



- ホスト証明書のCommon Name (CN) を空または空にすることはできません。また、localhostには設定しないでください。
- 有効開始日を将来の日付にすることはできません。また、証明書の有効期限を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が将来の日付ではなく、有効期限が過去の日付であってはなりません。



入力の秘密鍵は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、それらはシステムによって拒否されます。

#### 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-----
```

証明書のインストールに失敗した場合は、ナレッジベース (KB) の次の記事を参照してください。 [https://kb.netapp.com/mgmt/AIQUM/IQUM\\_fails\\_to\\_install\\_externally\\_generated\\_certificate](https://kb.netapp.com/mgmt/AIQUM/IQUM_fails_to_install_externally_generated_certificate)["外部で生成された証明書をActiveIQ Unified Managerでインストールできない"]

### 証明書管理のページの説明

[HTTPS Certificate]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 Certificate]ページ

[HTTPS Certificate]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 \*

認証局が署名して返し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 \*

新しい自己署名HTTPS証明書を生成して、現在のセキュリティ証明書と置き換えることができます。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Fully Qualified Domain Name (FQDN ; 完全修飾ドメイン名)。

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 \*

オプション。組織に連絡する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 \*

オプション。通常、会社の法人名です。

- \* 部門 \*

オプション。社内の部署の名前。

- \* 都市 \*

オプション。会社の所在地の市区町村。

- \* 状態 \*

オプション。会社の所在地の都道府県。

- \* 国 \*

オプション。会社の所在地の国。これは通常、国の2文字のISOコードです。

- \* 別名 \*

必須。既存のlocalhostまたは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追加の非プライマリドメイン名。各代行ユーザ名は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、生成される証明書に[別名]フィールドは表示されません。

- \* 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ことがあります。

詳細については、を参照してください ["HTTPS証明書の生成"](#)。

# ストレージの監視と管理

## 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で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と、問題をすぐに解決できるように一部のイベントには[修正]ボタンが表示されます。
- 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向けの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) を使用すると、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とアラート生成、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、問題を修正するための対処方法も提供されます。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、容量と健全性のグラフに表示される情報を使用して、クラスタオブジェクトの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では、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使用しています。

- 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。「使用済み物理容量」は、Storage Efficiency機能（重複排除や圧縮など）によってデータが削減されるため、通常は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。「使用済み論理スペース」は、使用済みの物理スペースと、設定されているStorage Efficiency機能（重複排除や圧縮など）による削減量を足したものです。この測定値は、データ圧縮などの物理スペースの削減量を反映していないため、使用済み物理容量よりも大きく表示されることがよくあります。したがって、合計論理容量がプロビジョニング済みスペースよりも大きくなる可能性があります。

## 容量の測定単位

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、およびPBとして表示されていました。ONTAP 9.10.1以降では、Unified Managerで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、ONTAPのすべてのリリースで、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）などです。

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
TB	TiB	1024 * 1024 * 1024 * 1024	1、099、511、627、776バイト

## Active IQ Unified Manager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することで、特定のパフォーマンスカウンタの最大値を指定して、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

これらのワークロードは、クラスタに作成したFlexVolとFlexGroupで構成されます。

- システム定義のワークロード

これらのワークロードは、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することもできます。

Unified ManagerでサポートされるAPIゲートウェイを使用して、ONTAP管理の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の詳細については、を参照してください"[Active IQ Unified Manager REST APIでの作業の開始](#)"。

## 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。

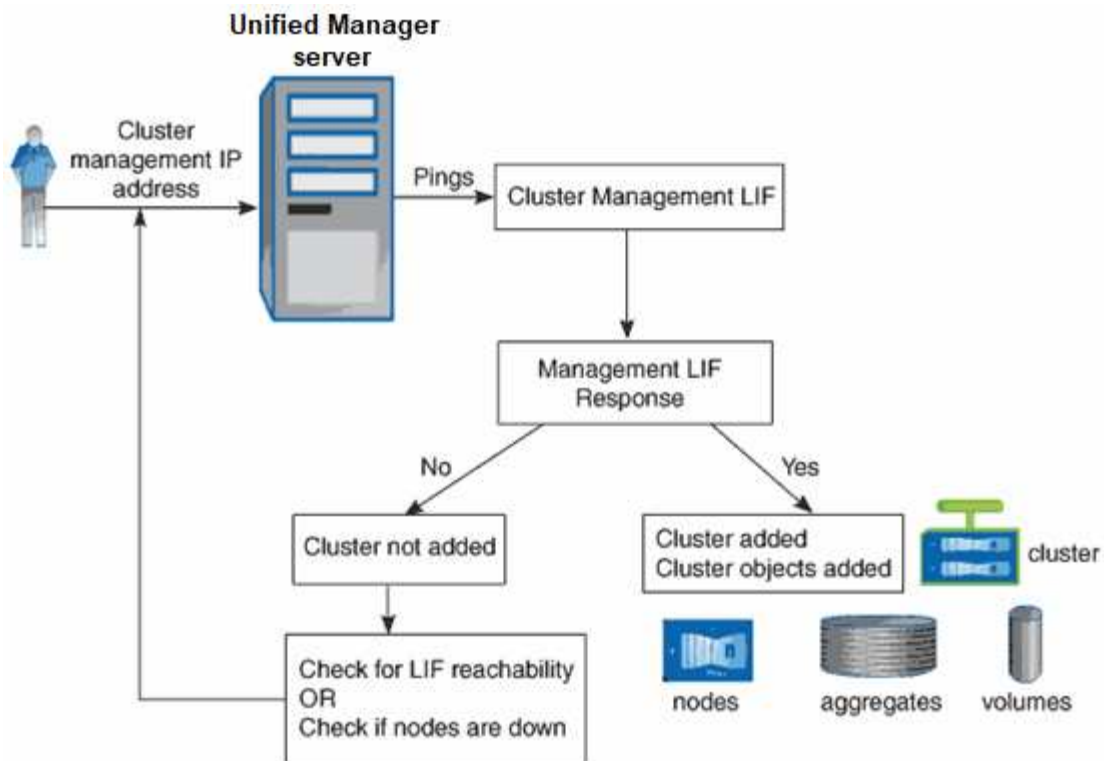
Unified Manager は、クラスタの情報を収集してデータベースにデータを格納し、そのデータを分析してクラスタに問題がないかどうかを確認します。

### 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のに役立ちます。

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。このユーザインターフェイスでは、すべてのクラスタオブジェクトを表示することもできます。

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、同じビューにならない場合があります。

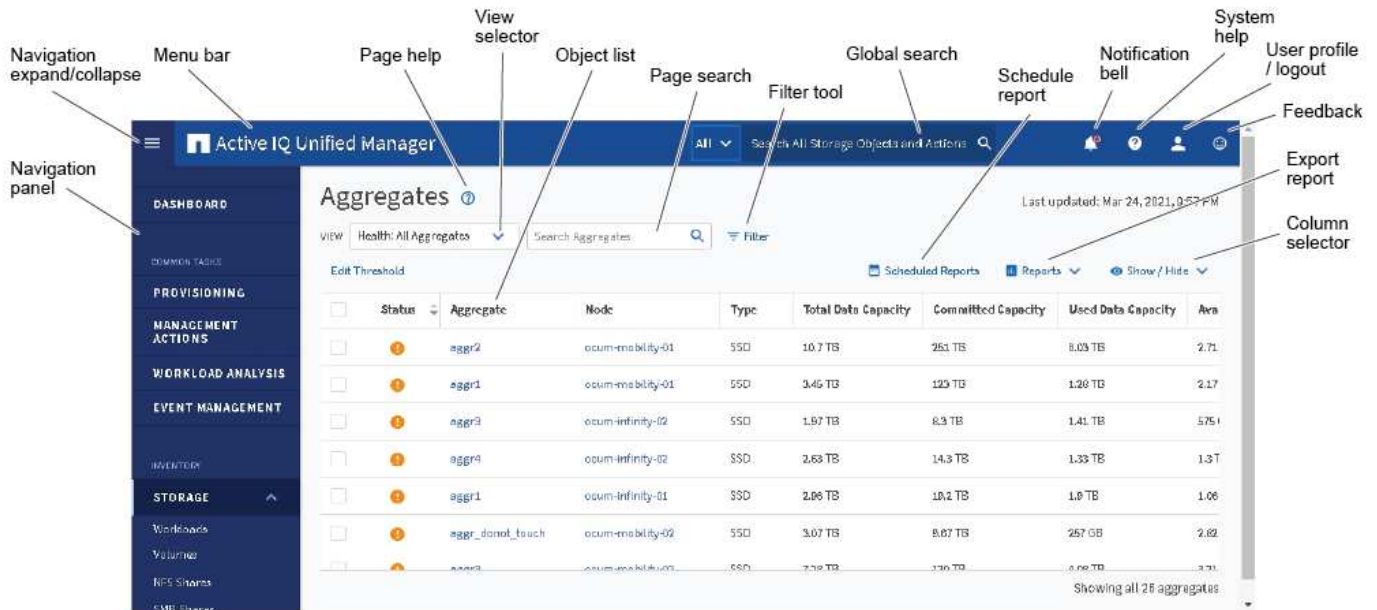
### 一般的なウィンドウレイアウト

一般的なウィンドウレイアウトを理解すると、Active IQ Unified Manager を効果的にナビゲートして使用するのに役立ちます。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。

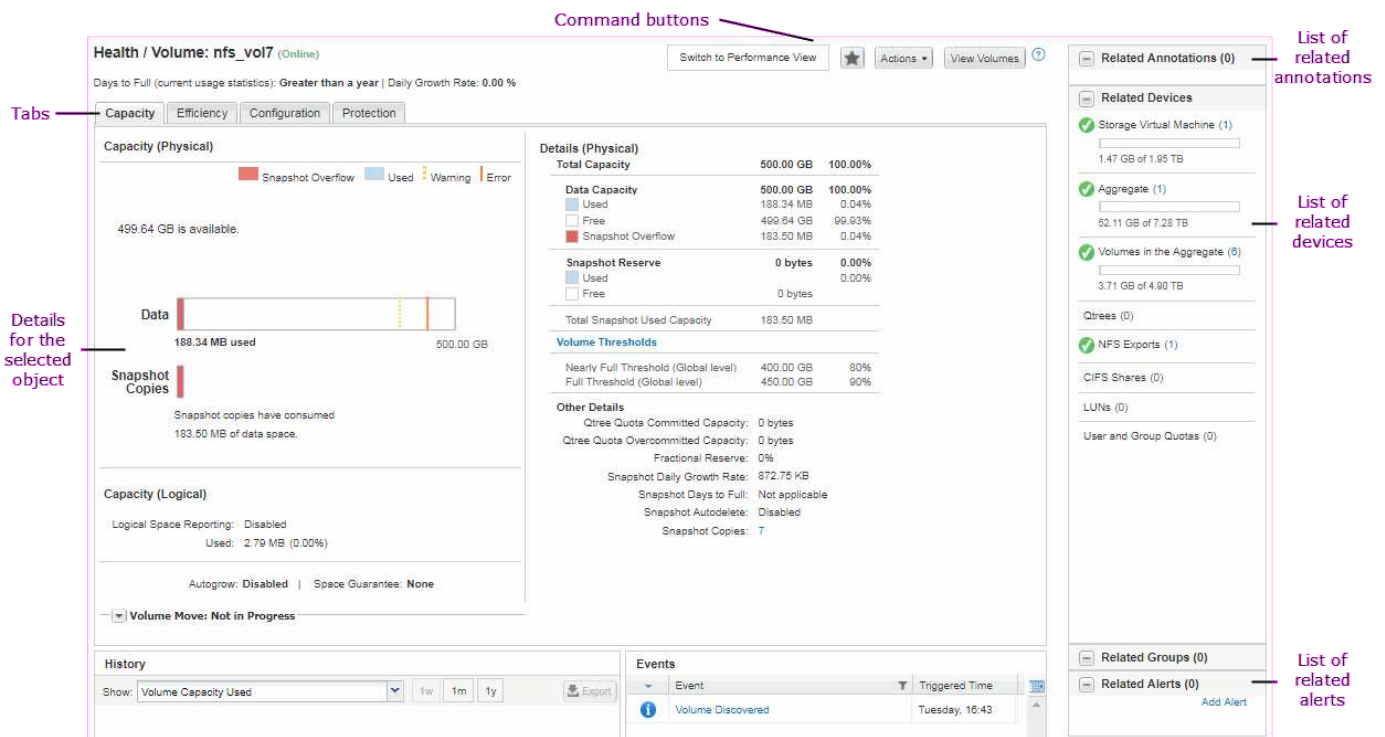
次の図のすべての要素がすべてのウィンドウに含まれているわけではありません。

### 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を使用すると、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 \*



列見出しをクリックすると、列エントリのソート順序を変更できます。列ヘッダーをクリックすると、▼ その列のソート矢印 (▲ と) が表示されます。

#### \* フィルタリング \*

フィルタアイコン ( ) をクリックすると、フィルタを適用して、指定した条件に一致するエントリのみ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できます 。フィルタは[Filters]ペインから適用します。

[Filters]ペインでは、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リングできます。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。

リスト内の容量関連の列には、容量データが小数点以下2桁に四捨五入された適切な単位で常に表示されます。これは、容量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、マウスを使用して列を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すると、インベントリページ内の項目のリストを絞り込むのに役立ちます。たとえば、「cloud」と入力してボリュームインベントリページのボリュームのリストを絞り込むと、「cloud」という単語を含むボリュームがすべて表示されます。

#### \* データのエクスポート \*

[レポート]ボタン (または[エクスポート]ボタン) をクリックすると、データをカンマ区切り値ファイル、(.pdf) `ドキュメント、またはMicrosoft Excel `(.xlsx) `ファイルにエクスポートし、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 `(.csv)。

## Unified Managerヘルプの使用

このヘルプには、Active IQ Unified Managerに含まれ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、機能とその使用方法に関する情報を検索できます。

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については、をクリックし<sup>?</sup>ます。
- すべてのヘルプコンテンツを表示するには、メニューバーの\*>[ヘルプ/ドキュメント]\*をクリックします<sup>?</sup>。

ナビゲーションペインで目次の任意の部分を展開すると、より詳細な情報を見つけることができます。

- 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、プリンタアイコンをクリックします。

## お気に入りのヘルプトピックをブックマークする

[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。ヘルプブックマークを使用すると、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. お気に入りの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の検索

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。
- 有効な検索文字は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の値「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総数が表示されます（オブジェクトカテゴリごとに最大25件の検索結果が表示されます）。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、返されるリストは上位25個のオブジェクトに制限されません。

検索できるオブジェクトタイプは次のとおりです。

- クラスタ
- ノード
- Storage VM
- アグリゲート

- 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表示される[Health]ページがない場合は、親オブジェクトの[Health]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。

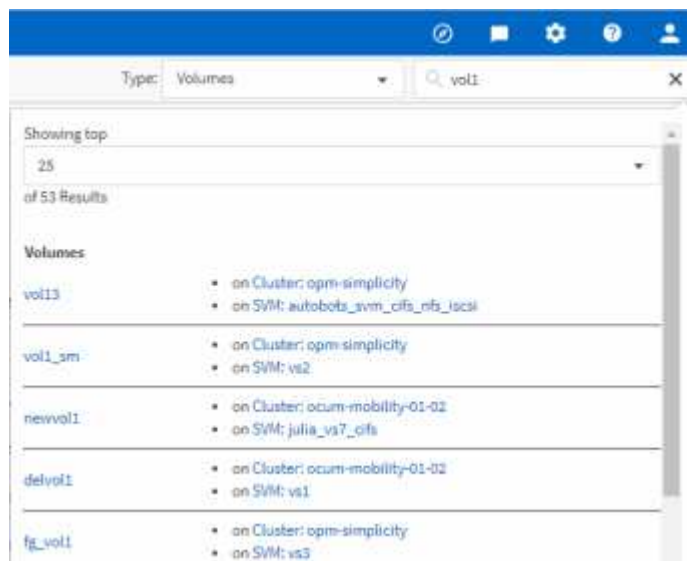


ポートとLIFはグローバル検索バーでは検索できません。

#### 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。



## レポートとしてのストレージデータのエクスポート

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件ある場合は、[イベント管理]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。

[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ファイル、`.xlsx`ファイル、`.pdf`またはドキュメントにデータをエクスポートし、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`.csv`。プロダクト内には、または`.pdf`ファイルのみを生成できる場所が他にもあり`.csv`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	操作
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。システムが提供するビュー、または作成したカスタムビューのいずれかを選択します。
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 \*

"[Health/Clustersインベントリページ]"

"レポートのスケジュール設定"

## インベントリページのコンテンツのフィルタリング

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、グリッドに表示され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、適用されているフィルタの数が[Filter]ボタンの右側に表示されます。

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、[Column]、[Operator]、および[Value]フィールドが必要です。使用可能なフィルタには、現在のページのフィルタ可能な列が反映されます。適用できるフィルタの最大数は4つです。フィルタリングされた結果は、組み合わせたフィルタパラメータに基づいて決まります。フィルタリングされた結果は、現在表示されているページだけでなく、フィルタリングされた検索のすべてのページに適用されます。

[Filtering]パネルを使用してフィルタを追加できます。

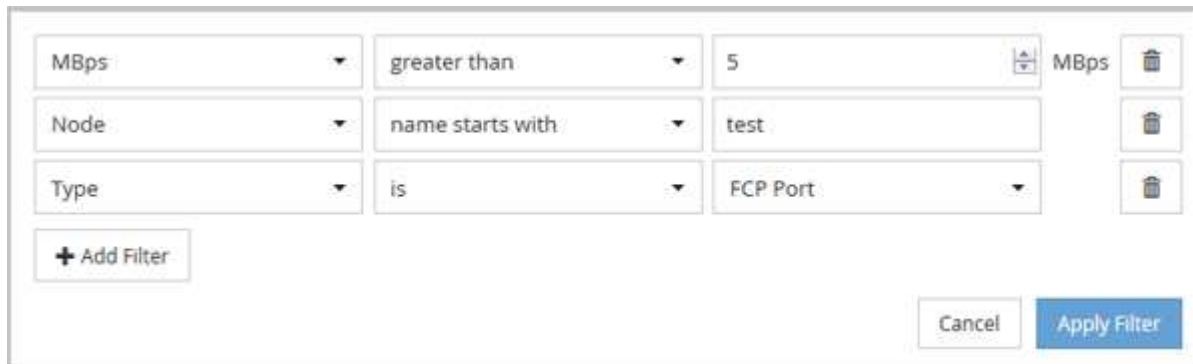
1. ページの上部にある \* Filter \* ボタンをクリックします。[Filtering]パネルが表示されます。
2. 左側のドロップダウンリストをクリックし、Cluster、パフォーマンスカウンタなどのオブジェクトを選択します。
3. 中央のドロップダウンリストをクリックし、使用する演算子を選択します。
4. 最後のリストで、値を選択または入力して、そのオブジェクトのフィルタを完了します。
5. 別のフィルタを追加するには、[\*+ フィルタの追加 \*]をクリックします。追加のフィルタフィールドが表示されます。前の手順で説明したプロセスを使用して、このフィルタを完了します。4番目の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、フィルタの数が[フィルタ]ボタンの右側に表示されます。
7. 個々のフィルタを削除するには、[Filtering]パネルで、削除するフィルタの右側にあるごみ箱アイコンを

クリックします。


- 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、3つのフィルターがある[Filtering]パネルを示しています。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。



The screenshot shows a 'Filtering' panel with three filter rows. Each row has a dropdown for the field name, a dropdown for the operator, and a text input for the value. The first row is 'MBps' with operator 'greater than' and value '5'. The second row is 'Node' with operator 'name starts with' and value 'test'. The third row is 'Type' with operator 'is' and value 'FCP Port'. To the right of each row is a trash icon. Below the rows is a '+ Add Filter' button. At the bottom right are 'Cancel' and 'Apply Filter' buttons.

[Apply Filter]\*をクリックすると、[Filtering]パネルが閉じてフィルタが適用され、適用されたフィルタの数が表示されます (  )。


### 通知ベルからのアクティブイベントの表示

メニューバーの通知ベル (  ) を使用すると、 Unified Managerで追跡している最も重要なアクティブイベントをすばやく確認できます。

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、および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、Information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が表示されます。

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。[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スペース不足やRAM不足など、スケール監視の問題も表示されます。

#### 手順

- メニューバーのをクリックします 。
- 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リンクをクリックします。

## ダッシュボードからのクラスタの監視と管理

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 ユーザー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	製品説明
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。
ワークロードパフォーマンス	定義されている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、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の数が表示されます。
使用方法の概要	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

[Dashboard]ページの各パネルには、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表示されます。また、このページの[管理操作]パネルには、Unified Managerで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せん。



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と、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だけを表示するようにフィルタリングされた[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。

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、個々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。



以下に示すパネルの一部は、構成に応じてダッシュボードに表示されます。

### [管理操作]パネル

一部の問題については、Unified Managerの詳細な診断によって単一の解決策が提供されます。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。これらの問題はUnified Managerからすぐに解決できます。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]をクリックして詳細を確認"[ONTAPの問題をUnified Managerから直接修正](#)"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による削減効果の適用後）と使用可能な物理容量（Storage Efficiencyによる削減効果を除く）、ディスクがフルになるまでの予測日数、およびONTAPのStorage Efficiency設定に基づくデータ削減率（Snapshotコピーなし）が表示されます。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]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、ローカル階層上の個々のディスクタイプ別にソートされたデータアグリゲートおよびクラウド階層について、使用済み物理容量と使用可能物理容量が表示されます。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。

### [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[Nodes]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時間の平均パフォーマンス容量が表示されます。「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ます。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、クラスタの使用済みパフォーマンス容量、合計IOPS、合計スループット（MBps）の値、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と、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ワークロード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。棒グラフの横にある数値をクリックすると、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、

- 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、[イベントの詳細]ページに詳細が表示されます。
- 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、暗号化されたボリュームと非暗号化されたボリューム、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、対応するページに移動して、フィルタリングされたクラスタ、Storage VM、ボリュームのセキュリティの詳細を確認できます。

準拠には基づいて ["ONTAP 9 セキュリティ設定ガイド"](#) ます。パネル上部の右矢印をクリックすると、[セキュリティ]ページにすべてのクラスタのセキュリティの詳細が表示されます。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"](#)。

## [Data Protection]パネル

このパネルには、データセンター内の単一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には、データ保護イベント、MetroClusterイベントの総数、および過去24時間に生成されたアクティブなイベントの数が表示されます。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。パネルには以下が表示されます

- クラスタ内のボリュームの数、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数。
- クラスタ内のボリュームの数、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数。SnapMirror関係の場合は、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経由の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くSnapMirrorの目標復旧時点 (RPO) 遅延があるボリューム関係の数。

マウスにカーソルを合わせると、それぞれのカウントと凡例が表示されます。パネル上部の右矢印をクリックすると、[Data Protection]ページで単一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を使用して、[ボリューム]ページに移動して詳細を確認します。
- [Clusters]ページに移動して詳細を表示するには、MetroCluster構成で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の棒グラフを使用します。
- すべての関係の棒グラフを使用して[Relationships]ページに移動すると、ソースクラスタに基づいて詳細がフィルタリングされます。

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の表示"](#)。

#### [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は、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の表示"](#)

["パフォーマンス容量と使用可能なIOPSの情報をを使用したパフォーマンスの管理"](#)

["\[ボリューム/健全性の詳細ページ\]"](#)

["パフォーマンスイベントの分析と通知"](#)

["イベントの重大度タイプの説明"](#)

["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の問題や機能をUnified Managerから直接管理

ONTAPの特定の問題を解決したり、特定のONTAP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することができます。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。

一部の問題については、Unified Managerの詳細な診断によって単一の解決策が提供されます。ランサムウェア

ア対策の監視など、特定のONTAP機能については、Unified Managerが内部チェックを実行し、特定のアクションを推奨します。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。この問題は、ワンクリックで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の問題と機能の詳細については、を参照してください"[Unified Managerで解決できる問題](#)"。

[修正]または[すべて修正]ボタンが表示されたときのオプション

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不明な場合は、次の操作を実行できます。

あなたは何をしたいのですか。	* 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で修正してもらいます。	「*すべて修正*」ボタンをクリックします。
この時点では特定されたオブジェクトの問題を修正せず、イベントが再度発生するまでこの管理操作を非表示にします。	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。

あなたは何をしたいのですか。	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せず、イベントが再度発生するまでこの管理操作を非表示にします。	下矢印をクリックし、* Dismiss * (キャンセル) をクリックします。

あなたは何をしたいのですか。	アクション
問題を詳しく把握するために、このイベントの詳細を表示します。	<ul style="list-style-type: none"> <li>• [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。</li> <li>• 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。</li> </ul> <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>
問題を詳しく把握するために、このストレージオブジェクトの詳細を表示します。	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。

場合によっては、次の15分間の設定ポーリングに修正が反映されることがあります。それ以外の場合は、設定の変更が検証されてイベントが廃止されるまでに最大数時間かかることがあります。

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。


#### 修正対象として選択した管理操作のステータスの表示

修正するように選択したすべての管理アクションのステータスは、[Management Actions] 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、一部の処理には時間がかかることがあります。

[Management Actions] 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、\* Dashboard の Management Actions \* パネルの上部にある  アイコン、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キ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。

- 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。
- 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キ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で解決できる問題

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するか、ONTAPの特定の機能（ランサムウェア対策の監視など）をUnified Managerで効果的に管理するかを選択できます。

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
<p>ボリュームスペースがフル</p> <p>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、デフォルトでボリュームサイズの90%に設定されています。</p>	<p>ボリュームの自動拡張を有効にする</p>	<p>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と判断したため、この機能を有効にして、必要に応じてボリュームの容量を拡張します。</p>
<p>inodeがフル</p> <p>このボリュームでinodeが不足しているため、新しいファイルを受け付けることができません。</p>	<p>ボリュームのinode数の増加</p>	<p>ボリュームのinodeの数が2%増加します。</p>
<p>ストレージ階層のポリシーの不一致を検出</p> <p>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は「snapshot-only」または「none」に設定されています。</p>	<p>クラウドの自動階層化を有効化</p>	<p>ボリュームはすでにFabricPoolに配置されているため、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。</p>
<p>ストレージ階層の不一致を検出</p> <p>アクセス頻度の低いデータが大量にありますが、クラウド対応のストレージ階層（FabricPool）にはありません。</p>	<p>ボリュームのストレージ階層の変更</p>	<p>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の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。</p>

イベント名と概要	管理操作	「修正」処理
<p>監査ログが無効</p> <p>Storage VMの監査ログが有効になっていません</p>	<p>Storage VMの監査ログを有効にする</p>	<p>Storage VMで監査ログを有効にします。</p> <p>Storage VMでローカルまたはリモートの監査ログの場所を設定しておく必要があります。</p>
<p>ログインバナーが無効</p> <p>セキュリティを強化するには、アクセス制限を明確にして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の設定</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</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のログインバナーの設定</p>	<p>Storage VMのログインバナーを「許可されたユーザのみがアクセスできます」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る</p> <p>サフィックスが「-cbc」の暗号はセキュア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する</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る</p> <p>サフィックスが「-cbc」の暗号はセキュアでないとみなされます。</p>	<p>セキュアでない暗号をStorage VMから削除する</p>	<p>安全でない暗号（aes192-cbcやaes128-cbcなど）をStorage VMから削除します。</p>
<p>AutoSupport HTTPS転送が無効</p> <p>テクニカルサポートへのAutoSupportメッセージの送信に使用する転送プロトコルを暗号化する必要があります。</p>	<p>HTTPSをAutoSupportメッセージの転送プロトコルとして設定する</p>	<p>クラスタでの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</p>	<p>Unified Managerは、不均衡を解消するためにノード間で移動するのが最適なボリュームを特定し、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ることを示します。このイベントは、アグリゲート間の使用済み容量の差異が70%を超えた場合に生成されません。</p>	<p>クラスタ容量を分散</p>	<p>Unified Managerは、不均衡を解消するためにアグリゲート間で移動するのが最適なボリュームを特定してから、ボリュームを移動します。</p>
<p>使用済みパフォーマンス容量のしきい値を超過</p> <p>非常にアクティブな1つ以上のワークロードの利用率を下げないと、ノードの負荷が過剰に利用される可能性があることを示します。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>	<p>ノードの高負荷を制限する</p>	<p>Unified ManagerはIOPSが高いボリュームを特定し、過去の想定IOPSレベルとピーク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>
<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、ノードがすでに過負荷状態で動作していることを示します。</p>	<p>ノードの過負荷を軽減</p>	<p>Unified ManagerはIOPSが高いボリュームを特定し、過去の想定IOPSレベルとピーク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>
<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>	<p>ノードフェイルオーバーを有効にする</p>	<p>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>
<p>オプションcf.takeover.on_panicがoffに設定されている</p> <p>ノードシェルオプション「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>	<p>パニック時のテイクオーバーを有効にする</p>	<p>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。</p>

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 nfs.enableを無効にします。</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</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</p> <p>Telnetは安全ではなく、暗号化されていない方法でデータを渡すため、潜在的なセキュリティ上の問題を示します。</p>	<p>Telnetを無効にする</p>	<p>Unified Managerが該当する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 Anti-Ransomware Learningの設定</p> <p>ランサムウェア対策監視のために、ライセンスがあるクラスタがないか定期的にチェックする。Storage VMがこのようなクラスタでNFSボリュームとSMBボリュームのどちらのみをサポートするかを検証します。</p>	<p>Storage VMをランサムウェア対策監視モードに切り替え learning</p>	<p>Unified Managerは、クラスタ管理コンソールを使用して、Storage VMのランサムウェア対策の監視を状態に設定します learning。Storage VMIに作成されたすべての新しいボリュームに対するランサムウェア監視は、自動的にラーニングモードに移行されます。この有効化により、ONTAPはボリューム上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できます。</p>
<p>ボリュームのAnti-Ransomware Learningの設定</p> <p>ランサムウェア対策監視のために、ライセンスがあるクラスタがないか定期的にチェックする。このようなクラスタでボリュームが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>ランサムウェア対策の監視モードにボリュームを配置 learning</p>	<p>Unified Managerは、クラスタ管理コンソールを使用して、ボリュームのAnti-Ransomware Monitoringを状態に設定します learning。この有効化により、ONTAPはボリューム上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できます。</p>



イベント名と概要	管理操作	「修正」処理
<p>ボリュームのランサムウェア対策を有効化</p> <p>ランサムウェア対策監視のために、ライセンスがあるクラスタがないか定期的にチェックする。ボリュームが45日以上ランサムウェア対策の監視モードになっているかどうかを検出し learning、アクティブモードに移行する可能性を判断します。</p>	<p>ランサムウェア対策の監視モードにボリュームを配置 active</p>	<p>Unified Managerは、クラスタ管理コンソールを使用して、ボリュームに対するランサムウェア対策の監視をに設定します active。これにより、ONTAPはボリューム上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、データ保護アクションに関するアラートを作成できます。</p>
<p>ボリュームAnti-Ransomwareを無効化</p> <p>ランサムウェア対策監視のために、ライセンスがあるクラスタがないか定期的にチェックする。ボリュームに対するアクティブなランサムウェア対策監視中に繰り返し通知を検出（たとえば、ランサムウェア攻撃の可能性に関する複数の警告が30日間にわたって返されるなど）。</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は、クラスタ管理コンソールからボリュームのAnti-Ransomware Monitoringを無効にします。</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操作を実行し、[Management Actions]ページやUnified Managerダッシュボードで使用できるデフォルトの管理操作を選択するのではなく、特定のイベントに対して特定の操作を実行できます。

イベントタイプに対して特定の操作を実行し、Unified Managerの管理操作機能で修正しないように選択する場合は、その操作用のカスタムスクリプトを設定できます。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て、そのようなイベントを個別に処理できます。この場合、[管理操作]ページまたはUnified Managerダッシュボードでは、そのイベントタイプに対する管理操作は生成されません。

## クラスタの管理

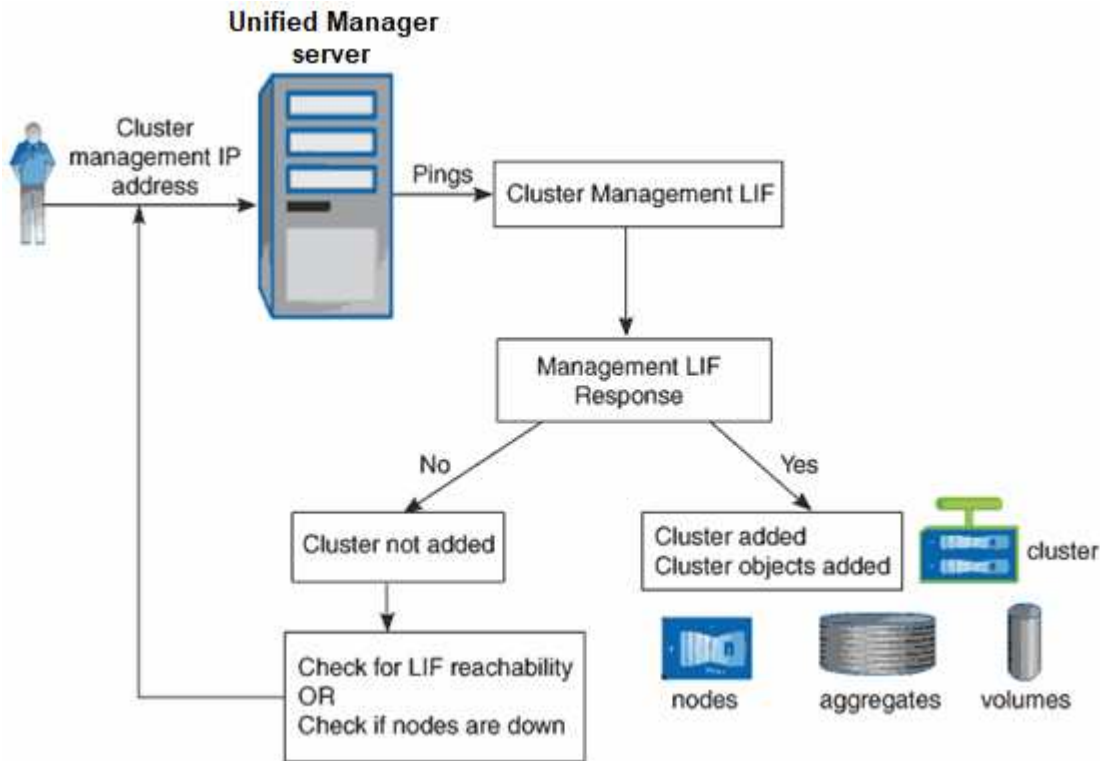
Unified Manager を使用してクラスタを監視、追加、編集、削除することで、ONTAP クラスタを管理できます。

#### 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て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、組織のクラスタとそのオブジェクトを管理するのに役立ちます。

クラスタの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。この期間は、クラスタに変更を加えた場合も同様です。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は過去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。この機能を使用すると、クラスタを追加した直後に2週間分のパフォーマンス情報を取得できます。データの継続性収集サイクルの完了後、リアルタイムのクラスタパフォーマンスデータが収集されます（デフォルトは5分間隔）。



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、時間をずらして追加することを推奨します。

## 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]ページでは、クラスタのインベントリを表示できます。クラスタについて、名前やIPアドレス、通信ステータスなどの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。

ストレージ環境内のUnified Managerで管理されている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。

## クラスタノツイカ

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、発生する可能性のある問題を見つけて解決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。
  - Unified Managerは、オンプレミスのONTAP クラスタ、ONTAP Select、Cloud Volumes ONTAP をサポートしています。
  - 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。すでに使用されているスペースが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。
- SSL (HTTPS) 証明書\*：この証明書の所有者はUnified Managerです。Unified Managerを新規にインストールすると、デフォルトの自己署名SSL (HTTPS) 証明書が生成されます。セキュリティを強化するために、NetAppではCA署名証明書にアップグレードすることを推奨しています。サーバ証明書の有効期限が切れた場合は、証明書を再生成し、Unified Managerを再起動して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"](#)。
- EMS証明書\*：この証明書はUnified Managerが所有しています。ONTAPから受信したEMS通知の認証時に使用されます。

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がONTAPのバージョンに基づいてクラスタに対して有効になっている。ONTAPバージョンが9.5よりも前のクラスタでは、証明書ベースの認証は有効になりません。

Unified Managerの古いバージョンを更新する場合、クラスタで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することができます。証明書の有効期限が切れた場合は、新しい証明書を組み込むために証明書を再生成する必要があります。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["クラスタの編集"](#)。



- Web UIからクラスタを追加すると、証明書ベースの認証が自動的に有効になります。
- Unified ManagerのCLIを使用してクラスタを追加できますが、証明書ベースの認証はデフォルトでは有効になっていません。Unified Manager CLIを使用してクラスタを追加する場合は、Unified Manager UIを使用してクラスタを編集する必要があります。クラスタを追加するには、["サポートされるUnified ManagerのCLIコマンド"](#) Unified Manager CLIを使用します。
- 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。この問題を回避するには、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["クラスタの編集"](#)。
- クラスタレベルでは、Active IQインターフェイスが認証方式「cert」に対して2つの新しいユーザグループエントリを追加します。

クラスタ証明書：この証明書の所有者はONTAPです。証明書の有効期限が切れているクラスタをUnified Managerに追加することはできません。証明書の有効期限が切れている場合は、クラスタを追加する前に証明書を再生成する必要があります。証明書の生成の詳細については、ナレッジベース (KB) の記事を参照して ["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"](#) ください。

- 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制限があります。サポートされるノード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て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。

クラスタの詳細を保存すると、クラスタの相互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はクラスタを最初に追加したときにのみ証明書をチェックします。Unified Managerでは、ONTAPに対するAPI呼び出しのたびに証明書は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は過去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。この機能を使用すると、クラスタを追加した直後に2週間分のパフォーマンス情報を取得できます。データの継続性収集サイクルの完了後、リアルタイムのクラスタパフォーマンスデータが収集されます（デフォルトは5分間隔）。



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、時間をずらして追加することを推奨します。また、データの継続性収集期間中にUnified Managerを再起動すると収集が停止し、その間の期間がパフォーマンスチャートに表示されません。



クラスタを追加できないというエラーメッセージが表示された場合は、次の問題が発生してい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になっている場合。NTPまたは同様のサービスを使用してクロックが同期されていることを確認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いる場合は、Unified Managerのアドレスを追加できません。デフォルトでは、クラスタに定義できるEMS通知の送信先は20個までです。

#### • 関連情報 \*

["ユーザの追加"](#)

["クラスタリストおよび詳細の表示"](#)

["CA署名済みおよび返されたHTTPS証明書のインストール"](#)

## クラスタの編集

[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に追加し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link:../storage-mgmt/task\\_add\\_clusters.html\["相互TLS通信用の証明書"\]](#)。[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 \*

["ユーザの追加"](#)

["クラスタリストおよび詳細の表示"](#)

## クラスタの削除

Unified Managerの[クラスタセットアップ]ページを使用して、クラスタを削除できません。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の運用を停止する場合に、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。これらの変更は、次のデータ収集サイクル後に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 \*

["ユーザの追加"](#)

["クラスタリストおよび詳細の表示"](#)

## クラスタの再検出

[クラスタセットアップ]ページでクラスタを手動で再検出すると、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確認できます。

クラスタを更新する場合（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増やすなどして）、その変更を Unified Manager で検出するには、クラスタを手動で再検出します。

Unified Manager を OnCommand Workflow Automation (WFA) とペアリングしている場合は、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仮想インフラの監視

Active IQ Unified Managerを使用すると、仮想インフラ内の仮想マシン (VM) を可視化し、仮想環境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。この機能を使用して、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上の一般的な仮想インフラ環境では、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、仮想環境におけるパフォーマンスの問題を分析し、問題が発生したコンポーネントを把握する必要があるストレージ管理者やvCenter Server管理者やITジェネラリストに役立ちます。

これで、[VMware]セクションの[vCenter]メニューからvCenter Serverにアクセスできます。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。

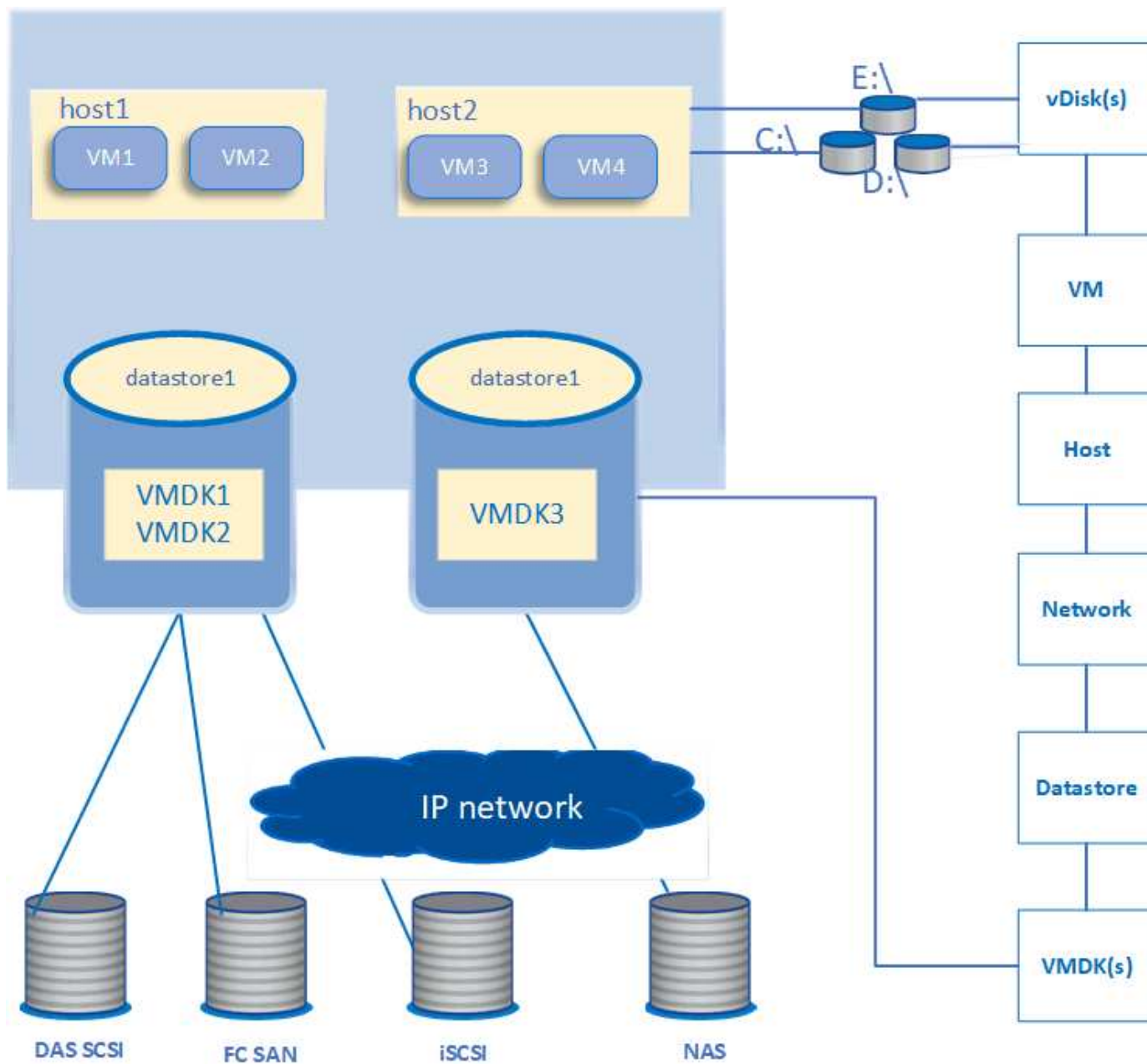
Unified Manager のトポロジビューには、仮想環境の基盤となるサブシステムが表示され、コンピューティングノード、ネットワーク、またはストレージでレイテンシ問題が発生したかどうかを確認されます。また、修復手順を実行して基盤となる問題に対応するために、パフォーマンス低下の原因となっているオブジェクトが強調表示されます。

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ます。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にマッピングされたONTAPの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。

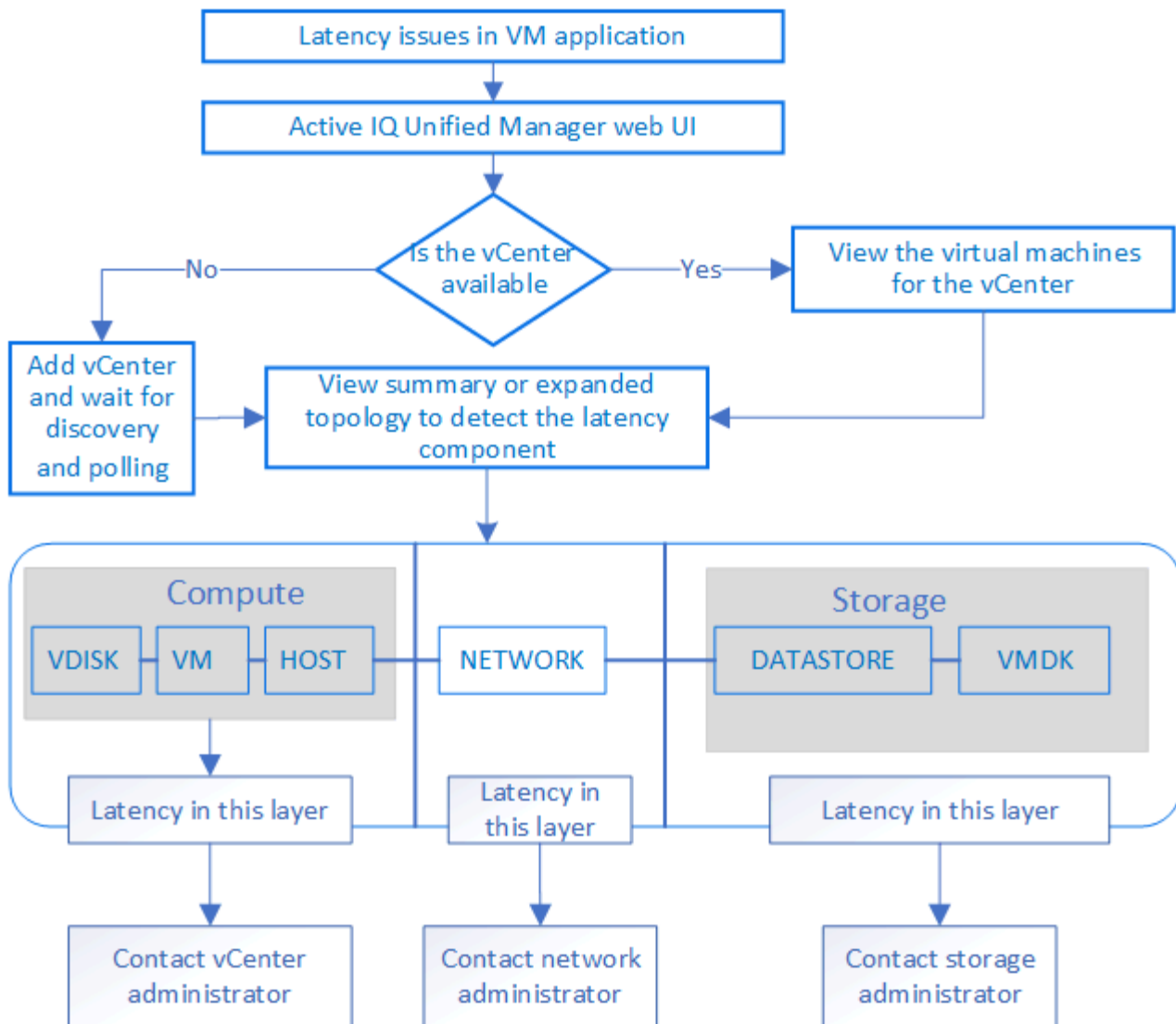
- ONTAP での VMware 仮想化 \*



- 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。





## サポート対象外

- ONTAPの外部にあり、vCenter Serverインスタンスにマッピングされているデータストアは、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を含む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。
- データLIF（アクセスエンドポイント）のマッピングにネットワークアドレス変換（NAT）を使用するデータストアはサポートされていません。
- 複数LIFを使用する構成の異なるクラスタにある同じIPアドレスのボリュームまたはLUNをデータストアとしてエクスポートすることはできません。Unified Managerで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ないためです。

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が同じIPアドレス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VM Aが作成されているとします。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、IPアドレスが同じx.x.xのデータLIFを使用してエクスポートされ、VM Bが作成されます。この場合、Unified Managerは、VM AのトポロジのデータストアAに対応するONTAPボリューム / LUNにマッピングすることも、VM Bをマッピングすることもできません。

- 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ていません。
- 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の仮想インフラでのみサポートされるStorage Virtual Machine (Storage VM) ディザスタリカバリ (DR) のセットアップでは、スイッチオーバーとスイッチバックのシナリオでアクティブなLUNをポイントするようにvCenter Serverで設定を手動で変更する必要があります。手動操作なしでデータストアにアクセスできなくなります。

## vCenter Serverの表示と追加

仮想マシン (VM) のパフォーマンスを表示およびトラブルシューティングするには、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アドレスを確認し、必要なクレデンシャルを用意しておきます。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。



VMware ESXiおよびvCenter Server向けのUnified Managerは、英語と日本語でサポートされます。

- vCenter Serverのデータ収集設定はの統計レベルに設定され *Level 3*、すべての監視対象オブジェクトに必要なレベルの指標が収集されるようにします。間隔の期間は、保存期間は *5 minutes*、*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のレイテンシ値がマイクロ秒単位ではなくミリ秒単位で設定されている。
- データストアをvCenter Serverに追加するときは、ホストのIPアドレスまたはFully Qualified Domain Name (FQDN；完全修飾ドメイン名) の両方を使用できます。FQDNを追加する場合は、ドメイン名をUnified Managerサーバで解決できることを確認してください。たとえば、Linuxをインストールしている場合は、ファイルにドメイン名が追加されていることを確認し `/etc/resolv.conf` ます。
- vCenter Serverの現在の時刻はvCenter Serverのタイムゾーンと同期しています。
- vCenter Serverに到達して検出に成功しました。
- vCenter ServerをUnified Managerに追加するときは、VMware SDKへの読み取りアクセス権が必要です。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]\*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ます。
- 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する場合は、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、サーバ証明書が表示され、承認が求められます。

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、関連するVMのデータ収集は行われず、収集はスケジュールされた間隔で実行されます。

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、次のステータスを確認できます。ただし、vCenter Serverの追加後、対応するVMのパフォーマンスとレイテンシのデータが正確に反映されるまでに最大で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サンプルを20秒収集し、サンプルを5分ごとに集計します。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いています。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時間平均を計算します。これらの

値は時間の先頭に表示されます。パフォーマンス指標はvCenter Serverを追加した直後には表示されず、次の1時間の開始時にのみ表示されます。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の設定とパフォーマンスデータの収集スケジュールについては、「クラスタ構成とパフォーマンスデータの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"](#)

## vCenter Serverの削除

Active IQ Unified ManagerインスタンスからvCenter Serverを削除できます。たとえば、vCenter Serverの検出が失敗した場合や不要になった場合は、vCenter Serverを削除できます。

vCenter Serverを削除すると、そのvCenterでホストされているすべての仮想マシン（VM）とその設定データも削除されます。削除したvCenter Serverは、関連付けられているオブジェクトおよび履歴データとともに監視されなくなります。これらの変更は、vCenterおよび仮想マシンのインベントリページに反映されます。

- 必要なもの \*

vCenter Serverを削除する前に、次の点を確認してください。

- 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。
- vCenter Serverの名前とそれぞれに関連付けられているIPアドレスを確認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、\*[VMware]>[vCenter]\*をクリックします。
2. [vCenters]ページで、削除するvCenter Serverを選択し、\*[削除]\*をクリックします。
3. [vCenterの削除]メッセージダイアログボックスで、\*[OK]\*をクリックして削除要求を確定します。

## 仮想マシンの監視

仮想マシン（VM）アプリケーションでレイテンシの問題が発生した場合は、原因の分析とトラブルシューティングを行うためにVMの監視が必要になることがあります。VMは、vCenter ServerおよびVMストレージをホストするONTAPクラスタがUnified Managerに追加されたときに使用可能になります。

VMの詳細は、\* vmware \* >> \* Virtual Machines \* ページに表示されます。VM、データストア、ホストの可用性、ステータス、使用容量と割り当て容量、ネットワークレイテンシ、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メトリックが表示されます。これらの列の中には、並べ替えやフィルタリングに使用できないものがあります。



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収集）が完了している必要があります。クラスタをUnified Managerから削除すると、次の検出サイクル後にVMを使用できなくなります。

このページからは、VMの詳細なトポロジも表示され、VMに接続されているホスト、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が表示されます。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して、レイヤ内で強調表示されているI/Oパスを決定できます。

### トポロジのサマリビューの表示

トポロジの概要で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、vCenter Serverでという名前のVM %\$VC\_AIQUM\_clone\_191124%`は、Unified Managerではと表示されます `25\$VC\_AIQUM\_clone\_191124%25。名前に特殊文字が含まれているVMを照会する場合は、この問題に注意する必要があります。

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。
  - 標準
  - 警告
  - アラート
  - 監視対象外
  - 不明
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は、すべての仮想ディスクの中でレイテンシが最も低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。1つのカテゴリに複数のノードがある場合（データストアやVMDKに複数のノードがある場合など）は、レイテンシが最も高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て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名のみが表示され、指標は表示されません。

。関連情報 \*

## "Workload Analyzerによる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設定での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ているMetroCluster構成のNASボリュームまたはLUNを表示できます。MetroCluster構成でホストされているデータストアは、標準環境のデータストアと同じトポロジビューに表示されます。

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構成の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。
- 必要なセットアップがONTAPおよびvCenter Serverで完了している必要があります。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ドキュメントセンター"

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をホストするプライマリサイトが想定どおりに機能している標準のシナリオでは、プライマリサイトのSVMクラスタの詳細が表示されます。
2. 災害が発生してセカンダリサイトに連続してスイッチオーバーされると、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、クラスタの次のサイクルとvServer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の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。
- ソースとデスティネーションの両方のクラスタピアとStorage VMピアをUnified Managerで管理する必要があります。
- 必要なセットアップがONTAPおよびvCenter Serverで完了している必要があります。
  - 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。

プライマリサイトにスイッチバックする場合は、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。災害発生時の手順として、セカンダリ Storage VM を起動し、データ LIF とルートを確認します。iSCSI ターゲット 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 アダプタの下デバイスとして使用できる必要があります。その後、新しい LUN を含む新しい VMFS データストアを作成し、古い VM を新しい名前登録する必要があります。VM が稼働し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 および新しい名前登録された古い VM を使用して、新しい VMFS データストアを再度作成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ドキュメントセンター"

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。標準のシナリオでは、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確認できます。
2. 災害が発生してセカンダリ Storage VM に連続してスイッチオーバーされると、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を示すデータストアのリンクが表示されます。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Storage VM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、クラスタの次のサイクルとvServerの検出が完了したあとに反映されます。

#### サポートされないシナリオ

- MetroCluster構成の場合は、次の制限事項に注意してください。
  - 状態と `SWITCHOVER` 状態にあるクラスタのみが `NORMAL` 稼働状態になります。や `NOT\_REACHABLE` などのその他の状態は `PARTIAL\_SWITCHOVER, PARTIAL\_SWITCHBACK` 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、次の制限事項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は、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、管理するために、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、およびストレージプロバイダAPIを提供します。



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、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ワークロードに割り当て、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。

この機能により、次の機能が有効になります。

- 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、ストレージワークロードの評価と導入を簡易化
- NFSプロトコルとCIFSプロトコルをサポートするNASワークロードのプロビジョニング
- iSCSIプロトコルとFCPプロトコルをサポートするSANワークロードのプロビジョニング
- 同じファイル共有でのNFSプロトコルとCIFSプロトコルの両方のサポート
- 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への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割り当て

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
- [ワークロードのプロビジョニング]ページでストレージワークロードを作成
- [ポリシー]からのパフォーマンスサービスレベルの作成と管理
- [ポリシー]からのストレージ効率化ポリシーの作成と管理
- [ワークロード]ページでストレージワークロードにポリシーを割り当てる
- 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) 処理を表します。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、ワークロードのIOPSとレイテンシの値は、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あとに表示されます。

[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。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。



パフォーマンスサービスレベルに準拠していない、利用できない、またはパフォーマンスサービスレベルで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、それらのワークロードが準拠していること、使用容量、IOPSが確保されるよう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の概要が表示されます。関連するデータは、データセンターレベルと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の履歴情報が一目でわかるように表示されます。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への準拠
- 割り当て済みの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ない

#### [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を管理する必要があります。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の観点から取得されます。

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処理が開始されたあとに、推奨事項（推奨PSL）について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チ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。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のすべてのワークロードについて、使用可能スペース（TiB）と使用済みスペース（TiB）とパフォーマンス（IOPS）の内訳も表示されます。

## [すべてのワークロード]ビュー

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対して推奨されるPSLが表示されます。

このページでは、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）をストレージワークロードに割り当てることもできます。次の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する
- ストレージワークロードにPSLを割り当てる
- システム推奨のPSLを評価してワークロードに割り当てる
- SEPをストレージワークロードに割り当て

## ストレージワークロードの追加またはプロビジョニング

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

[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、合計容量がバイトレベルで比較されるため、この場合は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、割り当てられているPSLとSEPに加えて、ホストクラスタやStorage VMなどの情報が表示されます。

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の分析

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](#)".

## ワークロードへのポリシーの割り当て

[すべてのワークロード]ページで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へのポリシーの割り当て

単一のワークロードにPSL、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、SEP、またはその両方を選択します。
4. チェッ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へのポリシーの割り当て

PSLまたはSEPを複数のストレージワークロードに同時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、ワークロードに一括でポリシーを適用するのに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を適用している場合、以前の一括割り当てジョブ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ています

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、割り当てられているPSLがシステム推奨のPSLと一致しない場合もあります。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やその他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ついてはスキップされます。およびラーニングステータスのストレージワークロード `Waiting for I/O` も除外されます。



Unified Managerがシステム分析よりも優先してワークロードに別のPSLを推奨するためにワークロード名に検索する特別なキーワードがあります。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 ["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

[ワークロードのプロビジョニング] ページで、既存のクラスターとStorage Virtual Machine (Storage VM) に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を作成できます。

- 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サービスの一方または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には、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ーを選択します。
2. 選択したクラスターに基づいて、Storage VM \* フィールドで、そのクラスターで使用可能な 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、[ホスト情報]セクションのNAS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に加え、必要に応じてワークロードのSEPを割り当てます。

SEPの仕様はLUNに割り当てられ、ワークロードの作成時にPSLの定義が適用されます。

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、ワークロードを作成するアグリゲートで、それぞれのポリシーで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ようになります。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、「最高レベルのパフォーマンス」ポリシーに定められたパフォーマンスと容量（SSDストレージなど）がサポートされている必要があります。



このチェックボックスをオンにしないかぎり、PSLはワークロードに適用されず、ダッシュボード上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、対応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の内部チェックが実行され、そのホストのエクスポートポリシーが作成されるか、既存のポリシーがある場合はそのポリシーが再利用されます。同じホストに対して複数のNFS共有が作成されている場合は、同じホストで使用可能な一致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、ファイル共有の作成時に新しいAccess Control List (ACL ; アクセス制御リスト) が生成されます。
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

[ワークロードのプロビジョニング] ページで、既存のクラスタと Storage Virtual Machine (Storage VM) に CIFS / SMB プロトコルと NFS プロトコルをサポートする LUN を作成できます。

- 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には、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。

選択した内容に応じて、[Host Information] 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 の仕様は LUN に割り当てられ、ワークロードの作成時に PSL の定義が適用されます。

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、ワークロードを作成するアグリゲートで、それぞれのポリシーで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ようになります。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、「最高レベルのパフォーマンス」ポリシーに定められたパフォーマンスと容量 (SSD ストレージなど) をサポートできる機能が必要です。



このチェックボックスをオンにしないかぎり、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. ホストマッピングを指定して、LUNへのイニシエータのアクセスを制御します。既存のイニシエータグループ (igroup) を割り当てたり、新しいigroupを定義してマッピングしたりできます。



LUNのプロビジョニング中に新しいigroupを作成した場合は、次回の検出サイクル（最大15分）まで使用する必要があります。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。

ストレージワークロードのリストにLUNが追加されます。

## 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、ワークロードのパフォーマンスとストレージの目標を定義できます。ワークロードの作成時または作成後にワークロードを編集してPSLを割り当てることができます。

ストレージリソースの管理と監視は、サービスレベル目標 (SLO) に基づいて行われます。SLOは、必要なパフォーマンスと容量に基づいた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とは、NetAppストレージで実行されているアプリケーションのPSLの定義を指します。ストレージサービスは、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差別化されます。PSLは、ストレージサービスの目標を表したものです。ストレージプロバイダはPSLを使用して、ワークロードの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に基づいて管理されます。各PSLは、ピークIOPS、想定最小IOPS、絶対最小IOPS、想定レイテンシによって決まります。

Unified Managerには次の種類の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
  - 値

最高レベルのパフォーマンス、パフォーマンス、バリューの各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のに適用されます。

Unified Managerには、データベースアプリケーション用に3つのパフォーマンスサービスレベルも用意されています。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。

- 最高レベル (データベースログ用)



- 最高レベル（データベース共有データ用）
- 最高レベル（データベースデータ用）
- 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。ワークロードにPSLを適用すると、パフォーマンスを最適化できます。

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、Beyond Extreme PSLの名前にという形式で付加され Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`ます。たとえば、ピークIOPSと想定IOPSがそれぞれ `37929`になるワークロードが見つかった場合 `106345`、そのワークロードに対して生成されるBeyond Extreme PSLの名前はになります Beyond Extreme 106345 37929。これらのPSLはシステムで推奨されますが、ワークロードに割り当てるとタイプが「in」とラベル付けされます User-defined。

## PSLの割り当てによるワークロードの管理

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いため便利です。変更は、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る方法については、[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ています"](#)

[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ポリシーが一覧表示され、ポリシーを追加、編集、削除できます。



システム定義のPSLや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、または使用可能なPSLが他にない場合、その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	製品説明
名前	PSLの名前。
タイプ	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予想される最小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。

フィールド	製品説明
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に基づいています。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て、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に設定されます。</p>
絶対最小IOPS	<p>想定IOPSがこの値より小さい場合は、絶対最小IOPSが無視されます。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"> <li>• 最高レベルのパフォーマンス：想定IOPS <math>\geq 6144</math>/TBの場合、絶対最小IOPS=1000</li> <li>• パフォーマンス：想定IOPS <math>\geq 2048</math>/TBで6144/TBの場合、絶対最小IOPS=500</li> <li>• 値：想定IOPS <math>\geq 128</math>/TBで2048/TB未満の場合、絶対最小IOPS=75</li> </ul> <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"> <li>• データベースログの最高レベル：想定 IOPS <math>\geq 22528</math> の場合、絶対最小 IOPS =4000</li> <li>• データベース共有データの最大 IOPS：想定 IOPS <math>\geq 16384</math> の場合、絶対最小 IOPS=2000</li> <li>• データベースデータの最高レベル：想定 IOPS <math>\geq 12288</math> の場合、絶対最小 IOPS=2000</li> </ul> <p>カスタムPSLの絶対最小IOPSの値は、最大75000になります。小さい方の値は次のように計算されません。</p> <p>1000 /想定レイテンシ</p>
想定レイテンシ	<p>ストレージIOPSの想定レイテンシ（処理あたりのミリ秒（ミリ秒/処理））。</p>
容量	<p>クラスタ内の使用可能容量と使用済み容量の合計。</p>

フィールド	製品説明
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を使用して、ONTAPクラスタで一貫した差別化されたパフォーマンスを達成する方法については、次の技術情報アート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](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で定義されたしきい値を超えているワークロードに対して生成されたイベント

過去1時間のうちにワークロードが想定レイテンシ値を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の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、レイテンシの値が上昇している原因を確認できます。

詳細については、次のリンクを参照してください。

- ["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  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	1	12288	6144	1000

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
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  データベースおよび仮想アプリケーションに最適	2	4096	2048	500
値	高いストレージ容量と中程度のレイテンシを実現  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	17	512	128	75
最高レベル (データベースログ用)	最小のレイテンシで最大スループットを実現  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。	1	45056	22528	4000

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
最高レベル (データベース共有データ用)	非常に高いスループットを最小のレイテンシで実現  共通のデータストアに格納され、データベース間で共有されるデータベースアプリケーションデータに最適です。	1	32768	16384	2000
最高レベル (データベースデータ用)	高いスループットを最小のレイテンシで実現  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。	1	24576	12288	2000

#### 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と一致しない場合は、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。次の予約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。

[パフォーマンスサービスレベル]ページで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、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。



現在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。

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	[追加]*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する	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。

パフォーマンスサービスレベルの新規または変更後のパフォーマンスサービスレベルは、[ワークロード]ページから、または新しいワークロードのプロビジョニング時にワークロード（LUN、NFSファイル共有、CIFS共有）に適用できます。

## ストレージ効率化ポリシーの管理

ストレージ効率化ポリシー（SEP）を使用すると、ワークロードのストレージ効率化特性を定義できます。ワークロードの作成時または作成後に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、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て、ストレージ利用率を高め、ストレージコストを削減します。SEPの作成時に、これらの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、指定し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適用されますが、システム定義のSEPが要件を満たしてい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や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は削除できません。また、使用可能なSEPが他にない場合は削除できません。

[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を追加、編集、削除できます。このページには、次の情報が表示されます。

フィールド	製品説明
名前	SEPの名前。

フィールド	製品説明
タイプ	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。
重複排除	ワークロードで重複排除が有効になっているかどうか。  <ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> <li>• Disable：ワークロードで重複排除が無効になります</li> </ul>
圧縮	ワークロードでデータ圧縮が有効になっているかどうか。  <ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> <li>• disable：ワークロードでデータ圧縮が無効になります</li> </ul>
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の作成に関するガイドライン

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を作成できません。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、必要な場合にのみカスタムSEP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]ページと[ボリューム/健全性の詳細]ページで確認できます。これらのStorage Efficiencyに基づいて、ダッシュボードの[容量]パネルと[容量：すべてのクラスタ]ビューで、クラスタレベルのデータ削減率（Snapshotコピーなし）を確認できます。

## 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と一致しない場合は、ワークロードに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。次の予約キーワードは使用できません。

High、 Low、 Unassigned、 Learning、 、 Idle Default、 および None。

[ストレージ効率化ポリシー]ページで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に必要なストレージ効率化の特性を定義します。



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の作成	[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する	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。

新しいストレージ効率化ポリシーまたは変更したストレージ効率化ポリシーは、[ワークロード]ページから、または新しいワークロードのプロビジョニング時にワークロード (LUN、 NFSファイル共有、 CIFS共有) に適用できます。

## MetroCluster設定の管理と監視

Unified Manager Web UIでMetroCluster構成を監視することで、MetroCluster over FCおよびIP構成に接続の問題がないかどうかを確認できます。接続の問題を早期に検出することで、MetroCluster構成を効率的に管理できます。

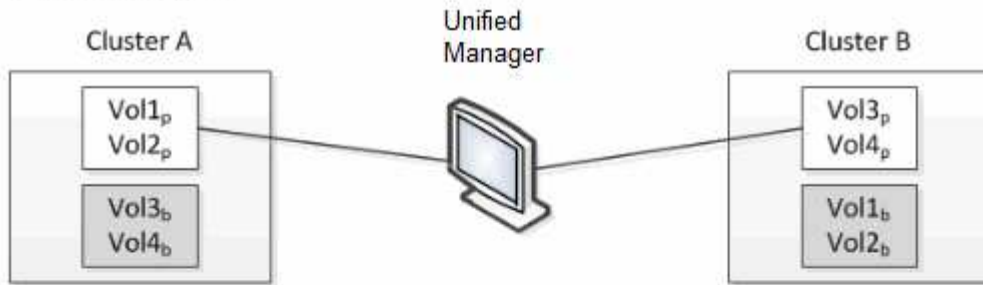
### スイッチオーバーおよびスイッチバックの発生時のボリュームの動作

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が発生すると、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アクティブなボリュームが移動されます。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上のボリュームは停止され、もう一方のクラスタ上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は、実行中のアクティブなボリュームのみを監視します。

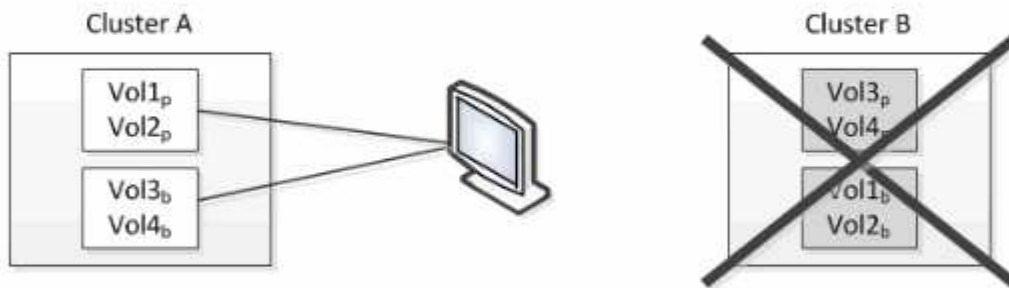


ボリュームはクラスタ間で移動されるため、両方のクラスタを監視することを推奨します。MetroCluster構成の両方のクラスタを単一のインスタンスで監視できますが、2つのサイト間の距離によっては、両方のクラスタを監視するためにUnified Managerインスタンスを2つ使用しなければならない場合があります。次の図は、Unified Managerの単一インスタンスを示しています。

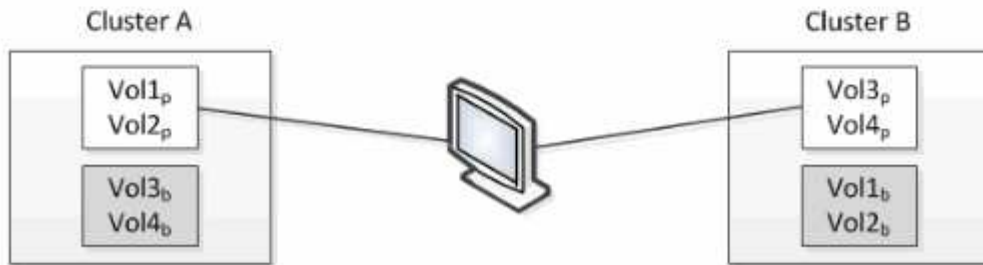
Normal operation



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」が付いたボリュームはプライマリボリュームで、「b」が付いたボリュームはSnapMirrorによって作成されたミラーバックアップボリュームです。

通常動作時：

- 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では、アクティブなボリュームごとに関連する情報（統計やイベントなど）が収集されます。Vol1pとVol2pの統計はクラスタAで収集され、Vol3pとVol4pの統計はクラスタBで収集されます。

重大な障害が発生してアクティブ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たあと、次の手順を実行します。

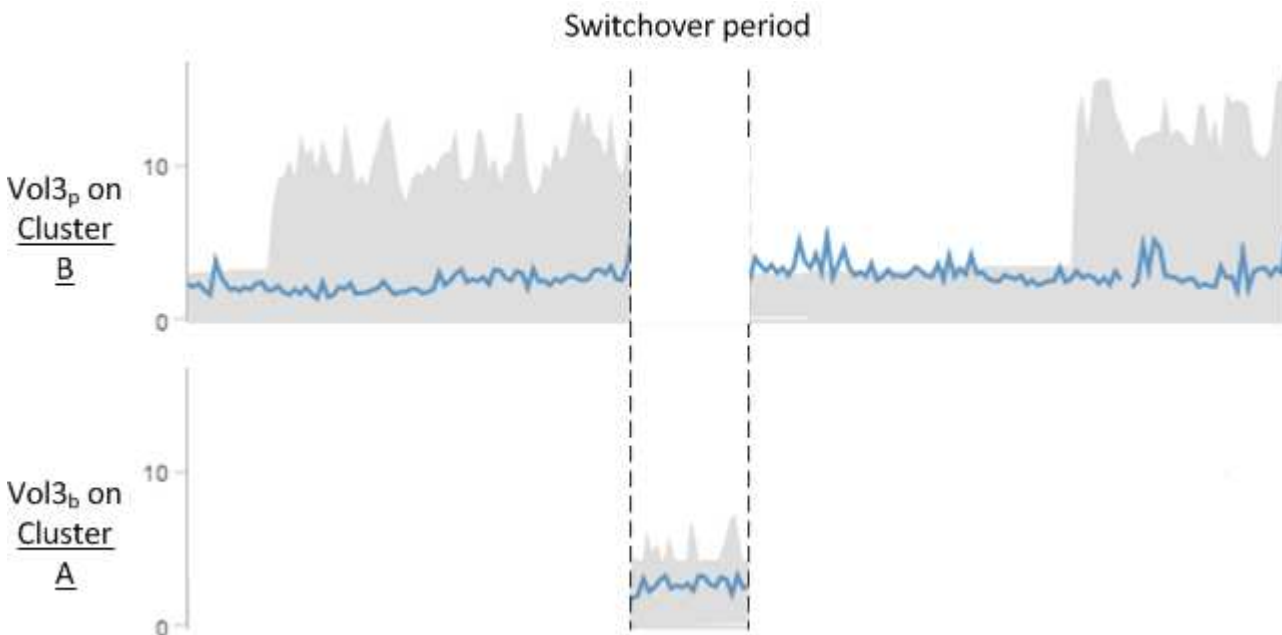
- クラスタ A には、Vol1p、Vol2p、Vol3b、Vol4b の 4 つのアクティブボリュームがあります。
- クラスタ B の 4 つのボリュームが非アクティブ：Vol3p、Vol4p、Vol1b、Vol2b。

通常運用時と同様に、Unified Managerによってアクティブ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Vol1pとVol2pの統計がクラスタAで収集され、Vol3bとVol4bの統計もクラスタAで収集されます。

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ありません。Unified ManagerのVol3pの情報がVol3bと同じではありません。

- クラスタAへのスイッチオーバー中は、Vol3pの統計とイベントは表示されません。
- スwitchオーバーの最初の時点では、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が修復されてスイッチバックが実行されると、クラスタBでVol3pが再びアクティブになり、スイッチオーバー中の期間の統計が一致しない状態になります。Vol3bは、別のスイッチオーバーが発生するまでクラスタAからは表示されません。



- 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ませんが、アクティブなボリュームではないためUnified Managerで現在監視されていません。
- 1つのUnified ManagerでMetroCluster構成の両方のクラスタを監視している場合、ボリューム検索ではその時点でアクティブなボリュームに関する情報が返されます。たとえば、スイッチオーバーが発生し、クラスタAでvol3がアクティブになった場合、「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ことで、MetroCluster構成を効果的に管理できます。

接続ステータス	製品説明	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場合、クラスタ間IPリンクが停止している場合、パートナークラスタに到達できない場合などです。	
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、災害が原因で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が実行され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ステータスの定義

MetroCluster over FC構成では、データがミラーリングされ、サイト全体が使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が追加されます。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」のいずれかです。ステータスを理解しておくことで、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	製品説明	アイコンが表示されます
標準	MetroCluster構成のクラスタ間のデータミラーリングは正常な状態です。	
ミラーリング利用不可	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使用できません。たとえば、災害が原因で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が実行され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設定の監視

MetroCluster構成の接続の問題を監視できます。これには、クラスタ内のコンポーネントと接続のステータス、およびMetroCluster構成内のクラスタ間の接続ステータスが含まれます。ここでは、MetroCluster over FC構成と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を学習します。

MetroClusterの設定は、Active IQ Unified Managerの左側のナビゲーションペインから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と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構成でメディアエーターをサポートする場合は、対応するAPIを使用してメディアエーターを設定し、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

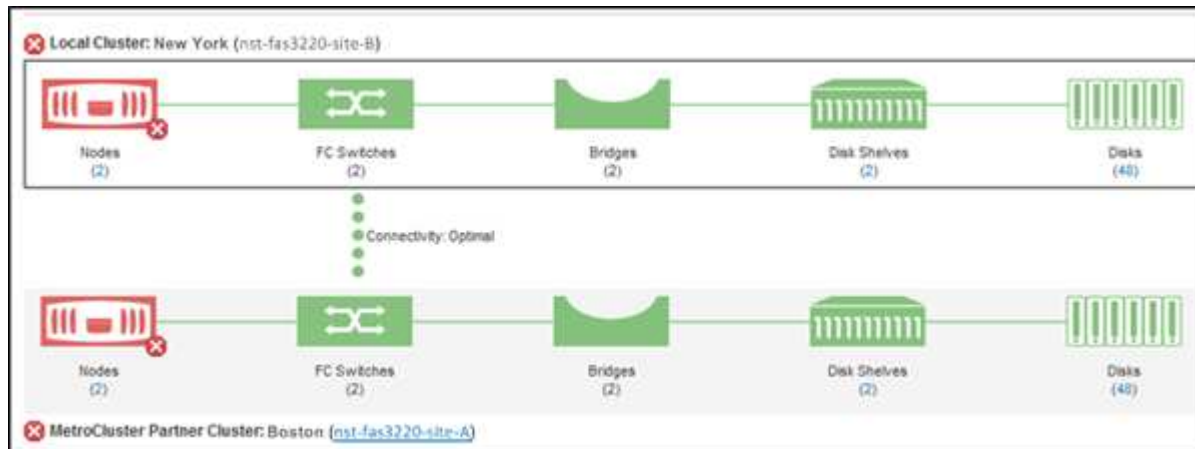
MetroCluster over FC構成のクラスタの場合は、接続グラフが\* Cluster/Health \* detailsページに表示されます。次の手順を実行します。

## 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リング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使用して、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断の詳細については、を参照してください"[MetroCluster over FC構成のクラスタの健全性の確認](#)".

## MetroCluster over IP構成の接続の問題を監視する

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リングすることもできます。
3. キャレットアイコンをクリックして行を展開します。キャレットアイコンは、MetroCluster over IP構

成で保護されているクラスタに対してのみ表示されます。

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エーター（ある場合）を表示できます。次の情報を表示できます。

- サイト間の接続
- 両方のサイトの健全性と可用性の問題（存在する場合）
- 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。



報告されるステータスは、Critical (❌)、Error (⚠️)、Normal (✅) です。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を表示することもできます。

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の間のサイト間接続は使用できず、クラスタ間のメディエーターも設定されていません。



4. 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が正常 (✅) に変わります。
5. 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 \*
- ["\[クラスタ/健全性の詳細ページ\]"](#)
- 関係：MetroCluster \*ビューの詳細については、を参照してください"[MetroCluster設定の監視](#)".



- [関係：過去1カ月の転送ステータス]\*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](#)"。
- [関係：過去1カ月の転送速度]\*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：すべての関係]\*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レプリケーションの監視

データのミラーリング中に論理接続の全体的な健全性状態を監視および診断できます。クラスタコンポーネント（アグリゲート、ノード、Storage Virtual Machineなど）のミラーリングを中断する問題やリスクを特定できます。

Unified Manager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と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、Unified Managerの左側のナビゲーションペインの次のビューから、MetroCluster over IPで保護されているクラスタのトポロジックビューにデータレプリケーションの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

MetroCluster over FC構成のデータレプリケーションに関する問題を特定するには、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 \* > \* 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、データのミラーリング先のリモートサイトに関する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。

[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て、レプリケーションの問題を修正できます。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すると、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数を制限できます。ディスクとファイルの使用量、ディスクに設定されているさまざまな制限など、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た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 /健全性の詳細]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 \*

["ユーザの追加"](#)



## Eメールアドレスを生成するルールを作成

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Eメールアドレスのルールを定義し、実行順序で入力する必要があります。たとえば、abcのクォータ違反に関する通知をEメールアドレスabc@xyz.comで受信し、他のすべてのグループにEメールアドレスDL-\$GROUP@\$DOMAINを使用する場合は、ルールを次の順序で指定する必要があります。

- if (\$user =='abc') then abc@xyz.com
- if (\$GROUP ==\*) THEN DL-\$GROUP@\$DOMAIN

指定したルールの条件が1つも満たされない場合は、デフォルトのルールが使用されます。

(\$USER\_OR\_GROUP==\*) の場合、\$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発生した場合（ソフトリミットを超過した場合、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されるEメールの通知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。Eメールアドレスを変更すると、[ユーザクォータと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で生成されたEメールアドレスを上書きできます。

- 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。指定したルールで生成された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	そしたら...
指定したルールで生成されたEメールアドレスに通知を送信する	<ol style="list-style-type: none"> <li>a. <b>[Email Address]</b> フィールドの電子メールアドレスを削除します。</li> <li>b. [保存 (Save)] をクリックします。</li> <li>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。</li> </ol>

状況	そしたら...
指定したEメールアドレスに通知を送信する	<p>a. <b>[Email Address]</b> フィールドで電子メールアドレスを変更します。</p> <p>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。</p>

## クォータに関する詳細情報

クォータの概念を理解すると、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。ソフトクォータでは、指定された制限を超えるとONTAPによって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えると書き込み処理が失敗します。

ONTAPは、ユーザまたはユーザグループからFlexVol volumeへの書き込み要求を受信すると、そのボリュームでその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確認し、次の点を判断します。

- ハードリミットに達するかどうか

「はい」の場合、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えるかどうか

「yes」の場合は、ソフトリミットを超えたときに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。

- 書き込み処理がソフトリミットを超えないかどうか

yesの場合、書き込み処理は成功し、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。クォータはファイルを使用して指定し、`/etc/quotas`で管理されます。クォータは、特定のボリュームまたはqtreeに適用されません。

### クォータの使用目的

クォータを使用すると、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
- 制限を課すことなく、ユーザ、グループ、またはqtreeによって使用されているディスクスペースの量やファイル数を追跡する場合
- ディスク使用量またはファイル使用量が多いときにユーザーに警告する

## クォータのダイアログボックスの説明

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

[Email Notification Format]ページには、クォータ関連の問題が発生した場合（ソフトリミットを超過した場合、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されるEメールのルールが表示されます。

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できます。デフォルトでは、[通知]ページに指定されているE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。必要に応じてテキストを変更できます。たとえば、クォータ属性に関連する情報を指定し、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。

#### ◦ \$イベント名

Eメール通知の原因となったイベントの名前を指定します。

- \$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\_used\_percent

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のうち、ユーザまたはユーザグループによって使用されている割合を示します。

- \$quota\_limit

ユーザまたはユーザグループが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に達し、次のいずれかのイベントが生成されます。

- 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

ユーザまたはユーザグループによって使用されているディスクスペース、または作成されたファイル数を示します。

- \$quota\_user

ユーザまたはユーザグループの名前を指定します。

## コマンドボタン

各コマンドボタンを使用して、Eメール通知形式に対する変更をプレビュー、保存、または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。

## [Rules to Generate User and Group Quota Email Address]ページ

[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、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。

## [Rules]領域

クォータEメールアドレスの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。基準が満たされていない場合は、次のルールの基準が考慮されます。各行には個別のルールが表示されます。デフォルト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、他のすべてのqtreeにEメールアドレスadmin@xyz.comを使用する場合は、ルールを次の順序で指定する必要があります。

- (`$qtree == 'qtree1'`) の場合はqtree1@xyz.com
- (`$qtree == *`) の場合はadmin@xyz.com

指定したルールの条件が1つも満たされない場合は、デフォルトのルールが使用されます。

(`$USER_OR_GROUP == *`) の場合、`$USER_OR_GROUP@$DOMAIN`

クォータが同じユーザが複数ある場合は、ユーザの名前がカンマで区切られた値で表示され、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#を使用する必要があります。各行には個別のコメントが表示されます。

### ルールの構文

ルールの構文は、次のいずれかである必要があります。

- `if valid variableoperator * ()`の場合 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`、`$GROUP`、または任意の文字と有効な変数 `$USER_OR_GROUP`、`$USER`、または `$GROUP` の組み合わせを使用できます。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` の組み合わせを含めることができます。有効な変数は大文字または小文字で指定できますが、両方を組み合わせて指定す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` ()`の場合 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`、`$GROUP`、または任意の文字と有効な変数 `$USER_OR_GROUP`、`$USER`、または `$GROUP` の組み合わせを使用できます。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` の組み合わせを含めることができます。有効な変数は大文字または小文字で指定できますが、両方を組み合わせて指定す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

作成したルールを保存、検証、キャンセルするには、各コマンドボタンを使用します。

- \* 検証 \*

作成したルールの構文を検証します。検証中にエラーが発生した場合は、エラーを生成するルールとエラーメッセージが表示されます。

- \* 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。検証中にエラーが発生した場合は、エラーを生成するルールとエラーメッセージが表示されます。

## 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へのディスクスペースの追加

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格納されています。状況によっては、データベースディレクトリのサイズを拡張しなければならない場合があります。

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が90%フルになると警告イベントが表示され、95%フルになると重大イベントが表示されます。



ディレクトリの使用率が95%に達すると、クラスタから追加データが収集されません。

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へのスペースの追加

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へのアクセスが必要です。

- 仮想マシンには、スナップショットがローカルに保存されていない必要があります。

- 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増やす前に、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。

まれに、Unified Manager環境のデータディスクに「Hard Disk 3」ではなく「Hard Disk 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、どちらか大きい方のディスクのスペースを増やしてください。データディスクには、常に他のディスクよりも多くのスペースがあります。

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へのスペースの追加

Linuxホストの最初のセットアップ時にUnified Managerをサポートするための十分なディスクスペースをに割り当てていなかった場合は /opt/netapp/data、Unified Managerのインストール後にディレクトリのディスクスペースを増やしてディスクスペースを追加できます。 /opt/netapp/data

- 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. 現在のディレクトリのデータを格納するのに十分なディスクスペースがある一時バックアップフォルダ（など）を /opt/netapp/data`作成します ` /backup-data。
4. 既存のディレクトリの内容と権限の設定をバックアップデータディレクトリにコピーし ` /opt/netapp/data` ます。

```
cp -arp /opt/netapp/data/* /backup-data
```

5. SE Linuxが有効な場合：
  - a. 既存のフォルダのフォルダのSE Linuxタイプを取得し ` /opt/netapp/data` ます。



```
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_b_t
```

- a. コマンドを実行し `chcon` で、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_b_t /backup-data
```

6. ディレクトリの内容を削除し `rm` します。

- a. `cd /opt/netapp/data`
- b. `rm -rf *`

7. LVM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以上に拡張します  
/opt/netapp/data。



をディスクから作成した場合は /opt/netapp/data、をNFS共有またはCIFS共有としてマウントしないで /opt/netapp/data` ください。この場合、ディスクスペースを拡張しようとする、や `extend` などの一部のLVMコマンドが想定どおりに動作しない可能性があるためです `resize`。

8. ディレクトリの所有者 (mysql) とグループ (root) が変更されていないことを確認し `ls` します。

```
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、ディレクトリのコンテキストが引き続きmysql\_d\_b\_tに設定されていることを確認し `ls` します。

- 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_b_t:s0  
/opt/netapp/data/abc
```

10. この無関係なファイルが将来データベースエラーの原因にならないように、ファイルを削除し `rm` します。

11. から展開した `/opt/netapp/data` ディレクトリに内容をコピーし `backup-data` ます。

```
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 `backup-data` ます。

```
rm -rf /backup-data
```

## Microsoft Windowsサーバの論理ドライブへのスペースの追加

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管理者Privileges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	製品説明
物理サーバで、Unified Managerサーバがインストールされている論理ドライブに容量を追加します。	Microsoftの次のトピックの手順に従います。 <a href="#">"基本ボリュームの拡張"</a>
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。 <a href="#">"ハードディスクドライブの追加"</a>
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のトピックに記載されている手順に従います。 <a href="#">"ディスクパーティションのサイズの拡張"</a>

## パフォーマンス統計の収集間隔の変更

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どおりに完了しない問題は、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>.

収集間隔を変更する必要があるのは、統計の収集に問題があるためです。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。5分間の収集を使用する場合は、6回の収集でポリシーの超過が連続して発生する必要があります。収集時間が15分の場合、2つの収集期間でのみポリシーの超過が必要です。

[Cluster Setup]ページの下部に、現在の統計データ収集間隔を示すメッセージが表示されます。

### 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番号を入力し、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。この時間が経過すると、古いデータは自動的に削除され、新しいデータ用のスペースが確保されます。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い

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。

[Data Retention]ページでは、これら2種類のデータの保持期間を変更できます。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分間の統計が1時間ごとのパフォーマンス統計に要約されます。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非常に長い時間がかかる場合だけにしてください。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せん。
- 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。
- 保持期間より前のイベントは、ユーザインターフェイスに表示できなくなります。
- 保持期間の前は、1時間ごとのパフォーマンス統計が表示されるUIの場所に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を超えると、古いパフォーマンスイベントに対応するグラフにバックアップデータが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

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、テストなどの認証関連の処理を実行すると、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可能性があります。

- 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、テストなどの認証関連の処理を実行すると、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、ベース識別名を誤った値に設定した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。

## 他の認証サービスを使用してLDAPを追加する場合の問題

認証サービスとして[その他]を選択した場合、ユーザーとグループの[オブジェクトクラス]には、前に選択したテンプレートの値が保持されます。LDAPサーバで同じ値が使用されていないと、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、次のいずれかの回避策を使用して手動で修正できます。

LDAP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およびgroupの場合は、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の場合は、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つの対処方法が当てはまらない場合は、APIを呼び出し `option-set`、オプションと ``auth.ldap.groupObjectClass`` オプションを正しい値に設定し ``auth.ldap.userObjectClass`` 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。これらのイベントは、Unified Managerで監視され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イベントと重複せず、システム構成、ケーブル接続、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が特定されます。

プラットフォームイベントのイネーブル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ルールファイルのアップロード"](#)。

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。詳細については、を参照してください ["NetApp Active IQ"](#)。

### イベント管理システムイベントとは

イベント管理システム（EMS）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。一元的な監視と管理により、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イベントが自動的に報告されます。
- EMSイベントを個別に受け取るようにサブスクライブ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	自動の <b>EMS</b> メッセージ	登録した <b>EMS</b> 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)	固有ではない (「Error EMS Received」の形式)。詳細なメッセージには、実際のEMSイベントのドット表記形式が記載されています。
受信したメッセージ	クラスタが検出されるとすぐに	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	EMSイベントはクラスタの更新後 (イベントが作成されてから15分後) に廃止になります。
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供	[ 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イベントの一部は、以前のイベントが解決されたことを示す情報イベントです。たとえば、「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」という情報イベントは、「FlexGroupコンスティチュエントのスペースに問題があります」エラーイベントが解決されたことを示しています。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拒否	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	gb.netra.ca.check.failed	アグリゲート	エラー
FabricPoolのミラーレプリケーションの再同期が完了しました	waf1.ca.resync.complete	クラスタ	エラー
FabricPoolスペースがほぼフル	FabricPoolほぼフル	クラスタ	エラー
NVMEの猶予期間-開始	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を破棄	lun.destroy	LUN	情報
Cloud AWS メタデータ接続エラー	Cloud.aws.metadataConnFail	ノード	エラー
Cloud AWS IAMクレデンシャルが期限切れ	Cloud.aws.iamCredsExpired	ノード	エラー
Cloud AWS IAMクレデンシャルが無効	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	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	objstore.host.unresolvable	ノード	エラー
クラウド階層のクラスタ間ネットワーク インターフェイスが停止	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.signatureMismatch	ノード	エラー
NFSv4プールの1つに空きなし	Nblade.nfsV4PoolExhaust	ノード	重大
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.縮小	ノード	情報
NVMe名前空間の破棄	NVMeNS.destroy	名前空間	情報
NVMe名前空間オフライン	NVMeNS.offline	名前空間	情報
NVMe名前空間オンライン	NVMeNS.online	名前空間	情報
NVMe名前空間スペース不足	NVMeNS.out.of.space	名前空間	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.of.sync	SnapMirror関係	警告
同期レプリケーションをリストア	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失敗	sms.resync.attempt.failed	SnapMirror関係	エラー
多数の CIFS 接続	Nblade.cifsManyAuth	SVM	エラー
最大CIFS接続数を超過	Nblade.cifsMaxOpenSameFile	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
ユーザあたりの最大CIFS 接続数を超過	Nblade.cifsMaxSessPerU srConn	SVM	エラー
CIFS NetBIOS名が競合し ています	Nblade.cifsNbNameConfli ct	SVM	エラー
存在しないCIFS共有への 接続試行	Nblade.cifsNoPrivShare	SVM	重大
CIFSシャドウコピー処理 が失敗しました	cifs.shadowcopy.failure	SVM	エラー
AVサーバでウイルスが検 出されました	nblade.vscanVirusDetecte d	SVM	エラー
ウイルススキャン用のAV サーバ接続がありません	Nblade.vscanNoScanner Conn	SVM	重大
AVサーバが登録されてい ない	Nblade.vscanNoRegdSca nner	SVM	エラー
応答するAVサーバ接続が ありません	nblade.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	Nblade.vscanConnBackPr essure	SVM	エラー
許可されていないユーザ によるAVサーバへの試行	Nblade.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.space.issues	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	FlexGroupコンスティチュ エントスペースステータ スオールOK	ボリューム	情報
FlexGroupコンスティチュ エントのinodeに問題あり	flexgroup.constituents.hav e.inodes.issues	ボリューム	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
FlexGroupコンスティチュエントのinodeステータスがすべて正常	flexgroup.constituents.inodes.status.all.ok	ボリューム	情報
ボリューム論理スペースがほぼフル	monitor.vol.nearFull.inc.sav	ボリューム	警告
ボリューム論理スペースがフル	monitor.vol.full.inc.sav	ボリューム	エラー
ボリューム論理スペースが正常	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	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イベントへのサブスクライブ

ONTAPソフトウェアがインストールされたシステムで生成されたイベント管理システム (EMS) 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 イベントの名前を表示するには、ONTAP クラスタシェルからコマンド (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 `event route show`。

["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]\* 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。名前が正しく入力されていない場合は、誤ったイベントを削除してから再度追加する必要があります。

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

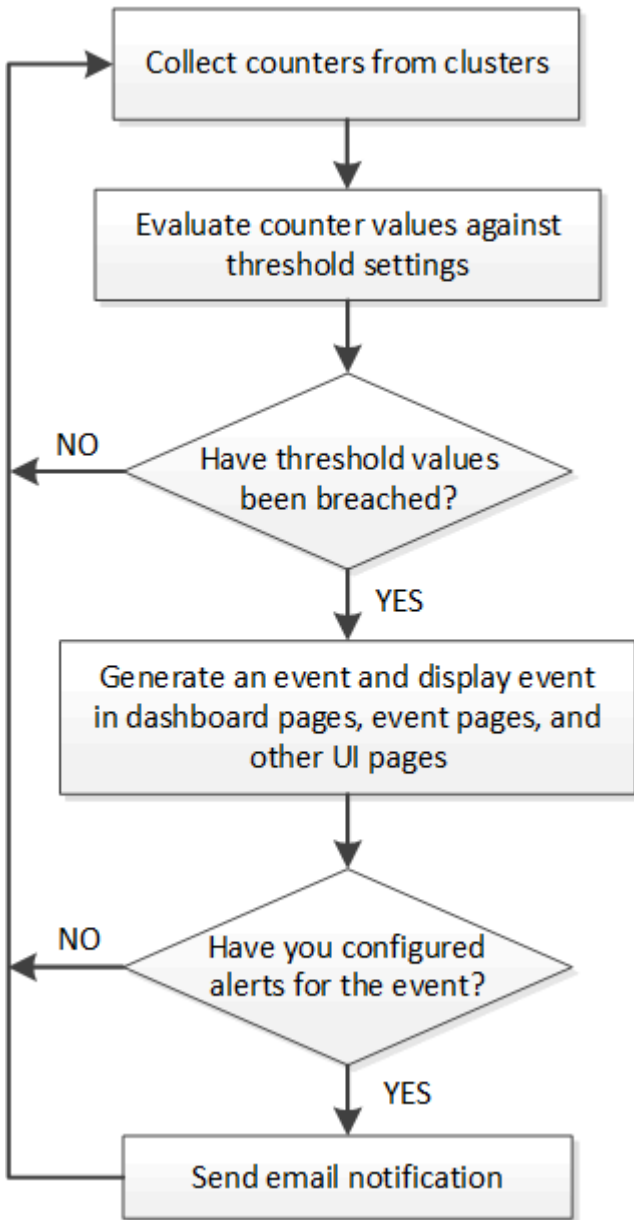
Unified Manager でイベントを受信すると、[ダッシュボード] ページ、[イベント管理] イベントリページ、[クラスタ/パフォーマンス] ページの [サマリ] タブと [エクスプローラ] タブ、およびオブジェクト固有のイベントリページ ([ボリューム/健全性] イベントリページなど) にイベントが表示されます。

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] ページでの設定方法に応じて、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。
- このイベントは、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。
- カスタムスクリプトを実行してアクションを実行できます。

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の表示

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「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。

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]ページにイベントの詳細が表示されます。

## 未割り当てイベントの表示

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、新規イベントと確認済みイベントは[イベント管理]インベントリページに表示されません。

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。

## イベントの確認と解決

イベントを生成した問題への対処を開始する前に、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。

同時に複数のイベント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. イベントリストで、次の操作を実行してイベントに確認応答します。

状況	操作
単一のイベントに確認応答して解決済みとしてマークする	<ol style="list-style-type: none"><li>a. イベント名をクリックします。</li><li>b. [イベントの詳細]ページで、イベントの原因を特定します。</li><li>c. [* Acknowledge (確認) ] をクリックし</li><li>d. 適切な方法で対処します。</li><li>e. [* 解決済みとしてマークする * ] をクリックします。</li></ol>
複数のイベントに確認応答して解決済みとしてマークする	<ol style="list-style-type: none"><li>a. それぞれの[イベントの詳細]ページで、イベントの原因を特定します。</li><li>b. イベントを選択します。</li><li>c. [* Acknowledge (確認) ] をクリックし</li><li>d. 適切な方法で対処します。</li><li>e. [* 解決済みとしてマークする * ] をクリックします。</li></ol>

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。

## 特定のユーザへのイベントの割り当て


未割り当てのイベントを自分自身や他のユーザ（リモートユーザを含む）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は、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 * &gt; * another user* ( * 他のユーザに割り当て) ] をクリックします</p> <p>b. [Assign Owner]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 style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <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>

## 不要なイベントの無効化

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場合は、それらの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が次の監視サイクルから生成されます。

オブジェクト（イベントなど）のイベントを無効にしたあとにそのイベントを有効にした場合、`vol offline` イベントが無効状態のときにオフラインになったオブジェクトについては、Unified Managerで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
イベントを無効にする	<ul style="list-style-type: none"> <li>a. <b>[Disable]</b> をクリックします。</li> <li>b. <b>[Disable Events]</b>ダイアログボックスで、イベントの重大度を選択します。</li> <li>c. <b>[Matching Events]</b>列で、イベントの重大度に基づいて無効にするイベントを選択し、右矢印をクリックして<b>[Disable Events]</b>列に移動します。</li> <li>d. <b>[保存して閉じる]</b> をクリックします。</li> <li>e. 無効にしたイベントが<b>[Event Setup]</b>ページのリストビューに表示されていることを確認します。</li> </ul>
イベントを有効にする	<ul style="list-style-type: none"> <li>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。</li> <li>b. <b>[Enable]</b> をクリックします。</li> </ul>

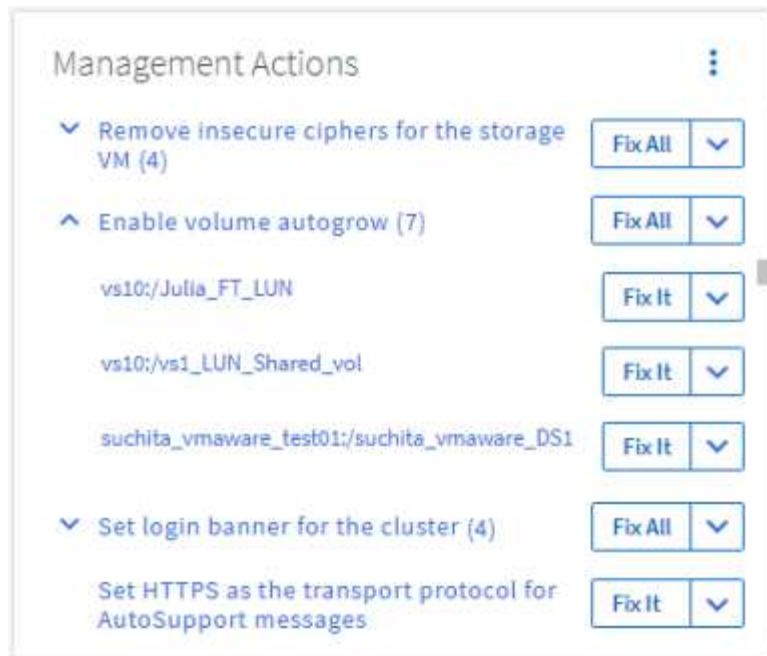
## Unified Managerの自動修復を使用した問題の修正

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、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]に表示されます。

ほとんどのイベントについては、[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を使用して最適なソリューションを実装できます。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の詳細については、を参照してください"[Unified Managerで解決できる問題](#)".

## 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。これらのイベントが「ノイズが多い」場合や Unified Manager で表示したくない場合は、これらのイベントが生成されないようにすることができます。これらの通知の受信を再開する場合は、あとで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、スライダボタンを右に動かします。

## 新しいActive IQルールファイルのアップロード

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、新しいルールが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特定のリリースにアップグレードする場合は、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できます。ただし、更新されたイベントが生成され、ストレージシステムが引き続き最適なパフォーマンスを維持するために、NetAppのサポートサイトから月に1回ほど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ポータルイベントレポートが有効になっている必要があります。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](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サポートサイトに移動し、現在のルールファイルをダウンロードします .zip。

バンドルされたルールパッケージには、ルールリポジトリ、データソース、NetAppの技術情報アークルが含まれています。



Windowsシステムの場合、ネットワークに接続されていないサイトでは、NetAppの技術情報アークルはデフォルトで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]ダイアログボックスで、ダウンロードしたルールファイルに移動して選択し、.zip、\*[アップロード]\*をクリックします。

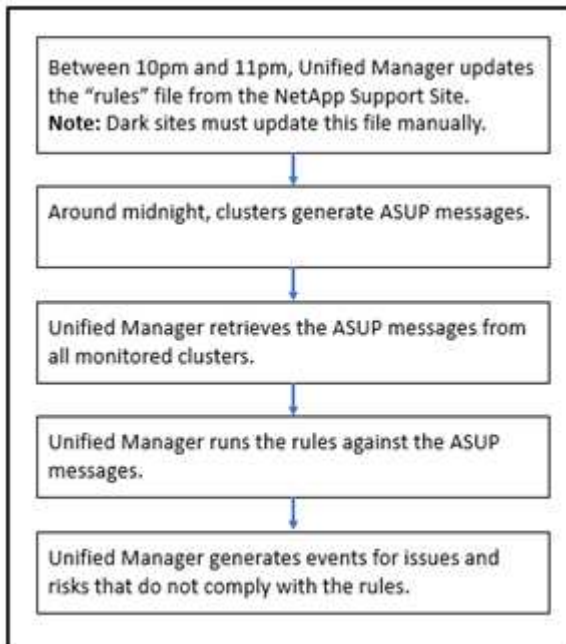
このプロセスには数分かかることがあります。

ルールファイルが Unified Manager サーバに解凍されます。午前0時を過ぎて管理対象クラスタでAutoSupportファイルが生成されると、Unified Managerはルールファイルに照らしてクラスタをチェックし、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、次のナレッジベース (KB) の記事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

次の図に示すように、Active IQプラットフォームのインシデントとリスクがUnified Managerのイベントに変換されます。

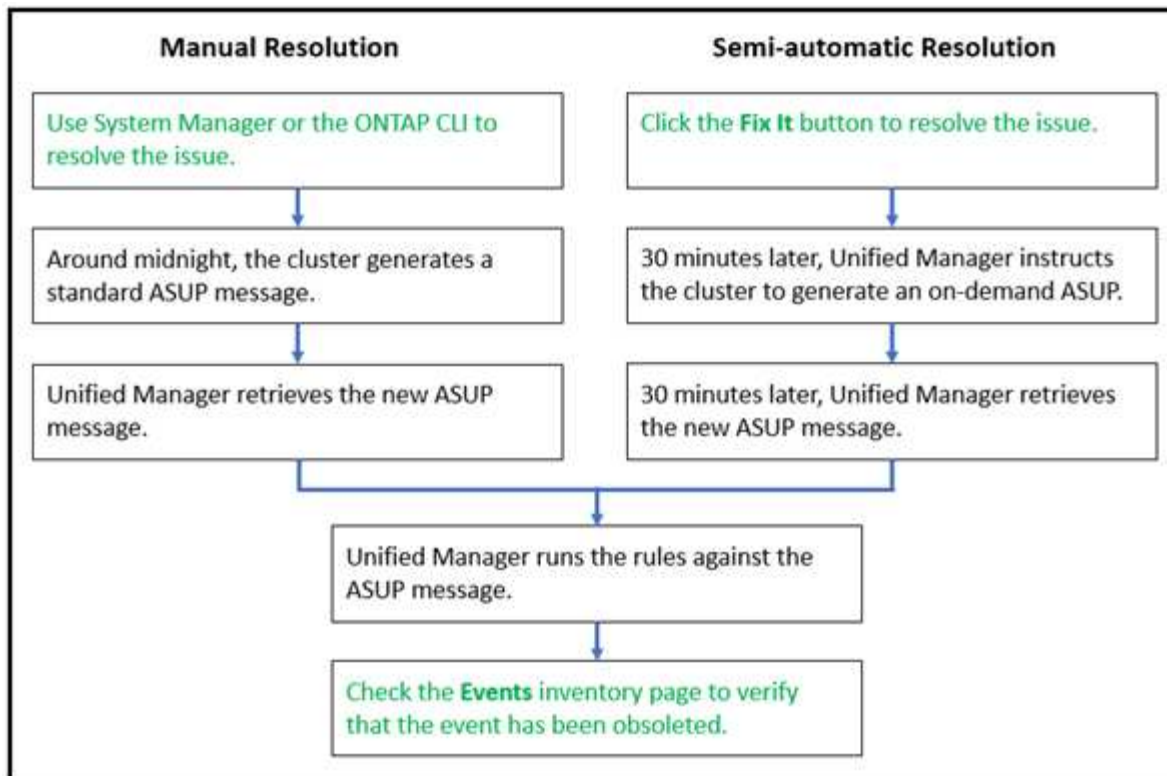


ご覧のように、Active IQプラットフォームでコンパイルされたルールファイルが最新の状態に保たれ、クラスタのAutoSupportメッセージが毎日生成され、Unified Managerはイベントのリストを毎日更新します。

## Active IQプラットフォームイベントの解決

Active IQプラットフォームのインシデントとリスクは、他のUnified Managerイベントと似ています。これらのイベントは解決のために他のユーザに割り当てることができ、使用可能な状態も同じであるためです。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プラットフォームから生成されたイベントの解決時に実行する必要がある操作（緑）とUnified Managerで実行する操作（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。問題を確認できるのは、午前0時にクラスターで新しい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。

## イベント保持の設定

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。

イベントを6か月以上保持するとサーバのパフォーマンスに影響する可能性があるため、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、クラスター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[Event Management] イ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せん。

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] イベントリページでいずれかの[表示]オプションを選択すると、すべてのストレージオブジェクトについてメンテナンス時間中に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タ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の変更またはキャンセル

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。

現在実行中のメンテナンス時間をキャンセルすると、スケジュールされたメンテナンス時間の終了時間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に便利です。

#### 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"><li>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。</li><li>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。</li></ol>
アクティブなメンテナンス時間の延長	<ol style="list-style-type: none"><li>a. スライダボタンの横にあるテキスト「アクティブ」をクリックします。</li><li>b. 終了日時を変更し、 * 適用 * をクリックします。</li></ol>
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。

#### 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。メンテナンス時間が完了し、すべてのシステムリソースが稼働状態に戻ると、ほとんどのイベントは廃止状態になります。

- 必要なもの \*

イベントを利用できるようにするには、少なくとも1つの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、アクティブな（新規および確認済みの）すべてのイベントが[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。

すべてのメンテナンス時間セッションおよびすべてのクラスタから過去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。使用可能なディスクスペースの不足やホストシステムのメモリ不足などの問題で管理ステーションイベントがトリガーされ、UIの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. 管理ステーションの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	操作
イベントの詳細を表示する	イベントバナーをクリックすると、問題の推奨される解決策が記載された[イベントの詳細]ページが表示されます。
すべての管理ステーションイベントを表示する	<ol style="list-style-type: none"><li>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。</li><li>b. [Event Management]インベントリページの[Filters]ペインで、[Source Type]リストの[Management Station]ボックスをクリックします。</li></ol>

## 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こと、クラスタと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するのに役立ちます。

### 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。「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の様子を示しています。

「クラスタに到達できません」イベントがトリガーされると、イベントの状態は「新規」になります。イベントに確認応答すると、イベントの状態が「確認済み」に変わります。適切に対処したら、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。

停電が原因で「クラスタに到達できません」イベントが生成された場合は、電源が復旧すると、管理者の介入なしでクラスタが動作を開始します。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は、イベントの状態が「廃止」または「解決済み」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は、イベントの状態に関する情報が表示されます。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。

#### イベントの重大度タイプの説明

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 \*

イベントソースで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外であり、重大な重大度に達していないことを確認する必要があります。この重大度のイベントではサービスは停止しないため、すぐに対処する必要はありません。

パフォーマンス警告イベントは、ユーザ定義、システム定義、または動的なしきい値から送信されます。

- \* 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が変更された場合は、重大度タイプが「情報」のイベントが生成されます。

情報イベントは、設定の変更を検出すると、ONTAPから直接送信されます。

## イベントの影響レベルの説明

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ためのスペース不足を引き起こす可能性のあ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 \*

リスクとは、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引き起こす可能性のある一連のイベントのことです。影響レベルが「リスク」のイベントはサービスの停止を引き起こす可能性があります。対処が必要な場合があります。

- \* イベント \*

イベントとは、ストレージオブジェクトとその属性の状態またはステータスの変化です。影響レベルが「イベント」のイベントは情報提供のイベントであり、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特定します。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。

## イベントの影響範囲の説明

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、セキュリティ）に分類され、担当するイベントのタイプに集中できます。

- \* 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で問題が発生した場合、またはハードウェアで問題が発生し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は異な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、削除、または名前変更を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でのデータストレージの入力速度や読み出し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、またはアクティビティの状態について通知するイベントです。

- \* 保護 \*

保護イベントは、SnapMirror関係に関連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、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)、およびボリュームがどの程度セキュアであるかを通知します "[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せん。

## オブジェクトステータスの計算方法

オブジェクトのステータスは、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になっています。対処方法が実施されると、イベントの状態は解決済みになります。

## 動的なパフォーマンスイベントグラフの詳細

動的なパフォーマンスイベントについては、[イベントの詳細]ページの[システム診断]セクションに、レイテンシが高いワークロードまたは競合状態のクラスタコンポーネントの使用量が多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、競合状態にある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が解消され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日時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）の場合は、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発生したイベントの分析](#)"。

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](#)"。

グラフのデータには、イベントが最後に分析される24時間前のパフォーマンス統計が表示されます。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間に基づいています。たとえば、イベント検出後にワークロードがイベントに関連するようになった場合、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。赤いバーは、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を示します。詳細については、を参照してください "[ワークロード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、ネットワークパフォーマンス統計はクラスタ外のアクティビティに基づくため、この列は表示されません。

##### ◦ \* コンポーネント使用率 \*

ネットワーク処理、Data Processing、およびアグリゲートコンポーネントの利用率の履歴（パーセント）、またはQoSポリシーグループコンポーネントのアクティビティの履歴（パーセント）が表示されます。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リソースコンポーネントの場合のみ、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、合計書き込みスループットが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および解決後に発生したイベントがグラフに表示されません。

## Unified Managerで検出される構成の変更

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。[Performance Explorer]ページに変更イベントアイコン ( ) が表示され、変更が検出された日時が示されます。

[パフォーマンスエクスプローラ]ページと[ワークロード分析]ページのパフォーマンスグラフで、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とほぼ同じ時間に変更が検出された場合は、変更が原因でイベント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場合。

ポリシーグループ制限を変更するとレイテンシ（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別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グループ化され、イベントとトラップの名前、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 (ocumEvtAggregateStateOffline)	インシデント	アグリゲート	重大
アグリゲートで障害が発生しました (ocumEvtAggregateStateFailed)	インシデント	アグリゲート	重大
Aggregate Restricted (ocumEvtAggregateStateRestricted)	リスク	アグリゲート	警告
アグリゲートの再構築 (ocumEvtAggregateRaidStateReconstructing)	リスク	アグリゲート	警告
アグリゲートがデグレード状態 (ocumEvtAggregateRaidStateDegraded)	リスク	アグリゲート	警告
クラウド階層に一部到達可能 (ocumEventCloudTierPartiallyReachable)	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
クラウド階層に到達不能 (ocumEventCloudTierUnreachable)	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で残ったアグリゲート (ocumEvtMetroClusterAggregateLeftBehind)	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 (ocumEvtMetroClusterAggregateMirrorDegraded)	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 (ocumEvtAggregateNearlyFull)	リスク	アグリゲート	警告
アグリゲートスペースがフル (ocumEvtAggregateFull)	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 (ocumEvtAggregateDaysUntilFullSoon)	リスク	アグリゲート	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
アグリゲートがオーバーコミット (ocumEvtAggregateOvercommitted)	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 (ocumEvtAggregateAlmostOvercommitted)	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 (ocumEvtAggregateSnapshotReserveFull)	リスク	アグリゲート	警告
アグリゲートの増加率が異常 (ocumEvtAggregateGrowthRateAbnormal)	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
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 (ocumAggregateIopsIncident)	インシデント	アグリゲート	重大

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の警告しきい値を超過 (ocumAggregateIopsWarning)	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 (ocumAggregateMbpsIncident)	インシデント	アグリゲート	重大
アグリゲートMBpsの警告しきい値を超過 (ocumAggregateMbpsWarning)	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 (ocumAggregateLatencyIncident)	インシデント	アグリゲート	重大
アグリゲートレイテンシの警告しきい値を超過 (ocumAggregateLatencyWarning)	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 (ocumAggregatePerfCapacityUsedIncident)	インシデント	アグリゲート	重大
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 (ocumAggregatePerfCapacityUsedWarning)	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 (ocumAggregateUtilizationIncident)	インシデント	アグリゲート	重大
アグリゲート利用率の警告しきい値を超過 (ocumAggregateUtilizationWarning)	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
利用率の高いアグリゲートディスクのしきい値を超過 (ocumAggregateDisksOverUtilizedWarning)	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 (ocumAggregateDynamicEventWarning)	リスク	アグリゲート	警告

### クラスタイベント

クラスタイベントは、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グループ化され、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がありません (ocumEvtDisksNoSpares)	リスク	クラスタ	警告
クラスタに到達できません (ocumEvtClusterUnreachable)	リスク	クラスタ	エラー
クラスタの監視に失敗しました (ocumEvtClusterMonitoringFailed)	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 (ocumEvtExternalCapacityTierSpaceFull)	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
NVME の猶予期間 - 開始 * ( nvmetfGracePeriodStart )	リスク	クラスタ	警告
NVME の猶予期間 - アク ティブ * ( nvmetfGracePeriodActive )	リスク	クラスタ	警告
NVME の猶予期間 - 終了 * ( nvmetfGracePeriodExpire d)	リスク	クラスタ	警告
オブジェクトのメンテナ ンス時間を開始 (objectMaintenanceWind owStarted)	イベント	クラスタ	重大
オブジェクトのメンテナ ンス時間を終了 (objectMaintenanceWind owEnded)	イベント	クラスタ	情報
MetroCluster残ったスペ アディスク (ocumEvtSpareDiskLeft Behind)	リスク	クラスタ	エラー
MetroCluster自動計画外 スイッチオーバーが無効 (ocumEvtMccAutomatic UnplannedSwitchOverDis abled)	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 (ocumConformanceNodeImbalanceWarning)	リスク	クラスタ	警告
クラスタのクラウド階層の計画 (clusterCloudTierPlanningWarning)	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
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
クラスタの削除 (該当なし)	イベント	クラスタ	情報
クラスタ追加失敗 (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	重大
重大な EMS を受信 (該当なし)	イベント	クラスタ	重大

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
重大	緊急 重大
エラー	アラート
警告	エラー 警告 デバッグ 通知 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 (ocumClusterIopsIncident)	インシデント	クラスタ	重大
クラスタIOPSの警告しきい値を超過 (ocumClusterIopsWarning)	リスク	クラスタ	警告
クラスタMBpsの重大しきい値を超過 (ocumClusterMbpsIncident)	インシデント	クラスタ	重大
クラスタMBpsの警告しきい値を超過 (ocumClusterMbpsWarning)	リスク	クラスタ	警告
クラスタ動的しきい値を超過 (ocumClusterDynamicEventWarning)	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 (ocumClusterASUPHttpsConfiguredDisabled)	リスク	クラスタ	警告
ログ転送が暗号化されていない (ocumClusterAuditLogUnencrypted)	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
デフォルトのローカル管理ユーザが有効 (ocumClusterDefaultAdminEnabled)	リスク	クラスタ	警告
FIPSモードが無効 (ocumClusterFipsDisabled)	リスク	クラスタ	警告
ログインバナーが無効 (ocumClusterLoginBannerDisabled)	リスク	クラスタ	警告
ログインバナーが変更されました (ocumClusterLoginBannerChanged)	リスク	クラスタ	警告
ログ転送先が変更されました (ocumLogForwardDestinationsChanged)	リスク	クラスタ	警告
NTPサーバ名が変更されました (ocumNtpServerNamesChanged)	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
クラスタピア通信が暗号化されていません (ocumClusterPeerEncryptionDisabled)	リスク	クラスタ	警告
SSHでセキュアでない暗号が使用されている (ocumClusterSSHInsecure)	リスク	クラスタ	警告
Telnetプロトコルが有効 (ocumClusterTelnetEnabled)	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
一部のONTAPユーザアカウントのパスワードでは、安全性の低いMD5ハッシュ関数を使用する (ocumClusterMD5PasswordHashUsed)	リスク	クラスタ	警告
クラスタで自己署名証明書が使用される (ocumClusterSelfSignedCertificate)	リスク	クラスタ	警告
クラスタリモートシェルが有効 (ocumClusterRshDisabled)	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 (ocumEvtClusterCertificateAboutToExpire)	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 (ocumEvtClusterCertificateExpired)	リスク	クラスタ	エラー

#### ディスクノイヘント

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グループ化され、イベントとトラップの名前、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-ほぼ使用済みのスペアブロック (ocumEvtClusterFlashDiskFewerSpareBlockError)	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
フラッシュディスク-スペアブロックなし (ocumEvtClusterFlashDiskNoSpareBlockCritical)	インシデント	クラスタ	重大
一部の未割り当てディスク (ocumEvtClusterUnassignedDisksSome)	リスク	クラスタ	警告
障害ディスクあり (ocumEvtDisksSomeFailed)	インシデント	クラスタ	重大

#### エンクロージャイベント

エンクロージャイベントは、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グループ化され、イベントとトラップの名前、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障害 (ocumEvtShelfFanFailed)	インシデント	ストレージシェルフ	重大
ディスクシェルフの電源装置で障害が発生しました (ocumEvtShelfPowerSupplyFailed)	インシデント	ストレージシェルフ	重大

イベント名 (トラップ名)	影響レベル	ソースタイプ	重大度
ディスクシェルフマルチパス未設定 (ocumDiskShelfConnectivityNotInMultiPath)  このイベントは次の場合には適用されません。  <ul style="list-style-type: none"> <li>• MetroCluster構成のクラスタ</li> <li>• FAS2554、FAS2552、FAS2520、およびFAS2240のプラットフォーム</li> </ul>	リスク	ノード	警告
ディスクシェルフパス障害 (ocumDiskShelfConnectivityPathFailure)	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
検出されたディスクシェルフ (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

#### ファンイベント

ファンイベントは、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グループ化され、イベントとトラップの名前、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 (ocumEvtFansOneOrMoreFailed)	インシデント	ノード	重大

#### フラッシュカードイベント

フラッシュカードイベントは、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グループ化され、イベントとトラップの名前、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
Flashカードがオフライン (ocumEvtFlashCardOffline)	インシデント	ノード	重大

#### 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ときの情報を提供します。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グループ化され、イベントとトラップの名前、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 (ocumEvtInodesAlmostFull)	リスク	ボリューム	警告
inodeがフル (ocumEvtInodesFull)	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グループ化され、イベントとトラップの名前、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 (ocumEvtLifStatusDown)	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-停止 (ocumEvtFCLifStatusDown)	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イルオーバーが実行できない (ocumEvtLifFailoverNotPossible)	リスク	インターフェイス	警告
ネットワークインターフェイスがホームポートにない (ocumEvtLifNotAtHomePort)	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の重大しきい値を超過 (ocumNetworkLifMbpsIncident)	インシデント	インターフェイス	重大
ネットワークインターフェイスMBpsの警告しきい値を超過 (ocumNetworkLifMbpsWarning)	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の重大しきい値を超過 (ocumFCpLifMbpsIncident)	インシデント	インターフェイス	重大
FCネットワークインターフェイスMBpsの警告しきい値を超過 (ocumFCpLifMbpsWarning)	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の重大しきい値を超過 (ocumNvmfFCLifMbpsIncident)	インシデント	インターフェイス	重大
NVMf FCネットワークインターフェイスMBpsの警告しきい値を超過 (ocumNvmfFCLifMbpsWarning)	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グループ化され、イベントとトラップの名前、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はオフライン (ocumEvtLunOffline)	インシデント	LUN	重大
LUN を破棄* ( lunDestroy )	イベント	LUN	情報
igroupでサポート対象外のオペレーティングシステムにLUNがマッピングされている (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単一パス (ocumEvtLunSingleActivePath)	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ない (ocumEvtLunNotReachable)	インシデント	LUN	重大
LUNにアクセスするための最適パスがない (ocumEvtLunOptimizedPathInactive)	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ありません (ocumEvtLunHaPathInactive)	リスク	LUN	警告
HAペアの一方のノードからLUNにアクセスするためのパスがない (ocumEvtLunNodePathStatusDown)	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 (ocumEvtLunSnapshotNotPossible)	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でサポート対象外のオペレーティングシステムにLUNがマッピングされている (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 (ocumLunIopsIncident)	インシデント	LUN	重大
LUN IOPSの警告しきい値を超過 (ocumLunIopsWarning)	リスク	LUN	警告
LUN MBpsの重大しきい値を超過 (ocumLunMbpsIncident)	インシデント	LUN	重大
LUN MBpsの警告しきい値を超過 (ocumLunMbpsWarning)	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 (ocumLunLatencyIncident)	インシデント	LUN	重大



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（ミリ秒/処理）の警告しきい値を超過 (ocumLunLatencyWarning)	リスク	LUN	警告
LUNレイテンシ/LUN IOPSの重大しきい値を超過 (ocumLunLatencyIopsIncident)	インシデント	LUN	重大
LUNレイテンシ/LUN IOPSの警告しきい値を超過 (ocumLunLatencyIopsWarning)	リスク	LUN	警告
LUNレイテンシ/LUN MBpsの重大しきい値を超過 (ocumLunLatencyMbpsIncident)	インシデント	LUN	重大
LUNレイテンシ/LUN MBpsの警告しきい値を超過 (ocumLunLatencyMbpsWarning)	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 (ocumLunLatencyAggregatePerfCapacityUsedIncident)	インシデント	LUN	重大
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 (ocumLunLatencyAggregatePerfCapacityUsedWarning)	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
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 (ocumLunLatencyAggregateUtilizationIncident)	インシデント	LUN	重大
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 (ocumLunLatencyAggregateUtilizationWarning)	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の重大しきい値を超過 (ocumLunLatencyNodePerfCapacityUsedIncident)	インシデント	LUN	重大
LUNレイテンシ/ノード使用済みパフォーマンス容量の警告しきい値を超過 (ocumLunLatencyNodePerfCapacityUsedWarning)	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-テイクオーバーの重大しきい値を超過 (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	インシデント	LUN	重大
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 (ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	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 (ocumLunLatencyNodeUtilizationIncident)	インシデント	LUN	重大

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/ノード利用率の警告しきい値を超過 (ocumLunLatencyNodeUtilizationWarning)	リスク	LUN	警告
QoS LUN最大IOPSの警告しきい値を超過 (ocumQosLunMaxIopsWarning)	リスク	LUN	警告
QoS LUN最大MBpsの警告しきい値を超過 (ocumQosLunMaxMbpsWarning)	リスク	LUN	警告
パフォーマンスサービスレベルポリシー (ocumConformanceLatencyWarning) 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	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グループ化され、イベントとトラップの名前、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 (ocumEvtUnifiedManagerDiskSpaceNearlyFull)	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 (ocumEvtUnifiedManagerDiskSpaceFull)	インシデント	管理ステーション	重大

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
管理サーバのメモリが減少 (ocumEvtUnifiedManagerMemoryLow)	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ありません (ocumEvtUnifiedManagerMemoryAlmostOut)	インシデント	管理ステーション	重大
MySQLログファイルのサイズが拡張されました。 再起動が必要です (ocumEvtMysqlLogFileSizeModeWarning)	インシデント	管理ステーション	警告
監査ログの合計サイズ割り当てがフルになりそうです	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
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 (ocumEvtUnifiedManagerDataMissingAnalyze)	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 (ocumEvtUnifiedManagerDataMissingCollection)	インシデント	管理ステーション	重大



最後の2つのパフォーマンスイベントは、Unified Manager 7.2でのみ使用できました。これらのイベントのいずれかが「新規」状態である場合、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ージされません。イベントを解決済みの状態に手動で移動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グループ化され、イベントとトラップの名前、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
Bridge Unreachable (ocumEvtBridgeUnreachable)	インシデント	MetroClusterブリッジ	重大
ブリッジの温度が異常 (ocumEvtBridgeTemperatureAbnormal)	インシデント	MetroClusterブリッジ	重大

### 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構成および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グループ化され、イベントとトラップの名前、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構成のどちらでも共通です。

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 (ocumEvtMetroClusterAllLinksBetweenPartnersDown)	インシデント	MetroCluster関係	重大
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 (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	インシデント	MetroCluster関係	重大
MetroClusterディザスタリカバリ機能への影響 (ocumEvtMetroClusterDRStatusImpacted)	リスク	MetroCluster関係	重大
スイッチオーバーされたMetroCluster構成 (ocumEvtMetroClusterDRStatusImpacted)	リスク	MetroCluster関係	警告

#### MetroCluster over FC構成

次のイベントは、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 (ocumEvtMetroClusterAllISLBetweenSwitchesDown)	インシデント	MetroClusterスイッチ間接続	重大
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 (ocumEvtBridgeSasPortDown)	インシデント	MetroClusterブリッジスタック接続	重大

イベント名 (トラップ名)	影響レベル	ソースタイプ	重大度
部分的にスイッチオーバーされたMetroCluster構成 (ocumEvtMetroClusterDRStatusPartiallyImpacted)	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 (ocumEvtMccNodeSwitchFcviLinksDown)	インシデント	MetroClusterノードのスイッチ接続	重大
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 (ocumEvtMccNodeSwitchFCLinksOneOrMoreDown)	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 (ocumEvtMccNodeSwitchFCLinksDown)	インシデント	MetroClusterノードのスイッチ接続	重大
スイッチからFC-SASブリッジへのFCリンクが停止 (ocumEvtMccSwitchBridgeFCLinksDown)	インシデント	MetroClusterスイッチのブリッジ接続	重大
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 (ocumEvtMccInterNodeLinksDown)	インシデント	ノード間の接続	重大
ノード間の1つ以上のFC VIインターコネクトリンクが停止 (ocumEvtMccInterNodeLinksOneOrMoreDown)	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 (ocumEvtMccNodeBridgeLinksDown)	インシデント	ノードのブリッジ接続	重大

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
ノードからストレージスタックへのすべてのSASリンクが停止 (ocumEvtMccNodeStackLinksDown)	インシデント	ノードのスタック接続	重大
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 (ocumEvtMccNodeStackLinksOneOrMoreDown)	リスク	ノードのスタック接続	警告

### MetroCluster over IP構成

これらのイベントは、MetroCluster over IP構成に関連します。

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down (mccIntersiteconnectivityStatusDown)	リスク	MetroCluster関係	重大
MetroCluster - IPノードからスイッチへの接続がオフライン (mccIpPortStatusOffline)	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グループ化され、イベントとトラップの名前、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 (ocumEvtSwitchTemperatureAbnormal)	インシデント	MetroClusterスイッチ	重大
スイッチに到達不能 (ocumEvtSwitchUnreachable)	インシデント	MetroClusterスイッチ	重大
スイッチのファンに障害が発生しました (ocumEvtSwitchFansOneOrMoreFailed)	インシデント	MetroClusterスイッチ	重大
スイッチの電源装置で障害が発生しました (ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	インシデント	MetroClusterスイッチ	重大
スイッチの温度センサーで障害が発生しました (ocumEvtSwitchTemperatureSensorFailed)	インシデント	MetroClusterスイッチ	重大



このイベントはCiscoスイッチにのみ該当します。

### 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グループ化され、イベントとトラップの名前、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

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 オンライン * (nvmeNamespaceOnline)	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 * (nvmeNamespaceDestroy)	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 (ocumNvmeNamespaceIopsIncident)	インシデント	ネームスペース	重大
NVMeネームスペースIOPSの警告しきい値を超過 (ocumNvmeNamespaceIopsWarning)	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 (ocumNvmeNamespaceMbpsIncident)	インシデント	ネームスペース	重大
NVMeネームスペースMBpsの警告しきい値を超過 (ocumNvmeNamespaceMbpsWarning)	リスク	ネームスペース	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
NVMeネームスペースレイテンシ (ミリ秒/処理)の重大しきい値を超過 (ocumNvmeNamespaceLatencyIncident)	インシデント	ネームスペース	重大
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 (ocumNvmeNamespaceLatencyWarning)	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 (ocumNvmeNamespaceLatencyIopsIncident)	インシデント	ネームスペース	重大
NVMeネームスペースレイテンシ/ IOPSの警告しきい値を超過 (ocumNvmeNamespaceLatencyIopsWarning)	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 (ocumNvmeNamespaceLatencyMbpsIncident)	インシデント	ネームスペース	重大
NVMeネームスペースレイテンシ/ MBpsの警告しきい値を超過 (ocumNvmeNamespaceLatencyMbpsWarning)	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グループ化され、イベントとトラップの名前、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。

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 (ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	リスク	ノード	警告
Cloud AWS MetaDataConnFail * (Document CloudAwsMetadataConnFail)	リスク	ノード	エラー
Cloud AWS IAM クレデンシャルが期限切れ * (Document CloudAwslamCredsExpired)	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 CloudAwslamCredsNotFound)	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

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 RoleNotFound * (ドキュメント CloudAwslamRoleNotFou nd)	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間ネットワークインターフェイスが停止* (ocumObjstoreInterClusterLifDown)	リスク	ノード	エラー
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	重大
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の重大しきい値を超過 (ocumNodelopsIncident)	インシデント	ノード	重大
ノードIOPSの警告しきい値を超過 (ocumNodelopsWarning)	リスク	ノード	警告
ノードMBpsの重大しきい値を超過 (ocumNodeMbpsIncident)	インシデント	ノード	重大
ノードMBpsの警告しきい値を超過 (ocumNodeMbpsWarning)	リスク	ノード	警告
ノードレイテンシ（ミリ秒/処理）の重大しきい値を超過 (ocumNodeLatencyIncident)	インシデント	ノード	重大
ノードレイテンシ（ミリ秒/処理）の警告しきい値を超過 (ocumNodeLatencyWarning)	リスク	ノード	警告
ノード使用済みパフォーマンス容量の重大しきい値を超過 (ocumNodePerfCapacityUsedIncident)	インシデント	ノード	重大

イベント名 (トラップ名)	影響レベル	ソースタイプ	重大度
ノード使用済みパフォーマンス容量の警告しきい値を超過 (ocumNodePerfCapacityUsedWarning)	リスク	ノード	警告
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 (ocumNodePerfCapacityUsedTakeoverIncident)	インシデント	ノード	重大
ノード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 (ocumNodePerfCapacityUsedTakeoverWarning)	リスク	ノード	警告
ノード利用率の重大しきい値を超過 (ocumNodeUtilizationIncident)	インシデント	ノード	重大
ノード利用率の警告しきい値を超過 (ocumNodeUtilizationWarning)	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 (ocumNodeHaPairOverUtilizedInformation)	イベント	ノード	情報
ノードディスク断片化のしきい値を超過 (ocumNodeDiskFragmentationWarning)	リスク	ノード	警告
使用済みパフォーマンス容量しきい値を超過 (ocumNodeOverUtilizedWarning)	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
ノード動的しきい値を超過 (ocumNodeDynamicEventWarning)	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	重大

### NVRAMバッテリーイベント

NVRAMバッテリーイベントは、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グループ化され、イベントとトラップの名前、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バッテリー残量低下 (ocumEvtNvramBatteryLow)	リスク	ノード	警告
NVRAMバッテリー放電 (ocumEvtNvramBatteryDischarged)	リスク	ノード	エラー
NVRAMバッテリー過充電 (ocumEvtNvramBatteryOverCharged)	インシデント	ノード	重大

### ポートイベント

ポートイベントは、クラスタポートのステータスを提供します。これにより、ポートでの変更や問題（ポートが停止しているかどうかなど）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 (ocumEvtPortStatusDown)	インシデント	ノード	重大

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 (ocumNetworkPortMbpsIncident)	インシデント	ポート	重大
ネットワークポートMBpsの警告しきい値を超過 (ocumNetworkPortMbpsWarning)	リスク	ポート	警告
FCPポートMBpsの重大しきい値を超過 (ocumFcpPortMbpsIncident)	インシデント	ポート	重大
FCPポートMBpsの警告しきい値を超過 (ocumFcpPortMbpsWarning)	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 (ocumNetworkPortUtilizationIncident)	インシデント	ポート	重大
ネットワークポート利用率の警告しきい値を超過 (ocumNetworkPortUtilizationWarning)	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 (ocumFCpPortUtilizationIncident)	インシデント	ポート	重大

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ポート利用率の警告 しきい値を超過 (ocumFCpPortUtilization Warning)	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グループ化され、イベントとトラップの名前、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 (ocumEvtPowerSupplyO neOrMoreFailed)	インシデント	ノード	重大

#### 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グループ化され、イベントとトラップの名前、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 (ocumEvtProtectionJobT askFailed)	インシデント	ボリュームまたはストレ ージサービス	重大
保護ジョブの中止 (ocumEvtProtectionJobA borted)	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の容量とファイルおよび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グループ化さ

れ、イベントとトラップの名前、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 (ocumEvtQtreeSpaceNearlyFull)	リスク	qtree	警告
qtreeスペースがフル (ocumEvtQtreeSpaceFull)	リスク	qtree	エラー
qtreeスペースが正常 (ocumEvtQtreeSpaceThresholdOk)	イベント	qtree	情報
qtreeのファイル数がハードリミットに達しました (ocumEvtQtreeFilesHardLimitReached)	インシデント	qtree	重大
qtreeのファイル数がソフトリミットを超過 (ocumEvtQtreeFilesSoftLimitBreached)	リスク	qtree	警告
qtreeのスペースがハードリミットに達しました (ocumEvtQtreeSpaceHardLimitReached)	インシデント	qtree	重大
qtreeのスペースがソフトリミットを超過 (ocumEvtQtreeSpaceSoftLimitBreached)	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グループ化され、イベントとトラップの名前、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 (ocumEvtServiceProcessorNotConfigured)	リスク	ノード	警告
サービスプロセッサはオフライン (ocumEvtServiceProcessorOffline)	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ディザスタリカバリ関係の一部であるコンスティ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グループ化され、イベントとトラップの名前、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関係イベントは、Storage VMディザスタリカバリで保護されているStorage VMに対して生成されますが、コンスティチュエントオブジェクト関係に対し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 (ocumEvtSnapmirrorRelationshipUnhealthy)	リスク	SnapMirror関係	警告
ミラーレプリケーションを切断 (ocumEvtSnapmirrorRelationshipStateBrokenoff)	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初期化失敗 (ocumEvtSnapmirrorRelationshipInitializeFailed)	リスク	SnapMirror関係	エラー
ミラーレプリケーションの更新失敗 (ocumEvtSnapmirrorRelationshipUpdateFailed)	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 (ocumEvtSnapMirrorRelationshipLagError)	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 (ocumEvtSnapMirrorRelationshipLagWarning)	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 (ocumEvtSnapmirrorRelationshipResyncFailed)	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
クラスタにONTAPメディアエーターが追加されている (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メディアーターをクラスタから削除 (snapmirrorMediatorRemoved)	イベント	クラスタ	情報
クラスタからONTAPメディアーターに到達できません (snapmirrorMediatorUnreachable)	リスク	メディアーター	警告
クラスタからONTAPメディアーターにアクセスできない (snapmirrorMediatorMisconfigured)	リスク	メディアーター	エラー
ONTAPメディアーターの接続が再確立され、再同期されてアクティブなSnapMirror同期の準備が完了しました (snapmirrorMediatorInQuorum)	イベント	メディアーター	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および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グループ化され、イベントとトラップの名前、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



SnapMirror関係イベントとバックアップ関係イベントは、Storage VMディザスタリカバリで保護されているが、コンスティチュエントオブジェクト関係に対しては生成されないStorage VMについても生成されます。

イベント名（トラップ名）	影響レベル	ソースタイプ	重大度
非同期ミラーバックアップは正常でない (ocumEvtMirrorVaultRelationshipUnhealthy)	リスク	SnapMirror関係	警告
非同期ミラーバックアップを切断 (ocumEvtMirrorVaultRelationshipStateBrokenoff)	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 (ocumEvtMirrorVaultRelationshipInitializeFailed)	リスク	SnapMirror関係	エラー
非同期ミラーバックアップの更新失敗 (ocumEvtMirrorVaultRelationshipUpdateFailed)	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 (ocumEvtMirrorVaultRelationshipLagError)	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 (ocumEvtMirrorVaultRelationshipLagWarning)	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 (ocumEvtMirrorVaultRelationshipResyncFailed)	リスク	SnapMirror関係	エラー



「SnapMirror update failure」 イベントがActive IQ portal（Config Advisor）によって生成されません。

## 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グループ化され、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の自動削除設定が変更されました（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グループ化され、イベントとトラップの名前、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 (ocumEvtSnapVaultRelationshipUnhealthy)	リスク	SnapMirror関係	警告
非同期バックアップを切断 (ocumEvtSnapVaultRelationshipStateBrokenoff)	リスク	SnapMirror関係	エラー
非同期バックアップの初期化失敗 (ocumEvtSnapVaultRelationshipInitializeFailed)	リスク	SnapMirror関係	エラー
非同期バックアップの更新失敗 (ocumEvtSnapVaultRelationshipUpdateFailed)	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遅延エラー (ocumEvtSnapVaultRelationshipLagError)	リスク	SnapMirror関係	エラー
非同期バックアップの遅延警告 (ocumEvtSnapVaultRelationshipLagWarning)	リスク	SnapMirror関係	警告
非同期バックアップの再同期失敗 (ocumEvtSnapvaultRelationshipResyncFailed)	リスク	SnapMirror関係	エラー

#### ストレージフェイルオーバー設定イベント

ストレージフェイルオーバー（SFO）の設定イベントは、ストレージフェイルオーバーが無効になっているかどうか、または設定されていないかどう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グループ化され、イベントとトラップの名前、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しています (ocumEvtSfoInterconnectOneOrMoreLinksDown)	リスク	ノード	警告
ストレージフェイルオーバーが無効 (ocumEvtSfoSettingsDisabled)	リスク	ノード	エラー
ストレージフェイルオーバーが設定されていません (ocumEvtSfoSettingsNotConfigured)	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の状態-テイクオーバー (ocumEvtSfoStateTakeover)	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 (ocumEvtSfoStatePartialGiveback)	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-停止 (ocumEvtSfoNodeStatusDown)	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ない (ocumEvtSfoTakeoverNotPossible)	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グループ化され、イベントとトラップの名前、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が作成されました（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サブスクライブ済み（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がアンサブスクライブされました（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EvtStorageServiceUnsupportedRelationshipDeletion	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（ocumEvtStorageServiceUnexpectedVolumeDeletion）	インシデント	ストレージサービス	重大

#### 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に異常が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グループ化され、イベントとトラップの名前、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（ocumEvtShelfVoltageAbnormal）	リスク	ストレージシェルフ	警告
異常な電流範囲（ocumEvtShelfCurrentAbnormal）	リスク	ストレージシェルフ	警告
異常な温度（ocumEvtShelfTemperatureAbnormal）	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、略称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グループ化され、イベントとトラップの名前、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
Storage VM CIFS サービス停止 (ocumEvtVserverCifsServiceStatusDown)	インシデント	SVM	重大
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	重大
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
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

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 FC / FCoEサービス停止 (ocumEvtVserverFCServiceStatusDown)	インシデント	SVM	重大
SVM iSCSIサービス停止 (ocumEvtVserverIscsiServiceStatusDown)	インシデント	SVM	重大
Storage VM NFSサービス停止 (ocumEvtVserverNfsServiceStatusDown)	インシデント	SVM	重大
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
Storage VM停止 (ocumEvtVserverDown)	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
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	重大
AV サーバが登録されていません*（ nbladeVscanNoRegdScanner）	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
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*（ nbladeVscanBadUserPriv Access）	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の名前を変更（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 （ocumSvmlopsIncident）	インシデント	SVM	重大
SVM IOPSの警告しきい値を超過 （ocumSvmlopsWarning）	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
SVM MBpsの重大しきい値を超過 (ocumSvmMbpsIncident)	インシデント	SVM	重大
SVM MBpsの警告しきい値を超過 (ocumSvmMbpsWarning)	リスク	SVM	警告
SVMレイテンシの重大しきい値を超過 (ocumSvmLatencyIncident)	インシデント	SVM	重大
SVMレイテンシの警告しきい値を超過 (ocumSvmLatencyWarning)	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
監査ログが無効 (ocumVserverAuditLogDisabled)	リスク	SVM	警告
ログインバナーが無効 (ocumVserverLoginBannerDisabled)	リスク	SVM	警告
SSHでセキュアでない暗号が使用されている (ocumVserverSSHInsecure)	リスク	SVM	警告
ログインバナーが変更されました (ocumVserverLoginBannerChanged)	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
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
ランサムウェア対策の監視に適したStorage VM（ラーニングモード）（ocumEvtSvmArwCandidate）	イベント	SVM	情報

#### ユーザクォータおよびグループクォータイベント

ユーザクォータとグループクォータのイベントは、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グループ化され、イベントとトラップの名前、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（ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached）	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ディスクスペースがハードリミットに達しました（ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached）	インシデント	ユーザクォータまたはグループクォータ	重大



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ファイル数がソフトリミットを超過 (ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	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達しました (ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	インシデント	ユーザクォータまたはグループクォータ	重大

#### 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グループ化され、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
ボリュームは制限状態 (ocumEvtVolumeRestricted)	リスク	ボリューム	警告
ボリュームはオフライン (ocumEvtVolumeOffline)	インシデント	ボリューム	重大
ボリュームは一部使用可能 (ocumEvtVolumePartiallyAvailable)	リスク	ボリューム	エラー
ボリュームをアンマウント（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 (ocumEvtVolumeJunctionPathInactive)	リスク	ボリューム	警告
ボリュームのオートサイズが有効 (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のスペースにリスクあり (ocumThinProvisionVolumeSpaceAtRisk)	リスク	ボリューム	警告
ボリューム効率化処理エラー (ocumEvtVolumeEfficiencyOperationError)	リスク	ボリューム	エラー
ボリュームスペースがフル (ocumEvtVolumeFull)	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
ボリュームスペースがほぼフル (ocumEvtVolumeNearlyFull)	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 (ocumEvtSnapshotFull)	リスク	ボリューム	警告
Snapshotコピーが多すぎる (ocumEvtSnapshotTooMany)	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 (ocumEvtVolumeQtreeQuotaOvercommitted)	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 (ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	リスク	ボリューム	警告
ボリュームの増加率が異常 (ocumEvtVolumeGrowthRateAbnormal)	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
ボリュームのフルまでの日数 (ocumEvtVolumeDaysUntilFullSoon)	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が無効（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が有効（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 (ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	リスク	ボリューム	エラー
FlexGroup コンスティテ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 コンスティテ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 コンスティテュエントの inode に関する問題*（ flexGroupConstitutionsHaveInodesIssues）	リスク	ボリューム	エラー
FlexGroup コンスティテュエント inode ステータスがすべて OK*（ flexGroupConstitutionsInodesStatusAllOK）	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
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	重大
ボリュームのストレージ効率化の異常（ocumVolumeAbnormalStorageEfficiencyWarning）	リスク	ボリューム	警告
利用率が低いボリュームのSnapshotリザーブ（volumeSnaphotReserveUnderutilizedWarning）	イベント	ボリューム	警告
利用率が低いボリュームのSnapshotリザーブ（volumeSnaphotReserveUnderutilizedCleared）	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
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

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 (ocumQosVolumeMaxIopsWarning)	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 (ocumQosVolumeMaxMbpsWarning)	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 (ocumQosVolumeMaxIopsPerTbWarning)	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 (ocumConformanceLatencyWarning) 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	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 (ocumVolumeIopsIncident)	インシデント	ボリューム	重大
ボリュームIOPSの警告しきい値を超過 (ocumVolumeIopsWarning)	リスク	ボリューム	警告
ボリュームMBpsの重大しきい値を超過 (ocumVolumeMbpsIncident)	インシデント	ボリューム	重大
ボリュームMBpsの警告しきい値を超過 (ocumVolumeMbpsWarning)	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の重大しきい値を超過 (ocumVolumeLatencyIncident)	インシデント	ボリューム	重大
ボリュームレイテンシの警告しきい値を超過 (ocumVolumeLatencyWarning)	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 (ocumVolumeCacheMissRatioIncident)	インシデント	ボリューム	重大
ボリュームキャッシュミス率の警告しきい値を超過 (ocumVolumeCacheMissRatioWarning)	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 (ocumVolumeLatencyIopsIncident)	インシデント	ボリューム	重大
ボリュームレイテンシ/IOPSの警告しきい値を超過 (ocumVolumeLatencyIopsWarning)	リスク	ボリューム	警告
ボリュームレイテンシ/MBpsの重大しきい値を超過 (ocumVolumeLatencyMbpsIncident)	インシデント	ボリューム	重大
ボリュームレイテンシ/MBpsの警告しきい値を超過 (ocumVolumeLatencyMbpsWarning)	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/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 (ocumVolumeLatencyAggregatePerfCapacityUsed Incident)	インシデント	ボリューム	重大
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 (ocumVolumeLatencyAggregatePerfCapacityUsed Warning)	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 (ocumVolumeLatencyAggregateUtilizationIncident)	インシデント	ボリューム	重大
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 (ocumVolumeLatencyAggregateUtilizationWarning)	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 (ocumVolumeLatencyNodePerfCapacityUsed Incident)	インシデント	ボリューム	重大
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 (ocumVolumeLatencyNodePerfCapacityUsed Warning)	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 (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	インシデント	ボリューム	重大
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 (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	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 (ocumVolumeLatencyNodeUtilizationIncident)	インシデント	ボリューム	重大
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 (ocumVolumeLatencyNodeUtilizationWarning)	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) (antiRansomwareVolumeStateEnabled)	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 (antiRansomwareVolumeStateDisabled)	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
ボリュームのランサムウェア対策監視が有効（ラーニングモード）（antiRansomwareVolumeStateDryrun）	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）（antiRansomwareVolumeStateDryrunPaused）	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）（antiRansomwareVolumeStateEnablePaused）	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（antiRansomwareVolumeStateDisableInProgress）	リスク	ボリューム	警告
ランサムウェア攻撃の発生（callHomeRansomwareActivitySeen）	インシデント	ボリューム	重大
ランサムウェア対策監視に適したボリューム（ラーニングモード）（ocumEvtVolumeArwCandidate）	イベント	ボリューム	情報
ランサムウェア対策の監視に適したボリューム（アクティブモード）（ocumVolumeSuitedForActiveAntiRansomwareDetection）	リスク	ボリューム	警告
ボリュームにノイズの多いランサムウェア対策アラートが表示される（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 (volumeLacksLocalProtectionWarning)	リスク	ボリューム	警告
ボリュームのローカル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グループ化され、イベントとトラップの名前、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
ボリューム移動ステータス-失敗 (ocumEvtVolumeMoveFailed)	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 (ocumEvtVolumeMoveCutoverDeferred)	リスク	ボリューム	警告

イベントのウィンドウとダイアログボックスの説明

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]インベントリページと[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。通知を設定する

には、[Notification Setup Options]ダイアログボックスを使用します。[Event Setup]ページを使用して、イベントを無効または有効にできます。

## [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、アラート通知の次の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」というアドレスが事前に入力されている場合、すべてのEメール通知が正しく送信されるように実際のEメールアドレスに変更する必要があります。

## SMTPサーバ

この領域では、次のSMTPサーバを設定できます。

- \* 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、指定した受信者にアラート通知を送信するために使用されます。

- \* ユーザー名 \*

SMTPユーザ名を指定します。SMTPユーザ名が必要なのは、SMTPサーバでSMTPAUTHが有効になっている場合だけです。

- \* パスワード \*

SMTPパスワードを指定します。SMTPユーザ名が必要なのは、SMTPサーバでSMTPAUTHが有効になっている場合だけです。

- \* ポート \*

アラート通知の送信にSMTPホストサーバが使用す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とも呼ばれます) を使用した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た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、[Version 1]、[Version 3]、[Version 3 With Authentication]、[Version 3 With Authentication and Encryption]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 \*

管理サーバから送信される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。トラップ送信先を複数指定するには、各ホストをカンマで区切ります。



他のSNMP設定（「バージョン」や「アウトバウンドポート」など）は、リスト内のすべてのホストで同じにする必要があります。

- \* アウトバウンドトラップポート \*

管理サーバから送信されたトラップをSNMPサーバが受信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。

- \* 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。管理サーバによって自動的に生成されます。[Engine ID]は、[SNMP Version 3]、[SNMP Version 3 with Authentication]、および[SNMP Version 3 with Authentication and Encryption]で使用できます。

- \* ユーザー名 \*

SNMPユーザ名を指定します。[User name]は、[SNMP Version 3]、[SNMP Version 3 with Authentication]、および[SNMP Version 3 with Authentication and Encryption]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。デフォルト値はMD5です。認証プロトコルは、[SNMP Version 3 with Authentication]および[SNMP Version 3 with Authentication and Encryption]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。[Authentication password]は、[SNMP Version 3 with Authentication]および[SNMP Version 3 with Authentication and Encryption]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。プロトコルオプションには、AES 128および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、[SNMPバージョン3、認証と暗号化を使用]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ときのパスワードを指定します。[プライバシーパスワード]は、[SNMPバージョン3、認証と暗号化を使用]とともに使用できます。

SNMPのオブジェクトとトラップの詳細については、NetAppサポートサイトからダウンロードして"[Active IQ Unified Manager MIB](#)です"ください。

### [イベント管理]インベントリページ

[イベント管理]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。
- [Filters]ペインを起動する[Filters]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を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、そのユーザ名とイベントを割り当てた時刻が追加されます。

- 自分

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、イベントを他のユーザに割り当てたり、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。

イベントに確認応答すると、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開き、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。

- \* 列セレクタの表示 / 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。

## [Events]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 (❌)、Error (⚠️)、Warning (⚠️)、Information (ℹ️)。

• \* 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。名前を選択すると、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している他のワークロードが[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 \*

イベントが「Active IQポータル」から発生したのか、「Active IQ Unified Manager」から直接発生したのか。

• \* 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ている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、ユーザに割り当てられた時点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、確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。

## [Event]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。また、問題を解決するための考えられる修正方法に関する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」のときは最後に確認された情報が不明なため非表示になります。

- \* イベント概要 \*

イベントの簡単な説明。

イベントの説明にイベントがトリガーされた理由が記載されている場合があります。

- \* 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は、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せん。

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]、[推奨される操作]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を開きます。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。

イベントをユーザーに割り当てると、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、そのユーザー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。

イベントに確認応答すると、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 ([確認者]) に、自分のユーザ名とイベントに回答した時刻が追加されます。確認応答したイベントは、ユーザーが管理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、イベントリストの選択したイベントの該当するフィールド ([解決者]) 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ます。このダイアログボックスで、選択したイベントのアラートを追加できます。

## [イベント情報]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非表示になります。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 \*

イベントを廃止する原因となった操作（問題が修正されたなど）。

- \* 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、解決または廃止後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 (❌)、Error (⚠️)、Warning (⚠️)、Information (ℹ️)。

- \* 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 \*

影響を受けるオブジェクトがメンバーであ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、および割り当てタイプ（割り当てスペースまたは使用済みスペース）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 \*

イベントの処理が割り当てられているユーザの名前。

- \* 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。

[Add Alert]ダイアログボックスを開くには、リンクをクリックします。

- 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、アラート名が表示されます。

[Edit Alert]ダイアログボックスを開くには、リンクをクリックします。

- 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。

[Alert Setup]ページを開くには、リンクをクリックしてアラートの詳細を表示します。

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。

[推奨される操作]セクションに表示される内容

[イベントの詳細]ページの[推奨される操作]セクションには、イベントの考えられる理由とイベントを解決するための推奨される対処方法が表示されます。推奨される対処方法は、イベントのタイプまたは違反したしきい値のタイプに基づいてカスタマイズされません。

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。一部の処理では、Unified Manager、ONTAP System

Manager、OnCommand Workflow Automation、ONTAP CLIコマンド、またはこれらのツールを組み合わせで使用します。

ここで推奨される対処方法は、このイベントを解決するためのガイダンスとしてのみ考慮してください。このイベントを解決するためのアクションは、環境の状況に基づいて実行する必要があります。

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、\* 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で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]セクションに表示される内容

[イベントの詳細]ページの[システム診断]セクションには、イベントの原因となった可能性がある問題の診断に役立つ情報が表示されます。

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を表示します。このように配置すると、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、またはレイテンシの影響を受けているストレージコンポーネントを確認できます。

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せん。

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、他のグラフが表示されます。

その他のイベントには、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説明が表示されます。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は、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場合があります。このシナリオでは、診断の横に緑または赤のアイコンが表示され、特定の診断で問題が見つかったかどうかを示されます。

## Event Setup ページ

[Event Setup]ページには、無効になっているイベントのリストと、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表示されます。イベントをグローバルに無効または有効にする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を開きます。このダイアログボックスで、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 \*

[ルールをアップロード]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、外部ネットワークへのアクセスがないサイトで、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イベントにサブスクライブ]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、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、無効な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。

## [Disable Events]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。特定の重大度に基づくイベントタイプまたは一連のイベントについて、イベントを無効に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。

#### [Event Properties]領域

[イベントプロパティ]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」のいずれかです。

- \* 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および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。

#### 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。

- \* 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（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）を選択できます。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。

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、イベントの原因となった違反したポリシーまたはしきい値の名前、およびイベントの説明が記載されています。また、各イベントのハイパーリンクもEメールメッセージに記載されており、UIでイベントの詳細ページを確認できます。

アラートEメールは、アラートを受信す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または容量の値が収集期間中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可能性があります。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通ずつ送信されることがあります。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け取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: sclaus@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、[スクリプト] 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。

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あとに [Event Details] ページから直接アラートを作成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 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。



ユーザに指定したEメールアドレスを変更し、アラートを編集用に再度開くと、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なくなるため、[Name]フィールドには何も表示されません。また、[ユーザ]ページで選択したユーザのEメールアドレスを変更しても、変更したEメールアドレスは更新されません。

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

次の例は、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」を含むすべてのボリュームを対象にし、名前に「xyz」を含むすべてのボリュームを除外します。
- イベント：健全性に関するすべての重大イベントを含む
- アクション：「[sample@domain.com](mailto:sample@domain.com)」、「テスト」スクリプトが含まれており、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. をクリックし、HealthTest\*[アラート名]\*フィールドに\*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. **abc**[名前に次の文字を含む]フィールドに「」と入力し、名前に「abc」を含むボリュームを表示します。
  - b. [Available Resources]領域で\*\*を選択し[All Volumes whose name contains 'abc']、[Selected Resources]領域に移動します。
  - c. をクリックし、xyz[名前に次の文字を含む]\*フィールドに\*と入力し、[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. をクリックし、sample@domain.com[アラートを通知するユーザ]フィールドに\*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。

#### アラートの追加に関するガイドライン

アラートは、リソース（クラスター、ノード、アグリゲート、ボリュームなど）と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。

- アラートの説明

アラートを効果的に追跡できるように、アラートの説明を指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、リソースを含め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（\*\*など）を選択すると、[\[All User or Group Quotas\]](#) そのカテゴリ内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すると、クラスタの重大イベントに対するアラートのみが送信されます。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

指定した重大度タイプ（Critical、Error、Warning）のイベントでアラートをトリガーするかどうかを決め、トリガーする場合はどの重大度タイプをトリガーするかを決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ても、個々のイベントを選択しない場合（[\[Selected Events\]](#)列を空のままにした場合）、カテゴリ内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。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の追加

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単一のアラ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。

次の例は、レイテンシ、IOPS、MBpsのすべての重大イベントの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、すべての警告イベントを選択できます。

### 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。

リソースが選択されていないため、これらのイベントを受信したすべてのクラスタ、アグリゲート、ボリュームなど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\*latency 「\*」 と入力し、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\*iops 「\*」 と入力し、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\*mbps 「\*」 と入力し、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トラップの発行およびスクリプトの実行について、このページのそ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、通知が送信されたかどうか、およびスクリプトが実行された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、イベントの状態が「新規」、「確認済み」、「解決済み」、「廃止」のいずれかになると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	操作
イベントが解決または廃止状態になったときのアラートの送信を停止する	スライダコントロールを左に移動します。
イベントが解決または廃止状態になったときのアラートの送信を開始する	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のアラート生成対象からの除外

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」上の同じ名前のボリュームではアラートは生成されないように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\*\*`vol1`を選択し、[名前に次の文字を含む]\*フィールドに\*と入力して、名前に「vol1」を含むボリュームを表示します。
  - b. [Available Resources]領域で\*+を選択し[All Volumes whose name contains 'vol1']、[Selected Resources]領域に移動します。
3. タブを選択し、[ボリューム]\*`vs1-dr`を選択し、[名前に次の文字を含む]フィールドに\*と入力して、[追加]\*をクリックします。

SVM「vs1-dr」上のボリューム「vol1」に対して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

[Alert Setup]ページでは、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を表示できます。また、アラートのプロパティ（アラートの説明、通知方法と頻度、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、影響を受けるリソース（クラスタ、アグリゲート、ボリュームなど）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。

アラートのリストが[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、関連付けられているスクリプトなど、アラートのプロパティ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。

## アラートのウィンドウとダイアログボックスの説明

[アラートの追加]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アラートを設定する必要があります。[Alert Setup]ページからアラートのリストを表示することもできます。



## 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開き、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、ユーザが不要な通知を受け取るのを防ぐことができます。

### 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情報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 ( ) か無効 ( ) か  を指定します .

- \* 警告 \*

アラートの名前が表示されます。

- \* 概要 \*

アラートの説明が表示されます。

- \* 通知方法 \*

アラートに対して選択された通知方法が表示されます。EメールまたはSNMPトラップを使用してユーザーに通知できます。

- \* 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 \*

アラートの説明が表示されます。

- \* 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

アラートを作成して特定のイベントが生成されたときに通知することで、問題に迅速に対処し、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、アラートの名前と説明を指定できます。

- \* アラート名 \*

アラート名を指定できます。

- \* Alert 概要 \*

アラートの説明を指定できます。

#### 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して、その文字列に一致するリソースをグループ化し、アラートに含めるグループを選択できます。たとえば、「abc」という文字列を名前に含む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」という文字列を名前に含むすべてのボリュームを除外できます。

[除外]タブは、特定のリソースタイプのすべてのリソース (+や[\[All Volumes whose name contains 'xyz'\]](#)+)など)を選択した場合にのみ表示され[\[All Volumes\]](#)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、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。特定の重大度に基づくイベントまたは一連のイベントに対してアラートを作成できます。

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」のいずれかです。

### • \* 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。

ユーザに指定したEメールアドレスを変更し、アラートを編集用に再度開くと、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なくなるため、[Name]フィールドには何も表示されません。また、[ユーザ]ページで選択したユーザのEメールアドレスを変更しても、変更したEメールアドレスは更新されません。

### • \* 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回のみ通知
- 指定した頻度で通知
- 指定した時間範囲内で指定した頻度で通知する

### • \* 問題 SNMP トラップ \*

このボックスを選択すると、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。

#### [Edit Alert]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、アラートの名前と説明を編集できます。

- \* アラート名 \*

アラート名を編集できます。

- \* Alert 概要 \*

アラートの説明を指定できます。

- \* 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して、その文字列に一致するリソースをグループ化し、アラートに含めるグループを選択できます。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]タブは、特定のリソースタイプのすべてのリソース（や<<All Volumes whose name contains 'xyz'>>など）を選択した場合にのみ表示され[All Volumes]ます。

## 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」のいずれかです。

### • \* 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 \*

通知を受信するEメールアドレスまたはユーザ名を編集したり、新しいEメールアドレスまたはユーザ名を指定したりできます。

### • \* 通知頻度 \*

イベントが確認または解決されるか、廃止状態になるまで、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回のみ通知
- 指定した頻度で通知
- 指定した時間範囲内で指定した頻度で通知する

### • \* 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実行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でイベントに対してアラートが生成され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、イベントを生成している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、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は、アラートEメールから確認できます。



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。
- スクリプトでサポートされるファイル形式は、Perl、Shell、PowerShell、Python、`.bat`およびファイルです。

Unified Manager がインストールされているプラットフォーム	サポートされる言語
VMware	Perlスクリプトとシェルスクリプト
Linux	Perl、Python、シェルスクリプト
ウィンドウ	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環境の場合、Perl 5はデフォルトでインストールされ、スクリプトではPerl 5がサポートする機能のみがサポートされます。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スクリプトの場合、スクリプトを実行できるように、Windowsサーバで適切なPowerShell



実行ポリシーを設定する必要があります。



アラートスクリプトの進捗状況を追跡するためのログファイルがスクリプトで作成される場合は、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説明を入力します。
5. [追加]\* 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た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	操作
アラートを追加する	<ol style="list-style-type: none"> <li>a. [追加]*をクリックします。</li> <li>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。</li> </ol>
アラートを編集する	<ol style="list-style-type: none"> <li>a. アラートを選択し、 * 編集 * をクリックします。</li> <li>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。</li> </ol>

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。

#### サポートされるUnified ManagerのCLIコマンド

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、LUNなどのストレージオブジェクトに対してクエリを実行できます。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や、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、および認証用の有効なユーザ名とパスワードを入力する必要があります  
um cli login。



\_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	製品説明	出力
um cli login -u <username> [-p <password>]	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。この方法で使用する、パスワードの入力を求められ、パスワードは履歴テーブルやプロセステーブルに記録されません。セッションはログインしてから3時間後に期限切れになり、その後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。
um cli logout	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。
um help	第1レベルのサブコマンドをすべて表示します。	第1レベルのサブコマンドをすべて表示します。
um run cmd [ -t <timeout> ] <cluster> <command>	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、ONTAPで操作を取得または実行するためのアラートスクリプトに使用されます。オプションのtimeout引数は、コマンドがクライアントで完了するまでの最大時間（秒）を設定します。デフォルトは0（無期限に待機）です。	ONTAPから受信したもの。
um run query <sql command>	SQLクエリを実行します。データベースから読み取るクエリのみが許可されます。更新、挿入、削除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不正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。

CLIコマンド	製品説明	出力
um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>	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、-u (ユーザ名) オプションと-P (パスワード) オプションを指定する必要があります。オプション-t (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 (httpまたはhttps) 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-p (port) 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。	ユーザに証明書の受け入れを求めるプロンプトが表示され、対応するメッセージが出力されます。
um datasource list [ <datasource-id>]	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
um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>	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。
um datasource remove <datasource-id>	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。
um option list [ <option> .. ]	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.

CLIコマンド	製品説明	出力
um option set <option-name>=<option-value> [ <option-name>=<option-value> ... ]	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せん。
um version	Unified Managerソフトウェアのバージョンが表示されます。	Version ("9.6")
um lun 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、svmのいずれかを指定できます。</p> <p>例：</p> <p><b>um lun list -cluster 1</b></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.
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、svmのいずれかを指定できます。</p> <p>例：</p> <p><b>um svm list -cluster 1</b></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>	次の値が表形式で表示されます。 Name and Cluster ID.

CLIコマンド	製品説明	出力
<pre>um qtree list [-q] [-Objectype &lt;object-id&gt;]</pre>	<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。Objectypeには、lun、qtree、cluster、volume、quota、svmのいずれかを指定できます。</p> <p>例：</p> <pre><b>um qtree list -cluster 1</b></pre> <p>この例では、objectype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>
<pre>um disk list [-q] [-Objectype &lt;object-id&gt;]</pre>	<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。Objectypeには、disk、aggr、node、clusterのいずれかを指定できます。</p> <p>例：</p> <pre><b>um disk list -cluster 1</b></pre> <p>この例では、objectype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、`Objectype and object-id` ます。</p>

CLIコマンド	製品説明	出力
<pre>um cluster list [-q] [-Objectype &lt;object-id&gt;]</pre>	<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。Objectypeには、disk、aggr、node、cluster、lun、qtree、volume、quota、svmのいずれかを指定できます。</p> <p>例：</p> <pre><b>um cluster list -aggr 1</b></pre> <p>この例では、objectypeが「-aggr」、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>
<pre>um cluster node list [-q] [-Objectype &lt;object-id&gt;]</pre>	<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。Objectypeには、disk、aggr、node、clusterのいずれかを指定できます。</p> <p>例：</p> <pre><b>um cluster node list -cluster 1</b></pre> <p>この例では、objectype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 `Name and Cluster ID` ます。</p>

CLIコマンド	製品説明	出力
<pre>um volume list [-q] [- ObjectType &lt;object-id&gt;]</pre>	<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、aggregateのいずれかを指定できます。</p> <p>例：</p> <pre><b>um volume list -cluster 1</b></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 `Volume ID and Volume Name` ます。</p>
<pre>um quota user list [-q] [- ObjectType &lt;object-id&gt;]</pre>	<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><b>um quota user list -cluster 1</b></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>	<p>次の値が表形式で表示され `ID, Name, SID and Email` ます。</p>



CLIコマンド	製品説明	出力
<code>um aggr list [-q] [-ObjectType &lt;object-id&gt;]</code>	<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> <p><b>um aggr list -cluster 1</b></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 `Aggr ID, and Aggr Name` ます。
<code>um event ack &lt;event-ids&gt;</code>	1つ以上のイベントを確認します。	対応するメッセージを表示します。
<code>um event resolve &lt;event-ids&gt;</code>	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。
<code>um event assign -u &lt;username&gt; &lt;event-id&gt;</code>	イベントをユーザに割り当てます。	対応するメッセージを表示します。
<code>um event list [ -s &lt;source&gt; ] [ -S &lt;event-state-filter-list&gt;.. ] [ &lt;event-id&gt; .. ]</code>	システムまたはユーザによって生成されたイベントを一覧表示します。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 `Source, Source type, Name, Severity, State, User and Timestamp` ます。
<code>um backup restore -f &lt;backup_file_path_and_name&gt;</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説明

[Scripts]ページでは、Unified Managerにスクリプトを追加できます。

### [スクリプト]ページ

[Scripts]ページでは、Unified Managerにカスタムスクリプトを追加できます。作成した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を自動的に再設定できます。

[Scripts]ページでは、Unified Managerの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、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 \*

スクリプトの説明が表示されます。

## [Add Script]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アラートを設定し、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 \*

アラートのスクリプトを選択できます。

- \* 概要 \*

スクリプトの説明を指定できます。

# クラスタのパフォーマンスの監視と管理

## Active IQ Unified Manager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することで、特定のパフォーマンスカウンタの最大値を指定して、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

これらのワークロードは、クラスタに作成したFlexVolとFlexGroupで構成されます。

- システム定義のワークロード

これらのワークロードは、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。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、多くのクラスタコンポーネントのさまざまなパフォーマンスカウンタを監視します。

応答時間 (レイテンシ) が長い場合は、ストレージオブジェクト (ボリュームなど) の処理速度が通常よりも遅いことを示しています。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ていることも示しています。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および分析します。
- 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、パフォーマンス容量、キャッシュ比率など、ワークロードのアクティビティの推移を示す詳細なグラフが表示されます。
- しきい値を超えたとき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。
- ボリュームやLUNに適用されているサービス品質（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。
- 競合状態にある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がデータストレージの容量、可用性、保護の問題をトラブルシューティングするために提供する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。

ここでは、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、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一般的な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。

この情報を使用して、メンテナンスコンソールにアクセスし、Unified Managerサーバの機能に関連する問題を解決できます。

## 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。このデータを分析して、パフォーマンスイベントと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、現在の月の非常に詳細なパフォーマンスの詳細と、最大1年間の一般的なパフォーマンスの傾向を表示できます。

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	製品説明
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	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。  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。
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	5分ごとに収集された最新12件のパフォーマンスデータを1時間の平均にまとめたものです。  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。
予測分析とデータの削除	毎日午前0時以降	クラスタのデータを分析して、次の24時間のボリュームレイテンシとIOPSの動的なしきい値を設定します。  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。

アクティビティ	時間間隔	製品説明
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時半から	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（デフォルトでは5分間隔）以外のパフォーマンスデータを収集します。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後に、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、前の期間にシステム定義のしきい値イベントがある場合は報告されます。

- 現在のパフォーマンスデータ収集サイクルが時間どおりに終了しません。

リアルタイムのパフォーマンスポーリングが5分間の収集期間を超えた場合は、不足している情報を収集するためにデータの継続性収集サイクルが開始されます。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。
  - 再起動されました。
  - ソフトウェアのアップグレード中またはバックアップファイルの作成中にシャットダウンされました。
  - 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。
  - 低速の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が遅れました。

データの継続性収集サイクルでは、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、リアルタイムのパフォーマンスデータ収集が開始される必要があります。

ます。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、またはイベントの検出時間として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おり、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GUIのページに移動し、ページのタブや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の監視とトラブルシューティングには、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
- ストレージオブジェクトと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)
- 設定ページとセットアップページ
- イベントページ

## UIへのログイン

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せん。

- 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。

サポートされているブラウザとバージョンの一覧については、Interoperability Matrixを参照してください "[mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix)"。

- Unified ManagerサーバのIPアドレスまたはURLが必要です。

1時間操作を行わないと、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URLを入力します。ここで、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]/`

サーバで自己署名デジタル証明書が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）が署名したサーバ認証用のデジタル証明書をインストールします。です。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。

[Dashboard]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。使用可能なナビゲーションの組み合わせをすべて示すわけではありませんが、代表的なシナリオのいくつかを理解しておく必要があります。

### 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できます。パフォーマンスとイベントの概要を表示したり、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細をさらに詳しく調査したりできます。

次に、クラスタオブジェクトを使用したさまざまな操作の例を示します。

1. [Dashboard]ページで、[Performance Capacity]パネルの詳細を確認してパフォーマンス容量を使用しているクラスタを特定し、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。

指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確認するか、ポリシーの設定を変更し、それらのボリュームが使用するIOPSの割合がそれほど高くないようにします。

The screenshot illustrates the navigation path in the dashboard to identify high IOPS volumes. It starts with the 'Capacity' section, moves to the 'Nodes' table, then to the 'Node / Performance' page for a specific node, and finally to the 'Aggregate / Performance' page for a specific aggregate.

**Dashboard - Capacity**

CLUSTER	USED	DAYS TO FULL	REDUCTION
opm-ak...lclby	40.5 TB	< 1 month	13.0:1
umeng...1-02	83.0 TB	51 days	8.0:1
symgr...0-1-4	33 TB	140 days	6.3:1

**Nodes**

Status	Node	Latency	IOPS	MB/s	Performance Capacity Used	Utilization	Fr
✖	umeng-aff220-01	21.7 ms/op	27,335 IOPS	221 MB/s	73%	50%	3.1
✖	umeng-aff220-02	8.33 ms/op	83.4 IOPS	102 MB/s	53%	42%	6.1

**Node / Performance : umeng-aff220-01**

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**

Volume	Latency	IOPS	MB/s
suchita_vmware_d...	6.38 ms...	16.8 IOPS	2.55 MB/s
suchita_vmware_d...	3.82 ms...	4,775 L...	18.7 MB/s
aiqum_scale_do_no...	0.114 m...	< 1 IOPS	< 1 MB/s

クラスタパフォーマンス監視時の操作

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できます。パフォーマンスとイベントの概要を表示したり、クラスタや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細を詳しく調査したりできます。

次に、クラスタパフォーマンスを監視するためのさまざまな手順の例を示します。

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]ページに移動します。
4. 必要に応じて、[表示して比較]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、いずれかのオブジェクトを比較ペインに追加します。

両方のオブジェクトの統計が比較のため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

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...	8.35 ...	<1 M...	<1%

Comparing 1 Additional Object

- aggr4
- aggr3

CHOOSE CHARTS: 7 Charts Selected

Events for Aggregate: aggr4

No data to display



## Latency for Aggregate: aggr4

Last updated: Nov 15, 2019, 1:23 PM

Event Timeline: aggr4

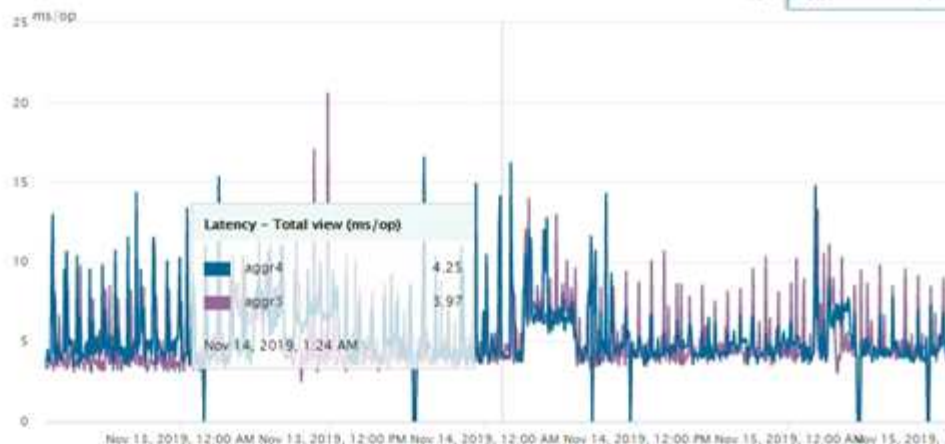
TIME RANGE: Last 72 Hours

- Critical Events
- Error Events
- Warning Events
- Information Events

No data to display

Comparing Objects

- aggr4
- aggr3



## イベント調査時の画面操作

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の詳細が表示されます。これは、パフォーマンスイベントの調査、トラブルシューティング、およびシステムパフォーマンスの微調整を行う場合に役立ちます。

パフォーマンスイベントのタイプに応じて、次の2種類のイベント詳細ページのいずれかが表示されます。

- ユーザ定義およびシステム定義のしきい値ポリシーのイベントの[イベントの詳細]ページ
- 動的なしきい値ポリシーのイベントの[イベントの詳細]ページ

これは、イベント調査時の操作例の1つです。

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[説明]と[推奨される操作]（該当する場合）を確認して、問題の解決に役立つイベントに関する詳細を確認します。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。

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	vs2:/julia_feb12_vol3	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_vmwarc...nt_delete_01	Volume
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency ... Service Level Policy	iscsi_boot/is.../ocum-c220-01	LUN
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency ... Service Level Policy	iscsi_boot/is.../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	SEVERITY	SOURCE
Nov 14, 2019, 11:39 AM	Warning	vs7:/julia_non_shared_3
STATE	IMPACT LEVEL	SOURCE TYPE
New	Risk	Volume
EVENT DURATION	IMPACT AREA	ON CLUSTER
1 day 40 minutes	Performance	ocum-mobility-01-02
LAST SEEN		AFFECTED OBJECTS COUNT
Nov 15, 2019, 11:19 AM		1
		TRIGGERED POLICY
		QoS Peak IOPS/TB threshold

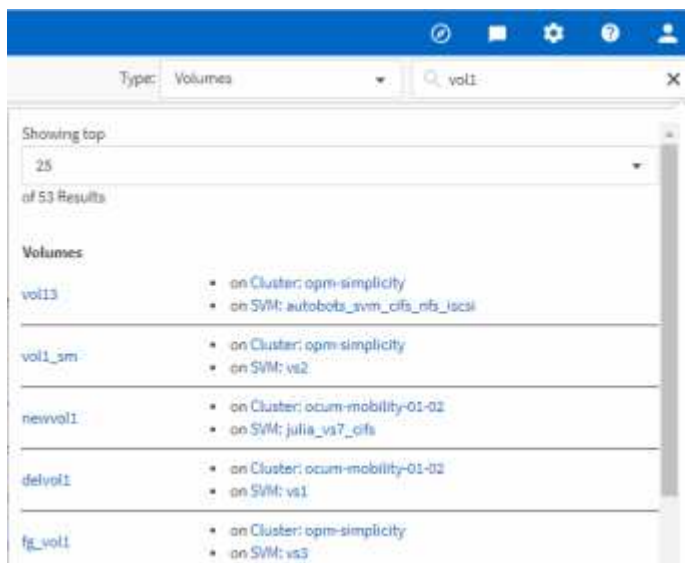
## ストレージオブジェクトの検索

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この方法を使用すると、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ソートされ、ドロップダウンメニューを使用してフィルタできます。有効な検索文字は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。このため、グローバル検索機能は、特定のアイテムをすばやく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。すべての検索結果を表示するには、オブジェクトのインベントリページで検索を実行し、関連するフィルタ機能を使用します。

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
- ノード：ノード名
- アグリゲート：アグリゲート名
- SVMs：SVM 名
- ボリューム：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[Volume]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コンテンツのフィルタリング

Unified Managerでインベントリページ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、グリッドに表示され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、適用されているフィルタの数が[Filter]ボタンの右側に表示されます。

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、[Column]、[Operator]、および[Value]フィールドが必要です。使用可能なフィルタには、現在のページのフィルタ可能な列が反映されます。適用できるフィルタの最大数は4つです。フィルタリングされた結果は、組み合わせたフィルタパラメータに基づいて決まります。フィルタリングされた結果は、現在表示されているページだけでなく、フィルタリングされた検索のすべてのページに適用されます。

[Filtering]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。[Filtering]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了します。
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。前の手順で説明したプロセスを使用して、このフィルタを完了します。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、フィルタの数が[フィルタ]ボタンの右側に表示されます。
7. 個々のフィルタを削除するには、[Filtering]パネルで、削除するフィルタの右側にあるごみ箱アイコンをクリックします。
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、3つのフィルタがある[Filtering]パネルを示しています。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

[Apply Filter]\*をクリックすると、[Filtering]パネルが閉じてフィルタが適用され、適用された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の概要

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のほかに、そのカテゴリのアクティブなイベントの数や、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、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だけを表示するようにフィルタリングされた[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[Nodes]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、クラスタのパフォーマンス容量、合計IOPS、合計スループットの値が表示されます。

#### \* 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、定義されている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合計数が表示されます。棒グラフをクリックすると、[ワークロード]ページでそのポリシーに割り当てられているワークロードが表示されます。

• \* 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は、クラスタをIOPSまたはスループット (MBps) が高い順に表示できます。

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) には、特定のクラスタで発生しているステータスの問題を知らせるバナーメッセージが表示される場合があります。

バナーメッセージ	製品説明	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を再起動してください。それでも問題が解決しない場合は、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で、データの継続性収集サイクルを実行中です。	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の収集間隔の変更

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い問題は、バナーメッセージまたは `Data collection is taking too long on cluster <cluster\_name>` で示され `Unable to consistently collect from cluster <cluster\_name>` ます。

収集間隔を変更する必要があるのは、統計の収集に問題があるためです。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。5分間の収集を使用する場合は、6回の収集でポリシーの超過が連続して発生する必要があります。収集時間が15分の場合、2つの収集期間でのみポリシーの超過が必要です。

[Cluster Setup]ページの下部に、現在の統計データ収集間隔を示すメッセージが表示されます。

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番号を入力し、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を使用すると、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に役立てることができます。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、ワークロードでパフォーマンスや容量の問題が発生している理由をより正確に把握できます。

このツールを使用すると、アプリケーションのパフォーマンスの問題の原因がストレージであるかどうか、または問題の原因がネットワークやその他の関連する問題であるかどうかを判断することもできます。

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[Workload Analysis]を選択

- [ 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）で詳細アイコンをクリックし、\* [ ワークロードを分析 ] \* をクリックします。
- [ 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すると、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する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すると、ワークロードの名前が自動的に入力され、ワークロードのデータにはデフォルトの2時間の期間が表示されます。[ 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

[ Workload Analyzer ] ページには、ワークロードに影響している可能性があるイベントの情報、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は、ボリュームのワークロードグラフと同じレベルの統計が表示されないため、この2つのタイプのワークロードで異なる値が表示されることがあります。

### \* イベントサマリ領域 \*

期間内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。複数の領域（パフォーマンスと容量など）に影響するイベントがある場合は、ここから必要な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つしか発生しなかった場合は、一部のイベントについて問題を解決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。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）

ここに表示されるクラスタコンポーネントの説明については、を参照してください"[クラスタコンポーネントと競合する理由](#)". \* **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、その他のプロセスで内訳） \* 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のデータ容量と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ビューはありません。
- \* 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日分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

通常、Workload Analyzerは、ユーザから報告されたレイテンシの問題のトラブルシューティング、報告されたイベントやアラートの詳細な分析、動作に異常があるワークロードの調査に使用します。

使用しているアプリケーションの実行速度が非常に遅いとユーザから連絡があった場合は、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、利用率のグラフを確認して、パフォーマンスの問題の原因がストレージであるかどうかを確認できます。容量の使用率が85%を超えているONTAPシステムはパフォーマンスの問題を引き起こす可能性があるため、容量グラフを使用して容量が不足しているかどうかを確認することもできます。これらのグラフは、問題の原因がストレージなのか、ネットワークなのか、その他の関連する問題なのかを判断するのに役立ちます。

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）で動作に異常があるワークロードが見つかった場合は、[詳細]アイコンをクリックし、**：**で\*[ワークロードを分析]\*をクリックすると、[ワークロード分析]ページが開き、ワークロードを詳しく調べることができます。

## Workload Analyzerの使用

Workload Analyzerは、さまざまな方法でユーザインターフェイスから起動できます。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。

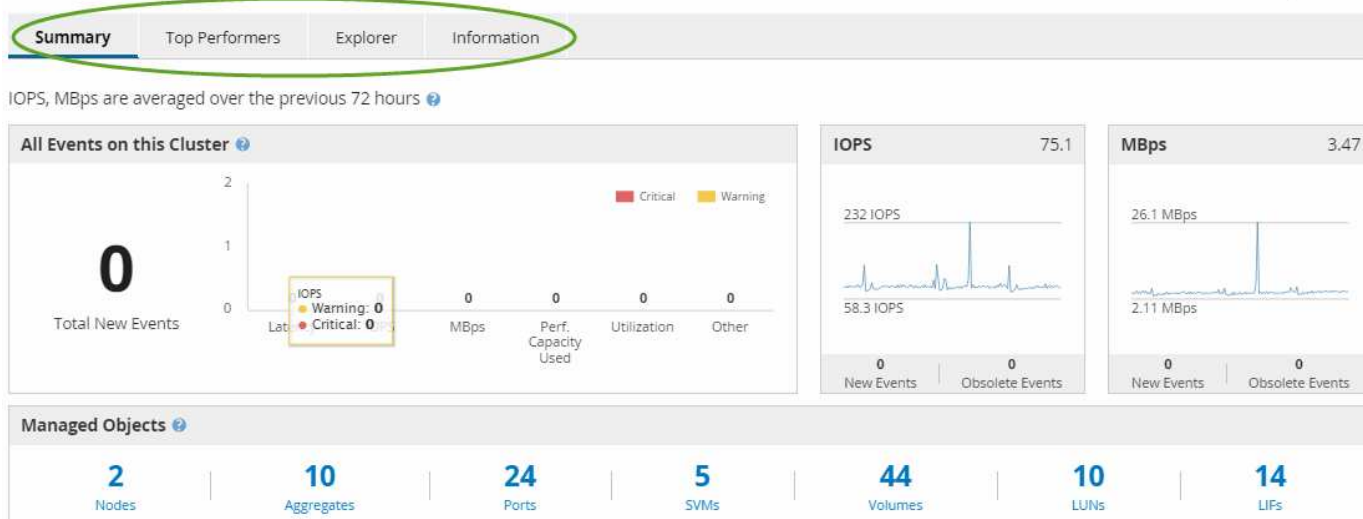
## [パフォーマンスクラスタランディング]ページからのクラスタパフォーマンスの監視

[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、クラスタ固有のイベントをすばやく把握して特定し、解決策を割り当てることができます。

### [パフォーマンスクラスタランディング]ページの概要

[Performance Cluster Landing]ページには、選択したクラスタのパフォーマンスの概要とクラスタ内の上位10個のオブジェクトのパフォーマンスステータスが表示されます。パフォーマンスの問題は、ページ上部の[All Events on this Cluster]パネルに表示されません。

[Performance Cluster Landing]ページには、Unified Managerのインスタンスで管理されてい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-mobilityというクラスタの[Performance Cluster Landing]ページの例を示しています。



[Cluster Summary]ページのイベント数が[Performance Event Inventory]ページのイベント数と一致しないことがあります。これは、組み合わせしきい値ポリシーに違反している場合は[Cluster Summary]ページの[Latency]バーと[Utilization]バーにそれぞれ1つのイベントが表示されるのに対し、[Performance Event Inventory]ページのイベントは組み合わせポリシーに違反している場合は1つだけ表示されるためです。



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。ページでは、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。

- [Summary]ページ
  - クラスタイベントペイン
  - MBps と IOPS のパフォーマンスチャート
  - [管理対象オブジェクト]ペイン
- [パフォーマンス上位]ページ
- Explorer ページ
- 情報ページ

## 【パフォーマンスクラスタサマリ】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。また、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]ペイン

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、ネームスペースの合計）
- IOPS（クラスタ、ノード、アグリゲート、SVM、ボリューム、LUN、ネームスペースの合計）
- MBps（クラスタ、ノード、アグリゲート、SVM、ボリューム、LUN、ネームスペース、ポート、LIFの合計）
- 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表示されます。

グラフのデータ（カウンタの縦棒）は、重大イベントについては赤色（）、警告イベントについては黄色（）で表示されます。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すると、凡例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、クラスタの処理速度（1秒あたりの入出力処理数）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（1秒あたりのメガバイト数）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の値を確認できます。

グラフの右上にあるグレーのバーの数字は、過去72時間の平均値です。トレンドライン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。グラフの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）を示します。自己修復または解決されていないイベントです。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。

- \* 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。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なくなりました。

- 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。

#### [管理対象オブジェクト]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。

管理オブジェクト数は、前回の収集期間における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。

オブジェクトタイプの数をクリックすると、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 \*

保護とプロビジョニングのために1つのユニットとして管理できる、複数のRedundant Array of Independent Disks (RAID) グループのセット。

- \* 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を使用して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1つ以上のアクセスプロトコルを使用してアクセス可能なユーザデータを保持する論理エンティティ。この数には、FlexVolとFlexGroupの両方が含まれます。FlexGroupコンスティチュエントは含まれません。

- \* LUN\*

Fibre Channel (FC ; ファイバチャネル) 論理ユニットまたはiSCSI論理ユニットの識別子。論理ユニットは通常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。この数には、すべてのインターフェイスタイプが含まれます。

## [パフォーマンス上位]ページ

[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。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）が発生しているかどうかも表示されます。

[パフォーマンス上位]ページには、各オブジェクトが最大10個表示されます。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ることに注意してください。

- \* 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。選択した期間はすべてのストレージオブジェクトに適用されます。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。カウンタオプションはオブジェクトタイプに固有です。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：

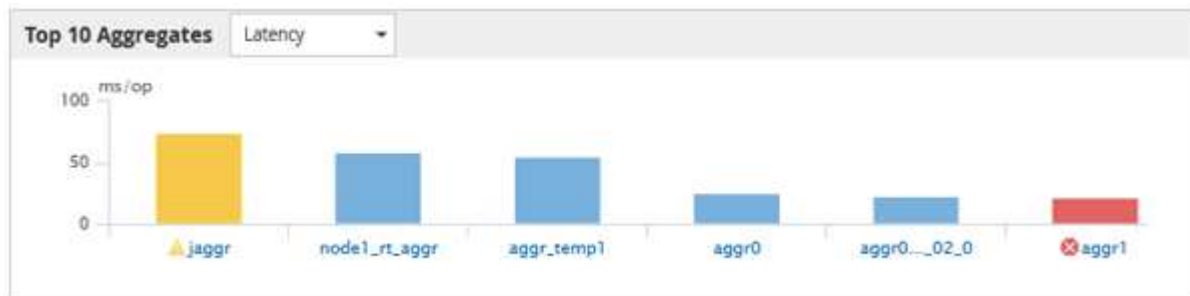
- レイテンシ
- IOPS
- MB/秒
- 使用済みパフォーマンス容量（ノードとアグリゲートの場合）
- 利用率（ノードとアグリゲートの場合）

• \* 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、パフォーマンスが上位または下位の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）の場合、バーはイベントの色で表示されます。警告イベントは黄色で表示され ( )、重大イベントは赤で表示され ( )。さらに、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。棒グラフの各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]ページが表示されます。

• \* イベントの重大度インジケータ \*

上位のオブジェクトのグラフでは、アクティブな重大イベント ( ) または警告 ( ) のイベントについて、オブジェクト名の左側に\*重大イベント\*インジケータアイコンが表示され ( ) ます。[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[イベントの詳細]ページに移動します。

- \* 2つ以上のイベント \*

[イベントインベントリ]ページに移動します。選択したオブジェクトのすべてのイベントが表示されます。

• \* 「エクスポート」 ボタン \*

カウンタバーに表示されるデータを含むファイルを作成します .csv。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。これにより、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るようになります。

[Object Inventory Performance]ページには、オブジェクトステータスの概要が表示され、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は、検索、ソート、フィルタリングによって絞り込むことができます。これは、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役立ちます。

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

デフォルトでは、パフォーマンスインベントリページのオブジェクトは、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発生し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発生し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。すべてのパフォーマンスデータは72時間の平均値に基づいています。

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の表示

[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。[Performance object detail]ページにリンクすると、特定のオブジェクトの詳細情報を表示できます。

デフォルトでは、ビューページ内のオブジェクト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

トが発生し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発生し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。

これらのページから(.pdf\* Reports \*ボタンを使用してデータをカンマ区切り値(.csv`ファイル、Microsoft Excelファイル(.xlsx`)、またはドキュメントにエクスポートし、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。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。

これらのページのすべてのフィールドは、カスタムビューおよび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ー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。左端にあるチェックボックスをクリックして1つ以上の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場合は、[その他のオプション]ボタンをクリック

して\*[ワークロードを分析]\*をクリックすると、[ワークロード分析]ページでパフォーマンスと容量のグラフを確認できます。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。
- 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、所定のストレージ容量で提供できるパフォーマンスを測定しません。
- 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へのパフォーマンスしきい値ポリシーの割り当て"](#)
- ["ストレージオブジェクトからのパフォーマンスしきい値ポリシーの削除"](#)
- ["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の表示"](#)
- ["Unified Managerによるクラウドへのデータ階層化の推奨事項の概要"](#)
- ["パフォーマンスグラフでの同じQoSポリシーグループ内のボリュームまたはLUNの比較"](#)

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。
  - ハイブリッド (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

- 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
  - VMDisk (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。ONTAPのバージョンでInactive Data Reportingがサポートされていない場合、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。左端にあるチェックボックスをクリックして1つ以上の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へのパフォーマンスしきい値ポリシーの割り当て"](#)
  - ["ストレージオブジェクトからのパフォーマンスしきい値ポリシーの削除"](#)

### 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 : ノードでの読み取り処理のうち、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た割合が返されます。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へのパフォーマンスしきい値ポリシーの割り当て"](#)
- ["ストレージオブジェクトからのパフォーマンスしきい値ポリシーの削除"](#)
- ["契約更新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フィールドには、すべてのI/O要求の平均応答時間が処理あたりのミリ秒で表示されます。



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へのパフォーマンスしきい値ポリシーの割り当て"](#)
- ["ストレージオブジェクトからのパフォーマンスしきい値ポリシーの削除"](#)

### 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場合は、[詳細]アイコンをクリックし、[ワークロードを分析]\*をクリックします。[ワークロード分析]\*ページでパフォーマンスと容量のグラフを確認できます。

詳細については、次のリンクを参照してください。

- ["整合性グループ関係にあるLUNの監視"](#)
- ["LUNのプロビジョニング"](#)
- ["ストレージオブジェクトへのパフォーマンスしきい値ポリシーの割り当て"](#)
- ["ストレージオブジェクトからのパフォーマンスしきい値ポリシーの削除"](#)
- ["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"](#)です。
- ["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の表示"](#)
- ["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へのパフォーマンスしきい値ポリシーの割り当て"](#)

- ["ストレージオブジェクトからのパフォーマンスしきい値ポリシーの削除"](#)

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が適用されず、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。NFS LIFとCIFS LIFには[レイテンシ]は該当せず、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。場所に省略記号（...）が表示された場合は、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。場所に省略記号（...）が表示された場合は、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。ポートロールの場合、ネットワークポート機能（[Data]または[Cluster]）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へのパフォーマンスしきい値ポリシーの割り当て"](#)
- ["ストレージオブジェクトからのパフォーマンスしきい値ポリシーの削除"](#)

### Performance：QoS Policy Groupsビュー

[QoSポリシーグループ]ビューには、Unified Managerで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サービスレベルマネージャ（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」上に作成された、想定レイテンシが「2ミリ秒/処理」のNSLMシステム定義の「Performance」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。このStorage VMタイプはクラスタを表すため、管理Storage VMにQoSポリシーが作成されている場合は空白になります。
- 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で定義されている最大スループットが無限であることを意味します。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。QoSポリシーグループ名の横にある展開ボタン（) をクリックすると、そのポリシーグループに関する詳細を確認できます▼。
- 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]ページの内容の絞り込み

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内容を絞り込むためのツールが用意されており、特定のデータをすばやく簡単に特定できます。

[Performance Object Inventory]ページには大量の情報が格納され、多くの場合複数のページにまたがって格納されます。この種の包括的なデータは、パフォーマンスの監視、追跡、改善に最適です。ただし、特定のデータを見つけるには、探しているデータをすばやく見つけるためのツールが必要です。そのため、[パフォーマンスオブジェクトインベントリ]ページには、検索、ソート、フィルタリングの機能が用意されています。さらに、検索とフィルタリングを組み合わせると、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パフォーマンス]ページでの検索

[Object Inventory Performance]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。特定のオブジェクトとその関連データを簡単に検索したり、ポリシーをすばやく検索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. 検索要件に基づいて、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パフォーマンス]ページでのソート

[Object Inventory Performance]ページでは、任意の列を基準に昇順または降順ですべてのデータをソートできます。これにより、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やトラブルシューティングプロセスの開始に役立ちます。

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パフォーマンス]ページでのデータのフィルタリング

[Object Inventory Performance]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、[Object Inventory Performance]ページの内容を絞り込んで、指定した結果のみを表示できます。この方法では、関心のあるパフォーマンスデータのみを効率的に表示できます。

[Filtering]パネルを使用して、グリッドビューを設定に基づいて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、グリッドに表示され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、適用されているフィルタの数が[Filter]ボタンの右側に表示されます。

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、[Column]、[Operator]、および[Value]フィールドが必要です。使用可能なフィルタには、現在のページのフィルタ可能な列が反映されます。適用できるフィルタの最大数は4つです。フィルタリングされた結果は、組み合わせたフィルタパラメータに基づいて決まります。フィルタリングされた結果は、現在表示されているページだけでなく、フィルタリングされた検索のすべてのページに適用されます。

[Filtering]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。[Filtering]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了します。
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。前の手順で説明したプロセスを使用して、このフィルタを完了します。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、フィルタの数が[フィルタ]ボタンの右側に表示されます。
7. 個々のフィルタを削除するには、[Filtering]パネルで、削除するフィルタの右側にあるごみ箱アイコンをクリックします。
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、3つのフィルタがある[Filtering]パネルを示しています。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

[Apply Filter]\*をクリックすると、[Filtering]パネルが閉じてフィルタが適用され、適用された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階層化の推奨事項の概要

**Performance** : All Volumes ビューには、ボリュームに格納されているアクセス頻度の低いユーザーデータ (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、特定のボリュームについて、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 **auto**、階層化ポリシーは ONTAP 9.4、階層化ポリシーは ONTAP 9.6 でも導入され、**all** 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、ボリュ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。

このフィールドの値は、ボリュームに対して設定されている階層化ポリシーを示します。ボリュームが現在 FabricPool アグリゲートにない場合も同様です。階層化ポリシーが適用されるのは、ボリュームが FabricPool アグリゲートにある場合のみです。

### \* コールドデータ \*

ボリュームに格納されているアクセス頻度の低いユーザーデータ (コールドデータ) のサイズが表示されます。

ここには、ONTAP 9.4 以降のソフトウェアを使用している場合にのみ値が表示されます。これは、ボリュームを導入するアグリゲートでがに設定されて **enabled** いる必要があり、最小クーリング日数のしきい値 (または **auto** 階層化ポリシーを使用するボリュームの場合) に達している **snapshot-only** 必要があるためです。 **inactive data reporting parameter** 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、[クラウドの推奨事項]フィールドは7日ごとに更新され、ボリュームに対してコールドデータ分析が実行されます。そのため、コールドデータの正確な量はフィールド間で異なる可能性があります。[クラウドの推奨事項]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含まれているため、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必要があると判断されました。場合によっては、まずボリュームをFabricPool対応アグリゲートに移動しなければならないことがあります。ボリュームがすでにFabricPoolアグリゲートにある場合は、階層化ポリシーを変更するだけで済みます。
- \* 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ペローラ]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ペローラページには、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。ページには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、さまざまな期間の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することができます。

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、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もできます。

## ルートオブジェクトの概要

ルートオブジェクトは、他のオブジェクトを比較する基準となるベースラインです。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改善に役立てることができます。

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。ルートオブジェクトの下に追加のオブジェクトが表示されます。[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。ルートオブジェクトは常に表示中のオブジェクトページに設定されます。たとえば、Volume1の[Volume Performance Explorer]ページを開くと、Volume1がルートオブジェクトになり、変更できません。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、グリッド内にボリュームが25個ある場合、フィルタを使用すると、スループットが90MBps未満またはレイテンシが1ミリ秒/処理を超えているボリュームのみを表示できます。

## 関連オブジェクトの期間の指定

[Performance Explorer]ページの[Time Range]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。期間を指定すると、[Performance Explorer]ページの内容が絞り込まれ、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のみを効率的に表示できます。事前定義された期間を選択するか、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。

### 事前定義の期間の選択

事前定義された期間を選択すると、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データ出力をすばやく効率的にカスタマイズして絞り込むことができます。事前定義された期間を選択すると、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。



## カスタムの期間の指定

[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の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データを絞り込む際に、事前定義された期間よりも柔軟に設定できます。

1時間から390日までの期間を選択できます。各月が30日としてカウントされるため、13カ月は390日になります。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または一連のイベントにズームインできます。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細に表示されるため、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。時間範囲に今日から30日を超える時刻/日付が含まれている場合、サマリデータはより短い時間範囲にも適用されます。

時間範囲（カスタムまたは事前定義）を選択する場合、5分間隔のデータサンプルに基づいて30日以下の時間範囲が設定されます。30日を超える期間は、1時間ごとのデータサンプルに基づいています。

From							To							Last Hour	
April 2015							April 2015							Last 24 Hours	
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Last 72 Hours	
29	30	31	01	02	03	04	29	30	31	01	02	03	04	Last 7 Days	
05	06	07	08	09	10	11	05	06	07	08	09	10	11	Last 30 Days	
12	13	14	15	16	17	18	12	13	14	15	16	17	18	Last 13 Months	
19	20	21	22	23	24	25	19	20	21	22	23	24	25	Custom Range	
26	27	28	29	30	01	02	26	27	28	29	30	01	02	Cancel	Apply Range
03	04	05	06	07	08	09	03	04	05	06	07	08	09		

Time: 6:00 am Time: 6:00 am

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。事前定義された期間を選択すると、最大13カ月分のデータを使用できます。選択した事前定義された時間範囲ボタンが強調表示され、対応する日付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限り、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. 必要に応じて、事前定義された日付範囲を選択する際に開始時刻と終了時刻を指定できます。前述のように事前定義された日付範囲を選択してから、前述のように開始時刻と終了時刻を選択します。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。グラフと[イベント]タイムラインには、その期間のパフォーマンス統計が表示されます。

## 比較グラフ用の関連オブジェクトのリストの定義

[Counter Chart]ペインでは、データとパフォーマンスの比較に関連する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) でパフォーマンスの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、問題の原因となっている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[Comparing]ペインと[Counter Chart]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、データ比較用に選択する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トレンドラインの色と一致します。

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する	[Comparing]ペインで、選択したオブジェクトの目のアイコン (  ) をクリックします  。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。
非表示のオブジェクトを表示する	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  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。



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除去	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。
選択したすべてのオブジェクトを除去	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のみが残ります。

## 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、パフォーマンスの問題を切り分けて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の場合、カウンタグラフは空になり、メッセージが表示されます。Not applicable for <object>

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。任意のトレンドライン上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が表示されます。

グラフ内の特定の期間を調査するには、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。[Reset Chart

Zoom]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。



トレンドラインにギャップが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チャートには、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、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には、その他の詳細情報が表示されます（グラフがズームビューに表示される場合）。

次の表に、使用可能なパフォーマンスカウンタグラフを示します。

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て、重大、エラー、警告、および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が表示され、パフォーマンスに影響を及ぼす可能性がある理由の全体像が示されます。
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の加重値です。
レイテンシ - 内訳	[レイテンシ-合計]と同じ情報が表示されますが、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。
レイテンシ-クラスタコンポーネント	[レイテンシ-合計]と同じ情報が表示されますが、パフォーマンスデータがクラスタコンポーネント別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。

使用可能なチャート	Chart 概要 (チャート)
IOPS - 内訳	<p>[IOPS -合計]と同じ情報が表示されますが、パフォーマンスデータが読み取りIOPS、書き込みIOPS、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>ズームビューに表示される場合、ボリュームのグラフにはQoS最小/最大スループット値が表示されます (ONTAPで設定されている場合)。</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	<p>[IOPS -合計]と同じ情報が表示されますが、パフォーマンスデータが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。</p>
IOPS/TB - 合計	<p>ワークロードで消費される合計スペース (TB) に基づく、1秒あたりの入出力処理数。I/O密度とも呼ばれます。このカウンタは、所定のストレージ容量で提供できるパフォーマンスを測定します。ズームビューに表示される場合、ボリュームのグラフにはQoS想定/最大スループット値が表示されます (ONTAPで設定されている場合)。</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>
MBps - 合計	<p>オブジェクトとの間で転送される1秒あたりのデータ量 (MB)。</p>

使用可能なチャート	Chart 概要 (チャート)
MBps - 内訳	<p>[MBps]グラフと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。ズームビューに表示される場合、ボリュームのグラフにはQoS最大スループット値が表示されます (ONTAPで設定されている場合)。</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 style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <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のデータをユーザプロトコルとシステムのバックグラウンドプロセスに分けて表示します。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。
利用率-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、ノードの利用率 (ノードの場合)、ディスクの利用率 (アグリゲートの場合)、帯域幅の利用率 (ポートの場合) です。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のうち、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の選択

[Choose charts]ドロップダウンリストでは、[Counter Charts]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	操作
個々のグラフを追加または削除する	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クリックします。
すべてのグラフを追加	[ * すべて選択 * ] をクリックします
すべてのグラフを削除	• 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。グラフを追加すると、[Choose charts]ドロップダウンリストと同じ順序で[Counter Charts]ペインに新しいグラフが挿入されます。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。

## [Counter Charts]ペインの拡張

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	操作
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

## カウンタグラフの対象期間の短縮

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、パフォーマンスデータ、イベント、しきい値のタイムラインの任意の部分について、より詳細かつ微細な情報を確認できます。

- 必要なもの \*

この機能がアクティブであることを示すには、カーソルが虫眼鏡に変わっている必要があります。



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。

カウンタグラフが元の状態で表示されます。

### イベントタイムラインでのイベントの詳細の表示

[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関連する詳細を確認できます。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。イベントの重大度にはそれぞれ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は、タイムライン上ではイベントドットで表されます。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、期間を短くします。これにより、複数のイベントが1つのイベントに分散され、各イベントを個別に表示および調査できます。

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チャートの急増と一致しているとは限りません。

#### 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。

ポップアップダイアログに、イベントタイプ、イベントが発生した日時、状態、およびイベント期間に関する情報が表示されます。

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
単一イベントの詳細を表示する	• ポップアップダイアログでイベントの詳細を表示*。

作業	オプション
複数のイベントの詳細を表示する	<ul style="list-style-type: none"> <li>ポップアップダイアログでイベントの詳細を表示*。</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <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。

Zoom Viewで表示した場合、一部の内訳グラフでは、Zoom View以外の場合に表示される情報よりも追加の情報が提供されます。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は、ボリュームと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

[Counter Charts Zoom View]では、選択したカウンタチャートと関連するタイムラインの詳細を確認できます。カウンタグラフのデータが拡大され、パフォーマンスイベントとその原因をより正確に把握できるようになります。

[Counter Charts Zoom View]は、任意のカウンタチャートについて表示できます。

### 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。

### ズームビューでの期間の指定

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。

1時間から390日までの期間を選択できます。各月が30日としてカウントされるため、13カ月は390日になります。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または一連のイベントにズームインできます。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細に表示されるため、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



摂するには、\* 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。時間範囲に今日から 30 日を超える時刻/日付が含まれている場合、サマリデータはより短い時間範囲にも適用されます。

時間範囲（カスタムまたは事前定義）を選択する場合、5分間隔のデータサンプルに基づいて30日以下の時間範囲が設定されます。30日を超える期間は、1時間ごとのデータサンプルに基づいています。

From							To							Last Hour	
April 2015							April 2015							Last 24 Hours	
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Last 72 Hours	
29	30	31	01	02	03	04	29	30	31	01	02	03	04	Last 7 Days	
05	06	07	08	09	10	11	05	06	07	08	09	10	11	Last 30 Days	
12	13	14	15	16	17	18	12	13	14	15	16	17	18	Last 13 Months	
19	20	21	22	23	24	25	19	20	21	22	23	24	25	Custom Range	
26	27	28	29	30	01	02	26	27	28	29	30	01	02	Cancel	Apply Range
03	04	05	06	07	08	09	03	04	05	06	07	08	09		

Time: 6:00 am Time: 6:00 am

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。事前定義された期間を選択すると、最大13カ月分のデータを使用できます。選択した事前定義された時間範囲ボタンが強調表示され、対応する日付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限り、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. 必要に応じて、事前定義された日付範囲を選択する際に開始時刻と終了時刻を指定できます。前述のように事前定義された日付範囲を選択してから、前述のように開始時刻と終了時刻を選択します。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。グラフと[イベント]タイムラインには、その期間のパフォーマンス統計が表示されます。




## カウンタグラフズームビューでのパフォーマンスしきい値の選択

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の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のイベントに関する正確なデータを表示できます。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。

[Counter Charts Zoom View]では、オブジェクトに一度に1つのポリシーのみを適用できます。

### ステップ

1. ポリシーに関連付けられているを選択または選択解除し  ます。

選択したしきい値がCounter Charts Zoom View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で表示されます。

## クラスタコンポーネント別のボリュームレイテンシの表示

[ボリュームパフォーマンスエクスプローラ]ページを使用して、ボリュームのレイテンシの詳細情報を表示できます。[レイテンシ-合計]カウンタグラフには、ボリュームでの合計レイテンシが表示されます。[レイテンシ-内訳]カウンタグラフは、ボリュームでの読み取りと書き込みのレイテンシの影響を特定するのに役立ちます。

また、[レイテンシ-クラスタコンポーネント]グラフには、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ます。これは、各コンポーネントがボリュームでの合計レイテンシにどのように影響しているかを判断するのに役立ちます。次のクラスタコンポーネントが表示されます。


- 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のリソース
- 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。

[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の比較チャートが表示されます。各クラスタコンポーネントに関連付けられているを選択または選択解除することで、比較を制限でき  ます。

3. 特定の値を表示するには、グラフ領域にカーソルを移動し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/SVM Explorer]ページで、SVMの詳細なIOPS情報を表示できます。[IOPS -合計]カウンタグラフには、SVMでのIOPS使用量の合計が表示されます。[IOPS -内訳]カウンタグラフは、SVM上の読み取り、書き込み、その他のIOPSの影響を特定する場合に便利です。

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-FC

### 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。プロトコルに関連付けられているを選択または選択解除することで、比較を制限でき  ます。

3. 特定の値を表示するには、いずれかのグラフのグラフ領域にカーソルを移動してポップアップウィンドウを表示します。

## ボリュームとLUNのレイテンシグラフでのパフォーマンス保証の確認

「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、この値を超えてはなりません。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に基づいています。

### 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ペローラ \* 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。

[Latency]グラフの水平線は、5分間の収集データが1時間あたりの平均データに置き換えられ、線がスムーズに表示されます。

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ペ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. [\* エクスペローラ \*] 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ペローラ \*] 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て長い期間の値を比較し、構成の問題を特定できます。

## ローカルノード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

を經由する場所を特定できます。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、ローカルノードを經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。ローカルノードを經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、パフォーマンスの問題が発生し、ノードでの高利用率が原因とな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、そのボリュームにアクセスするホストからのトラフィックを接続できるリモートノードにLIFを作成したりできます。

#### 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 -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 -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. 両方のグラフを横に表示して、IOPS値が大きく異な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て、特定の時点におけるローカルIOPSと合計IOPSを比較します。

### [Object Landing]ページのコンポーネント

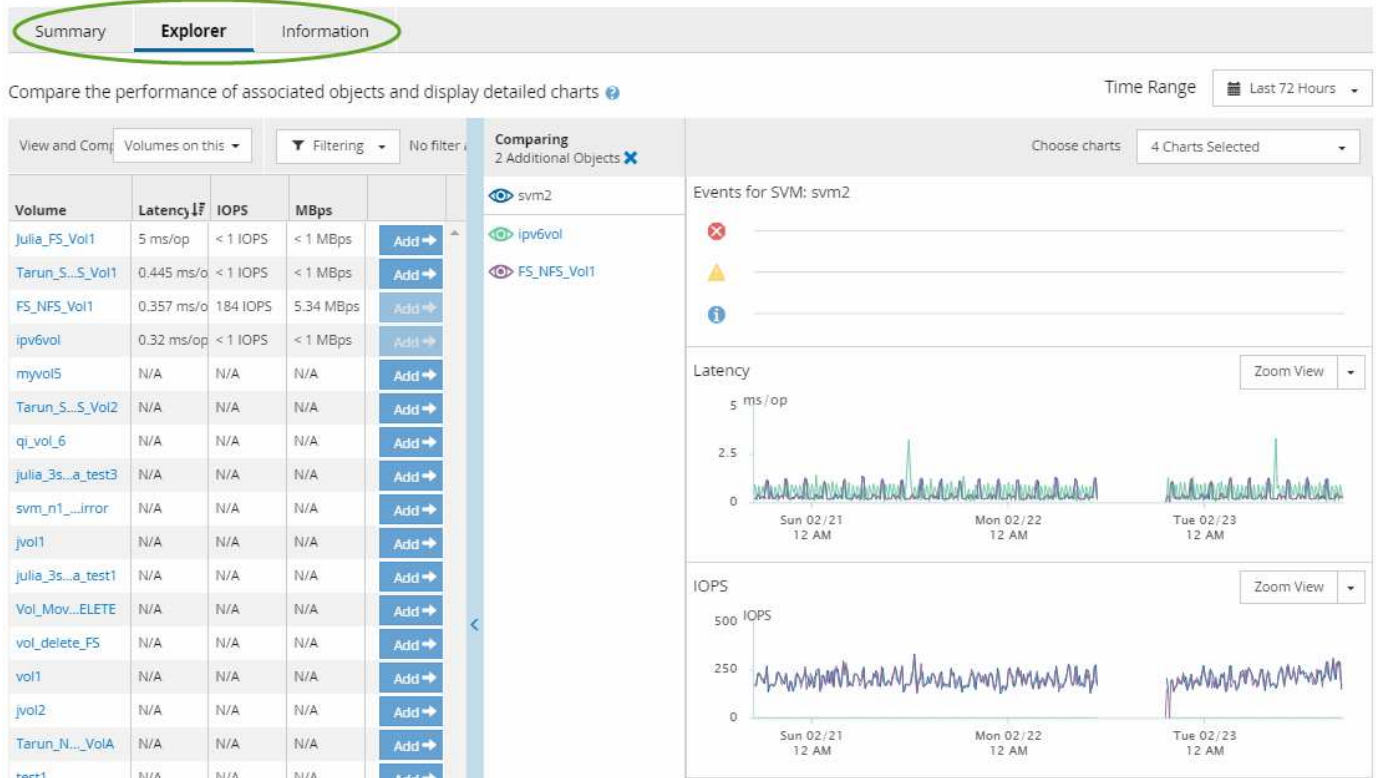
[Object Landing]ページには、重大、警告、情報のすべてのイベントに関する詳細が表示されます。すべてのクラスタオブジェクトのパフォーマンスの詳細が表示され、個々のオブジェクトを選択してさまざまな期間のオブジェクトを比較できます。

[Object Landing]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確認したり、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。これは、パフォーマンスを評価する場合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。



カウンタの概要パネルと[Counter Charts]には、5分間隔のサンプリングに基づくデータが表示されます。ページ左側のオブジェクト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が表示された[Object Landing]ページの例を示しています。



[Object Landing]ページには、表示しているストレージオブジェクトに応じて、オブジェクトに関するパフォーマンスデータを表示する次のタブがあります。

- 概要

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を含むカウンタグラフが3つか4つ表示されます。このグラフには、その期間の値の上限と下限を示す傾向線も表示されます。

- エクスプローラ

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のグリッドが表示され、現在のオブジェクトのパフォーマンス値と関連オブジェクトのパフォーマンス値を比較できます。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タが表示され、さまざまな比較を実行できます。

- 情報

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パートナー名、ポートとLIFの数など、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。

- 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。

- フェイルオーバーの計画

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ワークロードのすべての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、FlexVol、FlexGroup、およびFlexGroupのコンステイチュエントに対して表示されます。

## [Summary]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を含むカウンタグラフが表示されます。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

サマリグラフには、過去72時間の概要がすばやく表示され、さらに調査が必要な潜在的な問題を特定するのに役立ちます。

[Summary]ページのカウンタ統計がグラフで表示されます。

グラフのラインにカーソルを合わせると、特定の時点のカウンタ値が表示されます。サマリグラフには、次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総数も表示されます。

- \* 遅延 \*

すべてのI/O要求の平均応答時間（1処理あたりのミリ秒）。

すべてのオブジェクトタイプに対して表示されます。

- \* IOPS \*

平均動作速度。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対して表示されます。

- \* 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対して表示されます。

- \* 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。

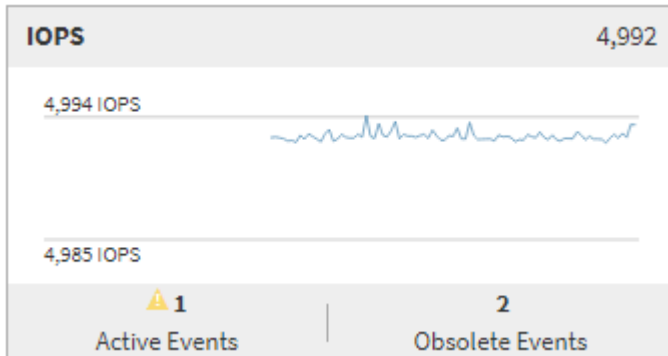
- \* 利用率 \*

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。

アクティブな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（■）、警告イベントは黄色（■）で表示されます。

グラフの右上にあるグレーのバーの数字は、過去72時間の平均値です。トレンドライン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。グラフの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]カウンタのグラフでは、過去72時間のオブジェクトのレイテンシの概要を確認できます。レイテンシとは、すべてのI/O要求の平均応答時間を指します。処理あたりのミリ秒、検討中のクラスタストレージコンポーネントのデータパケットまたはブロックのサービス時間、待機時間、またはその両方が含まれます。

- 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]カウンタのグラフでは、過去72時間のオブジェクトのIOPSの概要を確認できます。IOPSは、ストレージシステムの速度（1秒あたりの入出力処理数）を示します。

- 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]カウンタのグラフには、オブジェクトのMBpsパフォーマンスが表示されます。このグラフは、オブジェクトとの間で転送されたデータの量（1秒あたりのメガバイト数）を示します。[MBps]カウンタのグラフでは、過去72時間のオブジェクトのMBpsの概要を確認できます。

- 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]カウンタのグラフには、オブジェクトによって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 \*

[利用率]カウンタのグラフには、オブジェクトの利用率が表示されます。[利用率]カウンタのグラフでは、過去72時間のオブジェクトまたは帯域幅の利用率の概要を確認できます。

- 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、[イベントの詳細]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、クラスタ内のすべてのボリュームなど、クラスタ内の同様のオブジェクト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場合に役立ちます。オブジェクトをルートオブジェクトと比較することもできます。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。

- 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。このビューでは、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ペローラページには、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。

事前定義された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タイプとその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より大きい場合など、オブジェクトデータに適用するフィルタを作成できます。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

ボリュームとLUNの場合、各収集サイクル（デフォルトは5分）後に統計を表示するか、1時間あたりの平均として表示するかを選択できます。この機能を使用すると、NetAppの「パフォーマンス保証」プログラムをサポートするレイテンシグラフを表示できます。

• \* 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3つまたは4つのグラフのみが表示されます。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で定義されている場合があります。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。ワークロードが属するポリシーグループに上限が設定されていない場合（デフォルトのポリシーグループなど）や、設定された上限がニーズに合わない場合は、上限を引き上げるか、適切な上限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せん。

「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の上限をすべて使用できます。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制限を割り当てると、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。さらに、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含めることができます。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おり、最終的にスループットの大部分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。これにより、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、イベントの説明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をより制限の厳しいポリシーグループに割り当てることで、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、そのノードでのリソースの使用が削減されます。ただし、ワークロードがより多くのノードリソースを使用できるようにするには、ポリシーグループの値を大きくします。

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。

- ポリシーグループの作成
- 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のワークロードの移動
- ポリシーグループのスループット制限の変更
- 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ポリシーグループの表示

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. QoSポリシーグループ名の横にある展開ボタン ( ) をクリックすると、▼そのポリシーグループに関する詳細が表示されます。
4. [表示]メニューで、その他のいずれかのオプションを選択して、アダプティブQoSポリシーグループまたは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ポリシーグループをすべて表示します。

## 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与えることなくポリシーグループに他のボリュームを追加できるかどうかを判断するのにも役立ちます。

アダプティブQoSポリシーとUnified Managerパフォーマンスサービスレベルポリシーの場合は、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できます。

### 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。

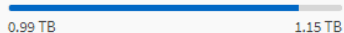
Performance : Traditional QoS Policy Groups ビューがデフォルトで表示されます。

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てください。それ以外の場合は、その他のいずれかの[表示]オプションを選択して、アダプティブQoSポリシーグループまたはUnified Managerのパフォーマンスサービスレベルで作成されたQoSポリシーグループをすべて表示します。
3. 目的のQoSポリシーで、QoSポリシーグループ名の横にある展開ボタン ( ) をクリックして▼詳細を表示します。

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

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
<b>Details</b> Allocated Capacity  0.99 TB / 1.15 TB Associated Objects <span style="border: 1px solid red; padding: 2px;">2 Volumes</span> <span style="border: 1px solid red; padding: 2px;">0 LUNs</span> 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]リンクをクリックすると、このQoSポリシーを使用しているオブジェクトが表示されます。

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リストでソートされて表示されます。

## 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の表示

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。

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ポリシーに対応する[QoS]ページが表示されます。

5. QoSポリシーグループの詳細な設定を表示します。

6. QoSポリシーグループ名の横にある展開ボタン ( ) をクリックすると、▼そのポリシーグループに関する詳細が表示されます。

## パフォーマンスグラフでの同じQoSポリシーグループ内のボリュームまたはLUNの比較

同じQoSポリシーグループ内のボリュームとLUNを表示し、1つの[IOPS]、[MBps]、または[IOPS/TB]グラフでパフォーマンスを比較して問題を特定できます。

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を次の表に示します。

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

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つの方法でQoSポリシーが表示されます。

ポリシーのタイプ	機能	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可能	「(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で共有	「(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可能	「(QoS アダプティブ)」を表示します。

次の図は、カウンタチャートでの3つのオプションの表示例を示しています。



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]グラフにパフォーマンスデータが表示されるのは、ボリュームで使用されている論理容量が128GB以上の場合だけです。選択した期間に使用済み容量が128GBを下回る期間があると、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]でのワークロードのQoS最小値と最大値の設定の表示

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。最大スループットを設定すると、競合するワークロードがシステムリソースに与える影響が制限されます。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。最小スループットの設定は、ONTAP 9.2以降のソフトウェアを実行しているシステム、AFFシステムでのみ使用でき、現時点ではIOPSに対し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ではなくIOPS/TBが使用されます。これらのポリシーは、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。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 イベントが表示されても、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可能性があります。

### 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	操作
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。
IOPSの下限 (QoSの最小値) 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。

状況	操作
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。

横の点線は、ONTAPで設定された最大スループットまたは最小スループットを示します。QoS値の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とMBpsの具体的な値をQoS設定と比較して表示するには、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確認します。

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の情報を使用したパフォーマンスの管理

**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て表示した場合、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の利用率が最大になるポイントは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ancing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状況を正確に判断できます。

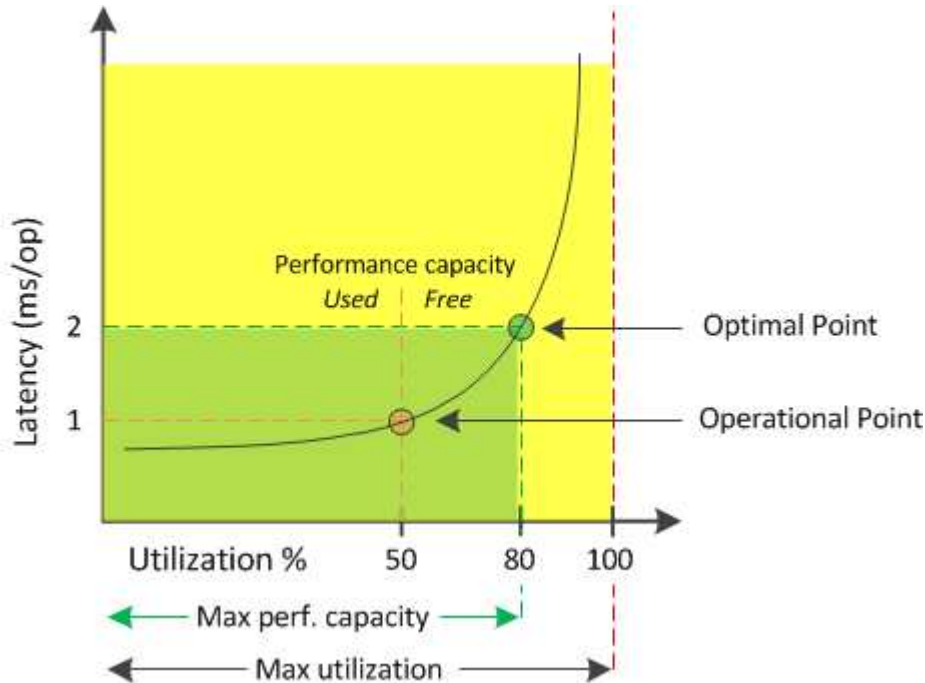
### 使用済みパフォーマンス容量とは

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の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利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ついて物理リソースで利用可



能な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。そのため、このアグリゲートにボリュームや LUN を追加して、システムをより効率的に使用することができます。

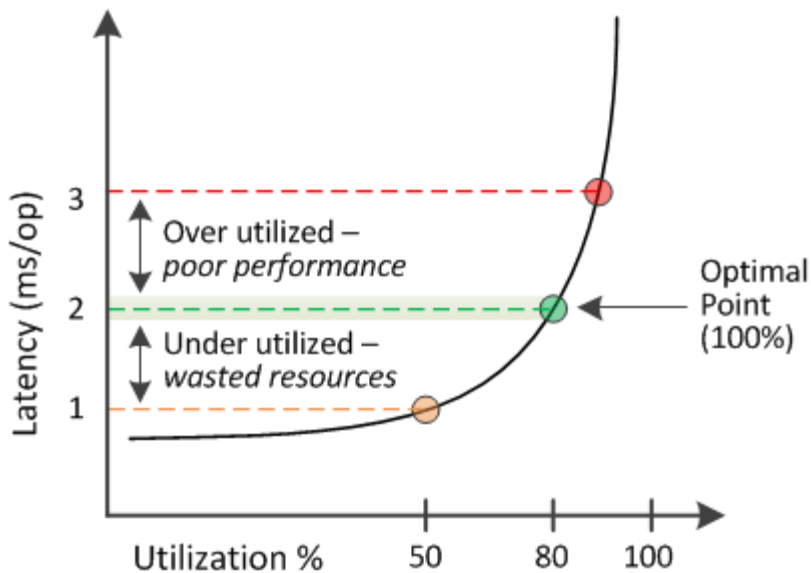
パフォーマンス容量にはレイテンシへの影響があるため、使用されるパフォーマンス容量カウンタは「利用率」カウンタよりも大きい値になることが予想されます。たとえば、ノードまたはアグリゲートの使用率が 70% の場合、レイテンシの値に応じて、パフォーマンス容量の値が 80~100% の範囲になることがあります。

ただし、場合によっては、[Dashboard] ページの使用率カウンタの方が高くなる場合があります。これは、ダッシュボードでは各収集期間の現在のカウンタ値が更新され、Unified Manager ユーザー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は表示されないためです。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の効率を高めるため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ており、現在の運用ポイントがわかる3つの領域を色付きの点で示しています。



- 使用済みパフォーマンス容量が100%であることが最適ポイントです。

この時点でリソースが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の割合が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ています。

新しいワークロードをリソースに追加しないでください。既存のワークロードの再配置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、リソースが効果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。割合の上限はありませんが、リソースの利用率が高すぎる場合は、通常110%から140%の範囲になります。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、リソースが上限に達する前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。

ノードで提供できる合計IOPSは、CPUの数、CPUの速度、RAMの容量など、ノードの物理特性によって決まります。アグリゲートで提供できる合計IOPSは、ディスクの物理プロパティ（SATA、SAS、SSDディスクなど）に基づいて決まります。

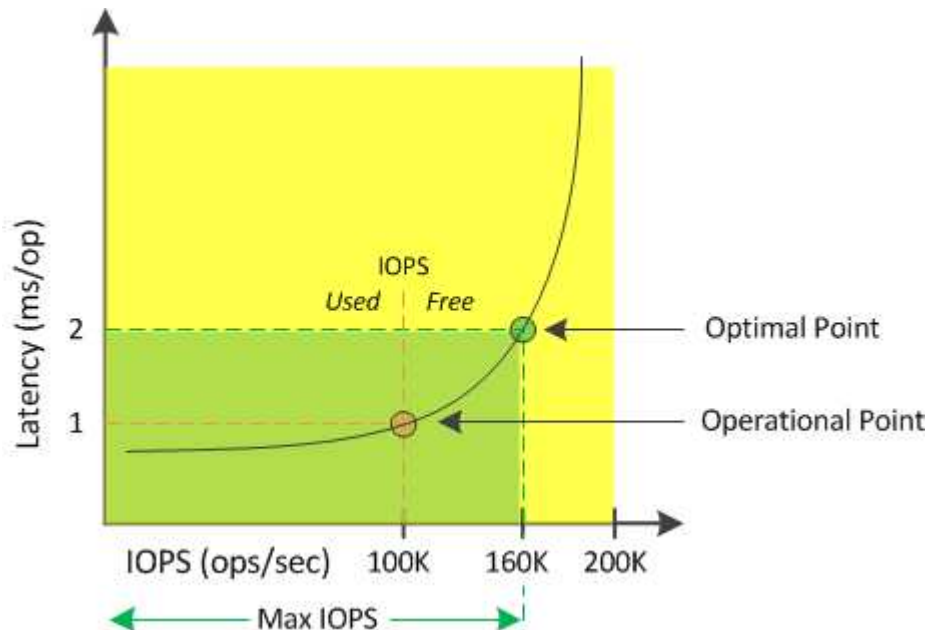
アグリゲート内のすべてのボリュームの合計IOPSがアグリゲートの合計IOPSと一致しないことがあります。これについては、次のナレッジベースの記事で説明しています。[KB"アグリゲート内のすべてのボリュームのIOPSの合計がアグリゲートのIOPSと一致しないのはなぜですか。"](#)

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しますが、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ペアで使用している場合、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あることを意味します。ただし、この値では、それらのノードに導入できるワークロードの数は可視化されません。[Available IOPS]カウンタに、使用可能なIOPSはFAS8060では500、FAS2520では100と表示されることがあります。

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。



リソースが提供できる最大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）のときのIOPSの数です。運用ポイントから、このノードの現在のIOPSは10万、レイテンシは1.0ミリ秒/処理であることがわかります。ノードからキャプチャされたUnified Managerの統計によると、ノードの最大IOPSは160Kであり、60Kの空きIOPSまたは使用可能なIOPSがあることがわかります。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最小限のリソースについては、一般的なワークロードを想定してCPUコアあたりのIOPSが約4、500であると仮定して、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にないためです。

## 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、または単一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、[パフォーマンス上位]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。

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used ↓↑	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
✓	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
✓	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
✓	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
✓	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
✓	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
✓	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
✓	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
✓	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS
⚠	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS

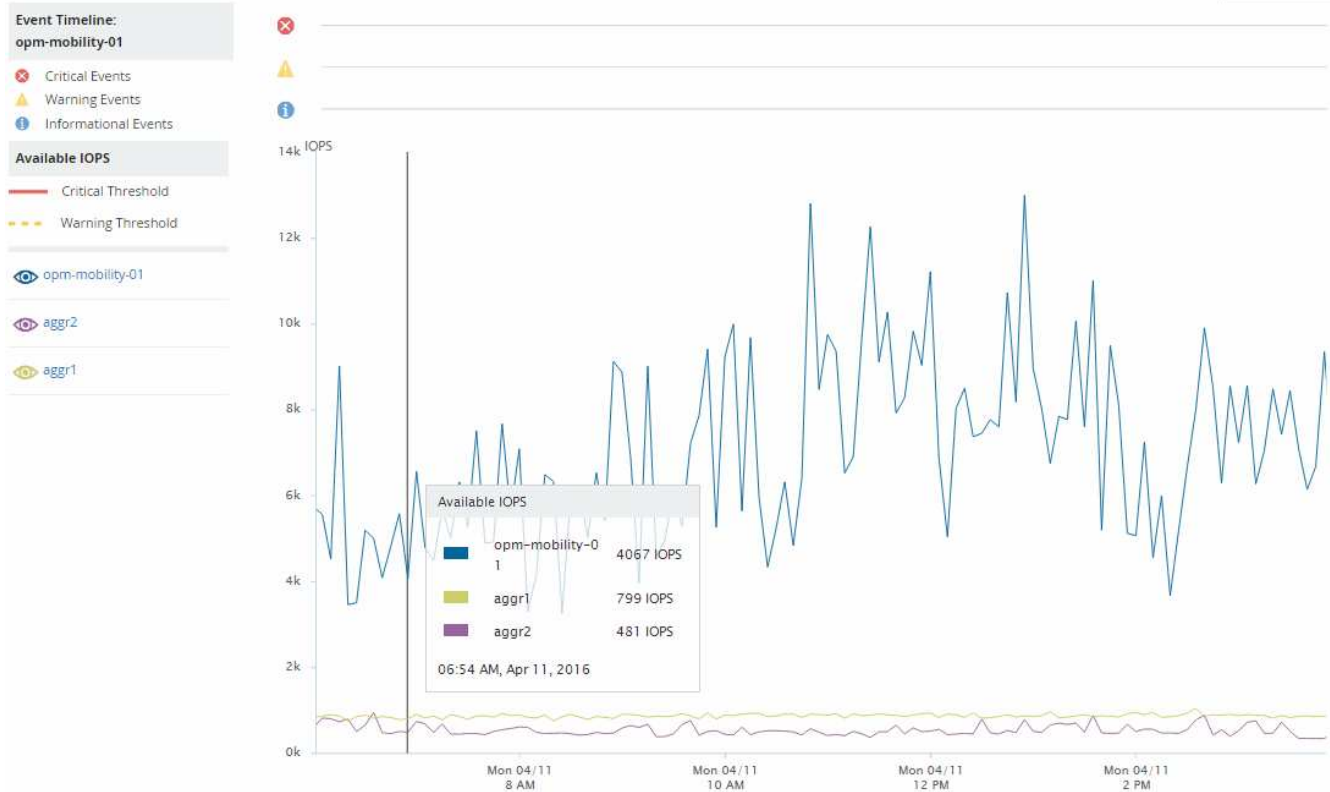
使用済みパフォーマンス容量のカウンタを監視すると、次の項目を特定できます。

- クラスタ上に使用済みパフォーマンス容量の値が高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大きいノードまたはアグリゲートの[レイテンシ]カウンタと[利用率]カウンタの値
- HAペアのいずれかのノードで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ビジーなボリュームと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の値を監視したり、単一のノードまたはアグリゲートの詳細を表示したりできます。

使用可能なIOPSの値は、ノードおよびアグリゲートの[パフォーマンスインベントリ]ページと[パフォーマンスエクスプローラ]ページ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プ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。



[Available IOPS]カウンタを監視すると、次の情報を特定できます。

- 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できる場所を判断するのに役立ちます。
- 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する必要がある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ビジーなボリュームと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

[パフォーマンスエクスプローラ]ページで、ノードおよびアグリゲートの使用済みパフォーマンス容量グラフを表示できます。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。



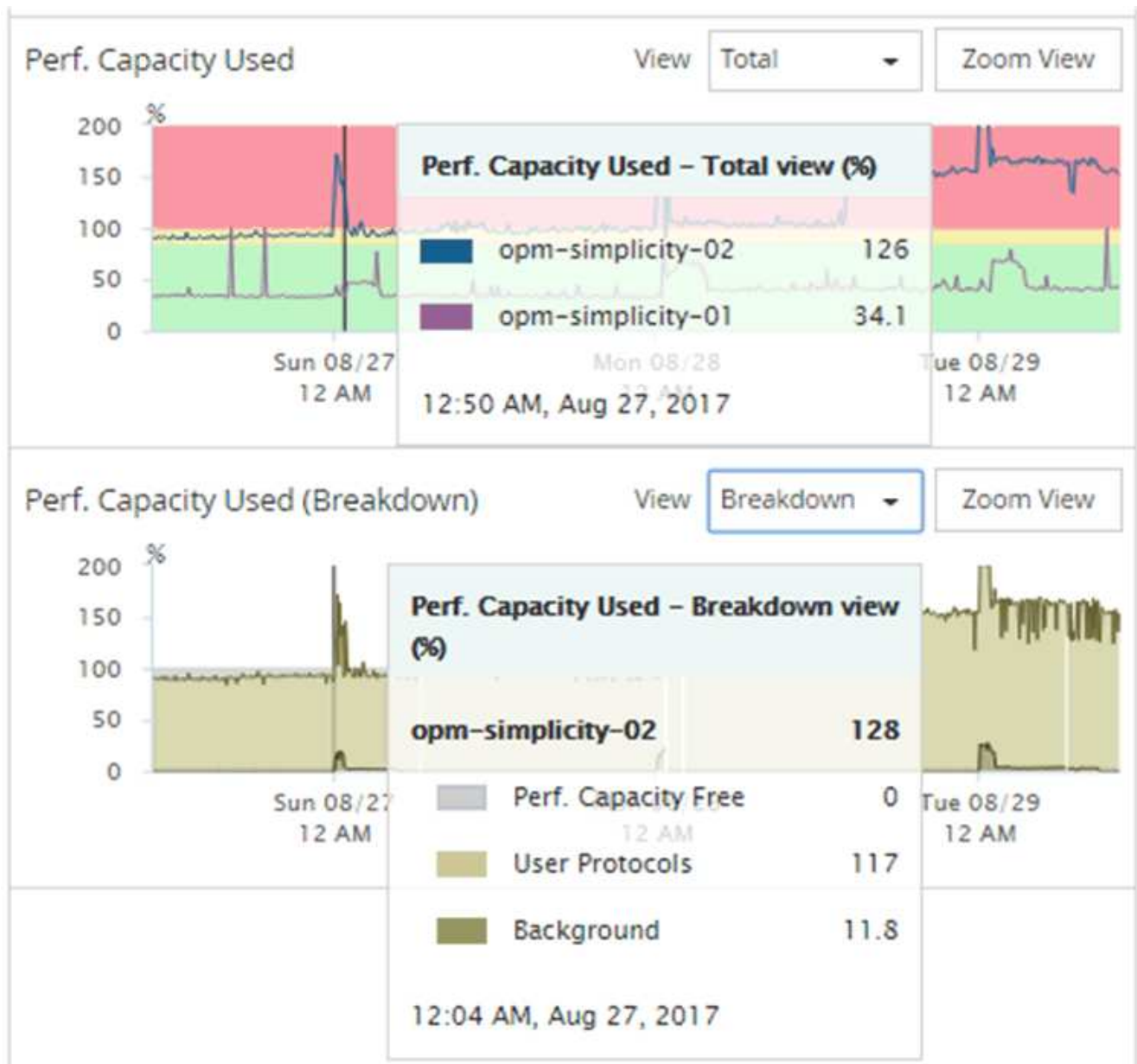
システムとデータの管理に関連する一部のバックグラウンドアクティビティはユーザワークロードとして識別され、ユーザプロトコルに分類されるため、プロセスの実行時にユーザプロトコルの割合が人為的に高く表示されることがあります。通常、これらのプロセスは、クラスタの使用率が低い午前0時頃に実行されます。ユーザプロトコルアクティビティが午前0時頃に急増している場合は、その時点でクラスタバックアップジョブまたはその他のバックグラウンドアクティビティが実行されるように設定されているかどうかを確認してください。



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. グラフが表示されるまで下にスクロールします。

標準グラフには、最適な範囲内のオブジェクト（黄色）、利用率の低いオブジェクト（緑）、利用率の高いオブジェクト（赤）が表示されます。内訳グラフには、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。

このようにして、複数のカウンタグラフを別々のウィンドウで開き、同じ期間の使用済みパフォーマンス容量の値とIOPSまたはMBpsの値を比較できます。

## 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一方のノードを宛先とする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実行したときの合計パフォーマンス容量は、障害が発生したノードによって多少異なる可能性があります。

LUNやボリュームのしきい値を定義する際に、使用済みパフォーマンス容量の条件をセカンダリ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、ボリュームまたは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を使用すると、期間全体にわたって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]カウンタを使用したパフォーマンスの管理

通常、組織は、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ながら、ピーク時の需要に対応するためにパフォーマンス容量を追加で確保したいと考えています。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、取り引き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。このような企業では、使用済みパフォーマンス容量のしきい値を70<sub>80%</sub>の範囲に設定する必要があります。マージンが小さい製造企業では、ITコストをより適切に管理するためにパフォーマンスを犠牲にしても構わない場合、確保するパフォーマンス容量を少なくすることを選択することができます。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<sub>95%</sub>の範囲に設定する可能性があります。

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、[イベントインベントリ]ページにイベントを追加します。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。これらのイベントは、ノードやアグリゲ

ート内でワークロードの移動や変更を行う際に必要な指標としても使用できます。

## [Node Failover Planning]ページの概要と使用方法

[Performance/Node Failover Planning]ページでは、そのノードのハイアベイラビリティ (HA) パートナーノード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を見積もります。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している場合は、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ための対処を検討できます。
- 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与える影響を見積もって、タスクを実行する最適なタイミングを判断することができます。

## [Node Failover Planning]ページを使用した対処方法の決定

[Performance/Node Failover Planning]ページに表示される情報を基に、フェイルオーバーによってHAペアのパフォーマンスが許容可能なレベルを下回ら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引き続き許容可能なパフォーマンスを提供できます。

## [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は、ノード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与える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 ヘエシには、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。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。

- 推定テイクオーバー

プライマリノードと同じ。このノードについて表示されるパフォーマンス統計には、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が表示されます。



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、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、パートナーノードの名前をクリックします。Performance/NodePerformance Explorer へエシが表示されたら、\* 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することができます。これにより、障害が発生したノードに応じて推定パフォーマンスがどのように変化するかを確認できます。

## 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に関係します。

- \* 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履歴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、ある時点でフェイルオーバーが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、利用率のグラフに、推定テイクオーバー ノードの2月8日午前11時の利用率が73%と表示されているとします。この時点でフェイルオーバーが発生していた場合、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、フェイルオーバーを開始する最適な時間を特定するのに役立ち、テイクオーバーノードに過剰な負荷がかかる可能性を最小限に抑えることができます。フェイルオーバーのスケジュールは、テイクオーバーノードの予測パフォーマンスが許容範囲内である場合にのみ設定できます。

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せん。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。グラフのカスタマイズ例を次に示します。

- 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]ページでのしきい値ポリシーの使用

ノードしきい値ポリシーを作成すると、フェイルオーバーによって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に低下する可能性がある場合に、[Performance/Node Failover Planning]ページで通知を受け取ることができます。

「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。

システム定義のしきい値ポリシーのイベントは、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に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/Node Failover Planning]ページに移動して、フェイルオーバーによるレイテンシの予測値を確認できます。

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場合は、しきい値を超えた最小期間を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。このポリシーは、HAペアを形成するノード1とノード2に適用できます。ノード1またはノード2のいずれかについて警告イベント通知を受信したら、そのノードの[Performance/Node Failover Planning]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への影響を評価できます。フェイルオーバーが発生した場合にテイクオーバーノードが過負荷にならないように対処することができます。ノードの使用済みパフォーマンス容量の合計が200%未満のときに対処すると、この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は許容できないレベルに達しません。

## [使用済みパフォーマンス容量の内訳]グラフを使用したフェイルオーバーの計画

[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。この情報は、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の問題が発生する可能性があるかどうかを判断するのに役立ちます。

内訳グラフには、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、およびシステムヘルスに関連する内部システムプロセスです。

この追加の詳細情報から、パフォーマンスの問題の原因がユーザアプリケーションのアクティビティとバックグラウンドのシステムプロセス（重複排除、RAID再構築、ディスクスクラビング、SnapMirrorコピーなど）

のどちらにあるかを判断できます。

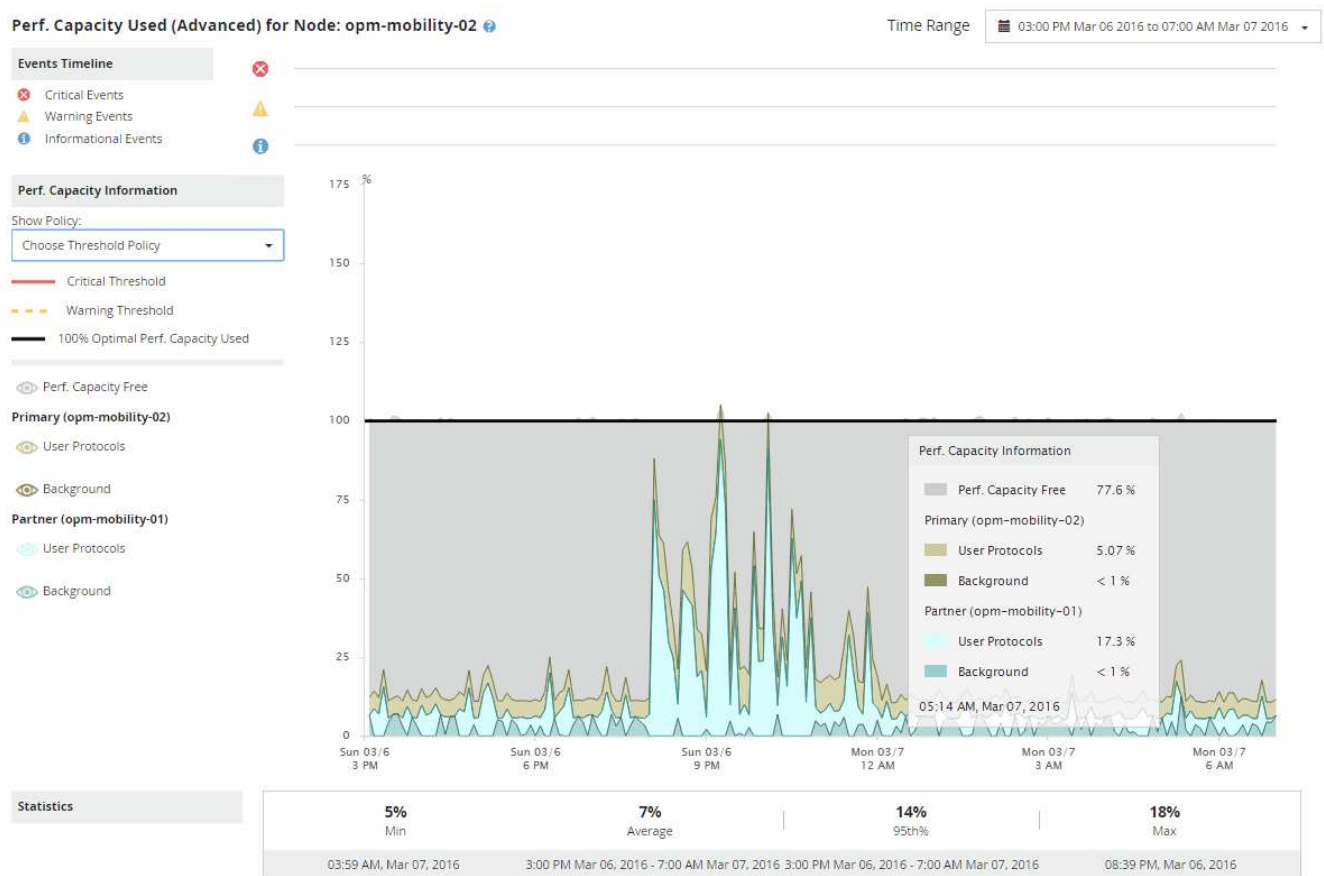
## 手順

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せん。

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。

## [Perf.Capacity Used (使用済み容量) の表示



5. 詳細グラフ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済みパフォーマンス容量の情報が表示されます。

使用済み空き容量の割合は、推定テイクオーバーノードで使用可能なパフォーマンス容量です。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、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場合は、空きパフォーマンス容量の割合が0

でないときにパートナーノードを停止する時間を選択してください。

## データの収集とワークロードパフォーマンスの監視

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、[Workload Analysis]ページおよび[Event details]ページに表示するI/O応答時間のレイテンシ予測を決定する必要があります。このアクティビティの収集中は、レイテンシ予測にワークロードアクティビティの変化がすべて表示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を反映して、より正確な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、監視対象のワークロードのパフォーマンス統計の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、完了までに約15日かかります。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な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、クラスタ上のワークロードアクティビティのみを監視します。アプリケーションやクライアント、アプリケーションとクラスタ間のパスは監視されません。

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) コピーです。(DPボリュームはユーザ生成のトラフィックについて監視されます)。
- オフラインデータクローンである。
- 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 \_ \*

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。次のプロセスが含まれます。

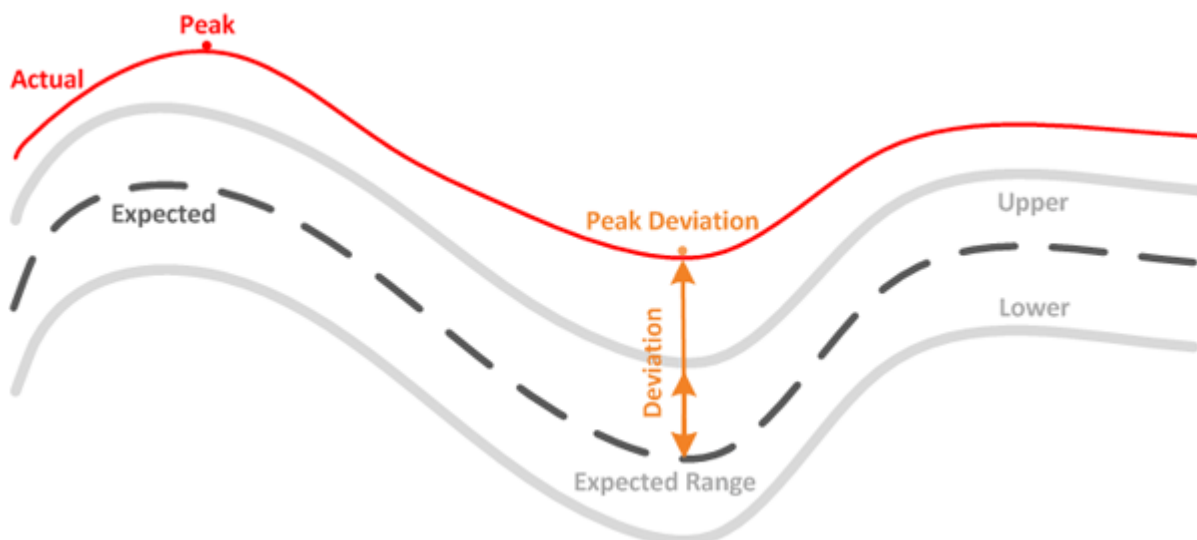
- ストレージ効率化（重複排除など）
- ディスクの健全性（RAIDの再構築、ディスククラビングなど）
- データレプリケーション（SnapMirrorコピーなど）
- 管理アクティビティ
- ファイルシステムの健全性（WAFLのさまざまなアクティビティなど）
- ファイルシステムスキャナ（WAFLスキャンなど）
- コピーオフロード（VMwareホストからオフロードされたStorage Efficiency処理など）
- システム健全性（ボリューム移動、データ圧縮など）
- 監視対象外のボリューム

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されているクラスタコンポーネントが競合状態にある場合にのみGUIに表示されます。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GUIで表示することはできません。

## ワークロード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して、ワークロードのパフォーマンスが高すぎるか低すぎるかを判断します。ワークロードのパフォーマンスが想定どおりでない場合、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値が赤で示されています。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	製品説明
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 style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <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。値が設定された制限値の100%を超えると、「&gt;100%」と表示されます。値が設定された制限の1%未満の場合は、1%未満と表示されます。</p> </div>
実際値	<p>特定の時点で測定された特定のワークロードのパフォーマンス値。</p>
偏差	<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 style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <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いことを示し、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高いことを示します。</p> </div>
期待値	<p>想定される値は、特定のワークロードの過去のパフォーマンスデータの分析に基づいています。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。</p>
レイテンシ予測（想定範囲）	<p>レイテンシ予測は、特定の時点で想定されるパフォーマンスの上限値と下限値を予測したものです。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が表示されます。実測値がパフォーマンスしきい値を超えると、Unified Manager は動的なパフォーマンスイベントをトリガーします。</p>
ピーク	<p>一定の期間に測定された最大値です。</p>
ピーク偏差	<p>一定の期間に測定された偏差の最大値です。</p>
キューの深さ	<p>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。</p>

測定	製品説明
利用率	ネットワーク処理、Data Processing、およびアグリゲートコンポーネントの場合、一定期間にワークロード処理を完了するためのビジー時間の割合。たとえば、ネットワーク処理またはData ProcessingコンポーネントがI/O要求を処理する時間の割合や、アグリゲートが読み取り要求や書き込み要求に対応する時間の割合が表示されます。
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 (MB/秒)。

## パフォーマンスの想定範囲とは

レイテンシ予測は、特定の時点で想定されるパフォーマンスの上限値と下限値を予測したものです。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が表示されます。実測値がパフォーマンスしきい値を超えると、Unified Managerは動的なパフォーマンスイベントをトリガーします。

たとえば、午前9時から午後5時までの通常の営業時間には、ほとんどの従業員が午前9時から午前10時30分までの間にEメールをチェックする場合があります。Eメールサーバへの需要の増加は、この間にバックエンドストレージでのワークロードアクティビティが増加することを意味します。従業員は、電子メールクライアントからの応答時間が遅いことに気付く場合があります。

午後12時から午後1時までのランチタイム、および午後5時以降の営業日の終わりには、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。通常、Eメールサーバの需要は減少し、バックエンドストレージの需要も減少します。また、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時以降に開始し、バックエンドストレージのアクティビティが増加するようにスケジュール設定することもできます。

ワークロードアクティビティの増減から数日間にわたる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。オブジェクトの実際のワークロードアクティビティが上限と下限の外側にあり、その外側にある期間がある場合は、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する必要があります。最小限必要なデータ収集には、ワークロードアクティビティで発生するすべての変更が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、ワークロードアクティビティの変化を反映して、より正確な動的なパフォーマンスしきい値を設定します。





システム時間が夏時間（DST）に切り替わると、監視対象のワークロードのパフォーマンス統計の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、完了までに約15日かかります。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な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では、レイテンシ予測を使用して監視対象のワークロードの典型的なI/Oレイテンシ（応答時間）アクティビティを表します。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超え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、パフォーマンスの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を設定します。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、または想定範囲外になったかを判断します。実際の値と想定値を比較することで、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。高ワークロードのアクティビティが長期間（たとえば数時間）にわたって継続した場合、Unified Managerはこれを正常なアクティビティとみなし、レイテンシ予測を動的に調整して新しい動的なパフォーマンスしきい値を作成します。

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。パフォーマンスイベントの分析中にイベントの数を最小限に抑えるために、Unified Managerは、アクティビティの少ないボリュームの処理数と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、処理あたり3.5ミリ秒（ms/op）が最低



で5.5ms/opです。ネットワークトラフィックの一時的な急増やクラスタコンポーネントの競合が原因で実際のレイテンシ（青）が突然10ms/opまで上昇した場合、レイテンシ予測を上回り、動的なパフォーマンスしきい値を超えます。

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以上のままである場合は、イベントを解決するための対処が必要に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。

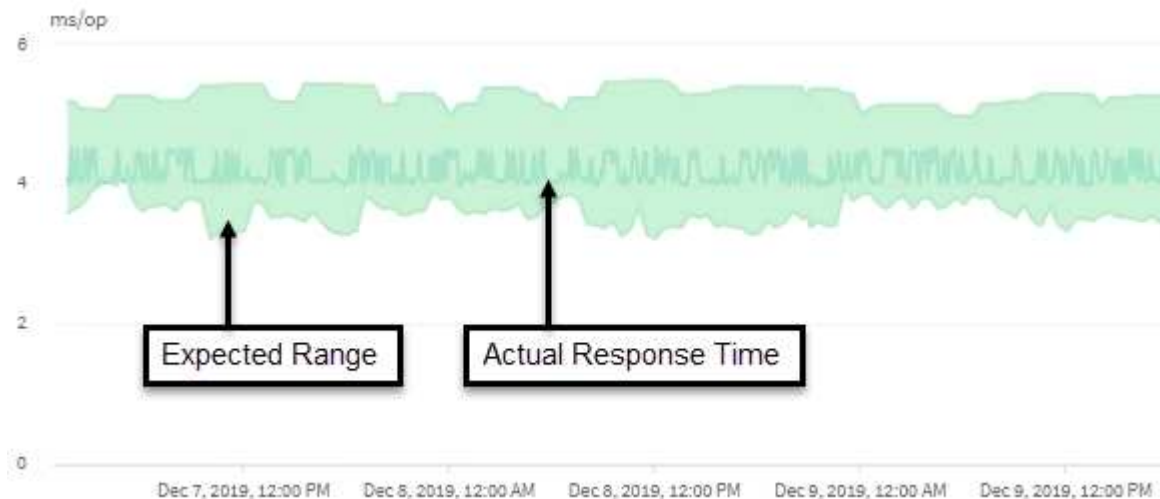
高レイテンシは、アプリケーションからクラスタ上のボリュームへの要求に通常よりも時間がかかっていることを意味します。高レイテンシの原因は、1つ以上のクラスタコンポーネントでの競合が原因で、クラスタ自体にある可能性があります。高レイテンシは、ネットワークのボトルネックなど、クラスタ外の問題、アプリケーションをホストしているクライアントの問題、アプリケーション自体の問題が原因で発生することもあります。



Unified Managerは、クラスタ上のワークロードアクティビティのみを監視します。アプリケーションやクライアント、アプリケーションとクラスタ間のパスは監視されません。

クラスタに対する処理（バックアップの作成や重複排除の実行など）も、他のワークロードと共有しているクラスタコンポーネントへの負荷を増大させるため、レイテンシの上昇につながる可能性があります。実際のレイテンシが想定範囲（レイテンシ予測）の動的な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）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、個々のプロセス（読み取り要求や書き込み要求など）のアクティビティを全体的なレイテンシ統計と比較できます。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ときは、レイテンシの統計を使用して、イベントの原因がクラスタの問題かどうかを判断できます。また、イベントに関連しているワークロードのアクティビティや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）は緑で表示されています。

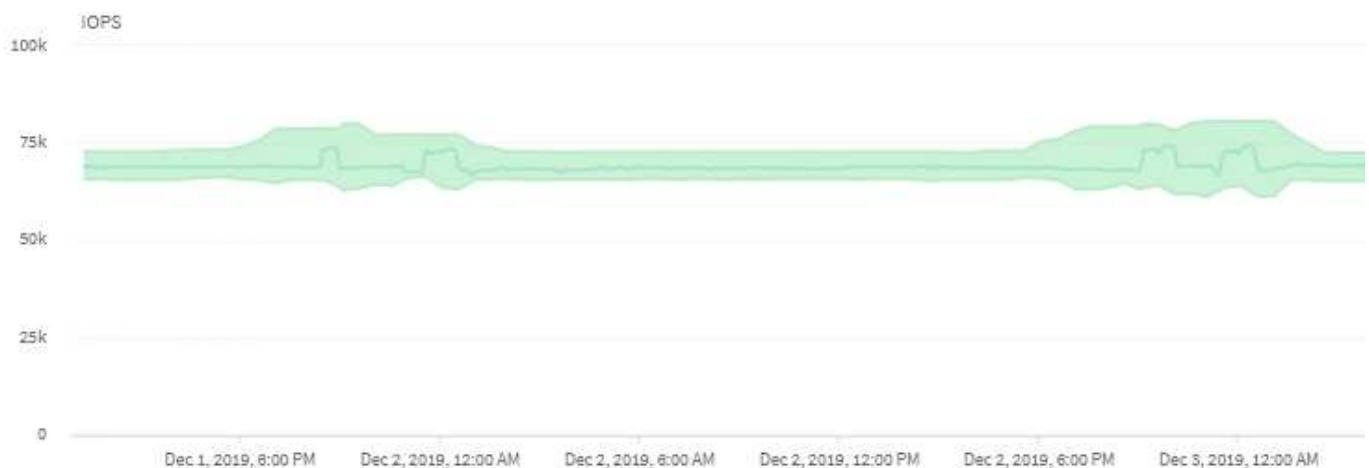


Unified Managerでデータを収集できなかった場合は、青い線が途切れている可能性があります。これは、クラスタまたはボリュームに到達できなかったか、その時間にUnified Managerがオフになっていたか、収集に5分以上かかっていた可能性があります。

## クラスタ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）は、クラスタ上のユーザ定義および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を表します。IOPSの統計は、クラスタプロセス（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るかどうか、または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る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ときは、IOPSの統計を使用して、パフォーマンスイベントの原因がクラスタの問題であるかどうかを判断できます。パフォーマンスイベントの原因となった可能性がある特定のワークロードアクティビティを特定できます。IOPSは1秒あたりの処理数（処理数/秒）で測定されます。



この例はIOPSグラフを示しています。実際の処理の統計が青い線、処理のIOPS予測が緑で表示されます。



クラスタが過負荷状態の場合、Unified Managerにというメッセージが表示されることがあり`Data collection is taking too long on Cluster *cluster\_name*`ます。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もありません。

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、データがNVRAMに書き込まれ、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。

次の画面で、対応するLUNとボリュームのワークロードを分析することで、MetroCluster構成内のいずれかのクラスタのスループットを確認できます。結果はクラスタで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、次の操作を行います。

- \* [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に関連したShark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ように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（レイテンシが高い）ストレージオブジェクトを特定するのに役立ちます。同時に発生した他の健全性イベントと一緒に確認することで、応答時間の低下の原因となった、または原因となった問題を特定できます。

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、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インフラの障害やエラー、またはクラスタリソースを過剰に消費しているワークロードに起因するパフォーマンスの問題。これらのイベントの原因は、時間が経つと修復される単純な問題や、修理や設定の変更によって解決できる単純な問題である可能性があります。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。

これら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ました。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外であるため、重大な重大度に達しないよ

うに監視する必要があります。この重大度のイベントではサービスは停止しないため、すぐに対処する必要はありません。

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が変更された場合は、重大度タイプが「情報」のイベントが生成されます。

情報イベントは、設定の変更を検出すると、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の追加"](#)

## Unified Managerで検出される構成の変更

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。[Performance Explorer]ページに変更イベントアイコン ( ) が表示され、変更が検出された日時が示されます。

[パフォーマンスエクスプローラ]ページと[ワークロード分析]ページのパフォーマンスグラフで、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とほぼ同じ時間に変更が検出された場合は、変更が原因でイベント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場合。

ポリシーグループ制限を変更するとレイテンシ (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、[イベントセットアップ]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している可能性がある状況を特定します。

これは、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て、24時間以上にわたって30%のしきい値を超えていないノードがないかどうかを確認することで行われます。これは警告イベントです。

- \* クラスタ容量の不均衡 \*

1つのアグリゲートの使用済み容量がクラスタ内の他のアグリゲートよりもはるかに多く、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、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 \*

単一のノードが運用効率の上限を超えて稼働しており、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%を超えると、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おり、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の再同期中やディスクスクラビング処理中にエラーが検出された場合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ー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。このような状況では、アグリゲート内のディスクの利用率が30分以上95%を超えているアグリゲートが検索されます。この複数条件ポリシーは、次の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。

ディスクでバックグラウンドで実行されるメンテナンス作業には、ディスクの再構築、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インターコネクタに通信のボトルネックはありますか。
- 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%を超えている場合のみ、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過去1時間のうちに30%の時間が経過したワークロードが検索されます。

## 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 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割り当てられているワークロードが1つだけの場合、割り当てられているQoSポリシーグループで定義されている最大スループットの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検出されます。

複数のワークロードで1つのQoSポリシーを共有している場合は、ポリシーに含まれるすべてのワークロードのIOPSまたはMBpsが加算され、その合計がしきい値を超えていないかが確認されます。

- \* 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。

アダプティブQoSポリシーで定義されている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がないかどうかを確認します。



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レベルのパフォーマンスを提供できません。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が生じ、レイテンシが増大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にしている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が大きい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、同じクラスタコンポーネントについて5分以内に再発生し、アクティブな状態のままのイベントです。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、およびボリューム、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つのボリュームが同時に複数のイベントに関与している可能性があります。

## 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）を示します。自己修復または解決されていないイベントです。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。

### • \* 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。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なくなりました。

## イベント通知

イベントは[ダッシュボード]ページおよびユーザインターフェイスの他の多くのページに表示され、それらのイベントに関するアラートが指定したEメールアドレスに送信されます。[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、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確認できます。

## イベントの相互作用

[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。

同じ期間に複数のイベントがある場合は、イベントの数がメッセージに表示されます。

- 単一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など、イベントの詳細情報を示す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。同じ期間に複数のイベントがある場合は、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]ページでのワークロード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AとワークロードBの2つのワークロードが含まれているとします。ワーク

ロードAのレイテンシ予測は5<sub>10</sub>ミリ秒/処理 (ms/op) で、実際のレイテンシは通常約7ミリ秒/処理です。ワークロードBのレイテンシ予測は10<sub>20</sub>ms/opで、実際のレイテンシは通常約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て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、ワークロードAの想定値からパフォーマンスしきい値を超える値までの偏差は約33ms/op、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に急上昇しましたが、ワークロードAの方がレイテンシの偏差が33ms/opに大きくなるため、パフォーマンスへの影響は大きくなりました。

[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。レイテンシの赤いドット (●) は、Victimワークロードがパフォーマンスしきい値を超え、それに伴うレイテンシへの影響を示します。赤い点はレイテンシの偏差の大きい方を示しており、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競合する理由

クラスタコンポーネントが競合状態になった場合のクラスタパフォーマンスの問題を特定できます。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を解消するには、パフォーマンスを通常のレベルに戻すために、ワークロードを減らすか処理能力を高める必要があります。Unified Managerはワークロードのパフォーマンスの収集と分析を5分間隔で行うため、クラスタコンポーネントの利用率が一貫して高い場合にのみ検出します。5分インターバルの間に短時間しか続かない過剰使用の一時的な急増は検出されません。

たとえば、ストレージアグリゲート上の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しているために、ストレージアグリゲートが競合状態になっている可能性があります。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には、いくつかの手順を実行します。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て、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軽減するなどです。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て、ワークロードが調整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 \*

クラスタ上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は、プロトコルレイヤでの長い待機時間が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。

### • \* 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処理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。

オールSANアレイクラスタをアクティブ/アクティブ構成で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、ノードで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）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は、ポリシーグループ内のすべてのワークロードがスループット制限によって調整されており、1つ以上のワークロードのレイテンシに影響しています。

- \* 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。

- \* データ処理 \*

クラスタとワークロードを含むストレージアグリゲート間の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。Data Processingを処理するノードは、イベント検出後に変更された可能性があります。Data Processingコンポーネントが競合状態にある場合は、Data Processingノードでの高利用率が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。

- \* 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を表します。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ために使用されます。MetroClusterコンポーネントが競合状態にある場合は、ローカルクラスタのワークロードによる高書き込みスループットまたはリンクの健全性の問題が、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、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は、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。アグリゲートは、HDDのみ、HDDとSSD（Flash Poolアグリゲート）、またはHDDとクラウド階層（FabricPoolアグリゲート）で構成されます。「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が格納されているクラウド階層間の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トに関連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は、SnapMirror同期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にすることができます。

ロール	製品説明
被害者	クラスタコンポーネントを過剰に消費している他のワークロード (Bully) のためにパフォーマンスが低下している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だけです。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。
Bully	クラスタコンポーネントの過剰な消費によって他のワークロード (Victim) のパフォーマンスが低下するユーザ定義またはシステム定義のワークロード。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と比較して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、アグリゲートやネットワーク用のCPUやData Processingなど、クラスタコンポーネントの多くを共有できます。ボリュームなどのワークロードが、クラスタコンポーネントの使用量を増やしてワークロードの要求を効率的に満たせなくなると、そのコンポーネントは競合状態になります。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はBullyです。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他のワークロードが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。ワークロードが自身の影響源になる可能性があります。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ている場合、そのワークロードも含めて、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BullyまたはVictimであるワークロードは、ロールが変更されたり、イベントに参加しなくなったりする可能性があります。

## 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を使用すると、多数のパフォーマンスカウンタと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、[イベントセットアップ]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の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には、次の手順を実行します。

- ストレージオブジェクトの選択
- 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の選択
- 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する
- カウンタが上限を超えなければならない期間を指定する

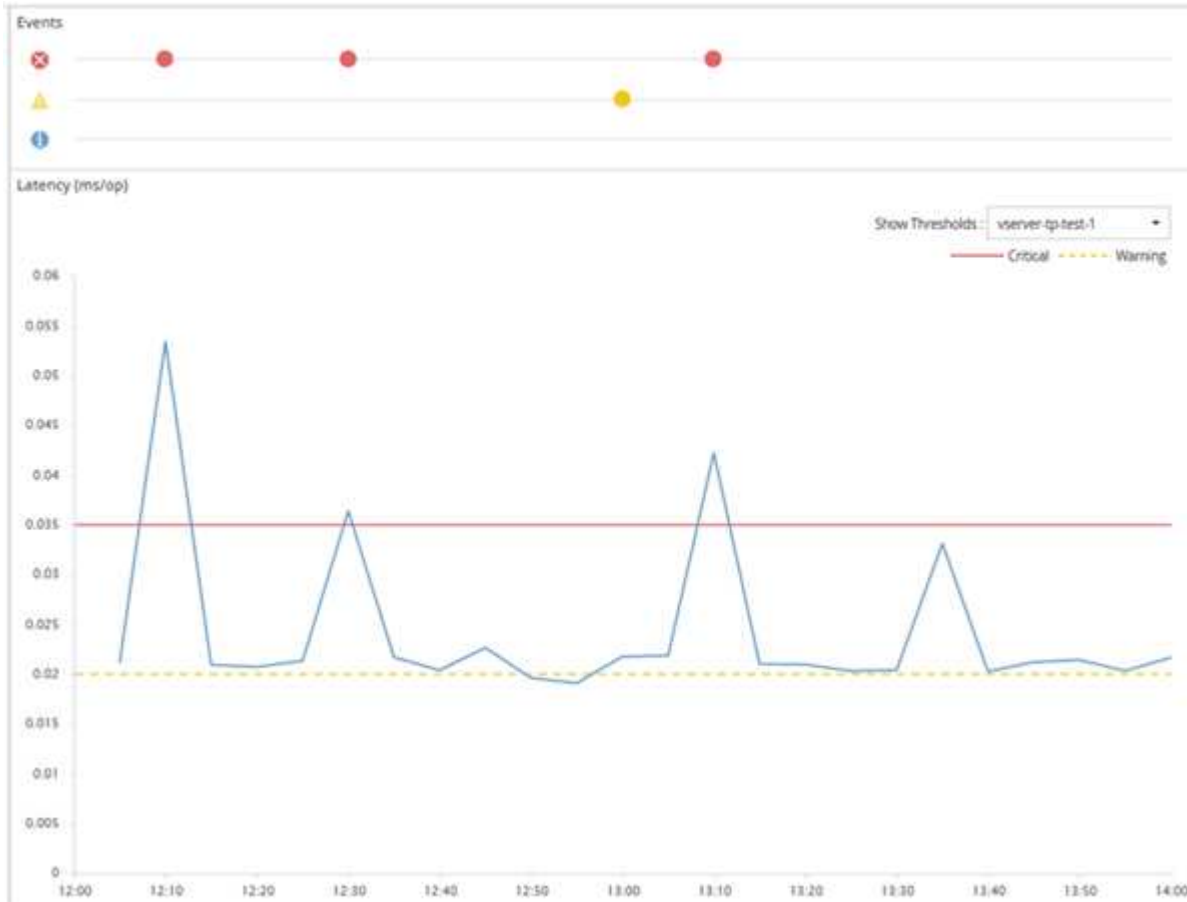


たとえば、ボリュームのIOPSが10分間連続で1秒あたり750件の処理数を超えたときに重大イベントの通知を受け取るように、ボリュームに対してパフォーマンスしきい値ポリシーを設定できます。同じしきい値ポリシーで、IOPSが10分間にわたって1秒あたり500件の処理数を超えた場合に警告イベントを送信するように指定することもできます。



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に警告しきい値（黄色のアイコン）に違反し、12:10、12:30、1:10に重大しきい値（赤のアイコン）に違反しています。



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が制限値を下回った場合は、その後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、イベントが生成される前に2つのパフォーマンスカウンタが最大値を超えるようにする組み合わせ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では、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、表に定義されているしきい値ポリシーを使用すると、次のようになります。

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	そしたら...
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。
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人以上のEメール受信者に送信したり、SNMPトラップをトラップ受信者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。警告または重大のしきい値ポリシーの違反に応じて、固有のアクションを定義できます。

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あとは、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、そのポリシーに対する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の終了時刻は継続的に更新され、イベントが継続中であることが示されます。

しきい値イベントは重大度とポリシー定義に関連する情報をキャプチャまたはフリーズします。これにより、今後しきい値ポリシーが変更された場合でも、イベントに固有のしきい値情報が表示されます。

## しきい値を使用して追跡できる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に対してしきい値を設定できます。他にも、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るカウンタがあります。

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	製品説明
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/秒	このクラスタとの間で転送される1秒あたりの平均データ量 (MB)	ノード
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/秒
このノードとの間で転送される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の平均利用率。	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/秒	このアグリゲートとの間で転送される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利用率
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/秒
このSVMとの間で転送される1秒あたりの平均データ量 (MB)	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

ストレージオブジェクト	パフォーマンスカウンタ	製品説明
MB/秒	このボリュームとの間で転送される1秒あたりの平均データ量 (MB)	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
LUN	IOPS	LUNで処理される1秒あたりの平均入出力処理数
MB/秒	このLUNとの間で転送される1秒あたりの平均データ量 (MB)	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/秒	このネームスペースとの間で転送される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
帯域幅の使用量	ポートの使用可能な帯域幅の平均使用率	MB/秒
このポートとの間で転送される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/秒

## 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のは、一部のパフォーマンスカウンタだけです。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、イベントが生成される前に両方のパフォーマンスカウンタが最大値を超えている必要があります。

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	ボリューム IOPS
ボリューム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
LUN レイテンシ	LUN IOPS
LUN MBps	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



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属性またはアグリゲート属性のいずれかが含まれている場合、ポリシーは FlexGroup ボリュームに適用されず、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配置できるためです。

## ユーザ定義のパフォーマンスしきい値ポリシーの作成

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します。イベント通知から、クラスタでパフォーマンスの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、[パフォーマンスしきい値ポリシーの作成]ページでしきい値の値を入力します。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せん。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	クリックする項目
新しいポリシーを作成する	・ 作成 *。
既存のポリシーのクローンを作成する	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。

- ストレージオブジェクトのタイプを選択し、ポリシーの名前と説明を指定します。
- 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。両方のタイプの境界を定義する必要はありません。

- 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含めるには、両方のカウンタが制限値を超えていないとしきい値を超えてイベントが報告されません。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。

- 制限値に違反してイベントを送信する期間を選択します。

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。

[パフォーマンスしきい値]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。また、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、その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へのパフォーマンスしきい値ポリシーの割り当て

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場合に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つだけ適用できます。

ストレージオブジェクトごとに最大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ときに、いずれかのオブジェクトにすでに最大数のポリシーが割り当てられている場合、Unified Managerは次の処理を実行します。

- 選択したオブジェクトのうち、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。
- ポリシーの最大数に達したオブジェクトを無視します。
- 一部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	クリックする項目
単一のオブジェクト	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をクリックし、*[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をクリックし、*[すべてのオブジェクトを選択]*を選択します。

ソートとフィルタの機能を使用してインベントリページのオブジェクトリストを絞り込むと、多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適用されてい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ます。また、このオブジェクトとポリシーにアラートを設定できるように、[Alerting]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アラートをEメールまたはSNMPトラップとして送信する場合は、[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の表示

[パフォーマンスしきい値]ページでは、現在定義されているすべてのパフォーマンスしきい値ポリシーを表示できます。

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、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、フィルタと検索のメカニズムを使用して、インベントリリストに表示するしきい値ポリシーのリストを絞り込みます。

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、表示されるボタンを使用して、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、削除することもできます。

### 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の編集

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の受信数が多すぎる、または少なすぎる場合に役立ちます。

- 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。

ポリシーの名前や既存のしきい値ポリシーで監視され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。

[Edit Performance Threshold Policy]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。

[パフォーマンスしきい値]ページに戻ります。

変更が保存されると、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ですぐに更新されます。

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対して設定

されているアラート設定を確認できます。

## ストレージオブジェクトからのパフォーマンスしきい値ポリシーの削除

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1つの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	操作
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	列ヘッダーのをクリックし <input type="checkbox"/> 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ポリシーの詳細が表示され、適切なポリシーが選択され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変更が適用されます。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アクティブなイベントがある場合、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。

しきい値が適用されているカウンタを[Counter Charts Detailed View]で表示すると、重大しきい値と警告しきい値の線に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ときに履歴データを表示した場合でも、このページには元のしきい値の設定は表示されません。



[Counter Charts Detailed View]には古いしきい値の設定は表示されないため、現在のしきい値の線の下に履歴イベントが表示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でも、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です。

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場合など、しきい値ポリシー（組み合わせポリシー）のセカンダリカウンタ条件が存在する場合は、ボリュームまたはLUNの移動先である新しいアグリゲートまたはノードにセカンダリカウンタ条件が適用されます。

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なイベントが発生すると、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を実行すると、ONTAPは情報変更イベントを送信します。[パフォーマンスエクスプローラ]ページと[ワークロード分析]ページの[イベントタイムライン]に変更イベントアイコンが表示され、移動処理が完了した時刻が示されます。



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や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、手動の移動処理と同じ方法で保持されます。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分間の設定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移動に関するパフォーマンス統計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

コマンドを使用してあるノードから別のノードにアグリゲートを移動した場合は aggregate relocation



start、単一のしきい値ポリシーと組み合わせの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スイッチオーバー時のしきい値ポリシーの機能

MetroCluster構成でクラスタ間を移動したオブジェクトの場合、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。必要に応じて、パートナークラスタに移動したボリュームとLUNにしきい値ポリシーを適用できます。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の分析

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）が廃止状態か、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の表示

[イベント管理]インベントリページを使用して、Unified Managerで監視し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。

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、[イベントの詳細]ページでイベント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、\* 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の分析

ユーザ定義の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（アグリゲートやボリュームなど）のパフォーマンスカウンタが、ポリシーに定義されたしきい値を超えたことを示します。これは、クラスタオブジェクトでパフォーマンスの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]ページでは、パフォーマンスイベントを分析し、必要に応じて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発生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. ポリシーの名前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ず。

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、違反して重大イベントまたは警告イベントとみなされるカウンタの値、およびこの値を超え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対処が必要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してそのオブジェクトのエクスプローラページを表示します	このページでは、オブジェクトの詳細を表示し、このオブジェクトを他の同様のストレージオブジェクトと比較して、他のストレージオブジェクトに同時にパフォーマンスの問題が発生していない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の問題が発生していないかどうかを確認できます。
クラスタ名をクリックして[Cluster Summary]ページを表示します。	このページでは、この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、同じ時間に他のパフォーマンスの問題が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の分析

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パフォーマンスカウンタまたは一連のパフォーマンスカウンタがシステム定義のポリシーのしきい値を超えたことを示します。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の問題が発生しています。

[イベントの詳細]ページでは、パフォーマンスイベントを分析し、必要に応じて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 の各システムでは有効になりません。

## 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発生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。それ以外のタイプのシステム定義のイベントについては、カウンタチャートに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を使用すると、多くのワークロードがレイテンシの影響を受ける前に、潜在的なパフォーマンスの問題を修正できます。

- 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発生している必要があります。

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イベントが発生しても、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可能性があります。

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。

- ワークロードの新しいポリシーグループの作成
- 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のワークロードの移動
- ポリシーグループのスループット制限の変更
- 別のアグリゲートまたはノードへのワークロードの移動

### 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や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。このように配置すると、ワークロードが最大QoSに達したときにレイテンシに最も影響しているクラスタコンポーネントを確認できます。

共有QoSポリシーのイベントの場合は、上位3つのワークロードがスループットグラフに表示されます。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ポリシーに含まれてい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については、[IOPS]グラフと[MBps]グラフには、ONTAPがボリュームのサイズに基づいて割り当てられている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してMBpsのしきい値を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のみが制限されます。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るため、処理を処理するノードの負荷はるかに大きくなります。

ワークロードのMBpsの値は次の式を使用して生成されます。

$$\text{MB/s} = (\text{IOPS} * \text{Block Size}) / 1000$$

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MBps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、このワークロードの実効MBpsは144です。ブロックサイズが大きいほど、ノードで処理されるデータが50%多くなっていることがわかります。

次に、ブロックサイズが定義されたアダプティブQoSポリシーを示し、クライアントに設定されているブロックサイズに基づいてイベントがどのようにトリガーされるかを確認します。

ポリシーを作成し、最大スループットを2、500 IOPS/TB、ブロックサイズを32KBに設定します。これにより、使用済み容量が1TBのボリュームのMBpsのしきい値が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/秒
1TB	2、250 IOPS	72 MB/秒
2TB	4、500 IOPS	144 MB/秒
5TB	11、250 IOPS	360 MB/秒

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/秒（ $(4,000 \text{ IOPS} * 32\text{KB}) / 1000$ ）になります。このシナリオでは、4、000 IOPSと128MB/秒のどちらも、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下回っているため、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/秒（ $(4,000 \text{ IOPS} * 64\text{KB}) / 1000$ ）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のしきい値である144MB/sを超えているためイベントが生成されます。

このため、ブロックサイズを含むアダプティブQoSポリシーに対するMBpsの違反に基づいてイベントがトリガーされた場合は、[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の両方に違反が発生すると、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を使用すると、多くのワークロードがレイテンシの影響を受ける前に、潜在的なパフォーマンスの問題を修正できます。

- 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発生している必要があります。

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ら、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使用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最大スループット制限を引き下げる
- 別のアグリゲートまたはノードへのワークロードの移動
- ノードにディスクを追加するか、高速CPUとRAMを搭載したノードにアップグレードして容量を拡張する

#### 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、「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。このように配置すると、ノードのレイテンシの原因となっているワークロードを確認できます。

IOPSグラフにカーソルを合わせると、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確認できます。

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への対処

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を使用すると、多くのワークロードがレイテンシの影響を受ける前に、潜在的なパフォーマンスの問題を修正できます。

- 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で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. 新しいノードで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 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ることで実行できます。

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どうかを確認します。



## 動的なパフォーマンスしきい値で発生したイベントの分析

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）が想定応答時間範囲と比較して高すぎる、または低すぎることを示しています。[イベントの詳細]ページでは、パフォーマンスイベントを分析し、必要に応じて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の各システムでは有効になりません。

## 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。これらのワークロードを特定すると、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低下し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。
- 動的なパフォーマンスイベントが新規、確認済み、または廃止状態になっている必要があります。

[イベントの詳細]ページには、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、コンポーネントのアクティビティや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。
- 動的なパフォーマンスイベントが新規、確認済み、または廃止状態になっている必要があります。

[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、または廃止状態の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の分析

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構成に対して新規、確認済み、または廃止状態のパフォーマンスイベントが発生している必要があります。
- 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. イベントの説明で、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、アイコンの説明が表示されません。

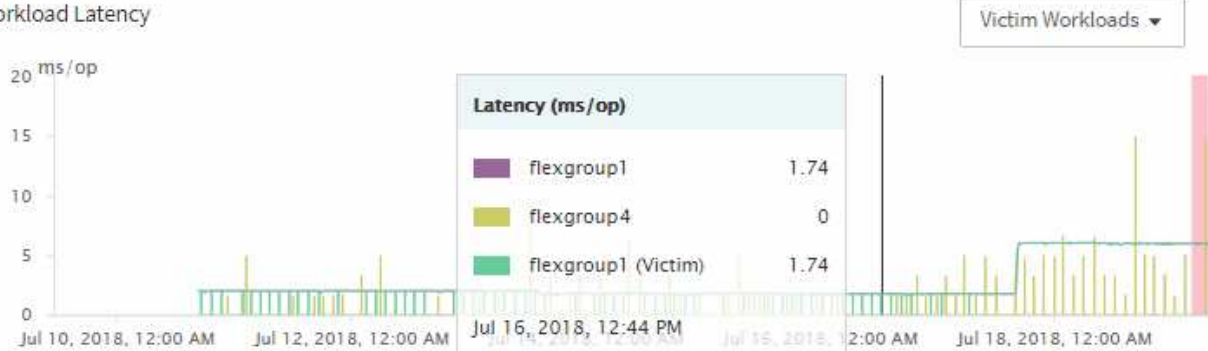


3. クラスタの名前とイベントの検出時刻をメモします。この情報を使用して、パートナークラスタのパフォーマンスイベントを分析できます。
4. グラフで、\_Victim ワークロードの応答時間がパフォーマンスしきい値を超えていることを確認します。

この例では、ホバーテキストに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ワークロードの一貫したレイテンシパターンが大まかに表示されます。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いるものの、I/Oの急増によってレイテンシが増加してイベントがトリガーされた可能性があります。

### 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、そのアプリケーションから大量のI/Oが送信されると、レイテンシが増大する可能性があります。ワークロードのレイテンシが想定範囲内に戻り、イベントの状態が「obsolete」に変わり、30分以上この状態のままになった場合は、このイベントは無視してかまいません。継続中のイベントが新しい状態のま

まの場合は、さらに詳しく調査して、イベントの原因が他の問題であるかどうかを確認できます。

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ことが原因でイベントが発生した可能性があります。Bullyワークロードの書き込みスループット (MB/秒) の偏差が大きくなっています。

このグラフには、ワークロードの書き込みスループット (MB/秒) のパターンが大まかに表示されます。書き込みMBpsのパターンからスループットの異常を特定できます。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の健全性の問題、またはパートナークラスタのパフォーマンスの問題がイベントの原因である可能性があります。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の分析

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。この分析は、リモートクラスタのイベントがパートナークラスタのイベントの原因かどうかを判断するのに役立ちます。

- 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。
- 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、イベントの検出時間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取得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時間がない場合は、パートナーでイベントが検出された時間にクラスタでパフォーマンスの問題が発生していないことを示しています。

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で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Data Processingコンポーネントの競合を引き起こしているBullyワークロードが含まれている場合は、これらのBullyワークロードの一部がローカルクラスタでのイベントの原因となっている可能性があります。イベントをクリックすると、イベントを分析し、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は発生していません。

## 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）が長くなりました。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を追加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発生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. 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。



スロットルによってワークロードが自身のVictimになるため、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で使用されている割合です。

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。イベントが発生した時点で、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を超えていたため、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。

どちらのグラフも、レイテンシが高い読み取り要求の数は多いものの、書き込み要求の数とレイテンシが低いことを示しています。これらの値は、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数があるかどうかを判断するのに役立ちます。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適用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]グラフが表示されます。

13. ページ上部で、ポリシーグループ制限の変更の変更イベントアイコン ( ) にカーソルを合わせます .
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、レイテンシは減少しています。

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発生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。[Component in Contention]にある[Aggregate]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、アグリゲートでの競合および関連イベントが発生している可能性があります。



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、イベントが解決されたことを示す「State」が「Obsolete」になっていることを確認します。

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の赤いドット (●) は、ディスク障害イベントが発生した時刻を示します。

10. [ノードとアグリゲートの利用率]グラフで、ノード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。

イベント発生時の[アグリゲート利用率]には、RAIDの再構築プロセスが原因の大量の読み取り/書き込みアクティビティが表示されており、これが選択したボリュームのレイテンシ増加につながりました。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高Data Processing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発生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たData Processingノードが、競合状態のクラスタコンポーネントです。[Component in Contention]の下にData Processingアイコンが赤で強調表示され、イベント発生時にData Processingを処理していたノードの名前がかっこ内に表示されます。

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[Events]タイムラインにある変更イベントアイコン (●) は、Unified ManagerがHAテイクオーバーの開始を検出した時刻を示します。

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ると、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]グラフでは、HAテイクオーバーと同じタイミングで高レイテンシが原因で、選択したボリュームがパフォーマンスしきい値を超えたことを示すイベントが表示されます。

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、Data Processing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、Data Processingノードでのワークロード需要の増加に起因するData Processingの急増がありました。CPU利用率の上昇によってレイテンシが上昇し、イベントがトリガーされました。

8. 障害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。これにより、ワークロードがパートナーノードから固定ノードに移動されます。
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」になり、イベントが解決されたことを示します。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の解決

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独自に解決することができます。最初の3つの推奨事項は常に表示され、4番目の推奨事項の下のアクションは表示されるイベントのタイプに固有です。

[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。一部の処理では、Unified Manager、ONTAP System Manager、OnCommand Workflow Automation、ONTAP CLIコマンド、またはこれらのツールを組み合わせて使用します。

### レイテンシが想定範囲内であることの確認

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する

ディスクの障害、HAフェイルオーバー、ボリュームの移動など、クラスタでの構成変更は、ボリュームのパフォーマンスに悪影響を及ぼし、レイテンシを増大させ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、最近の設定変更がいつ発生したかを確認し、処理やレイテンシ（応答時間）と比較して、選択したボリュームワークロードのアクティビティに変化がなかっ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。健全性ページには、設定の変更を原因とするその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向上させ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を送信しているクライアントワークロード（アプリケーションやデータベースなど）を確認することで、クライアント側の変更によってイベントが修正された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ているクライアントのI/O要求が増加すると、その要求を満たすためにクラスタの負荷が増大します。クラスタ上の特定のボリュームに対するI/O要求数が多いクライアントがわかっている場合は、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、ボリュームに対する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できます。ボリュームが属しているQoSポリシーグループに対して、制限を適用または増やすこともできます。

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を送信しており、クラスタコンポーネントの競合を引き起こしている可能性があるかどうかを確認できます。[イベントの詳細]ページの[システム診断]セクションには、競合状態のコンポーネントを使用してい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ないかを確認できます。

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は、リモートクラスタ上のボリュームにミラーリングされます。ローカルクラスタのソースボリュームとリモートクラスタのデスティネーションボリュームの同期を維持すると、MetroCluster構成での両方のクラスタの要求が増加する可能性もあります。これらの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への影響が軽減されます。

## クライアントまたはネットワークに問題がないか確認する

クラスタ上のボリュームに接続されているクライアントのI/O要求が増加すると、その要求を満たす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]セクションには、競合状態のコンポーネントを使用している上位の

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ないかを確認できます。必要に応じて、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問い合わせてください。

ネットワークインフラを調べて、クラスタと接続されているクライアント間のI/O要求のパフォーマンスが想定よりも遅くなる原因となってい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ないかどうかを確認できます。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サービス品質 (QoS) ポリシーグループ内のワークロードを確認して、複数のワークロードがイベントの原因になっていない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]セクションでは、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上部に表示できます。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[Workload Analysis]ページに移動して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、次のようにポリシーグループを管理できます。

- 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する。
- 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、負荷分散の改善、メンテナンス処理やパフォーマンス調整、間接アクセスの削減に役立ちます。

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がネットワーク処理とData Processingに異なるノードを使用している場合に発生します。間接アクセスを減らすには、LIFの配置を変更します。そのためには、ネットワーク処理とData Processingに同じノードを使用するようにLIFを移動します。負荷の高いLIFがONTAPによって別のポートに自動的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"> <li>• 負荷分散を改善します。</li> <li>• 間接アクセスが軽減されます。</li> </ul>	<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または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を手動で移動するには、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処理を処理す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のワークロードの負荷が低いときに実行することができます。

Storage Efficiency処理では、大量のクラスタCPUリソースが使用され、処理を実行するボリュームがBullyになることがあります。Storage Efficiency処理の実行時にVictimボリュームのアクティビティが高いと、レイテンシが増加し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]セクションには、Bullyワークロードを特定するために、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別に表示されます。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ると、Storage Efficiency処理によるクラスタの競合を回避できます。

効率化ポリシーは、ONTAP System Managerを使用して管理できます。効率化ポリシーとスケジュールを管理するには、ONTAPコマンドを使用します。

### Storage Efficiencyとは

Storage Efficiencyを使用すると、コストを最小限に抑えながら最大限のデータを格納し、スペースを削減しながら急増するデータに対応できます。NetApp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を使用すると、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)、およびセカンダリストレージを1つのプラットフォームに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。

## ディスクの追加とデータの再割り当て

アグリゲートにディスクを追加して、ストレージ容量とその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。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は、[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。

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イベントを受信した場合は、[イベントの詳細]ページでイベントの説明テキスト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割り当てできます。

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。アグリゲートにディスクを追加するには、ONTAP System ManagerまたはONTAPコマンドを使用します。



データの再割り当ては、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にのみ行ってください。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向上させる仕組み

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（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、ランダムリードが大量に発生する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動作します。

Unified Managerの[イベントの詳細]ページでは、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。アイコンの下には、アグリゲートを識別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いるか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とその使用要件の詳細については、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向上させる仕組み

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を使用すると読み取り/書き込みキャッシュのパフォーマンスが向上し、アグリゲートのパフォーマンスが向上します。

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が取り付けられている場合は、コマンドラインインターフェイスを使用して有効にできます。SSDが搭載されている場合は、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`

このコマンドの`aggr\_name`はアグリゲートの名前です（競合状態にあるアグリゲートなど）。

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、IPまたはFC経由のMetroCluster構成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の確認"](#)

## MetroCluster構成の検証

MetroCluster over FC / IP構成でミラーされたワークロードでパフォーマンスの問題が発生しないようにするには、MetroCluster構成を正しく設定します。また、構成を変更したり、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したりして、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。

Fibre Channel (FC; ファイバチャネル) スイッチ、ケーブル、スイッチ間リンク (ISL) など、MetroCluster構成でクラスタをセットアップする手順については、を参照してください ["MetroClusterのドキュメント"](#)。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の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設定に固有の情報については、を参照してください ["MetroCluster IP設定のインストール"](#)。

MetroCluster構成をの要件と比較して、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できます ["MetroClusterのドキュメント"](#)。この比較は、次の点を確認するのに役立ちます。

- コントローラはワークロードに適していますか？
- スループットを向上させるために、ISLバンドルをより広い帯域幅にアップグレードする必要がありますか。
- 帯域幅を増やすために、スイッチのバッファ間クレジット (BBC) を調整できますか。
- ワークロードのソリッドステートドライブ (SSD) ストレージへの書き込みスループットが高い場合、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りますか？
- 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の詳細については、を参照して ["MetroClusterのドキュメント"](#) ください。
- コントローラのアップグレードについては、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"](#) 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たMetroCluster FC構成のコントローラのアップグレード"](#)

## 別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に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. パフォーマンスに問題があるアグリゲートをクリックします。

[パフォーマンス/アグリゲートエクスプローラ] ページにアグリゲートの詳細が表示されます。

- 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時間よりも長いパフォーマンス履歴期間を表示できます。過去72時間だけでなく、大量のリソースを使用しているボリュームを移動する必要があります。

- 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ボリュームと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の高い順にソートし、IOPSの高い順にソートして、最も負荷の高いボリュームを確認します。

- 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 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ることで実行できます。

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. この新しいノードで最も利用率が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 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ることで実行できます。

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. この新しいノードで最も利用率が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 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ることで実行できます。

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多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で特定で

きます。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 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ることで実行できます。

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 ペアの別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
- この新しい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. この新しいノードで最も利用率が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 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ることで実行できます。

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の優先順位を決定

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。ワークロードが属するポリシーグループに上限が設定されていない場合 (デフォルトのポリシーグループなど) や、設定された上限がニーズに合わない場合は、設定された上限を引き上げるか、適切な上限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である場合は、[イベントの詳細] ページのイベントの説明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をより制限の厳しいポリシーグループに割り当てることで、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、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。

- ポリシーグループの作成
- 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のワークロードの移動
- ポリシーグループのスループット制限の変更

## 非アクティブなボリュームと LUN の削除

アグリゲートの空きスペースに問題が見つかった場合は、未使用のボリュームと LUN を

検索してアグリゲートから削除できます。これは、ディスク容量不足の問題を軽減するのに役立ちます。

アグリゲート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やLUNをいくつかの方法で確認できます。

未使用のボリュームを特定するには：

- 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。

未使用のLUNを特定するには：

1. [Event Details] 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。

未使用のボリュームと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。

## ディスクの追加とアグリゲートレイアウトの再構築

アグリゲートにディスクを追加して、ストレージ容量とその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。ディスクを追加したあとにアグリゲートを再構築すると、パフォーマンスが向上するだけです。

[イベントの詳細] ページでシステム定義のしきい値イベントを受信すると、問題があるアグリゲートの名前がイベントの説明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。アグリゲートにディスクを追加するには、ONTAP System ManagerまたはONTAPコマンドを使用します。

"[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、監視している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送信できます。

統計グループ	データが含まれます	詳細
パフォーマンスモニタ	次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"> <li>• LUN</li> <li>• ボリューム</li> </ul>	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または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"> <li>• ノード</li> <li>• アグリゲート</li> </ul>	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の統計を提供します。  また、Performance Monitorグループで収集された統計情報も提供します。
ドリルダウン	追跡対象のすべての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下位レベルの統計情報： <ul style="list-style-type: none"> <li>• ノード</li> <li>• アグリゲート</li> <li>• LUN</li> <li>• ボリューム</li> <li>• ディスク</li> <li>• LIF</li> <li>• ポート/NIC</li> </ul>	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を提供します。  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提供します。  提供する統計データが最も多いグループです。





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つのオブジェクトは同じオブジェクトとして関連付けられません。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できるすべてのパフォーマンスカウンタのリストについては、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ための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正しく設定する必要があります。

NetAppでは、特定のバージョンのGraphiteや他社製ツールのテストや検証は行いません。



GraphiteサーバがUnified Managerからボリュームのパフォーマンスデータを受信しません。

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から統計データを転送できるようにするために、次の変更を行う必要があります。

- /opt/graphite/conf/carbon.conf`ファイルで、Graphiteサーバで1分あたりに作成できる最大ファイル数を`\_200\_` (**MAX\_CREATES\_PER\_MINUTE = 200**に設定する必要があります)。

構成内のクラスタ数や送信するように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場合があります。1分あたり200ファイルの場合、すべての指標ファイルが最初に作成されるまでに15分以上かかることがあります。一意の指標ファイルがすべて作成されると、このパラメータは関係ありません。

- IPv6アドレスを使用して導入されたサーバでGraphiteを実行している場合は、ファイルの`LINE\_RECEIVER\_INTERFACE`の値を /opt/graphite/conf/carbon.conf 「0.0.0.0」から「:::」に変更する必要があります(`LINE\_RECEIVER\_INTERFACE = ::`ます)
- /opt/graphite/conf/storage-schemas.conf`ファイルでは、`retentions`パラメータを使用して、頻度を5分、保持期間を環境に応じた日数に設定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可能ですが、頻度の値は少なくとも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、パラメータを使用してUnified Manager用のセクションを定義し`pattern`、初期頻度を5分、保持期間を100日に設定しています。 [OPM]

```
pattern = ^netapp-performance\..
```

```
retentions = 5m:100d
```



デフォルトのベンダータグを「NetApp - performance」から別のものに変更した場合は、その変更をパラメータにも反映する必要があります`pattern`。



Unified Managerサーバがパフォーマンスデータを送信する際にGraphiteサーバを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と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。
  - サーバ名または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。
- 送信する統計のグループを把握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、各送信で送信されるデータ量は、デフォルトの5分間隔を使用した場合の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、maintenance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]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、と入力して `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（デフォルトポート2003と異なる場合）を入力します。
6. プロンプトが表示されたら、と入力して、`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、と入力して`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、統計の送信間隔、および統計の送信を今すぐイネーブル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	<b>0</b> -performance_indicator（デフォルト）  <b>1</b> -resource_utilization  <b>2</b> -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。  ドット付き表記を使用すると、階層的なフォルダ構造を定義できます。たとえば、と入力する`stats.performance.netapp`と、`* stats > performance > NetApp *`に統計が表示されます。
送信間隔	<b>5</b> （デフォルト）、 <b>10</b> 、または` <b>15</b> `分
有効化/無効化	<b>0</b> -無効化  <b>1</b> -有効（デフォルト）

11. プロンプトが表示されたら、と入力して、`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. と入力し`x`で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間隔でデスティネーションサーバに送信されます。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。

# クラスタの健全性の監視と管理

## Active IQ Unified Managerの健全性監視の概要

Active IQ Unified Manager (旧OnCommand Unified Manager) を使用すると、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とアラート生成、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、問題を修正するための対処方法も提供されます。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、容量と健全性のグラフに表示される情報を使用して、クラスタオブジェクトの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では、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使用しています。

- 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。「使用済み物理容量」は、Storage Efficiency機能（重複排除や圧縮など）によってデータが削減されるため、通常は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。「使用済み論理スペース」は、使用済みの物理スペースと、設定されているStorage Efficiency機能（重複排除や圧縮など）による削減量を足したものです。この測定値は、データ圧縮などの物理スペースの削減量を反映していないため、使用済み物理容量よりも大きく表示されることがよくあります。したがって、合計論理容量がプロビジョニング済みスペースよりも大きくなる可能性があります。

### 容量の測定単位

Unified Manager は、1024 (2<sup>10</sup>) 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、およびPBとして表示されていました。ONTAP 9.10.1以降では、Unified Managerで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、ONTAPのすべてのリリースで、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) などです。

Unified Manager for ONTAP 9.10.0 以前の容量ユニットが表示され 表示されず	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
TB	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、Flash Cache
  - 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、FCoE
  - 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の表示
- MetroCluster over FC / IP構成：クラスタコンポーネントの構成、問題、および接続ステータスの表示と監視。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、しきい値インフラの強化
- LDAP、LDAPS、SAML認証、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
- ダッシュボードを強化し、容量、可用性、保護、パフォーマンスの環境の健全性を表示
- ボリューム移動の相互運用性、ボリューム移動の履歴、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のサポート
- Snapshotコピーの監視機能の強化（再利用可能なスペースの計算やSnapshotコピーの削除など）
- ストレージオブジェクトのアノテーション
- ストレージオブジェクトの情報（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）に関するレポートの作成と管理
- OnCommand Workflow Automation と統合してワークフローを実行

Storage Automation Storeには、OnCommand Workflow Automation（WFA）用に開発された、NetApp認定のストレージワークフロー自動化パックが含まれています。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、

["Storage Automation Store"](#)

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**インターフェイス

ここでは、Active IQ Unified Managerがデータストレージの容量、可用性、保護の問題をトラブルシューティングするために提供する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。

ここでは、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、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一般的な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。



この情報を使用して、メンテナンスコンソールにアクセスし、Unified Managerサーバの機能に関連する問題を解決できます。

## クラスタとクラスタオブジェクトの健全性の管理と監視

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することを推奨します。

ノードのルートボリュームの使用済み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システムマネージャまたはONTAP CLIを使用して、ノードの停止を防ぐための適切な対処を行うことができます。



クラスタでONTAP 9 14.1バージョン以降が実行されている場合、ノードのルートボリュームの監視機能は使用できません。

### 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、ノードが停止しないようにすることを推奨します。

デフォルトでは、ルートアグリゲートについては容量イベントとパフォーマンス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適用されます。

ONTAPシステムマネージャまたはONTAP CLIを使用して、ノードの停止を防ぐための適切な対処を行うことができます。



クラスタでONTAP 9 14.1バージョン以降が実行されている場合、ノードのルートアグリゲートの監視機能は使用できません。

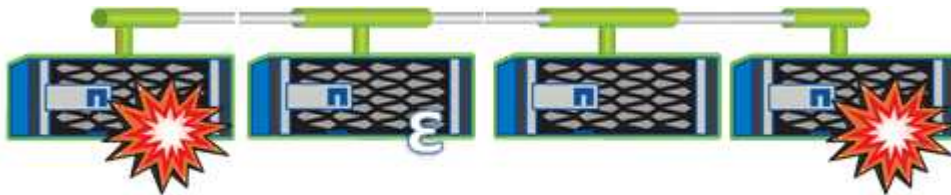
## クォーラムとイプシロンの概要

クォーラムとイプシロンは、クラスタの健全性と機能の重要な指標であり、通信や接続に関する潜在的な課題にクラスタがどのように対処するかを示します。

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、相互に通信できます。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。すべてのノードがまとめてデータの単一のビューを共有するため、一度にクォーラムを持つことができるノードの集まりは1つだけです。したがって、通信していない2つのノードが異なる方法でデータを変更できる場合、データを単一のデータビューに調整することはできなくなります。

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、クラスタ全体で情報を同期する役割を果たします。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り、クラスタがクォーラムに参加している場合は、オンラインのノード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前提として、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、次の図は、2つのノードで障害が発生した4ノードクラスタを示しています。ただし、サバイバーノードの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ではないにもかかわらず、クラスタはクォーラムを維持します。



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が正常な状態にならなくなった場合、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場合、または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、クラスタのクォーラムが失われたり、あと1つの停止によってクォーラムが失われる処理を実行しようとすると、ONTAPで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で信頼性の高い接続が確立されていれば、小規模なクラスタよりも大規模なクラスタの方が安定します。半分のノードの過半数とイプシロンを組み合わせたクォーラムの要件は、2ノードのクラスタよりも24ノードのクラスタで簡単に管理できます。

2ノードクラスタには、クォーラムの維持に固有の課題がいくつかあります。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。

[クラスタ/健全性の詳細]ページでは、個々のクラスタの健全性、容量、構成、LIF、ノード、ディスクなどの詳細を確認することもできます。

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設定の監視"
  - "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の確認

MetroCluster over FC構成およびMetroCluster over IP構成では、Active IQ Unified Manager (Unified Manager) を使用して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。
- FCおよびIPを介したMetroCluster構成の両方のクラスタを、同じUnified Managerインスタンスで監視する必要があります。

## MetroCluster over FC構成のクラスタの健全性の確認

MetroCluster over FC構成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

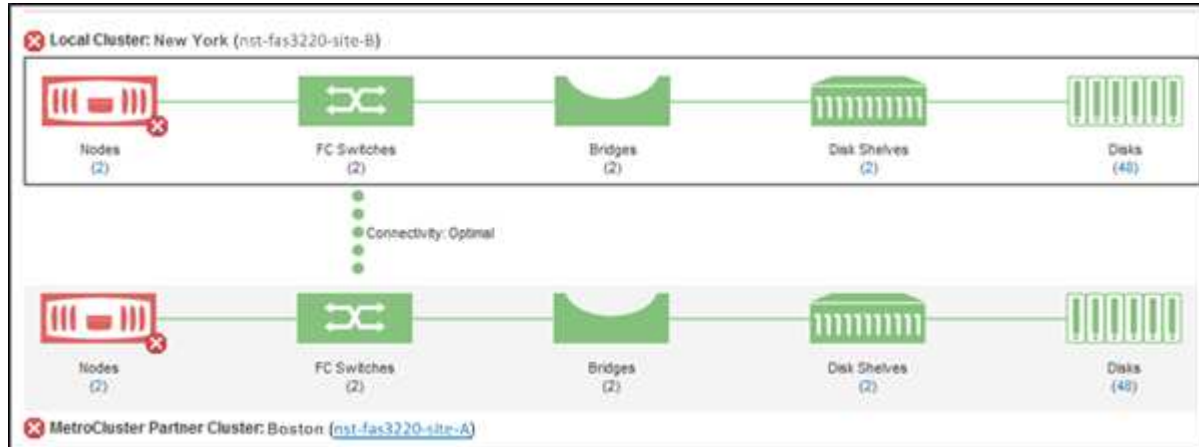
1. 左側のナビゲーションペインで、\* イベント管理 \* をクリックしてイベントリストを表示します。
2. フィルタパネルで、「\* ソースタイプ \*」カテゴリの下の「すべての MetroCluster」フィルタを選択します。すべてのMetroCluster構成について、環境で発生したすべてのイベントが表示されます。
3. MetroClusterイベントの横にあるクラスタの名前をクリックします。



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。

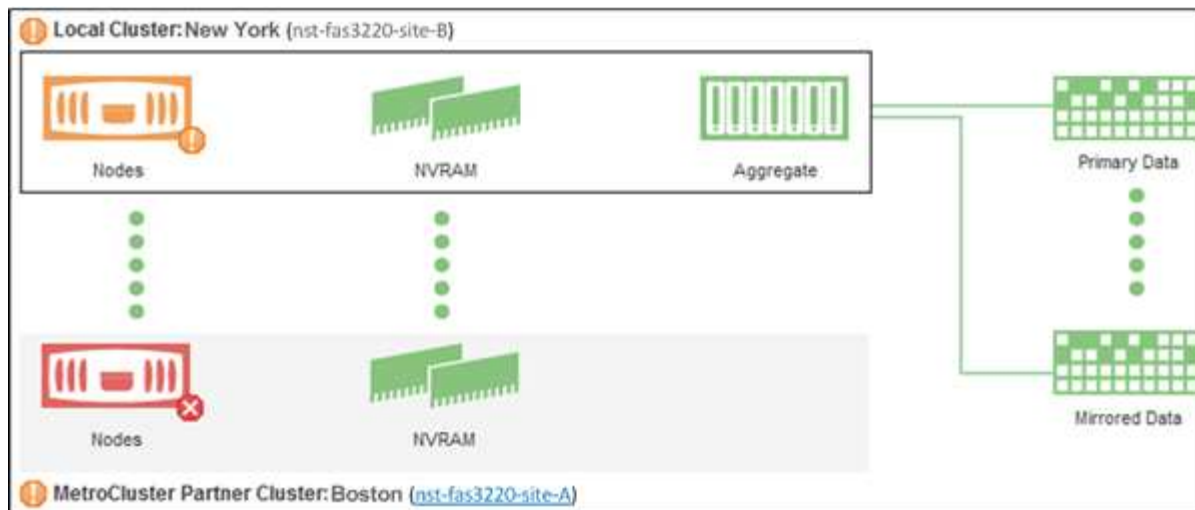
4. MetroCluster Connectivity \* タブを選択して、選択したクラスタとそのパートナークラスタ間の接続のヘルスを表示します。



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が表示され、アイコンをクリックするとイベントが表示されます。いずれかのクラスタでの健全性の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。

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の健全性の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。ページ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のパフォーマンスの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の確認

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. フィルタパネルの\* ソースタイプ \* カテゴリで、フィルタを選択します MetroCluster Relationship。すべてのMetroCluster構成について、環境で発生したすべてのイベントが表示されます。



報告された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構成に関連するイベントに関連した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。[Clusters]ページに、そのクラスタの詳細が表示されます。正常性に関する問題の特定については、[を参照してください"MetroCluster over IP構成の接続の問題を監視する"](#)。

## 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を使用して、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]、[ノード]の各タブで詳細を確認する

## 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]ページでは、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、ディスクセルフ、およびポートに関する情報も確認できます。

### 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 Details]は開いており、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	クリックする項目
ディスクセルフの詳細	• ディスクセルフ * :
ポート関連の情報	• ポート * :

詳細については、次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、現在の日付の完全な情報が記載された.csvファイルとしてダウンロードされます。

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リストおよび詳細の表示

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]ページでは、監視対象のSVMに関する詳細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。

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の表示

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せん。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/健全性の詳細]ページでは、アグリゲートの容量と構成、ディスクの情報などの詳細を確認できます。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の容量情報の表示

クラスタ、アグリゲート、ボリュームのFabricPoolの容量情報は、それらのオブジェクト

トの[容量]インベントリページと[パフォーマンス]インベントリページおよび詳細ページで確認できます。ミラー階層が設定されている場合、これらのページには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、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などの情報が表示されます。

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	操作
クラスタ	<p>a. Capacity : All Clusters ビューで、クラスタをクリックします。</p> <p>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。</p> <p>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。</p>
アグリゲート	<p>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。</p> <p>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。</p> <p>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。</p> <p>c. [ ディスク情報 ] タブをクリックします。</p> <p>クラウド階層の名前と使用済み容量が表示されます。</p> <p>d. [* 構成 *] タブをクリックします。</p> <p>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。</p>



容量の情報を表示するオブジェクト	操作
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、<b>[Configuration]</b> 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の表示

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を使用している場合のみ表示されます。

4. [キャッシュ]テーブルで、必要なストレージプールの名前にポインタを合わせます。

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の表示

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]ページを使用して、監視対象のボリュームに関する詳細情報（ボリュームの容量、効率性、設定、保護など）を表示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の表示"
  - "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またはFlexVol）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	>[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 /健全性の詳細]ページで、*[NFS共有]*タブをクリックします。

詳細については、およびを参照して["ファイル共有ボリュームのプロビジョニング"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](#)ください。

## SMB/CIFS共有に関する詳細の表示

すべてのSMB / CIFS共有に関する詳細を表示できます。これには、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情報が含まれます。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	>[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 /健全性の詳細]ページで、*[SMB共有]*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コピーリストの表示

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できる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、\* 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、Snapshotコピーのリストが表示されます。

- 関連情報 \*

["\[Health/Volumesページ\]"](#)

## Snapshotコピーの削除

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コピーを削除するには、Snapshotコピーを使用していた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が親ボリューム内のベース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、親ボリュームと同様にステータスとアプリケーション依存関係が `Busy, Vclone``表示されます `Busy`。

- 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、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の計算

1つ以上のSnapshotコピーを削除した場合に再利用でき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 volumeである必要があります。この機能はFlexGroupで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、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。

ボリューム上の再生可能なスペース（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説明

該当するストレージオブジェクトのページで、すべてのクラスタと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。インベントリの以下の[ストレージ]セクションと[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]、[クラスタ健全性]、[クラスタパフォーマンス]の各ページ
- [アグリゲートインベントリ]、[アグリゲート健全性]、[アグリゲートパフォーマンス]の各ページ
- [ボリュームインベントリ]、[ボリューム健全性]、[ボリュームパフォーマンス]の各ページ
- [Node Inventory]ページと[Node Performance]ページ
- StorageVMインベントリ、StorageVMメンテナンス、StorageVMパフォーマンス
- 保護関係のページ

## Unified Managerの一般的な健全性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、失われ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（必要な場合）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、発生の可能性が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ボリュームに関連する最も重要な問題が、[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。重大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。

関連する管理ツール（OnCommand Workflow Automation (WFA) など）が含まれるワークフローにUnified Managerを組み込むことで、ストレージリソースを直接設定できるようにすることもできます。

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。

- 可用性の問題の診断と管理

ハードウェア障害やストレージリソース設定の問題によってデータ可用性イベントが[Dashboard]ページに表示される場合、ストレージ管理者は組み込みのリンクを参照して、影響を受け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確認し、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および管理できます。詳細については、"[Active IQ Unified Manager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の診断と管理

ボリュームの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をたどって、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たり、トラブルシューティングのアドバイスを参照したり、他の管理者に問題の解決を割り当てたりできます。

- 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。詳細については、"[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復元。

- ストレージオブジェクトと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を使用してUnified Managerで収集された健全性、容量、パフォーマンスの情報を表示することで、クラスタの管理に役立ちます。詳細については、[を参照してください](#) "[Active IQ Unified Manager REST APIでの作業の開始](#)"。

- 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てテクニカルサポートに送信できます。AutoSupportメッセージよりも詳細な診断とトラブルシューティングが必要な問題の場合は、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のスキャンと解決

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、管理者は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するのが一般的です。

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、[ アクティブな可用性イベント \* ] を選択します。
3. インベントリページ[名前]\*列の上部でをクリック☰してテキストボックスにと入力し、`\*failover` 表示するイベントをストレージフェイルオーバー関連のイベントだけに限定します。

ストレージフェイルオーバー条件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]ページでは、次のタスクを1つ以上実行できます。
  - [Cause]フィールドで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 \*

["\[Event詳細ページ\]"](#)

["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インターコネクトリンクが停止した場合の対処方法の実行

ストレージフェイルオーバー関連のイベントの[イベントの詳細]ページでは、ページの概要情報を確認して、イベントの緊急性、問題の考えられる原因、および問題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。1つのリンクがアクティブであるため、Remote Dynamic Memory Access (RDMA；リモート動的メモリアクセス) 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成功します。

ただし、両方のリンクで障害が発生し、ストレージフェイルオーバー保護が完全に無効になるのを防ぐために、Link1が停止した理由を詳しく診断することになります。

#### 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。このノード名をクリックすると、[Cluster/Health]詳細ページの[Nodes]タブに、該当するHAペア（ツチブタおよびbonobo）のHAの詳細と、該当する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、[Events]テーブルに関連情報が表示されます。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 Details]のノードの場所情報を使用して、該当するHAペアノードで発生したストレージフェイルオーバーの問題の物理的な調査と修復を依頼するか、担当者に依頼します。



- 関連情報 \*

["\[Event\]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の解決

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と報告される理由はいくつかあります。

- 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Storage Virtual Machine (SVM) が停止したために、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。
- 2つのRAIDディスクで同時に障害が発生したため、ボリュームをホストしているアグリゲートが停止しています。

[イベント管理]インベントリページと[クラスタ/健全性]、[Storage VM /健全性]、[ボリューム/健全性]の詳細ページを使用して、該当する可能性を確認または排除できます。

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[イベントの詳細]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。

- 考えられる診断ガイダンスについては、[原因]フィールドに表示される情報を確認してください。

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（ここではオフラインと報告されたボリューム）をクリックして、そのボリューム

に関する詳細情報を表示します。

- 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の診断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または排除できます。

- 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 "[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 "[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 "[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の判別](#)"

- 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、ボリュ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れに続く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/健全性の詳細]ページには、オフラインボリュームのホストしている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. の[状態]列見出しで、フィルタ記号をクリックし、[オフライン]\*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. [健全性：すべてのボリューム]ビューで、グリッド記号をクリックし、\*[クラスタノード]\*オプションを選択します。

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。

[Cluster Nodes]列がボリュームインベントリに追加され、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、ホストノードが属するノードの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が画面に表示されます。

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確認

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が停止したためにボリュームがオフラインになっている可能性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. [健全性：すべてのStorage VMs]\*ビュー[SVM]列の見出しで、フィルタ記号をクリックし、停止した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. ビューで、 をクリックし、[ルートボリューム]\*オプションを選択します。

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[Volume/Health]詳細ページにある[Related Devices]ペインで、[Aggregate]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。
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するノードの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、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ってホストアグリゲートがオフラインになったことであるかどうかを確認するには、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]ページには、ホストしているアグリゲートのオンラインステータスまたはオフライン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、ボリュームがオフラインになっている原因はRAIDディスクの問題ではありません。

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ホストアグリゲートのオフライン状態の原因となった場合は、[影響を受けるアグリゲート]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伴うホストアグリゲートのオフライン化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、破損ディスクを手動で交換し、アグリゲートをオンラインに戻します。

## 容量の問題の解決

このワークフローでは、容量の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[Dashboard]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。問題の考えられる原因と解決策を特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。

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。
  - [Source]フィールドでオブジェクト（ここではボリューム）の名前をクリックして、オブジェクトの

詳細を表示します。

- このイベントについ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 \*

## "[Event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 Event Managementのインベントリページに「Volume Space Full」エラーイベントが表示され、イベント名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。

- ボリュームでの自動拡張、重複排除、または圧縮の有効化
- ボリュームのサイズ変更または移動
- ボリュームのデータの削除または移動

これらの操作はいずれも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がわかります。
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 \*

["\[Event詳細ページ\]"](#)

## 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に対して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。オブジェクトまたはオブジェクトのグループに必要なに応じて設定を変更できます。

## グローバル健全性しきい値の設定

アグリゲート、ボリューム、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条件を設定できます。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。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の設定"](#)。

すべてのアグリゲートの容量、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の設定"](#)。

すべてのボリュームの容量、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、およびinode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 ["qtreeのグローバル健全性しきい値の設定"](#)。

すべてのqtreeの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の設定

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に設定すると、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、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とみなされます。



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適切に設定します。
3. [保存 (Save)] をクリックします。

- [関連情報](#) \*

#### ["ユーザの追加"](#)

#### ボリュームのグローバル健全性しきい値の設定

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オプションには、監視しやすくするため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、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とみな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。古いバージョンでは、1000（および 1000~250 の間の任意の数）を Unified Manager は 250 と解釈するため、Snapshot コピーの数が 250 に達してもイベントが引き続き受信されます。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、ボリュームの増加率、および inode について適切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 \*

#### "ユーザの追加"

##### qtree のグローバル健全性しきい値の設定

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 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に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に対する遅延健全性しきい値のグローバルなデフォルト設定を編集して、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。

- 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、遅延時間が1時間を超えないようにする必要があります。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。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つの保護関係にのみ設定を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 \*

#### "ユーザの追加"

#### 個々のアグリゲートの健全性しきい値の設定

1つ以上のアグリゲートの容量、増加率、およびSnapshotコピー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せん。

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、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とみなされます。

#### 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 \*

## "ユーザの追加"

### 個々のボリューム健全性しきい値の設定の編集

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、次回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せん。

ボリュームで自動拡張が有効になっている場合、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とみな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。古いバージョンでは、1000 (および 1000~250 の間の任意の数) を Unified Manager は 250 と解釈するため、Snapshot コピーの数が 250 に達してもイベントが引き続き受信されます。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 \*

## "ユーザの追加"

### 個別の qtree の健全性しきい値の設定の編集

1つ以上の qtree の容量に関する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、次回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せん。

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。



[Storage VM/健全性の詳細]ページの[qtree]タブで、qtreeのしきい値を個別に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わない場合もあるため、変更が不要な場合もあります。

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 ["ONTAP 9 セキュリティ設定ガイド"](#)。

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、新しい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に通知されるように、イベントにアラートを設定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 ["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

詳細については、準拠カテゴリに関するトピックおよびを参照してください ["ONTAP 9 セキュリティ設定ガイド"](#)。



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特定します。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前に、SVMのセキュリティの問題の修正が必要に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はAutoSupport、UIページに[クラスタピアリング]または[HTTPS転送]の項目は表示されません。

パラメータ	製品説明	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（Federal Information Processing Standard）140-2準拠モードが有効になっているか無効になっているかを示します。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アクセスが有効か無効かを示します。NetAppでは、セキュアなリモートアクセスにセキュアシェル（SSH）を推奨しています。	無効	はい

パラメータ	製品説明	推奨事項	クラスタコンプライアンスに影響します
安全でない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か無効かを示します。	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
ネットワークタイムプロトコル	クラスタにNTPサーバが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。	設定済み	はい
OCSP	ONTAPにOCSP（オンライン証明書ステータスプロトコル）が設定されていないアプリケーションがあるため、通信が暗号化されていないかどうかを示します。非準拠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

パラメータ	製品説明	推奨事項	クラスタコンプライアンスに影響します
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
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

パラメータ	製品説明	推奨事項	クラスタコンプライアンスに影響します
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	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を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には、Secure Shell (SSH) を使用することを推奨します。	無効	はい
MD5使用中	ONTAPユーザーアカウントが安全性の低い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ーアカウントは、SHA-512のようなより安全な暗号化ハッシュ関数に移行することが推奨されます。	いいえ	はい
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シヨメイ	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基準、NetApp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	製品説明	推奨事項	SVM コンプライアンスに影響 します
監査ログ	監査ログが有効か無効かを示します。	有効	はい
安全でないSSH設定	SSHでセキュアでない暗号（で始まる暗号など）が使用されているかどうかを示します cbc*。	いいえ	はい



パラメータ	製品説明	推奨事項	SVM コンプライアンスに影響 します
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暗号化が有効か無効かを示します。	有効	いいえ
NTLM 認証	NTLM認証が有効か無効かを示します。	有効	いいえ
LDAP ペイロードの署名	LDAPペイロード署名がイネーブルかディセーブルかを示します。	有効	いいえ
CHAP設定	CHAPが有効か無効かを示します。	有効	いいえ
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	FPolicyが作成されたかどうかを示します。	はい	いいえ
SMB暗号化が有効	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	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が準拠とみなされるかどうかには影響しません。




ん。

パラメータ	製品説明
ソフトウェアで暗号化	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。
ハードウェアで暗号化	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で暗号化	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のステータスアイコンには、コンプライアンスに関して次の意味があります。

- -パラメータは推奨されるように設定されています。
- -パラメータは推奨されるように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、インターフェイスのさまざまなポイントから、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表示できます。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して分析し、監視対象のクラスタとStorage VMでの不審な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]ページでのオブジェクトレベルのセキュリティステータスの表示

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、およびリンクをクリック `View Reports` すると、[Volumes]、[Clusters]、または[Storage VMs]ページに移動し、必要に応じて対応する詳細を表示したり、レポートを生成したりできます。

[Security]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クラスタまたは60日以内に有効期限が切れる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する

[\*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。

デフォルトのセキュリティパラメータ（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、クラスタ証明書の有効期限のステータスなど）が表示されます。

[その他のオプション]ボタンをクリックすると、Unified Managerの\*[セキュリティ]\*ページまたはSystem Managerでセキュリティの詳細を表示できます。System Managerで詳細を表示するための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、\*[クラスタ証明書の有効期限]\*をクリックし、System Manager (9.10.1以降) で更新できません expired。System Managerインスタンスが9.10.1より前のリリースの場合は、をクリックできません expired。

[Storage VM]ページからすべてのクラスタのセキュリティの詳細を表示する

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せん。

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を含むクラスタのリストが表示されます。

Storage VM、クラスタ、ログインバナー、監査ログ、セキュアでないSSH設定などのセキュリティパラメータを確認することで、Storage VMのセキュリティ準拠状況をデフォルトで確認できます。

[その他のオプション]ボタンをクリックすると、Unified Managerの\*[セキュリティ]\*ページまたはSystem Managerでセキュリティの詳細を表示できます。System Managerで詳細を表示するための有効なクレデンシャルが必要です。

ボリュームと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回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、通知を受けたくないセキュリティアップグレードイベントがある場合は、このリストを使用してこれらのイベントを特定して無効に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、\* 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。

アクティブなアップグレードセキュリティイベントがすべて表示されます。

すべてのクラスタでのユーザ認証の管理状況の表示

[セキュリティ]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タイプと、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の表示

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と Storage VM のランサムウェア対策ステータスの表示

すべてのボリュームと Storage VM (SVM) のリストとその現在のランサムウェア対策ステータスを表示して、ボリュームと 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。

さまざまなランサムウェア対策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検出機能を使用して、すべてのボリュームのセキュリティの詳細を表示する

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。



Anti-Ransomwareは、オフラインボリューム、制限されたボリューム、SnapLockボリューム、FlexGroupボリューム、FlexCacheボリューム、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、データ保護ボリュームではサポートされていません。

ランサムウェア対策検出機能付きで、すべての**Storage VM**のセキュリティの詳細を表示

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ステータスの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の監視はサポートされません。

アクティブなすべてのセキュリティイベントの表示

アクティブなセキュリティイベントをすべて表示して、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、受信したくないセキュリティイベントがある場合は、このリストを使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、新規イベントと確認済みイベントは[イベント管理]インベントリページに表示されません。

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」および「確認済み」のセキュリティイベントがすべて表示されます。

## セキュリティイベントのアラートの追加

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単一のアラ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ている場合、アラートが送信されます。同じ方法で、すべてのセキュリティイベントの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タップの発行、およびスクリプトの実行について、このページのそ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の無効化

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が次の監視サイクルから生成されます。

## 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
イベントを無効にする	<ol style="list-style-type: none"><li>a. <b>[Disable]</b> をクリックします。</li><li>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。</li><li>c. [Matching Events]列で、無効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]列に移動します。</li><li>d. [ 保存して閉じる ] をクリックします。</li><li>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ていることを確認します。</li></ol>
イベントを有効にする	<ol style="list-style-type: none"><li>a. 無効になっているイベントのリストで、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。</li><li>b. <b>[Enable]</b> をクリックします。</li></ol>

## 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ため、重大度を評価して必要に応じて問題を修正できます。

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、クラスタとStorage VMのイベントカテゴリに表示されます。

## バックアップ処理とリストア処理の管理

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と同じ（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。

バックアップとリストアの方法は、Unified Managerをインストールしたオペレーティングシステムと、管理対象のクラスタとノードの数に基づいて3つあります。



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	任意	Unified Manager仮想アプライアンスのVMwareスナップショット
Red Hat Enterprise LinuxまたはCentOS Linux	小規模	Unified Manager 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	小規模	Unified Manager MySQLデータベースダンプ
	大規模	iSCSIプロトコルを使用したUnified ManagerデータベースのNetApp Snapshot

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。

#### カソウアプライアンスノUnifiedManagerノハツクアツフオヨヒリストア

仮想アプライアンスにインストールされている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と、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でデータストアがホストされていない場合は、ストレージベンダーのガイドラインに従ってVMwareスナップショットのバックアップを作成します。

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をリストアするには、作成したVMwareスナップショットを使用してVMをバックアップのポイントインタイム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データベースのダンプバックアップは、Active IQ Unified Managerデータベース

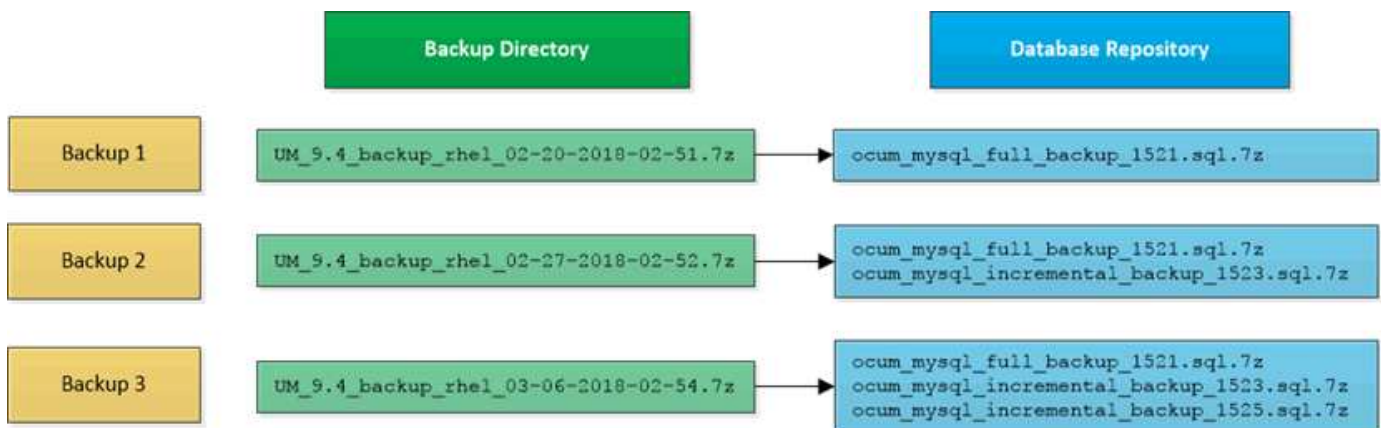
と構成ファイルのコピーです。システム障害やデータ損失が発生した場合に使用できません。バックアップはローカルにもリモートにも保存できますが、Active IQ Unified Managerホストシステムとは別のリモートの場所を定義することを強く推奨します。



MySQLデータベースダンプは、Unified ManagerがLinuxサーバおよびWindowsサーバにインストールされている場合のデフォルトのバックアップメカニズムです。ただし、Unified Managerで多数のクラスタとノードを管理している場合や、MySQLのバックアップに数時間かかっている場合は、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、バックアップの再作成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だけが含まれています。

データベースバックアップの初回生成時には、バックアップディレクトリに1つのファイルが作成され、データベースリポジトリディレクトリにフルバックアップファイルが作成されます。次回バックアップを生成すると、バックアップディレクトリに1つのファイルが作成され、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。



この2つのディレクトリ内のバックアップファイルの名前を変更したり、削除したりしないでください。削除すると、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は、完全な復元を必要とするシステムの問題が発生した場合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は整合性チェックを実行して、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を確認します。また、バックアップファイルを作成するのに十分なスペースがシステムにあることも確認します。

#### 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とスケジュールの設定

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。毎日または毎週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のバックアップを使用している場合は、バックアップディレクトリに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のバックアップを使用している場合は、バックアップディレクトリへのアクセスが管理者だけに許可されてい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を超えることがあり、3~4時間かかることがあります。以降のバックアップは増分バックアップであり、所要時間は短くなります。



- 増分バックアップファイルの数がバックアップ用に割り当てた容量に対して大きすぎる場合は、フルバックアップを定期的に行って、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。
- 新しいクラスタの追加の最初の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には正確で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。

データベースダンプバックアップファイル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、[Database Backup]ページで確認できます。

データベースリストアとは

MySQLデータベースリストアとは、Unified Managerの既存の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プロセスです。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し、バックアップファイルがすべてローカルに格納されてい

る場合は、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。リストアプロセスの完了後に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、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際に、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ニンショウノユウコウカ"](#)

["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をデフォルトのディレクトリ/data/ocum-backupにコピーすることを推奨します。データベースリポジトリファイルは、ディレクトリの下サブディレクトリに'/ocum-backup`コピーする必要があります'/database-dumps-repo`ます。

- バックアップファイルのタイプはである必要があります `7z` 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または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。バックアップファイルには、リストアプロセス中にこの情報が入力されます。
2. 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。
3. 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。
4. コマンドを入力し maintenance\_console、Enterキーを押します。
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: /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。

バックアップのリストア後に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指すように変更します。
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。

## 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は、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し、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管理者Privileges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を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ファイルは、ディレクトリの下の子ディレクトリに`backup`コピーする必要があります `database\_dumps\_repo`ます。

- バックアップファイルのタイプはである必要があり`.7z`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。バックアップファイルには、リストアプロセス中にこの情報が入力されます。
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. コマンドを入力し maintenance\_console、Enterキーを押します。
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。

バックアップのリストア後に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指すように変更します。
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スナップショットを使用したバックアップとリストア

NetAppのSnapshotコピーを作成すると、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が作成されます。このイメージを使用して、システム障害やデータ損失が発生した場合のリストアに使用できます。Snapshotコピーは、いずれかのONTAPクラスタ上のボリュームに定期的書き込まれるようにスケジュールを設定して、常に最新のコピーが保持されるようにします。



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。



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スナップショットを使用してバックアップとリストアを設定できます。

Snapshotコピーにはごくわずかな時間（通常は数分）しかかかりません。また、Unified Managerデータベースがロックされるのはごく短時間であるため、インストールが中断されること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てからのファイルへの変更のみが記録されるため、ストレージスペースは最小限しか消費されず、パフォーマンスのオーバーヘッドもわずかです。SnapshotはONTAPクラスタ上に作成されるため、必要に応じて、SnapMirrorなどの他のNetApp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によって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かどうかを検証されます。



- 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 9.14で作成したバックアップは、Unified Manager 9.14のシステムにのみリストアできます。

- Snapshotの設定に変更があると、Snapshotが無効になる可能性があります。

### Snapshotコピーの場所の設定

ONTAPシステムマネージャまたはONTAP CLIを使用して、いずれかのONTAPクラスタに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

du -sh /opt/ NetApp /data/コマンドを使用して、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ボリュームを作成する詳細な手順については、および ["ONTAP 9 NFS構成エクスプレスガイド"](#)を参照して ["ONTAP 9 で NFSv4 を設定する方法"](#)ください。

### Snapshotコピーのデスティネーションの指定

いずれかのONTAPクラスタで設定済みのボリュームで、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。場所を定義するには、メンテナンスコンソールを使用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。
- ボリュームをActive IQ Unified Managerホストにマウントし、マウントパスを確認しておく必要があります。

### 手順

1. セキュアシェルを使用して、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. コマンドを入力し maintenance\_console、Enterキーを押します。
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、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でのバックアップの設定

Active IQ Unified Managerでは、iSCSIプロトコルを使用するLUNを使用して、WindowsオペレーティングシステムでNetApp Snapshotを使用したバックアップとリストアをサポートしています。

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。バックアップ時にデータベース全体にグローバル読み取りロックが設定され、同時書き込みができなくなるため、整合性のあるデータベースの状態がSnapshotの一部としてキャプチャされます。Windows OSにインストールされているUnified ManagerシステムでNetApp Snapshotを使用してバックアップとリストアを実行するには、まずメンテナンスコンソールを使用してUnified ManagerのSnapshotベースへのバックアップを設定する必要があります。

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クラスタの設定
- Windowsホストマシンの設定

#### Windowsのバックアップ先の設定

WindowsでUnified Managerをバックアップしたあとに、Snapshotコピーを格納する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つしかなく、それ以外のLUNは含まれていません。
- 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クラスタノセッテイ

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設定前の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Storage VMにiSCSI LIFとして割り当てられるように設定します。次の手順では、System Managerのユーザインターフェイスを使用してiSCSIが有効なStorage VMを設定します。LIFが発信トラフィックをネットワークでどのように使用するかを制御するには、このStorage VMの静的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が必要です。選択したボリュームに含まれるLUNは1つだけにする必要があります。LUNのサイズは、Active IQ Unified Managerで処理される想定データサイズの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が有効なStorage VMを設定するか、同じ構成の既存のStorage VMを使用してください。
2. 設定したStorage VMのネットワークルートを設定します。
3. 適切な容量のボリュームと単一のLUNを構成し、ボリュームがこのLUN専用になるようにします。



System ManagerでLUNを作成すると、LUNのマッピングを解除するとigroupが削除され、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の作成時に明示的に作成され、LUNのマッピングを解除しても削除されないようにしてください。

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ホストマシンの設定

NetAppスナップショットを使用して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時、確認を求めるプロンプトが表示され、確認後に[iSCSIのプロパティ]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、アクティブでないターゲットまたは接続しようとしているターゲットを示す[iSCSIのプロパティ]ダイアログボックスが表示されます。そのため、Windowsホスト上の以前の設定がすべて削除されていることを確認する必要があります。

### 手順

1. ホストマシンの以前の設定をすべてクリーンアップします。
2. ターゲットポータルを検出します。
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. 検出したLUNをWindowsで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クラスタで設定済みのボリュームで、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。場所を定義するには、メンテナンスコンソールを使用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. コマンドを入力し maintenance\_console、Enterキーを押します。
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、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）があるかどうかを検証されます
- 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の**Snapshot**コピーによるバックアップの設定

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ノクレデンシャル

#### 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、から提供された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、ドライブなどが正しいことが確認されます。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。

バックアップ処理を開始する前に、Snapshotが無効になる可能性があるため、Snapshotの設定に変更がないかどうかを確認する必要があります。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、新しい構成に従ってデータがEドライブに保存されます。Gドライブにあるときに作成されたSnapshot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が表示されて失敗します。

#### Linuxおよび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の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。
- Snapshotコピーを作成するデスティネーションを特定するために、メンテナンスコンソールでSnapshotコピーを作成するための設定を行っておく必要があります。

Snapshotコピーは数分で作成され、Unified Managerデータベースは数秒間だけロックされます。



新しいクラスタの追加の最初の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には正確で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して、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、[Database Backup]ページで確認できます。

このボリュームとSnapshotは重要であるため、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して、次のいずれかのタイミングで通知を受け取ることができます。

- ボリュームスペースが90%使用されています。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の数が上限に近づいています。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、常に新しいSnapshotコピー用のスペースを確保できます。

アラートは[Alert Setup]ページで設定します。

## 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またはリモートのオペレーティングシステムにリストアできます。

- 必要なもの \*
- Unified ManagerがインストールされているLinuxホストおよび管理Privileges (Windowsホストマシン)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. コマンドを入力し maintenance\_console、Enterキーを押します。
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のユーザインターフェイスにログインします。

バックアップのリストア後に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指すように変更します。
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の変更

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。

実行される処理（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）が表示されます。

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、[全般]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 ヨウノ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、必要なときにいつでもオンデマンドバックアップを生成できます。オンデマンドバックアップでは、既存のバックアップ方式を使用してバックアップを瞬時に作成できます。オンデマンドバックアップでは、MySQLとNetAppのSnapshotベースのバックアップは区別されません。

[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は依存しません。

## 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システムの場合：
  - の手順に従って、LinuxサーバにUnified Managerをインストールしておく必要があります"[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。
  - インストール後は、LinuxシステムでUIを起動したり、クラスタ、ユーザ、認証設定を設定したりしないでください。バックアップファイルには、リストアプロセス中にこの情報が入力されます。
  - Linuxホストのrootユーザのクレデンシャルが必要です。

以下の手順では、仮想アプライアンスで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/support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を超えることがあり、完了までに3~4時間かかることがあります。

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の/supportからSCPを使用してバックアップファイルをコピーします。`.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ていることを確認します。

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/support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) に変更するか、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認証を再設定します (SAMLを使用する場合) 。

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実行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でイベントに対してアラートが生成され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、イベントを生成しているストレージ

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、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は、アラートEメールから確認できます。



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を使用されます。

- -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。

- スクリプトでサポートされるファイル形式は、Perl、Shell、PowerShell、Python、`.bat`およびファイルです。

Unified Manager がインストールされているプラットフォーム	サポートされる言語
VMware	Perlスクリプトとシェルスクリプト
Linux	Perl、Python、シェルスクリプト
ウィンドウ	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環境の場合、Perl 5はデフォルトでインストールされ、スクリプトではPerl 5がサポートする機能のみがサポートされます。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スクリプトの場合、スクリプトを実行できるように、Windowsサーバで適切なPowerShell実行ポリシーを設定する必要があります。



アラートスクリプトの進捗状況を追跡するためのログファイルがスクリプトで作成される場合は、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説明を入力します。
5. `[追加]\*` 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たことを確認できます。

- 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. [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	操作
アラートを追加する	<ol style="list-style-type: none"><li>a. [追加]*をクリックします。</li><li>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。</li></ol>
アラートを編集する	<ol style="list-style-type: none"><li>a. アラートを選択し、 * 編集 * をクリックします。</li><li>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。</li></ol>

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、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あります。
- 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。
- グループ内のすべてのストレージオブジェクトに、ボリュームのしきい値の設定などの操作を同時に適用することができます。

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含めるための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。グループルールに関連付けられるオブジェクトタイプは1つだけです。
- ストレージオブジェクトは、各監視サイクルの完了後、またはルールの作成、編集、削除時にグループに対して追加または削除されます。
- 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ている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。グループルールを作成または変更すると条件が作成され、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、およびグループ化されます。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場合は、条件グループで複数の条件を使用できます。

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"><li>• オブジェクト名</li><li>• 所有クラスタ名</li><li>• 所有SVM名</li><li>• アノテーション</li></ul>
SVM	<ul style="list-style-type: none"><li>• オブジェクト名</li><li>• 所有クラスタ名</li><li>• アノテーション</li></ul>
クラスタ	<ul style="list-style-type: none"><li>• オブジェクト名</li><li>• アノテーション</li></ul>

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。

- 運用者

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ています。

- 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

ボリュームの条件グループで、次の2つの条件が設定されているとします。

- 名前に「vol」を含む
- SVM名は「`d ata\_svm」です。

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には、いずれかの条件グループを満たしている必要があります。すべての条件グループのストレージオブジェクトが組み合わせられます。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

ボリュームに対して2つの条件グループがあり、各グループに次の2つの条件が含まれているとします。

- 条件グループ1
  - 名前に「vol」を含む
  - SVM名が「`d ata\_svm」の場合、条件グループ1では、名前に「vol」を含み、名前が「`d ata\_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すると、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

グループ操作は、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操作です。たとえば、ボリュームしきい値のグループ操作を設定して、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つだけです。ただし、可能な場合は、同じグループに対して別のタイプのグループアクションを設定できます。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、グループアクションのランクによって決まります。ストレージオブジェクトに適用されてい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に表示されます。

## 固有のグループ操作の例

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対して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` ランク1のグループ操作。ボリュームの容量を設定します。
- `Change\_snapshot\_copies` ボリュームのSnapshotコピーを設定するためのランク2のグループ操作

`Change\_capacity\_threshold` グループ操作はグループ操作よりも常に優先され `Change\_snapshot\_copies`、ボリュームAに適用されます。Unified Managerによる監視が1サイクル完了すると、ボリュームAの健全性しきい値関連イベントがグループ操作ごとに再評価され `Change\_capacity\_threshold` ます。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

管理を容易にするために、グループを作成してクラスタ、ボリューム、Storage Virtual Machine (SVM) を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]\* 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ときは、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 \*
- 削除するグループに関連付けられているグループルールに関連付けられてい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）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、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、これらのグループ操作はグループを削除するとマッピング解除されます。

## グループルールの追加

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グループに動的に追加できます。グループルールを作成するには、条件を1つ以上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、グループルールの作成後すぐに追加されます。新しいオブジェクトは、監視サイクルが完了するまで追加されません。

## 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	操作
条件	<ul style="list-style-type: none"> <li>a. オペランドのリストからオペランドを選択します。</li> <li>b. 演算子として「* Contains *」または「* is *」を選択します。</li> <li>c. 値を入力するか、使用可能なリストから値を選択します。</li> </ul>
条件グループ	<ul style="list-style-type: none"> <li>a. [条件グループの追加 (Add Condition Group)] をクリックする</li> <li>b. オペランドのリストからオペランドを選択します。</li> <li>c. 演算子として「* Contains *」または「* is *」を選択します。</li> <li>d. 値を入力するか、使用可能なリストから値を選択します。</li> <li>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。</li> </ul>

7. [追加]\*をクリックします。

#### グループルールの作成例

[グループルールの追加]ダイアログボックスで、条件の設定や条件グループの追加などのグループルールを作成するには、次の手順を実行します。

#### 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. 値としてを入力し `svm\_data` ます。
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. 値としてを入力し `vol` ます。
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。

#### グループルールの編集

グループルールを編集して条件グループや条件グループ内の条件を変更し、特定のグループに対するストレージオブジェクトの追加や削除を行うことができます。

- 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。

#### グループルールの削除

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。グループの操作を設定すると、これらの操作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と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]\*をクリックします。

### グループ操作の編集

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の設定

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説明を入力します。
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]\*をクリックします。

#### グループ操作の削除

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設定されている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変更

グループ内のストレージオブジェクトに適用されるグループ操作の順序を変更できます。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できます。ただし、優先順位の変更がグループ操作のグリッドに反映されるようにするには、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 \* > \* 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ことで、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識別してフィルタリングできます。

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 ) に割り当てられるテキスト文字列 ( 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、それら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指定できます。名前と値の各ペアをルールを使用し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設定できます。また、特定のアノテーションのアノテーションルール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。アノテーションルールを作成または変更すると条件が作成され、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、およびアノテートされます。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場合は、条件グループで複数の条件を使用できます。

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"><li>• オブジェクト名</li><li>• 所有クラスタ名</li><li>• 所有SVM名</li><li>• アノテーション</li></ul>
SVM	<ul style="list-style-type: none"><li>• オブジェクト名</li><li>• 所有クラスタ名</li><li>• アノテーション</li></ul>
クラスタ	<ul style="list-style-type: none"><li>• オブジェクト名</li><li>• アノテーション</li></ul>

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 'Is' 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つの条件が設定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をアノテートするには、いずれかの条件グループの要件を満たしている必要があります。すべての条件グループの条件を満たす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

ボリュームに対して条件グループが2つ設定されたアノテーションルールで、各グループに次の2つの条件が設定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すると、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の値の説明

- 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。これらの値を使用すると、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の優先度が低い場合があります。



## 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。これらのルールでは、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と、ストレージオブジェクトをより効率的に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。

事前定義されたアノテーションには値を追加できません。

### 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]\* をクリックします。

## アノテーションの削除

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してください。

#### 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ているアノテーションのリストを表示できます。説明、作成者、作成日、値、ルール、アノテーションに関連付けられているオブジェクトなどの詳細も確認できます。

#### 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 \* 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の値の削除

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に適用されなくなった場合は、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。
- アノテーション値がアノテーションルールまたはグループルールに関連付けられていないことを確認してください。

事前定義されたアノテーションの値は削除できません。

#### 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に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と同時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	操作
条件	<ol style="list-style-type: none"><li>a. オペランドのリストからオペランドを選択します。</li><li>b. 演算子として「 * Contains * 」または「 * is * 」を選択します。</li><li>c. 値を入力するか、使用可能なリストから値を選択します。</li></ol>
条件グループ	<ol style="list-style-type: none"><li>a. [条件グループの追加 ( Add Condition Group ) ] をクリックする。</li><li>b. オペランドのリストからオペランドを選択します。</li><li>c. 演算子として「 * Contains * 」または「 * is * 」を選択します。</li><li>d. 値を入力するか、使用可能なリストから値を選択します。</li><li>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。</li></ol>

7. [追加]\*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など）、[アノテーションルールの追加]ダイアログボックス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. 値としてを入力し `svm\_data` ます。
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. 値としてを入力し `vol` ます。
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]\*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、およびSVM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、アノテーションに必要な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	操作
クラスタ	<ol style="list-style-type: none"><li>a. [* ストレージ * &gt; * クラスタ *] をクリックします。</li><li>b. 1つ以上のクラスタを選択します。</li></ol>

アノテーションの追加先	操作
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や条件グループ内の条件を変更し、ストレージオブジェクトに対するアノテーションの追加や削除を行うことができます。

- 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。

関連付けられてい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と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を満たす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、条件を考慮しません。

条件を設定するには、[Add Annotation Rule]ダイアログボックス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. 値としてを入力し `svm\_data` ます。
7. [追加]\* をクリックします。

#### アノテーションルールの削除

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変更

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を設定する場合、ランクは最も低くなります。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。

単一の行または複数の行を選択してドラッグアンドドロップ操作を繰り返し実行することで、アノテーションルールのランクを変更できます。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。

リオーダーを表示するには、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

AutoSupportメッセージよりも詳細な診断とトラブルシューティングが必要な問題については、サポートバンドルを送信する必要があります。Unified Manager Web UIおよびメンテナンスコンソールを使用して、テクニカルサポートにサポートバンドルを送信できます。

Unified Managerには、一度に最大2つのフルサポートバンドルと3つの軽量サポートバンドルが格納されます。

- 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へのAutoSupportメッセージとサポートバンドルの送信

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、環境が正しく運用されるようにしたり、環境の整合性を維持したりすることができます。AutoSupportはデフォルトで有効になっています。無効にしないでください。NetAppActive IQのメリットを活用できます。

Unified Managerサーバに関するシステムの診断情報や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送信するようにスケジュール設定したりできます。また、サポートバンドルを生成

してテクニカルサポートチームに送信することもできます。



ストレージ管理者のロールを持つユーザは、オンデマンドの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プロキシサーバのセットアップのセクションの説明に従ってHTTPを設定したりできるのは、管理者ユーザ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テクニカルサポートにオンデマンドのAutoSupportメッセージとサポートバンドルを送信する前に、設定が完了している必要があります。

#### オンデマントAutoSupportメッセージの送信

オンデマンドメッセージを生成して、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

事前に定義された特定のメッセージをテクニカルサポートに定期的送信して、問題の診断と解決を依頼できます。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プロキシサーバのセットアップのセクションの説明に従って、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。
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のアップロード

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て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、クラスタリソースが大量に使用されたり、完了までに時間がかかることがあるため、フル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含めるか除外してサポートバンドルのサイズを小さくすることができます。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。このバンドルには、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または除外するデータタイプを選択します。



いずれのデータタイプも選択しなかった場合でも、Unified Managerの他のデータでサポートバンドルが生成されます。

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てUnified Managerサーバに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、VMwareシステムの場合は/supportディレクトリ、Linuxシステムの場合には、Windowsシステムの場合には  
ProgramData\NetApp\OnCommandAppData\ocum\support\あります  
\opt/netapp/data/support/。
6. [送信 ( Send ) ] をクリックします。

#### HTTPプロキシサーバのセットアップ

Unified Managerサーバからの直接アクセスが環境で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に、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されているサーバを識別するには、この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されてい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。



基本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 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。

操作を行わないまま15分が経過すると、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、Secure Shellを使用して同時にログインすることはできません。

#### 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"> <li>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。</li> <li>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。</li> </ol>
Linux	<ol style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>c. コマンドを入力し maintenance_console 、Enterキーを押します。</li> </ol>
ウィンドウ	<ol style="list-style-type: none"> <li>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。</li> <li>b. Windows管理者としてPowerShellを起動します。</li> <li>c. コマンドを入力し maintenance_console 、Enterキーを押します。</li> </ol>

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

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ように、診断情報が含まれたサポートバンドルを生成できます。

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は、メンテナンスコンソールからサポートバンドルをNetAppに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は大量のクラスタリソースを使用したり、完了までに時間がかかることがあるため、フルサポートバンドルを選択した場合は、対象に含めるデータタイプまたは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小さくすることができます。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。このバンドルには、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、サポートバンドルに含めるまたは除外する次のデータタイプを選択または選択解除します。

- \* 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てください。

- \* 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. と入力し `g`、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はメモリを大量に消費する処理であるため、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プロンプトが表示されます。

5. と入力し `y`、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、と入力して `\n``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た場合は、パフォーマンス統計を含める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取り込みには時間とスペースがかかることがあるため、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、2021年1月1日の場合はと入力し `20210101``ます。パフォーマンス統計を含めない場合はと入力します `\n``。

b. 統計を収集する期間（指定した開始日の午前0時からの日数）を入力します。

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、そのサポートバンドルをNetAppにアップロードするかどうかを確認するメッセージが表示されます。と入力し *y*、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、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NetApp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、その他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。データを取得するには、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できます。

生成されたサポートバンドルの場所は、VMwareシステムの/supportディレクトリ、NetApp Linuxシステムの/opt/vmware/data/support/、NetApp WindowsシステムのProgramData\OnCommandAppData\ocum\supportです。

• 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、問題の詳細な診断を依頼できます。使用できるツールの例としては、FileZillaまたはWinSCP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。

ツールに/supportディレクトリの内容が表示され、既存のすべてのサポートバンドルを表示できます。

4. サポートバンドルのコピー先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できます。サポートバンドルは、SCPまたはSFTPを使用して取得できます。

- 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またはコンソールからCLIにアクセスします。
2. ディレクトリにアクセスし`support`ます。
3. 次のコマンドを使用して、サポートバンドルを取得し、ローカルディレクトリにコピーします。

使用する機能	使用するコマンド
SCP	<code>scp &lt;maintenance-user&gt;@&lt;vApp-name-or-ip&gt;:/support/support_bundle_file_name.7z &lt;destination-directory&gt;</code>
SFTP	<code>sftp &lt;maintenance-user&gt;@&lt;vApp-name-or-ip&gt;:/support/support_bundle_file_name.7z &lt;destination-directory&gt;</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表示されます。

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ています。

```
`$ 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

問題について、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できます。

- 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。

["NetApp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は、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、イベントの確認と解決、ポリシー、Storage Virtual Machine (SVM)、アグリゲートの詳細など、一般的なタスクと参照テキストがあります。

クラスタコンポーネントと競合する理由

クラスタコンポーネントが競合状態になった場合のクラスタパフォーマンスの問題を特定できます。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を解消するには、パフォーマンスを通常のレベルに戻すために、ワークロードを減らすか処理能力を高める必要があります。Unified Managerはワークロードのパフォーマンスの収集と分析を5分間隔で行うため、クラスタコンポーネントの利用率が一貫して高い場合にのみ検出します。5分インターバルの間に短時間しか続かない過剰使用の一時的な急増は検出されません。

たとえば、ストレージアグリゲート上の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し

ているために、ストレージアグリゲートが競合状態になっている可能性があります。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には、いくつかの手順を実行します。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て、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軽減するなどです。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て、ワークロードが調整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 \*

クラスタ上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は、プロトコルレイヤでの長い待機時間が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。

- \* 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処理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。

オールSANアレイクラスタをアクティブ/アクティブ構成で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、ノードで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）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は、ポリシーグループ内のすべてのワークロードがスループット制限によって調整されており、1つ以上のワークロードのレイテンシに影響しています。

- \* 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。

- \* データ処理 \*

クラスタとワークロードを含むストレージアグリゲート間の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。Data Processingを処理するノードは、イベント検出後に変更された可能性があります。Data Processingコンポーネントが競合状態にある場合は、Data Processingノードでの高利用率が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。

- \* 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を表します。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ために使用されます。MetroClusterコンポーネントが競合状態にある場合は、ローカルクラスタのワークロードによる高書き込みスループットまたはリンクの健全性の問題が、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、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は、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。アグリゲートは、HDDのみ、HDDとSSD (Flash Poolアグリゲート)、またはHDDとクラウド階層 (FabricPoolアグリゲート) で構成されます。「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が格納されているクラウド階層間の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トに関連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は、SnapMirror同期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関する詳細情報 (容量、ストレージ効率、設定、保護、アノテーション、生成されたイベントなど) を確認できます。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 \*

◦ アラートの追加

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。

◦ アノテーションの適用

選択したボリュームをアノテートできます。

◦ 保護する

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ます。このダイアログボックスで、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。ボリュームは削除されず、ボリューム上のSnapshotコピーも削除されません。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れが使用されます。

- 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。

- 逆再同期

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"](#)。



[リストア]ボタンと[関係]の処理のボタンは、同期保護関係にあるボリュームに対しては使用できません。

- \* ボリュームの表示 \*

Health : All Volumes ビューに移動できます。

### [容量]タブ

[容量]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にアグリゲートの容量の問題が原因でスペースを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。データグラフには、ボリュームのデータに使用できる実効ストレージスペースが表示されます。次のいずれかになります。

- 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いる場合、それ以上拡張することはできません。
- 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の場合は、ボリュームが最大サイズに達するためのスペースがアグリゲートにある場合）
- 次回の自動拡張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が設定されている場合）

- [Snapshotコピー]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リザーブを超えた場合に超過した容量が表示されません。

- \* 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

ペーア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に設定すると、ボリュームの使用済み論理サイズを、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的に拡張されるかどうかが表示されます。

- \* スペース保証 \*

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FlexVol volume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

書き込まれていないファイル（LUNなど）のフルサイズが保証されます。

- 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

FlexCacheボリュームでは、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、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、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増分されません。



ボリュームのタイプがData-Cacheの場合、スペースギャランティはPartialになります。

- \* 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リザーブの合計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Snapshotコピーの作成に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（使用できない容量）が表示されます。

- \* 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。デフォルトでは、フラクショナルリザーブは100に設定されています。これは、オブジェクトの上書きが完全に保護されるように、必要なリザーブスペースが100%リザーブされることを意味します。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フラクショナルリザーブの割合まで削減されます。

- 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したしきい値に達するまでの推定日数が表示されます。

[Snapshotのフルまでの日数]フィールドには、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、またはデータが不十分で増加率を計算できない場合は「該当なし」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した場合に、Snapshotコピーを自動的に削除してスペースを解放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コピー数が異なる場合があります。

- \* 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、およびその他の詳細（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、推定終了時刻など）が表示されます。

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。

## [Configuration]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、ストレージ効率化に関連する機能などの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」のいずれかです。

- 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（アクティブまたは非アクティブ）が表示されます。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

ボリュームに対して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

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。

- タイプ

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」、「一時的」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タイプは、RAID 0、RAID 4、RAID-DP、RAID-TECのいずれかです。



FlexGroupのコンスティチュエントボリュームは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場合があります。

- 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した場合に、Snapshotコピーを自動的に削除してスペースを解放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。ボリュームがSnapVault関係にある場合は、SnapVaultと表示されます。それ以外のボリュームの場合、タイプは「Regular」と表示されず。

- ストレージ効率化ポリシー

Unified Managerを使用してこのボリュームに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指定します。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

[保護]タブには、選択したボリュームの保護の詳細（遅延情報、関係タイプ、関係のトポロジなど）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。その他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せん。

- 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管理されているかどうか（「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

[Yes]、[Yes with backup option]、または[None]のいずれかが表示されます。[Yes]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ソフトウェアが実行されていても、SnapMirrorレプリケーションが可能であることを示します。「はい（バックアップオプションあり）」の場合は、SnapMirror保護が実装されており、複数のバージョンのバックアップコピーをデスティネーションに保持できます。[None]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ないことを示します。

- 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で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せん。

- 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、関係の状態は適用できず、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。

▪ チュウシ

SnapMirror転送が有効になっていますが、転送の中止処理（チェックポイントの削除など）を実行中です。

▪ カクニン

デスティネーションボリュームで診断チェックを実行中で、実行中の転送はありません。

▪ ファイナライズ中

SnapMirror転送が有効になっています。現在SnapVault差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いますが、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差分転送の転送前のフェーズです。

▪ キューに登録済み

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

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

SnapMirror転送を実行中です。追加の転送は無効になっています。

▪ 転送中

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データ転送が完了し、同期処理への移行が開始されました。

- 待機中

SnapMirror転送が開始されましたが、一部の関連タスクがキューに登録されるのを待っています。

- 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」と表示されず。

- 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、「XDPDefault」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ている詳細を確認できます。これには次の情報が含まれます。

- 転送の優先順位
- アクセス時間の設定を無視
- 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。

- スケジュールの更新

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。ポリシーは、「デフォルト」、「なし」、またはカスタムポリシーに指定された任意の名前です。

- 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とSnapMirrorボリュームの関係によって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。このフィールドには、統合された関係ステータスを表示するための[関係]ページにリダイレクトするリンクもあります。このリンクはコンスティテュエント関係にのみ適用されます。

- 整合グループ

SnapMirrorのアクティブな同期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性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グラフィカルに表示されます。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が左から右に表示され、各関係のソースが左側、デスティネーションが右側に表示されます。

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、ボリュームを保護するかデータをリストアするかを選択できます。関係を右クリックすると、関係を編集、中止、休止、解除、削除、再開するメニューが表示されます。

次の場合、メニューは表示されません。

- RBACの設定でこの操作が許可されていない場合（オペレータのPrivileges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。ボリュームの左上隅にある疑問符（）は、ボリュームが見つからないか、まだ検出されていないことを示します。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。

トポロジが複数の一般的なトポロジテンプレートのいずれかに準拠している場合は、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、トポロジビューでは、選択したボリュームとそのソースボリュームの関係が太線と青い点で示されます。

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、[Current Threshold Settings]ダイアログボックスにそのボリュームの現在の警告しきい値と重大しきい値の設定が表示されます。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。

- Snapshot

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コピーアイコン (  ) をクリックすると、 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コピー数が異なる場合があります。

- 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、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受信SnapMirrorおよびSnapVault保護関係の履歴がグラフに表示されます。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つがあります。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とSnapMirror同期関係で保護されている場合、関係の転送時間と関係の転送サイズの情報は表示されません。

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特定するのに役立ちます。たとえば、1日または1週間の同じ時間に大量のデータが転送されている場合や、遅延警告や遅延エラーのしきい値を一貫して超えている場合は、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、横軸 (x軸) には日、月、または年が、選択した期間に応じて表示されます。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、横軸 (x軸) には日、月、または年が、選択した期間に応じて表示されます。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、月、または年) 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ーベーション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。

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、ボリュームの使用済み容量と、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。期間は横軸 (x軸) に表示されます。期間は、週、月、または年を選択できます。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。該当する凡例をクリックすると、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、凡例で[ボリューム使用容量]をクリックすると、ボリュームの使用容量を示す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の詳細が縦軸 (y軸) に表示されます。期間は横軸 (x軸) に表示されます。期間は、週、月、または年を選択できます。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。該当する凡例をクリックすると、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、凡例で[トレンド-使用済み容量]をクリックすると、使用済み容量を示す線が非表示になります。

• \* 使用容量 (%) \*

折れ線グラフの形式で、ボリュームの使用済み容量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。期間は横軸 (x軸) に表示されます。期間は、週、月、または年を選択できます。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。該当する凡例をクリックすると、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、凡例で[ボリューム使用容量]をクリックすると、ボリュームの使用容量を示す線が非表示になります。

- \* Snapshot の使用容量 ( % ) \*

面グラフの形式で、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オーバーフローはさまざまな色で表されます。期間は横軸 (x軸) に表示されます。期間は、週、月、または年を選択できます。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。該当する凡例をクリックすると、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、凡例で[Snapshotリザーブ]をクリックすると、Snapshotリザーブを示す線が非表示になります。

#### [Events]リスト

[Events]リストには、新規および確認済みの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 Annotations]ペイン

[Related Annotations]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。[Related Annotations]ペインから手動の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コピーを確認し、それらの情報に移動できます。

- \* 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個のボリュームが含まれていて、そのうちの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ボリュームの場合は表示

されません。

- \* qtree \*

選択したボリュームに含まれるqtreeの数、およびクォータが適用されたqtreeの容量が表示されます。クォータが設定されたqtreeの容量は、ボリュームのデータ容量に対して表示されます。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クォータと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。親ボリュームは、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。

#### [Related Groups]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。

#### [Related Alerts]ペイン

[Related Alerts]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確認できます。[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、設定、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、保護の詳細情報を確認できます。また、Storage VMの関連する



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のみです。

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 \*

- アラートの追加

選択したStorage VMにアラートを追加できます。

- アノテーションの適用

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。

#### [Health]タブ

[健全性]タブには、ボリューム、アグリゲート、NAS LIF、SAN LIF、LUN、プロトコル、サービス、NFS共有、CIFS共有など、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情報が表示されます。

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。グラフ内の色は、問題のさまざまな重大度レベルを表します。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とSAN LIF、およびオフラインのボリュームに関する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、NFS共有と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の形式で表示されます。グラフ内の色は、問題のさまざまな重大度レベルを表します。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の概要を示すために、フィールドダイアログボックスに関係の総数（保護の問題がある関係とない関係を含む）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。ここにはStorage VM DR関係のイベントが表示され、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。グラフ内の色は、問題のさまざまな重大度レベルを表します。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。

#### [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 volume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た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]リストには、容量の問題があるボリュームの詳細が表形式で表示されません。

##### ◦ ステータス

ボリュームに、容量に関する所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、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

ボリュームの使用容量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[Yes]および[No]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ボリュームの場合は、FlexGroupで使用されているアグリゲートの数が表示されます。

#### [Configuration]タブ

[設定]タブには、選択したStorage VMの設定の詳細が表示されます。これには、Storage VMのクラスタ、ルートボリューム、含まれるボリュームのタイプ (FlexVolボリューム)、ポリシー、Storage VMに作成された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。

- 使用できるプロトコル

Storage VMに設定できるプロトコルのタイプが表示されます。また、プロトコルがアップ ( )、ダウン ( )、●または設定されていない (●) のいずれであるかを示します●。

- \* 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。また、インターフェイスがアップ ( ) またはダウン (●) のどちらであるかを示します●。

- 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。また、インターフェイスがアップ ( ) またはダウン (●) のどちらであるかを示します●。

- 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。また、インターフェイスがアップ ( ) またはダウン (●) のどちらであるかを示します●。

- \* 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。また、管理インターフェイスが稼働している ( ) か停止している ( ) か●を示します●。

- \* ポリシー \*

- スナップショット

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名前が表示され、複数作成されている場合は数が表示されます。

- \* 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は、ソースStorage VMの詳細が表示されます。ファンアウトの場合、このフィールドには、Storage VMが保護されているデスティネーションStorage VMの総数が表示されます。数のリン

クをクリックすると、ソースStorage VMでフィルタされたStorage VM関係グリッドに移動します。

- 保護されているボリューム

合計ボリュームのうち、選択したStorage VMで保護さ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が表示されます。

- 保護されていないボリューム

選択したStorage VM上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 \*

- タイプ

Storage VMに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 ; ネットワーク情報サービス)」のいずれかです。

- 都道府県

サービスの状態が表示されます。稼働 ( )、停止 ( )、未設定 ( ) のいずれ かです 。

- ドメイン名

DNSサービスの場合はDNSサーバ、NISサービスの場合はNISサーバのFully Qualified Domain Name (FQDN ; 完全修飾ドメイン名) が表示されます。NISサーバが有効になっている場合は、NISサーバのアクティブな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、NISサーバのアクティブな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。




## [ネットワークインターフェイス]タブ

[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 () のいずれかです 。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 (  ) のいずれかです 。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 \*

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 (CIFS、NFS、iSCSI、FC / FCoE、FC-NVMe、FlexCacheなど) のリストが表示されます。

- \* 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ると、現在のポートがホームポートと異なる場合があります。

- \* 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、CIFS、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インターフェイスと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されません。

- \* 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、これらのクラスタについては空の列が表示されます。

- \* 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とそのクォータの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、データセンター内のすべてのクラスタのすべてのStorage VMを対象に選択できます。エクスポートしたCSVファイルには、qtreeに関するその他のフィールドもいくつか表示されません。

### • \* ステータス \*

qtreeの現在のステータスが表示されます。Critical ( ) 、 Error ( ) 、  Warning ( ) 、  Normal ( ) のいずれ  かです  。

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重大度のイベントが複数存在する場合があります。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。エクスポートされた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。エクスポートされた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無効になっているかを示します。

- \* クォータタイプ \*

ユーザ、ユーザグループ、またはqtreeのクォータを示します。エクスポートされた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。クォータタイプがqtreeの場合、またはクォータが設定されていない場合、列は空になります。エクスポートされたCSVファイルにのみ表示されます。

- \* 使用ディスク %\*

使用されているディスクスペースの割合が表示されます。ディスクのハードリミットが設定されている場合は、ディスクのハードリミットに基づきます。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、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に割り当てられているディスクスペースの最大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量が表示されます。この量を超えると、警告イベントが生成されます。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、ファイルのハードリミットに基づきます。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のユーザークォータとユーザーグループ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ーグループの名前、ディスクとファイルに設定されている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表示できます。ユーザまたはユーザー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ーグループの現在のEメールアドレスが表示されます。Eメールアドレスは変更できます。[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、選択したユーザーまたはユーザーグループのメールアドレスが生成されます。

クォータが同じユーザが複数ある場合は、ユーザの名前がカンマで区切って表示されます。また、デフォルトルールはEメールアドレスの生成には使用されないため、通知の送信に必要な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に設定されているユーザまたはユーザー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。Critical ( )、Warning ( )、 Normal ( ) のいずれかです 。

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。クォータが同じユーザが複数ある場合は、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クォータを指定します。

- \* ボリュームまたは qtree \*

ユーザクォータまたはユーザグループ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、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 %\*

使用されているディスクスペースの割合が表示されます。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 \*

クォータに割り当てられているディスクスペースの最大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」と表示されません。

- \* ディスクソフトリミット \*

クォータに対して割り当てられているディスクスペースの量が表示されます。この量を超えると、警告イベントが生成されます。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、値は「無制限」と表示されません。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 \*

クォータに違反があった場合に通知を送信す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 (SMB 共有) タブ

[NFS共有]タブには、NFS共有に関する情報が表示されます。これには、ステータス、ボリューム (FlexGroupまたはFlexVol) 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含まれます。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。Error()またはNormal()の  いずれかです .

• \* 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列に表示されます。

• \* 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

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。

- mixed

FlexGroupボリュームの一部のコンスティチュエントが同じ状態ではありません。

- \* 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。セキュリティ形式は、UNIX、unified、ntfs、mixedのいずれかです。

- 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る。

- 統合

ボリューム内のファイルおよびディレクトリのセキュリティ形式はunifiedです。

- 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。

- mixed

ボリューム内のファイルおよびディレクトリにUNIXアクセス権またはWindows NTFSアクセス権を設定できます。

- \* UNIX 権限 \*

エクスポートされているボリュームに対して設定されたUNIX権限ビットを8進数の文字列形式で表示します。UNIX形式の権限ビットに似ています。

- \* 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関する詳細（認証プロトコルやアクセス権限など）を確認できます。

## SMB Shares (SMB 共有) タブ

選択したStorage VM上の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表示できます。SMB 共有に相当する NFS パスが存在するかどうかも確認できます。



フォルダ内の共有は[SMB共有]タブに表示されません。

- \* 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と権限の詳細を確認できます。

- \* ステータス \*

共有の現在のステータスが表示されます。Normal ( ) または Error (  ) のいずれかです .

- \* 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には、ボリュームまたはqtreeを指定できます。

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

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。

- mixed

FlexGroupボリュームの一部のコンスティチュエントが同じ状態ではありません。

- \* 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。セキュリティ形式は、UNIX、unified、ntfs、mixedのいずれかです。

- 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る。

- 統合

ボリューム内のファイルおよびディレクトリのセキュリティ形式はunifiedです。

- 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。

- mixed

ボリューム内のファイルおよびディレクトリにUNIXアクセス権またはWindows NTFSアクセス権を設定できます。

- \* エクスポートポリシー \*

共有に適用され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関する詳細（アクセスプロトコルや権限など）を確認できます。このリンクは、選択したStorage VMで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、[LUN]ビューが表示されます。イニシエータグループに関する詳細は[イニシエータグループ]タブで、イニシエータに関する詳細は[イニシエータ]タブで確認できます。

- \* 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名、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確認できます。[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。

また、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、および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も表示できます。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、サポートされているプロトコルなどの詳細を表示できます。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が表示されます。

- \* 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表示できます。[Mapped Interfaces]列の個数のリンクをクリックすると、すべてのインターフェイスまたはポートセットの特定のインターフェイスのいずれかが表示されます。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の総数が表示されます。

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とイニシエータも表示できます。

- \* 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総数が表示されます。

```
initiator groups that are mapped to the selected initiator group.
```

#### [Related Annotations] ペイン

[Related Annotations] 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。[Related Annotations] ペインから手動のアノテーションを削除することもできます。

#### [Related Devices] ペイン

[関連デバイス] ペインでは、Storage VMに関連するクラスタ、アグリゲート、および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、そのうち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」と表示されません。

- \* 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もカウントされます。FlexGroupコンスチチュエントは含まれません。

#### [Related Groups] ペイン

[関連グループ] 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。

#### [Related Alerts] ペイン

[Related Alerts] 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関する詳細情報（健全性、容量、構成の詳細など）が表示されます。また、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表します。フェイルオーバーのステータスやクラスタ全体のステータスを表すものではありません。

#### 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は、WFAからキャッシュデータがあれば再検出処理でも再取得されます。

再検出処理が開始されると、関連す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。

### [Health]タブ

ノード、SVM、アグリゲートなど、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提供機能に関連しています。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ています。

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SVMのリストが表示されます。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のリストを確認できます。

### 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。グラフ内の色は、問題のさまざまな重大度レベルを表します。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のアグリゲートに関する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の状態に基づいています。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。グラフ内の色は、問題のさまざまな重大度レベルを表します。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。

### [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。

- 使用済みの論理スペース

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テクノロジーによる削減を適用する前のサイズです。Snapshotコピーは含まれません。

- データ削減

Snapshotコピーを含まず、有効な2桁の比率（1.8：1など）が表示されます。この比率は、ONTAPのStorage Efficiency設定に基づいて計算されます。

- 使用済み

すべてのアグリゲートのデータで使用されている物理容量。これには、パリティ、サイズ適正化、リザーベーション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

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の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、サイズ適正化、リザーベーション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

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

クラスタ上の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と、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には、ライセンスが設定されているかどうかを指定できます。

## 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内訳]領域には、クラスタ内の各種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、[ディスク]タブでディスクタイプに関する詳細を確認できます。

- 使用可能な合計容量

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内のデータディスクのスペア容量が点線で示されます。

- 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]リスト

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、重大度レベルが「Error」と「Critical」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「Critical」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。

#### [Configuration] タブ

選択したクラスタに関する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がクラスタへの接続に使用するクラスタ管理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するクラスタ管理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アレイが設定された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構成の場合にのみ表示されます。

- 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構成または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構成に対してのみ表示されます。

- タイプ

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。

- 構成

FCおよびIPを介した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では、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せん。

- IPの場合\*
- イーサネットスイッチを使用したIP設定（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。デフォルトでは、Unified Managerの2ノードMetroCluster構成のすべてのクラスタでAUSOが有効になっています。AUSO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。

- スイッチオーバーモード

MetroCluster over IP設定のスイッチオーバーモードを表示します。使用可能な値はActive、Negotiated Switchover、および`Automatic Unplanned Switchover`です。

## ノード

- 可用性

クラスタ内で稼働しているノード ( ) または停止しているノード ( ● ) の数が表示されます ●。

- OSバージョン

ノードで実行されているONTAPのバージョンと、特定のバージョンの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

クラスタ内で稼働 ( ) または停止 ( ● ) しているSVMの数が表示されます ●。

## ネットワークインターフェイス

- 可用性

クラスタ内で稼働している ( ) または停止 ( ) して ● いるデータLIF以外のLIFの数が表示されます ●。

- 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、およびメディエーターの接続ステータスが表示されます。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

クラスタでメディエーターがサポートされ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。緑色は、メディエーターステータスが到達可能であることを示します。赤色はメディエーターステータスに到達できないことを示します。

## 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の[Connectivity]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を表示します。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ボックスで表示されます。



MetroClusterの[Connectivity]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、デフォルトの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。

問題が発生したコンポーネントにカーソルを合わせると、クラスタの詳細と接続ステータスや、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の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。[詳細を表示]ボタンをクリックすると、イベントに関する詳細情報が表示されます。

コンポーネント間の接続の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の間でデータを同期的にミラーリングすることでデータを確実に保護できます。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ボックスで表示されます。



MetroClusterの[Replication]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論理接続および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表したものを表示できます。これは、メタデータとデータのミラーリング中に発生する可能性がある問題を特定するのに役立ちます。

MetroClusterの[Replication]タブでは、選択したクラスタがローカルクラスタに、リモートクラスタがMetroClusterパートナーに表示されます。



#### [ネットワークインターフェイス]タブ

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。

#### ネットワークインターフェイス




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 ( ? ) のいずれかです。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 () のいずれかです 。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異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、これらのクラスタについては空の列が表示されます。


## 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。

## [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、ディスクセルフ、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ているか、環境上の問題が発生しています。

- \* 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表示し、リスクを回避するために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バッテリー、フラッシュカード、サービスプロセッサ、ディスクシェルフの接続など、HAペアとその環境に関連するイベントのリストを表示できます。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。

ディスクシェルフと環境コンポーネントに対して生成されたイベント、および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。

- \* 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、電圧センサーなど、ディスクシェルフの環境の詳細が表示されます。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」、「不明」、「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

関連付けられているFCポート、FCoEポート、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。ポートアイコンをクリックすると、ポートおよび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のように指定できます。

- 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。

- タイプ

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。指定できるタイプは、イーサネット、ファイバチャネル、およびFCoEです。


- WWPN

ポートのWorld Wide Port Name (WWPN) 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」 ( ) のいずれかです .

[イベント]リストでポート関連のイベントを確認できます。関連付けられているLIFの詳細 (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) も確認できます。

## [Disks]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。使用済みディスク、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、その他の詳細も確認できます。

### ディスクプールの概要

実質的タイプ (FCAL、SAS、SATA、MSATA、SSD、NVMe SSD、SSDキャップ、アレイLUN、VMDISK) 別のディスク数、およびディスクの状態が表示されます。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、サポート対象外ディスクの数など、その他の詳細も確認できます。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。

### 都道府県

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とリモートクラスタのどちらに配置されているかを示す「はい」または「いいえ」と表示されます。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

コンテナタイプ (コピー、データ、パリティなど) に基づいてディスクの位置が表示されます。デフォルトでは、この列は表示されません。

## 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

サイズ適正化およびRAID構成前の未フォーマット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。

## タイプ

ディスクのタイプ（ATA、SATA、FCAL、VMDISKなど）が表示されます。

## 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、アグリゲートの作成、アグリゲートへの追加、およびスペアの管理において同じタイプとみなされます。ONTAPでは、各ディスクタイプに実質的ディスクタイプが割り当てられません。

## 使用済みスペアブロック

SSDディスクで使用されている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の場合は空白になります。

## 使用済み寿命

SSDの実際の使用状況とメーカーによるSSDの寿命予測に基づいて、SSDの推定使用済み寿命の割合が表示されます。値が99より大きい場合は推定寿命が消費されていることを示しますが、SSDで障害が発生しているとは限りません。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。

### **[Related Annotations]ペイン**

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。[Related Annotations]ペインから手動の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、デバイスのタイプ、サイズ、数、健全性ステータスなど、クラスタに接続されているデバイスのプロパティが含まれます。カウントリンクをクリックすると、その特定のデバイスに関する詳細な分析が表示されます。

[SVMパートナー]ペインを使用してMetroCluster、リモートMetroClusterパートナーとそれに関連付けられているクラスタコンポーネント（ノード、アグリゲート、SVMなど）の数と詳細を確認できます。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、およびアグリゲートを確認して移動できます。

### **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すると、さらに詳しい情報に移動して、クラスタコンポーネントの健全性と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。

### [Related Groups] 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。

### [Related Alerts] ペイン

[Related Alerts] 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。[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 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関する詳細情報（容量、ディスク情報、設定の詳細、生成されたイベントなど）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している場合、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（パフォーマンス階層）の容量のみに関連します。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 \*

- アラートの追加

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。

## [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対して容量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適用されます。

- \* 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。

- 使用済みの論理スペース

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

アグリゲート内の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（アグリゲートのスペースがほぼフルである）場所に点線が表示されます。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

エラーしきい値が設定されている（アグリゲートのスペースがフルである）場所に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リザーブを超えた場合に超過した容量が表示されません。



• \* 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せん。FabricPoolには、ライセンスが設定されているかどうかを指定できます。

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。

• \* 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の使用済み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が表示されます。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は、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合計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には、ライセンスが設定されているかどうかを指定できます。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）または割り当て単位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

アグリゲート容量の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。

▪ オーバーコミットのしきい値

アグリゲートがオーバーコミットされたら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時間続く場合に、アグリゲートで使用されているディスクスペースが表示されます。

たとえば、アグリゲートが午後2時に10GB、午後6時に12GBのディスクスペースを使用している場合、このアグリゲートの日次増加率（GB）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。

▪ 送信されたボリューム

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。

▪ 追加されたボリューム

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の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。

表示するグラフを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、プロビジョニング済みサイズ、使用可能な容量、1日あたりの最大増加率、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も確認できます。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。

#### [ディスク情報]タブ

選択したアグリゲート内のディスクに関する詳細情報（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）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）も図で表示されます。パリティディスクと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グラフィカルに表示されます。データディスクに専用ディスクと共有ディスクが含まれている場合は、専用データディスクと共有データディスクの両方の詳細図が表示されます。

##### ◦ \* 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。

##### ▪ タイプ

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グループで許可されている最大ディスク数が表示されます。

##### ▪ 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

アグリゲート内のデータディスクのタイプ（ATA、SATA、FCAL、SSD、VMDISKなど）が表示されます。

##### ▪ 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可能な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ディスクの詳細が表示されます。

専用キャッシュSSDディスクについて次の詳細が表示されます。

- \* RAIDの詳細\*

- タイプ

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グループで許可されている最大ディスク数が表示されます。

- 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のタイプがSSDであることを示します。

- 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、次の詳細を確認できます。

▪ ステータス

ストレージプールのステータス（正常または異常）が表示されます。

▪ 割り当て合計

ストレージプール内の割り当て単位の合計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、破損しているディスクがあり、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は、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ここに表示されます。

#### [Configuration]タブ

[構成]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

アグリゲートのブロック形式（32ビットまたは64ビット）が表示されます。

- RAIDタイプ

RAIDタイプ（RAID 0、RAID 4、RAID-DP、RAID-TEC、またはMixed 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は、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（StorageGRID、Amazon S3、IBM Cloud Object Storage、Microsoft Azureクラウド、Google Cloud Storage、Alibaba Cloud Object Storageなど）が表示されます。

### ◦ 名前

ONTAPでの作成時の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するポート。

### ◦ 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

クラウド階層で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か月、または1年を選択して、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済み容量とアグリゲート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。期間は横軸（x軸）に表示されます。期間は、週、月、または年を選択できます。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。該当する凡例をクリックすると、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、凡例で[使用

済み容量]をクリックすると、使用済み容量を示す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と合計容量（バイト、KB、MBなど）が縦軸（y軸）に表示されます。期間は横軸（x軸）に表示されます。期間は、週、月、または年を選択できます。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。該当する凡例をクリックすると、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、凡例で[トレンド-使用済み容量]をクリックすると、使用済み容量を示す線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使用状況が縦軸（y軸）に表示されます。期間は横軸（x軸）に表示されます。期間は、週、月、または年を選択できます。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。該当する凡例をクリックすると、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、凡例で[スペースコミット済み]をクリックすると、[スペースコミット済み]グラフの線が非表示になります。

### [Events]リスト

[Events]リストには、新規および確認済みの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すべてのアグリゲート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、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、そのうち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コンステイ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。

#### [Related Alerts] ペイン

[Related Alerts] 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。[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の表示"](#)

# データの保護とリストア

## 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保護の種類

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。SnapMirror保護では、フェイルオーバーによるディスタリカバリによる保護がすべて提供されますが、パフォーマンス、バージョンの柔軟性、複数のバックアップコピーによる保護の機能は異なります。

#### 従来のSnapMirror非同期保護関係

従来のSnapMirror非同期保護は、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を提供します。

従来の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、従来のSnapMirror保護を使用するには、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以降である必要があります（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、デスティネーションで以前のメジャーバージョンが実行されているためサポートされません。

#### バージョンに依存しないレプリケーションによる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の間で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。ボリュームがONTAP 8.3以降の異なるバージョン（バージョン8.3から8.3.1、8.3から9.1、9.2.2から9.2など）で実行されている場合でも同様です。

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関係では、ミラー処理が従来のSnapMirror関係ほど高速ではありません。

実行速度が遅いため、次のいずれかの状況では、バージョンに依存しないレプリケーション保護を使用したSnapMirrorの実装は適していません。

- ソースオブジェクトには保護対象のファイルが1,000万個以上含まれています。
- 保護されるデータの目標復旧時点が2時間以下である。（つまり、ソースのデータよりも2時間以上古いリカバリ可能なミラーデータがデスティネーションに常に含まれている必要があります）。

上記のいずれかの状況では、デフォルトのSnapMirror保護をブロックレプリケーションベースで高速に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による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と、ミラーされた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コピーを指定できます。また、ソースのコピーが削除された場合でも、それらのコピーをデスティネーションに保持する期間を指定することもできます。

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するSnapMirror関係では、ミラー処理が従来の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（ミラーとバックアップ）

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を初めて起動したとき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ではベースラインに古い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時に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へのクライアント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時に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の同期が失われ、プライマリボリュームへのクライアントI/Oが続行されます。



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アクティブ同期

SnapMirrorのアクティブな同期機能はONTAP 9.8以降で使用できます。この機能を使用すると、LUNでアプリケーションを保護できます。これにより、アプリケーションが透過的にフェイルオーバーされ、災害発生時にビジネス継続性が確保されます。

クラスタおよびStorage Virtual Machineで使用可能な整合グループ（CG）の同期SnapMirror関係をUnified Managerから検出および監視することができます。SnapMirrorアクティブ同期は、AFFクラスタまたはオールSANアレイ（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には、AFFまたはASAを使用できます。SnapMirror Active Sync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。

SnapMirrorのアクティブな同期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、ボリュームインベントリ内のコンシステンシグループ、コンシステンシグループ関係の保護トポロジ、コンシステンシグ

ループ関係の過去1年間の履歴データの表示が統一されます。レポートをダウンロードすることもできます。また'コンシステンシ・グループ関係の概要の表示'コンシステンシ・グループ関係のサポートの検索'コンシステンシ・グループによって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

[Relationships]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に対して、保護のソート、フィルタ、拡張を行うこともできます。

SnapMirrorアクティブ同期の詳細については、を参照してください"[SnapMirror Active Sync \(旧SM-BC\) に関するONTAP 9ドキュメント](#)"。

## Unified Managerでの保護関係の設定

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) の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](#)"です。
  - "[Workflow AutomationでのUnified Managerデータソースのキャッシングの確認](#)"です。

### 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](#)"です。
  - "[SnapVault 保護関係を作成する](#)"です。
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](#)"です。
  - "[SnapMirror ポリシーを作成する](#)"です。
3. "[SnapMirror または SnapVault スケジュールを作成します](#)"です。

## 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設定できます。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」が含まれているため、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 \*

"[NetApp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、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した場合の動作

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。

### Unified ManagerからのOnCommand Workflow Automationセットアップの削除

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の実行

ハードウェア障害や災害によって保護関係のソースボリュームが無効になった場合は、Unified Managerの保護関係機能を使用して保護関係のデスティネーションを読み取り/書き込み可能にし、そのボリュームにフェイルオーバーして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できます。その後、ソースがデータを提供できるようになったら、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のセットアップが完了している必要があります。

#### 手順

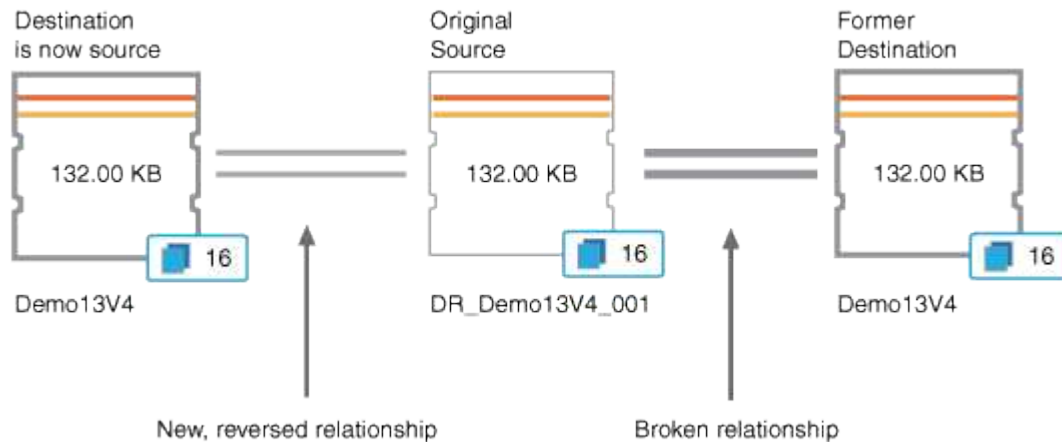
1. "SnapMirror関係を解除する"です。

デスティネーションをデータ保護ボリュームから読み取り/書き込み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"です。

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することもできます。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、ソースボリュームを以前のデスティネーションと同期します。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"です。

元のソースボリュームが再同期されて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した関係を解除します。

4. "関係を削除します"です。

反転した関係が不要になった場合は、元の関係を再確立する前にその関係を削除する必要があります。

5. "関係を再同期します"です。

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]ページでの**SnapMirror**関係の解除

[ボリューム/健全性の詳細]ページで保護関係を解除して、SnapMirror関係が確立された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の場合、またはアプリケーションのテストの場合に行うことができます。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更されます。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。

[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]ページでの保護関係の反転

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関係を使用することはできません。
- 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。
- ソースを別のデータ保護ボリュームのデスティネーションにす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上のデータが削除されます。
- 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。

[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]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]ページでの保護関係の削除

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。

[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。

[ボリューム/健全性の詳細]ページで関係が削除されます。

#### [ボリューム/健全性の詳細]ページでの保護関係の再同期

SnapMirror関係またはSnapVault関係を解除してデスティネーションが読み取り/書き込み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またはSnapVaultの更新が失敗した場合にも実行できます。

- 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。

- 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。

[Resynchronize]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。

[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。

[Resynchronize]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。

## 保護ジョブの失敗の解決

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では、管理者ロールでログインする必要があるため、各種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、考えられる原因と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。



イベントのリンクテキストは、などの `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed` 形式で記述されます。`object\_name:/object\_name - Error Name`。

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 "[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

[イベントの詳細]ページの[原因]フィールドでジョブの失敗に関するエラーメッセージを確認し、ジョブが失敗した原因がSnapshotコピーエラーであることを確認します。その後、[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。

[Event details]ページの[Cause]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。

このジョブには、仮想サーバ上の `cluster2\_src\_svm` ソースボリュームと、という名前の仮想サーバ上の `cluster3\_dst\_svm` デスティネーションボリュームの `managed\_svc2\_vol3` 間の保護関係が関係している `cluster2\_src\_vol2` でした。

- ソースボリューム上の `cluster2\_src\_svm:/cluster2\_src\_vol2` に対する Snapshot コピージョブが失敗しました `0426cluster2\_src\_vol2snap` た。

このシナリオでは、ジョブの失敗の原因と考えられる対処方法を特定できます。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たことを確認します。これは、ソースボリュームに問題がある可能性があることを示しています。

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。

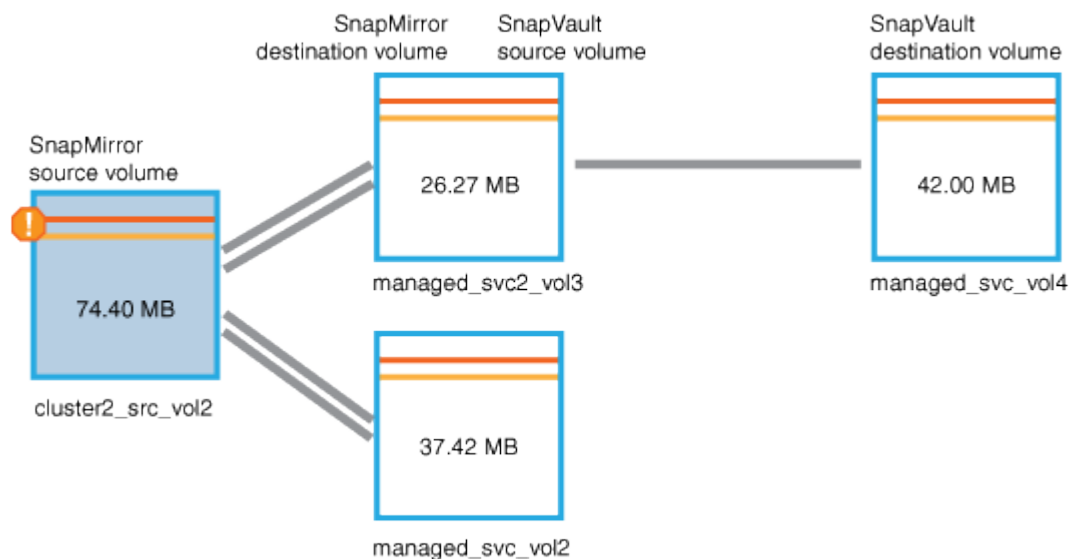
2. イベントを解決するために、次の作業を行います。
  - a. [\* Assign to \* (\* への割り当て) ] ボタンをクリックし、メニューから [\* Me\* (\* Me \* ) ] を選択します
  - b. [\* Acknowledge \* (確認) ] ボタンをクリックして、イベントにアラートが設定されている場合は、繰り返しアラート通知を受信しないようにします。
  - c. 必要に応じて、イベントに関するメモを追加することもできます。
3. [Summary] \* ペインで [Source] \* フィールドをクリックして、ソース・ボリュームの詳細を表示します。

「\* 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、`cluster2\_src\_vol2`、[保護]タブの内容が表示されます。

4. 保護トポロジグラフを見ると、トポロジの最初のボリューム (SnapMirror関係のソースボリューム) にエラーアイコンが関連付けられています。

ソースボリュームアイコンには、そのボリュームに設定された警告およびエラーのしきい値を示す水平バーも表示されます。



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ボックスが表示され、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が発生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` が表示されます。

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おり、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します。

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、ソースボリュームの[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]\*領域で、イベントの[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. サマリ領域の下に推奨される対処方法が表示されます。



[推奨される対処方法] は一部のイベントに対してのみ表示されるため、すべてのタイプのイベントで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行する推奨される対処方法のリストをクリックして確認します。

- 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、そのためには、親アグリゲートの使用可能な空きスペースとボリュームの現在の増加率を確認する必要があります。
    - a. [関連デバイス] ペインで、親アグリゲートを確認し `cluster2\_src\_aggr1` 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、重大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 にアクセスするか、ONTAP CLI にアクセスしてオプションを有効にして `volume autogrow` ください。



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。

## チエンノモンタイノカイケツ

このワークフローでは、遅延の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[Dashboard]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見つけます。

- 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]ページの[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]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。
  - このイベントについ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。
  - イベントに回答するか、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つのボリュームからなる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に注意してください。選択したボリュームはダークグレーの線で囲まれ、ソースボリュームからのオレンジの二重線はSnapMirror関係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、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転送を実行しようとしていることがわかりました。

7. 遅延の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2つのスケジュールを変更して、ソースの転送完了後に各デスティネーションがSnapMirror転送を開始するようにします。

## 保護関係の管理と監視

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行うことができます。

SnapMirror処理には、次の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決定されます。

- 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。

保護ジョブは最大10個まで同時に実行でき、パフォーマンスに影響はありません。11~30個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の表示

[Data Protection]ページには、単一のクラスタ内またはデータセンター内のすべてのクラスタについて、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包括的に表示

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. [Data Protection]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。

このページには、データセンターで単一のクラスタとすべてのクラスタのどちらを選択したかに応じて、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。

このページの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]イン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。マウスにカーソルを合わせると、それぞれのカウントと凡例が表示されます。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を使用して、[ボリューム]ページに移動して詳細を確認します。
- すべての関係の棒グラフで[Relationships]ページが表示され、ソースクラスタで詳細が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の表示

- 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
- Snapshotコピーで保護されているが保護されていないボリュームの総数。
- Snapshotコピー用のリザーブスペースを使用しているボリューム、または超過しているボリュームの総数。
- 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を含む）。
- Snapshotコピーで保護されているボリュームと保護されていないボリュームの詳細グラフ。
- リザーブされたSnapshotコピー容量を使用しているボリューム、使用していないボリューム、および超過しているボリューム。
- Snapshotコピー数を基準にしたボリューム数の分割。


### Snapshotコピーの注意事項

- Snapshotコピーで保護されているボリュームをカウントする場合は、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についてのみ返されます。
- Snapshotコピー数のグラフ範囲は動的です。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みなすには、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表示したり、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したりする場合に重要です。

### SnapMirror関係の保護ステータスの表示

- 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。
- 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（Volume SnapMirror関係、Storage VM ディザスタリカバリ（SVM-DR）、それらの組み合わせなど）。
- 遅延ステータスに基づくRecovery Point Objective（RPO；目標復旧時点）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関係に対して生成された個々のイベント（過去24時間に生成されたイベントを含む）
- 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。
- SnapMirror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、StricxtSync、SnapMirrorのアクティブな同期整合性グループ、Syncなど）で保護されている関係の数。
- 正常な関係と正常でない関係の数。
- ボリューム関係数の内訳。RPOの遅延時間とステータス別にグラフを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 ( ) をクリックすると、遅延しきい値を設定できます 。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しきい値の設定"](#)。

### SnapMirror関係の注意事項

- SnapMirror関係をカウントする場合は、読み取りと書き込みが有効になっている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関係の場合は、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の関係に基づきます。ステータスは、設定されている関係のしきい値に基づいて、`warning`または`error`に分類され`ok`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、または問題への対処が必要かどうかを確認できます。
- ボリュームにSnapMirror関係が複数ある場合は、各関係タイプがRPO遅延の対象としてカウントされません。
- ソースとデスティネーション間のデータレプリケーションに問題がある場合（関係が解除されている場合など）は、ボリューム関係は正常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

[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[Clusters]ページが表示され、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構成の監視の詳細については、[を参照してください "MetroCluster設定の監視"](#)。

## ボリュームの保護関係の表示

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。

## 整合性グループ関係にあるLUNの監視

ONTAP環境でSnapMirror Active Syncがサポートされ、LUNを使用するアプリケーションを保護している場合は、Active IQ Unified ManagerでそれらのLUNを表示および監視できます。

SnapMirrorアクティブ同期により、SAN環境でフェイルオーバー時の目標復旧時間（RTO）がゼロになります。SnapMirrorアクティブ同期をサポートする一般的な構成では、ボリューム上のLUNがコンシステンシンググループ関係によって保護されます。

これらのプライマリLUNとセカンダリLUNは、同じUUIDとシリアル番号を持つ複合LUN、またはレプリカLUNペアです。I/O処理（読み取りと書き込みの両方）は、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、透過性が確保されます。

複合LUNを表示するには、整合性グループ関係に含まれる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がUnified Managerで追加および検出されている必要があります。iSCSI LUNとFCP LUNのみがサポートされます。

SnapMirrorアクティブ同期の詳細については、を参照してください"[SnapMirror Active Sync \(旧SM-BC\) に関するONTAP 9ドキュメント](#)"。

環境内の複合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の詳細 (LUN名、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) を表示できます。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。[整合グループ]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]ページにある[SAN]タブで設定の詳細を確認できます。イニシエータとイニシエータグループ、およびパートナーLUNのその他の要素などの情報が表示されます。

環境内の保護されたLUNのレポートのソート、フィルタリング、生成、アップロードなど、標準的なグリッドレベルの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の設定でこの操作が許可されていない場合：たとえば、オペレータのPrivilegesしかない場合
- 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. [\* 健全性：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]ダイアログボックスが表示されます。

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、[Job details]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リングされたリストが表示されず。

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]ページでのSnapVault保護関係の作成

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には、[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。
- 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の設定でこの操作が許可されていない場合：たとえば、オペレータのPrivilegesしかない場合
- 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]ダイアログボックスが表示されます。

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」ページの上にある保護設定ジョブのリンクをクリックします。

[Job details]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の設定でこの操作が許可されていない場合：たとえば、オペレータのPrivilegesしかない場合
- 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]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、[Job details]ページが表示されます。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。

設定時に指定したデスティネーションSVMや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を指定した場合は、デフォルトでブロックレプリケーションベースのSnapMirror関係が作成されません。
- ソースボリュームと同じか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は、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、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る場合は、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]ページでの**SnapMirror**保護関係の作成

[ボリューム/健全性の詳細]ページでは、データレプリケーションを保護用に有効にするためのSnapMirror関係を作成できます。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の設定でこの操作が許可されていない場合：たとえば、オペレータのPrivilegesしかない場合

- 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など

保護ジョブは最大10個まで同時に実行でき、パフォーマンスに影響はありません。11~30個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]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[Job details]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。

設定時に指定したデスティネーションSVMや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を指定した場合は、デフォルトで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は、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。
- 以前のバージョンのONTAP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を指定した場合は、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するSnapMirror関係が自動的に作成されます。

## 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で異なるバージョンのONTAPが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]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で実行されているデスティネーションSVMを指定し、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る場合は、SnapMirrorで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、\* アドバンスト \* 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[Job details]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保護を実装し、デスティネーションの場所に複数のバージョンのバックアップコピーを保持できます。

- 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。

バックアップオプション機能を使用してSnapMirrorを設定すると、ボリュームのフェイルオーバーなどのSnapMirrorディザスタリカバリ機能でデータを保護しながら、複数のバックアップコピーによる保護などのSnapVault機能を提供できます。

### 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]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[Job details]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の設定

[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での効率化設定（重複排除、圧縮、自動拡張、スペースギャランティなど）を指定できます。これらの設定は、デスティネーションまたはセカンダリボリュームのスペース利用率を最大限に高める場合に使用します。

- 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、効率化の設定はソースボリュームと同じです。ただし、SnapVault関係の圧縮の設定は例外で、デフォルトでは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 \* ） ]

[Advanced Destination Settings]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スケジュールの作成

SnapMirrorおよびSnapVaultの基本スケジュール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。これにより、ボリュームでデータが変更される頻度に応じて、転送の実行頻度を増減できます。

- 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[デスティネーション情報]領域の設定が完了し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]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。

## 保護を既存の保護関係から拡張するためのカスケード関係またはファンアウト関係の作成

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場合や、バックアップを追加で作成して保護を強化する場合に実行します。

複数のボリュームを格納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し、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。Unified Managerの[関係]ページで、SnapMirrorアクティブな同期整合性グループと同期整合性グループ関係を確認できます。

- 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。
- 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、[ボリュームの詳細]ページで関係を確認することもできます。
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、[統合関係/ボリューム関係]および[ボリューム/健全性]の詳細ページで確認できません。

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。

## [Volume Relationships]ページでの保護関係の編集

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。関係を編集して、転送に使用する帯域幅を減らしたり、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頻度を増やしたり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]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]ページでの保護関係の編集

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。関係を編集して、転送に使用する帯域幅を減らしたり、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頻度を増やしたり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のSnapMirrorポリシーの作成

SnapMirrorポリシーを作成して、保護関係の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の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限に高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。
- 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、[Configure Protection]ダイアログボックスの[Destination Information]領域の設定が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。

[Create SnapMirror Policy]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ポリシーの作成

新しいSnapVaultポリシーを作成して、SnapVault転送の優先順位を設定できます。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[デスティネーション情報]領域の設定が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]ページでのアクティブなデータ保護転送の中止

実行中のSnapMirrorレプリケーションを停止する場合は、アクティブなデータ保護転送を中止できます。ベースライン転送後の転送については、再開チェックポイントをクリア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。



整合性グループで保護されているボリューム関係を中止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。

中止処理は、次の場合には表示されません。

- RBACの設定でこの操作が許可されていない場合：たとえば、オペレータのPrivilegesしかない場合
- 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。

[Abort Transfer]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]ページでのアクティブなデータ保護転送の中止

実行中のSnapMirrorレプリケーションを停止する場合は、アクティブなデータ保護転送を中止できます。ベースライン転送でない場合は、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。



整合性グループで保護されているボリューム関係を中止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。

中止処理は、次の場合には表示されません。

- RBACの設定でこの操作が許可されていない場合：たとえば、オペレータのPrivilegesしかない場合
- 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. [\* 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。

[Abort Transfer]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]ページでの保護関係の休止

[Volume Relationships]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することができます。関係の休止は、データベースが格納されている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コピー処理中にデータベース内容の安定を確保するために行うことができます。

- 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。

次の場合は休止操作が表示されません。

- RBACの設定でこの操作が許可されていない場合（たとえば、オペレータのPrivilegesしかない場合）
- 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]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]ページでの保護関係の休止

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、データベースが格納されている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内容の安定を確保するために行うことができます。

- 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。

次の場合は休止操作が表示されません。

- RBACの設定でこの操作が許可されていない場合（オペレータのPrivileges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。

## [Volume Relationships]ページでのSnapMirror関係の解除

保護関係を解除すると、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中止できます。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の場合、またはアプリケーションのテストの場合に行うことができます。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更されません。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。

[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。

[Relationship State]列はデフォルトでは非表示になっているため、必要に応じて[show/hide column]リストで選択します。

## [ボリューム関係]ページでの保護関係の削除

[Volume Relationships]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。

[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。

[Volume Relationships]ページで関係が削除されます。

## 休止中の関係のスケジュールされた転送を[Volume Relationships]ページで再開

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。転送は、次のスケジュールされた転送の実行時にチェックポイント（存在する場合）から再開されます。

- 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]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. [Jobs]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

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。転送は、次のスケジュールされた転送の実行時にチェックポイント (存在する場合) から再開されます。

- 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]ページでの保護関係の初期化または更新

[ボリューム関係]ページでは、新しい保護関係の初回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してただちに転送する場合は、関係を更新できます。



整合性グループで保護されているボリュームを初期化または更新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。
- 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。

[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]ページでの保護関係の初期化または更新

新しい保護関係では初回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。

初期化/更新 (Initialize/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。

[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。

[初期化/更新 (Initialize/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。

すべてのジョブタスクが正常に完了すれば、初期化処理または更新処理は終了です。

## [ボリューム関係]ページでの保護関係の再同期

[Volume Relationships]ページでは、ソースボリュームを無効にした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、関係を再同期できます。

- 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。

### 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。

[Resynchronize]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。

[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。

[Resynchronize]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、[Volume Relationships]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]ページでの保護関係の反転

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関係を使用することはできません。
- 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。
- ソースを別のデータ保護ボリュームのデスティネーションにす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上のデータが削除されます。
- 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。

[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、[Volume Relationships]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]および[ボリューム/健全性]の詳細ページのリストア機能を使用して、上書きまたは削除されたファイル、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用に設定されている。

### 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。[Restore]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"[\[Restore\]ダイアログボックス](#)".
3. デフォルトと異なる場合は、データのリストア元となるボリュームおよびSnapshotコピーを選択します。
4. リストアする項目（ソースLUNなど）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. リストア先のクラスタ、Storage VM (SVM) 、およびボリュームを選択します。
    - ii. [Name]テーブルで、リストアが必要な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ことで、監視とプロビジョニングのためにプールを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時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。

- アグリゲートが（ルートアグリゲートではなく）データアグリゲートであり、オンラインになっている。
- アグリゲートがデスティネーションクラスタノードにあり、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以上である。
- アグリゲートには、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スペースがあります。
- デスティネーションボリュームのプロビジョニング後、アグリゲートスペースがアグリゲートに定義されている「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のいずれか該当する値）の範囲内に収まっている。
- 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。

## リソースプールの作成

[リソースプールの作成]ダイアログボックスを使用して、プロビジョニング用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。

## リソースプールの編集

既存のリソースプールを編集して、リソースプールの名前や説明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。

- 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. リストからリソースプールを1つ選択します。
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. リソースプールの名前と説明を必要に応じて編集します。
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説明が表示されます。

## リソースプールインベントリの表示

[Resource Pools]ページでは、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の追加

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最大200個です。[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の領域に、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。

[Aggregates]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]\*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のアグリゲートの削除

アグリゲートを他の目的に使用する場合など、既存のリソースプールからアグリゲ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、リソースプールを選択した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[Members]ペインから削除されます。

## リソースプールの削除

不要になったリソースプールを削除できます。たとえば、ある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て、元のリソースプールを廃止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の監視

Active IQ Unified Manager は、Storage VM ディザスタリカバリ関係の監視をサポートしており、Storage VM レベルでのディザスタリカバリを実現します。Storage VM ディザスタリカバリでは、Storage VM のコンスチチュエントボリュームに存在するデータをリカバリし、Storage VM の設定をリカバリできます。

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 関係を作成します。クラスセットアップに基づいて、Storage VM のすべての設定または一部の設定（ネットワークとプロトコルの設定を除く）とデータボリュームをレプリケートするように選択できます。

Storage VM ディザスタリカバリ関係を設定したあとに、ハードウェア障害や環境災害によってソース Storage VM が使用できなくなった場合は、デスティネーション Storage VM が起動され、システム停止を最小限に抑えて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、データを提供するためにソース Storage VM が再起動されます。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。

### [Relationships] ページを使用した Storage VM の監視

Storage VM ディザスタリカバリ関係は、インベントリの [Protection] セクションにある [Relationships] ページで監視できます。デフォルトでは、コンスチチュエント関係フィルタが適用されると、[関係] ページに最上位の関係のみが表示されます。

- 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できます。

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。

すべてのタイプの関係（ボリューム、整合性グループ、Storage VM関係）がページに表示されます。

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、コンスティ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。

ページには、Storage VMディザスタリカバリ関係のみが表示されます。

### [Storage VM]ページでの保護関係の表示

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。

また、保護関係の詳細（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）を確認することもできます。必要な形式でレポートをスケジュールしたり、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く 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 VMs]ビューに、Storage VMが保護されているかどうかを示す新しい列[Protection Role]が追加されま

した。



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内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であるか3番目のデスティネーションであるかに関係なく、ソースStorage VMとデスティネーションStorage VMの間に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**を関連付け：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の間で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**を関連付け：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の間で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、そ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で関連付けを作成できます。

## Storage VMの関連付けを作成

[Create Storage Virtual Machine Associations]ウィザードを使用すると、パートナーの保護アプリケーションでソース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関係で使用できます。パートナーアプリケーションは、デスティネーションボリュームの初期プロビジョニング時にこれらの関連付けを使用して、選択するリソースを決定します。dd

- 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。

ソースStorage VMと関係タイプについては、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て関連付けを変更すると、以降のプロビジョニング処理にのみ影響します。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の間で関連付けを作成する場合は、このオプションを選択します。つまり、現在保護が必要なすべての既存のStorage VMと今後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を選択する場合は、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、そ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は、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を1つまたは両方選択します。
  - \* 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

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できます。たとえば、デスティネーションStorage VMがいっぱいになったときに、Storage VM保護の新しい関連付けを作成する場合などに削除できます。

- 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。

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。関連付けの削除機能と作成機能を使用して変更すると、以降のプロビジョニング処理にのみ影響します。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 (SnapMirrorソースまたはSnapVaultプライ



マリボリュームからデスティネーションSnapMirrorまたは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)をサポートするには、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、ジョブが正常に完了したかどうかを確認できます。

ジョブは、SnapMirror関係とSnapVault関係の作成時、関係の処理（解除、編集、休止、削除、再開、再同期、逆再同期）の実行時、データのリストアタスクの実行時、クラスタへのログイン時などに開始されます。

ジョブを開始したときに、[Jobs]ページと[Job details]ページを使用して、ジョブと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

[Jobs]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タイプ、状態、送信時刻、完了時刻などのジョブプロパティを表示して、ジョブが正常に完了したかどうかを確認したりできます。

- 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。

### 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. ジョブ名をクリックすると、そのジョブの詳細が表示されます。

[Job details]ページが表示されます。

## ジョブの詳細の表示

ジョブを開始したら、[Job details]ページで進捗状況を追跡し、関連するタスクにエラーの可能性がないかを監視できます。

- 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。

## ジョブの中止

ジョブの完了に時間がかかりすぎる、エラーが多すぎる、または不要になった場合は、[Jobs]ページを使用してジョブを中止できます。ジョブを中止できるのは、ステータスとタイプで許可されている場合だけです。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の再試行

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つだけ再試行できます。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。

### 保護関係のウィンドウとダイアログボックスの説明

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。該当する[健全性しきい値]ページで、アグリゲート、ボリューム、および関係のグローバル健全性しきい値を設定できます。

#### [Resource Pools]ページ

[Resource Pools]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。このページでは、プロビジョニングを目的としたリソースプールの作成、監視、および管理を行うことができます。

#### 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。

- \* 作成 \*。

[Create Resource Pool]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説明を編集できます。

- \* 削除 \*

1つ以上のリソースプールを削除できます。

#### [Resource Pools]リスト

[Resource Pools]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SnapLockです。リソースプールに含めることができるSnapLockタイプのアグリゲートは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。

#### [Members]リストのコマンドボタン

[Members]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。

#### [Members]リスト

[Members]リストには、リソースプールを選択すると、リソースプールの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。Critical ( )、Error ( )、 Warning ( )、 Normal ( ) のいずれかです。 かです 。

- \* 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

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

アグリゲートを作成中です。

◦ サクシヨ

アグリゲートを削除中です。

◦ 失敗

アグリゲートをオンラインにできません。

◦ フリーズ

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しています。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

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、足りないディスクが複数あります。

◦ 休止中

アグリゲートを休止中です。

- 休止

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

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

アグリゲートをオフラインにしています。

- 不明

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。
- RAID 4：すべてのRAIDグループのタイプがRAID 4です。
- raid：すべてのRAID-DPグループのタイプがRAID-DPです。
- raid：すべてのRAID-TEC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、およびRAID-TEC）の異なる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。

### [Create Resource Pool]ダイアログボックス

[リソースプールの作成]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たり、そのリソースプールに対するアグリゲートの追加や削除を行ったりできます。

リソースプール名

テキストボックスを使用すると、次の情報を追加してリソースプールを作成できます。

リソースプール名を指定できます。

製品説明

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 \*。

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る[アグリゲート]ダイアログボックスを開きます。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。

## [Edit Resource Pool]ダイアログボックス

[リソースプールの編集]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説明を変更できます。たとえば、元の名前と説明が不正確または間違っている場合は、より正確になるように変更できます。

### 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 \*

新しい説明を入力できます。

### 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 \*

リソースプールの名前と説明に対する変更を保存します。

- \* 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]ダイアログボックス

[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、[アグリゲート]ダイアログボックスを閉じます。



## [アグリゲート]リスト

[Aggregates]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。Critical ( )、Error ( )、 Warning ( )、 Normal ( ) のいずれ  かです 。

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

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

アグリゲートを作成中です。

#### ◦ サクシヨ

アグリゲートを削除中です。

#### ◦ 失敗

アグリゲートをオンラインにできません。

#### ◦ フリーズ

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しています。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

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、足りないディスクが複数あります。

- 休止中

アグリゲートを休止中です。

- 休止

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

アグリゲートがオフラインです。

- アンマウント中

アグリゲートをオフラインにしています。

- 不明

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てい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合計スペース (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の量（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タイプは、RAID 0、RAID 4、RAID-DP、RAID-TEC、Mixed RAIDのいずれかです。

## [Jobs]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、および完了したジョブに関する現在のステータスとその他の情報を確認できます。この情報を使用して、実行中のジョブや、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開します。失敗したジョブは一度に1つだけ再試行できます。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。失敗したストレージサービスジョブは再試行できません。

- \* 更新 \*

ジョブのリストおよびジョブに関連付けられている情報を更新します。

## [Jobs]リスト

[Jobs]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、このリストには過去1週間に生成されたジョブのみが表示されます。列のソートと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。Error()またはNormal()の  いずれかです .

- \* ジョブ ID \*

ジョブの識別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。

ジョブ識別番号は一意で、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 \*

ジョブの名前が表示されます。

- \* タイプ \*

ジョブタイプを表示します。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 \*

リストアジョブが実行中です。

- \* クリーンアップ \*

リストアに不要に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アンサブスクライブしています。

◦ \* 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 \*

ジョブの実行状態が表示されます。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が表示されます。

- \* 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。

## [Job]詳細ページ

[Job details]ページでは、実行中、キューに登録されている、または完了した特定の保護ジョブ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
- タイプ
- 都道府県
- 送信時刻
- 完了時間
- 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 \*

[Jobs]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には、特定のジョブに関連付けられたすべてのタスク、および各タスクに関連するプロパティが表形式で表示されます。

- \* 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、最新のタスクが列の上部に表示され、古いタスクが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。

- \* 標準()\* 

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を表示します。列はソートおよびフィルタ処理できます。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 \*

タスク名、タスクの説明、タスクが失敗した理由など、各ジョブタスクに関する追加情報を表示します。

- \* 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。タスクメッセージが表示されないタスクもあります。

## [Advanced Secondary Settings]ダイアログボックス

[セカンダリの詳細設定]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、複数コピーのバックアップ、およびスペース関連の設定を有効にできます。[セカンダリの詳細設定]ダイアログボックスは、現在の設定の有効化または無効化を変更する場合に使用できます。

スペース関連の設定では、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、格納されるデータの量を最大限に増やすことができます。

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を使用すると、デスティネーションボリュームでソースボリュームよりも前のバージョンのONTAPが実行されている場合でも、ソースボリュームのSnapMirror保護が可能になります。

- バックアップを有効にする

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もできます。

- \* 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、データが頻繁に上書きされない場合に使用できます。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せん。

- 圧縮を有効にする

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る場合や、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使用します。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

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、ピーク時に新しい書き込みやCPUの追加に対応できる場合に使用します。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 \*

ボリュームを拡張できる最大割合を設定します。デフォルトでは、ソースボリュームサイズよりも20%大きくなります。現在のサイズが自動拡張時の最大サイズ以上の場合、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 \*

ボリュームがソースボリュームの最大割合に達するまでに自動的に拡張される割合を指定します。

- \* 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は次のいずれかに設定できます。

- 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 だけであるとします。Volume Guaranteeは、ソースの内容に関係なく、200GBをデスティネーションボリュームに割り当てます。[File]を選択すると、ソースで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[None]を選択すると、ソースで実際にファイルデータに使用されているスペースに対して10GBだけがデスティネーションに割り当てられます。

スペースギャランティはデフォルトで[Volume]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、[詳細なデスティネーション設定]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の詳細設定]ダイアログボックスを使用して、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設定を有効にできます。詳細設定は、ソースでスペースギャランティが無効になっていて、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選択できます。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て、データ転送が常に成功するようにします。スペースギャランティは次のいずれかに設定できます。

- 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いて、それらのファイルに格納されているデータは10GBだけであるとします。Volume Guaranteeは、ソースの内容に関係なく、200GBをデスティネーションボリュームに割り当てます。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され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[Volume]に設定されています。

## [Restore]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して、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。

### リストア元

[Restore from]領域では、データのリストア元を指定できます。

#### • \* 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含む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コピーリストは、選択したボリュームに応じて変わります。

#### • \* 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。アイテム数が非常に多い場

合、この操作には時間がかかることがあります。

リストアするアイテムを選択

[Select items to restore]領域では、リストアするボリューム全体または特定のファイルやフォルダを選択できます。最大10個のファイル、フォルダ、またはその両方を選択できます。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。パスを選択または入力するまで、このフィールドは空です。パスを選択した後でをクリックすると、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、ルートフォルダが最初に表示されます。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。

リストアするアイテム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、またはその両方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示すメッセージが表示され、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。

リストア先

[リストア先]領域では、データのリストア先を指定できます。

• \* 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。[参照]\*ボタンを使用してデータのリストア先に移動することも、パスを「cluster://svm/volume/path」の形式で手動で入力することもできます。

- ディレクトリ階層を保持

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[Restore]ダイアログボックスを閉じます。

- \* 復元 \*

選択内容を適用し、リストアッププロセスを開始します。

#### [Browse Directories]ダイアログボックス

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。デフォルトでは元のソースクラスタとボリュームが選択されます。

[ディレクトリを参照]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内の読み取り/書き込みボリュームがすべて表示されます。名前および使用可能なスペースでボリュームをフィルタできます。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使用可能な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。フォルダを選択した後でをクリックすると、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、[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]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がレプリケートされるようにすることができます。

#### [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次の情報を含む詳細が表示されます。

- 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

次の情報が表形式で表示されます。

- 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。

- タイプ

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。オプションは、[Compliance]、[Enterprise]、およびSnapLock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 copy]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 copy]列の[Default]の値は、新しいSnapshotコピーが作成されず、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ることを示します。[Snapshot copy]の値をクリックすると、ベースライン転送に使用する既存のSnapshotコピーを選択できるSnapshotコピーのリストが表示されます。ソースタイプがデータ保護の場合、別のデフォルト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宛先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開きます。

- 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。[Aggregate]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別のノードに配置されているアグリゲートが優先され、フォールトドメインの分離が可能になります。
- B. ボリュームの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負荷を分散できます。
- 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。ランク1は、3つの条件に基づいてアグリゲートが最も優先されることを意味します。

- アグリゲート名

アグリゲートの名前

- 使用可能容量

- データ用のアグリゲートで使用可能なスペースの量

- 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。

エントリが無効な場合は、[命名規則]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。関係の作成時にデスティネーション名に001~999の\_SUFFIXが追加され、プレビューテキストに表示されるnnnが置き換えられます。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（以降も同様）。

- \* 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。スケジュールには、None、5min、8hour、daily、hourly、weeklyがあります。デフォルトは[なし]で、関係にスケジュールが関連付けられていません。スケジュールの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。

- スケジュールの作成

[スケジュールの作成]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、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開きます。

- 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。[Aggregate]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ノードとは別のノードに配置されたアグリゲートが優先され、フォールトドメインの分離が可能になります。
- B. ボリュームの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負荷を分散できます。
- 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。ランク1は、3つの条件に基づいてアグリゲートが最も優先されることを意味します。

- アグリゲート名

アグリゲートの名前

- 使用可能容量
- データ用のアグリゲートで使用可能なスペースの量
- 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。

エントリが無効な場合は、[命名規則]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、プレビュー領域には無効な情報が赤い疑問符で表示されます。関係が作成されると、セカンダリ名に001~999のサフィックスが追加され、プレビューテキストに表示されるnnnが置き換えられます。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（以降も同様）。

- \* 関係設定 \*

保護関係で使用される最大転送速度、SnapVaultポリシー、およびSnapVaultスケジュールを指定できません。

- 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

[ SnapVault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。スケジュールには、None、5min、8hour、daily、hourly、weeklyがあります。デフォルトは[なし]で、関係にスケジュールが関連付けられていません。スケジュールの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。

- スケジュールの作成

[Create Schedule]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、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[保護の設定]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 Schedule]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関係および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。新しいスケジュールを作成して、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ことも、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同期関係に対して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[保護]タブまたは[保護の設定]タブで選択したクラスタの名前SnapVault SnapMirror。

- \* 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<sub>z</sub>、a<sub>z</sub>、0~9、および特殊文字「!@#\$% { 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。

- リピート

スケジュールされた転送が発生する頻度。選択できるのは、Hourly、Daily、Weeklyです。

- 日

「Weekly」の繰り返しを選択した場合、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は日曜日を表し、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。曜日を指定しても日にちを指定しない場合、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。

## [Create SnapMirror Policy]ダイアログボックス

[Create SnapMirror Policy]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 \*

[保護の設定]ダイアログボックスの[保護の設定]タブで選択したクラスタの名前SnapMirror。

- \* 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 (-)、アンダースコア (\_) を使用できます。

• \* 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 (Normal) または低 (Low) 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 \*

転送が中止処理または何らかのタイプの障害 (ネットワークの停止など) によって中断された場合に実行する再開アクションを示します。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、存在する場合はチェックポイントから転送を再開し、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。

◦ しない

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[保護の設定]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と、プライマリボリュームからセカンダリボリュームへの転送効率を最大限に高めることができます。

• \* デスティネーションクラス \*

[保護の設定]ダイアログボックスの[保護]タブで選択したクラスタの名前SnapVault。

• \* 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<sub>z</sub>、a<sub>z</sub>、0~9、ピリオド (.)、ハイフン (-)、アンダースコア ( \_ ) を使用できます。

• \* 転送優先順位 \*

転送を実行する優先順位。標準 (Normal) または低 (Low) 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ポリシーに関する最大255文字のコメントを追加できます。

• \* 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 \*

ポリシー内の特定のレプリケーションラベルが設定されたONTAPによって選択されたSnapshotコピーに関連付けられているルールを表形式で表示します。次の情報とアクションも使用できます。

◦ 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

Snapshotコピーラベルと保持数を作成できます。

▪ 保持数の編集

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の数字にする必要があります。すべてのルールのすべての保持数の合計は251個以下にする必要があります。

▪ 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ボリュームを1つ以上選択すると、ポリシー内の各ラベルのエントリが表示されます。複数のローカルSnapshotコピーポリシーが設定された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

ル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

指定したラベルに一致するSnapVaultセカンダリに保持されている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。

## [Edit Relationship]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。

### デスティネーション情報

- \* 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。

- \* 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。このオプションを選択すると、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、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）のいずれかを選択できます。最大転送速度は1KBps以上4TBps未満に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。プライマリクラスタとセカンダリクラスタが同じ場合、この設定は無効になります。

- 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。スケジュールには、None、5min、8hour、daily、hourly、weeklyがあります。デフォルトは[なし]で、関係にスケジュールが関連付けられています。スケジュールの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。

- スケジュールの作成

[スケジュールの作成]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、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[保護の設定]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。

#### [初期化/更新]ダイアログボックス

[初期化/更新]ダイアログボックスでは、新しい保護関係の初回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、転送の初期化優先度を変更したり、転送中に使用す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 (Normal) または低 (Low) 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、次のいずれかの最大転送速度設定を指定できます。

- 個々の関係の設定または編集時に指定した値を使用する

選択した場合、初期化処理と更新処理では、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表示されます。

- 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表示されます。

◦ 帯域幅の制限

このオプションを選択すると、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、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）のいずれかを選択できます。最大転送速度は1KBps以上4TBps未満にする必要があります。

**[Source Snapshot Copies]**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 copy]の値をクリックすると、[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。このダイアログボックスで、確立されている保護関係のタイプと実行中の処理に応じて、転送用のSnapshotコピーを選択できます。データ保護タイプのソースには、別のSnapshotコピーを指定するオプションは使用できません。

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、[初期化/更新]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]**ダイアログボックス

[Resynchronize]ダイアログボックスでは、以前に解除して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SnapMirror関係またはSnapVault関係のデータを再同期できます。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またはSnapVaultの更新が失敗した場合にも実行できます。

#### 再同期オプションタブ

[Resynchronization Options]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 (Normal) または低 (Low) を選択できます。ポリシーで転送の優先順位「Normal」が指定されている関係は、転送の優先順位「Low」が指定された関係よりも先に実行されません。

- \* 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。このオプションを選択すると、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のいずれかを選択できます。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。

#### [Source Snapshot Copies]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 (読み取り/書き込みまたはデータ保護) が表示されます。

- \* 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 copy]の値をクリックすると、[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。このダイアログボックスで、確立されている保護関係のタイプと実行中の処理に応じて、転送用の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[Resynchronize]ダイアログボックスを閉じます。

## [Select Source Snapshot Copy]ダイアログボックス

[ソースの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、またはデフォルトの動作を選択します。デフォルトの動作は、関係を初期化、更新、再同期するか、および関係がSnapMirrorかSnapVaultかによって異なります。

### デフォルト

SnapVault関係とSnapMirror関係の初期化、更新、および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 <b>SnapVault</b> の動作	ソースがデータ保護（DP）の場合のデフォルトの <b>SnapVault</b> の動作
初期化	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Snapshotコピーをすべて転送します。	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 <b>SnapMirror</b> の動作	関係が <b>SnapMirror-to-SnapMirror</b> 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 <b>SnapMirror</b> の動作
初期化	新しいSnapshotコピーを作成し、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。	ソースからすべてのSnapshotコピーを転送します。
更新	新しいSnapshotコピーを作成し、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。

操作	デフォルトの <b>SnapMirror</b> の動作	関係が <b>SnapMirror-to-SnapMirror</b> カスケードの <b>2</b> 番目のホップである場合の、デフォルトの <b>SnapMirror</b> の動作
再同期	新しいSnapshotコピーを作成し、ソースからすべてのSnapshotコピーを転送します。	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

既存のSnapshotコピーをリストから選択できます（その処理でSnapshotコピーを選択できる場合）。

- \* Snapshot コピー \*

転送用に選択できる既存の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せん。

SnapVault転送を実行しているときに、ソースからデスティネーションに転送する既存のSnapshotコピーを選択すると、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 <b>SnapVault</b> の動作	カスケード構成の <b>Snapshot</b> コピーを指定する場合の <b>SnapVault</b> の動作
初期化	指定したSnapshotコピーを転送します。	データ保護ボリュームでは、ソースSnapshotコピーの選択は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では、ソースSnapshotコピーの選択はサポートされません。
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では、ソースSnapshotコピーの選択はサポートされません。

SnapMirror転送を実行しているときに、ソースからデスティネーションに転送する既存のSnapshotコピーを選択すると、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	ソース上のすべての Snapshot コピー（指定した Snapshot コピーまで）を転送します。	データ保護ボリュームでは、ソース Snapshot コピーの選択はサポートされません。
更新	ソース上のすべての Snapshot コピー（指定した Snapshot コピーまで）を転送します。	データ保護ボリュームでは、ソース Snapshot コピーの選択はサポートされません。
再同期	ソースから選択した Snapshot コピーまでのすべての 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。	データ保護ボリュームでは、ソース Snapshot コピーの選択は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、[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、[ソース Snapshot コピーの選択] ダイアログボックスを閉じます。

#### [Reverse Resync] ダイアログボックス

ソースボリュームが無効になったために保護関係を解除し、デスティネーションを読み取り/書き込み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して、デスティネーションが新しいソースになり、ソースが新しいデスティネーションになるよう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、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。

#### キヤクサイトウキセン

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。

キヤクサイトウキコ

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[Reverse Resync]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の両方の最上位レベルの保護関係が表示されるレポートに表示されます。ページの上部にあるコントロールを使用して、特定のビューの選択、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/削除/並べ替え、ページ上のデータの.csv、.pdf、または.xlsxファイルへのエクスポートを行うことができます。ページをカスタマイズしたら、結果をカスタムビューとして保存し、この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。選択したストレージエンティティについてのみ、[Storage]ページに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ーのリンク \* 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()、Warning()、OK()のいずれかです。

- \* 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。

クラスタに存在するSVMがUnified Managerインベントリにまだ追加されていない場合や、前回のクラスタ更新後にSVMが作成された場合、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。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の詳細を確認できます。

メッセージが表示された場合は Resource-key not discovered、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の詳細が表示されます。

- \* 関係オブジェクトタイプ \*

関係で使用されているオブジェクトのタイプ（Storage VM、ボリューム、整合性グループなど）が表示されます。整合性関係のオブジェクトの場合、関係のソースとデスティネーションに整合性グループが表示され、それらをクリックすると[LUN]ページに移動して関係を確認できます。

- \* 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ている詳細を確認できます。これには次の情報が含まれます。

- 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「標準」または「低」です。優先度が「中」の転送は、優先度が「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

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が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固有のコメントを入力するテキストフィールドを提供します。

- SnapMirrorラベル

Snapshotコピーポリシーに関連付けられている最初のスケジュールの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、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、指定したラベルに一致する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コピーの最大保持数を指定します。この数に達すると、保持数の上限に近づいていることを示す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。

- OK

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の処理が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 \*

ボリュームのレプリケートに使用される関係タイプが表示されます。関係の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

- 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。

- チュウシ

SnapMirror転送が有効になっていますが、転送の中止処理（チェックポイントの削除など）を実行中です。

- カクニン

デスティネーションボリュームで診断チェックを実行中で、実行中の転送はありません。

- ファイナライズ中

SnapMirror転送が有効になっています。現在SnapVault差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いますが、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差分転送の転送前のフェーズです。

- キューに登録済み

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

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

SnapMirror転送を実行中です。追加の転送は無効になっています。

- 転送中

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データ転送が完了し、同期処理への移行が開始されました。

- 待機中

SnapMirror転送が開始されましたが、一部の関連タスクがキューに登録されるのを待っています。

- \* 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アクティブ同期をサポートしていない場合。

- 未設定

設定されていない場合、または設定されているのにデスティネーションクラスタのみが追加され、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

設定済みで、ソースとデスティネーションの両方のクラスタがUnified Managerに追加されている場合。

- \* 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、関係の状態は適用できず、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。

- \* 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「標準」または「低」です。優先度が「中」の転送は、優先度が「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 \*

[Yes]、[Yes with backup option]、または[None]のいずれかが表示されます。

- \* 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のリンクの名前が表示されます。オブジェクトがStorage VMまたは整合性グループの場合は、SnapMirror関係のノード数の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、それらの整合性グループのボリュームがSnapMirrorのアクティブな同期関係に属している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、その関係に関連付けられている各ノードが表示されたノード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または整合性グループの場合は、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、その関係に関連付けられている各ノードが表示されたノード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の順序に関するボリューム関係と整合グループ関係を表示できます。これには次のような情報が含まれます。

- 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 \*

- 関係：MetroCluster \*ビューの詳細については、を参照してください"[MetroCluster設定の監視](#)"。
- [関係：過去1カ月の転送ステータス]\*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](#)"。
- [関係：すべての関係]\*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。このページには、転送が成功したか失敗したかも表示されます。

ページの上部にあるコントロールを使用すると、検索を実行して特定のオブジェクトを検索したり、フィルタを作成および適用して、表示されるデータのリストを絞り込んだり、ページ上の列を追加/削除/並べ替えたり、ページ上のデータを、`.pdf`または`.xlsx`ファイルにエクスポートしたりでき`.csv`ます。ページをカスタマイズしたら、結果をカスタムビューとして保存し、この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。選択したストレージエンティティについてのみ、[Storage]ページに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 \*

- [関係：すべての関係]\*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](#)"。
- 関係：MetroCluster \*ビューの詳細については、を参照してください"[MetroCluster設定の監視](#)"。
- [関係：すべての関係]\*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、日次転送に関する詳細と、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も表示されます。

ページの上部にあるコントロールを使用すると、検索を実行して特定のオブジェクトを検索したり、フィルタを作成して適用して表示データのリストを絞り込んだり、ページ上の列を追加/削除/並べ替えたり、ページ上のデータを.csv、.pdf、または.xlsxファイルにエクスポートしたりできます。ページをカスタマイズしたら、結果をカスタムビューとして保存し、この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 (GB) が表示されます。

- \* 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 \*

- 関係：MetroCluster \*ビューの詳細については、を参照してください"[MetroCluster設定の監視](#)"。
- [関係：過去1カ月の転送ステータス]\*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"。

- [関係：すべての関係]\*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"

# カスタムレポートの生成

## 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。このレポートには、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が表示されます。

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、結果の検索を行うことで、ビューをカスタマイズできます。カスタムビューを保存して再利用したり、レポートとしてダウンロードしたり、定期的なレポートとしてスケジュール設定してEメールで配信したりできます。

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、グラフなどの高度なExcel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、レポートをスケジュールして共有するたびにExcelファイルをアップロードして使用できます。

ユーザインターフェイスからレポートを生成するだけでなく、次の方法を使用してUnified Managerから健全性、セキュリティ、パフォーマンスのデータを抽出することもできます。

- Open Database Connectivity（ODBC）およびODBC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、レポートに次の機能拡張が加えられています。

- 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、この機能拡張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します。

- 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の**Unified Manager**データベースへのアクセス

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データベース内のさまざまなスキーマに保持されます。

次のデータベースのすべてのテーブルデータを使用できます。

データベース	製品説明
NetAppモデル	ONTAPコントローラ上のオブジェクトに関するデータ。
NetAppモデルビュー	ONTAPコントローラ上のオブジェクトに関するデータ。レポートツールの使用に適しています。
NetApp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	インベントリ構成および容量関連の情報のデータ。
ocum_report_birt	インベントリ構成と容量関連データを表示するビュー。レポートツールでの使用に適しています。
OPM	パフォーマンスの設定としきい値の情報。
スキャレモニタ	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	NetApp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	NetApp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のビュー。レポートツールの使用に適しています。
vmware_performance	NetApp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の詳細については、を参照してください"[Active IQ Unified Manager REST APIでの作業の開始](#)"。

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、Quality of Service (QoS ; サービス品質)、保護関係に関する詳細情報が表示されるため、潜在的な問題を未然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ときは、あとで使用できるように一意の名前で保存できます。そのビューに基づいてレポートを定期的に行い、他のユーザと共有するようにスケジュールを設定できます。Excelで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にアップロードすることもできます。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、共有できる堅牢なレポートが作成されます。

[Report Schedules]ページでは、スケジュールされたすべてのレポートを管理できます。



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の概要

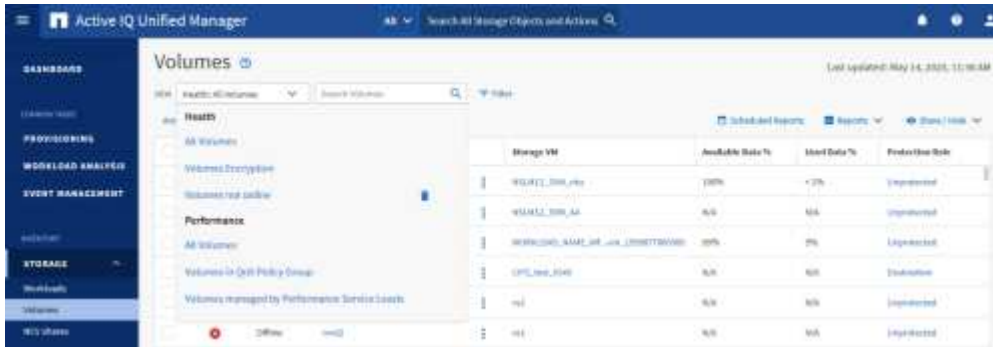
ビューとインベントリページは、ダウンロードまたはスケジュール設定するとレポートになります。

ビューとインベントリページを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、削除アイコンの付いたアイテムは、自分または別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ファイルまたは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時に変更が反映されます。ビューを変更する場合は、レポートに使用されるExcelの関連付けられたカスタマイズに変更が反映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。

## レポートの種類

この表には、カスタマイズ、ダウンロード、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

タイプ	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 ボリューム qtree

タイプ	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 VM ボリューム SMB/CIFSキヨウユウ NFSキヨウユウ
パフォーマンス	クラスタ ノード アグリゲート Storage VM ボリューム LUN NVMeネエムスヘエス ネットワークインターフェイス (LIF) ポート
サービス品質 (QoS)	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
ボリュームの保護関係 ([ボリューム]ページからアクセス)	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
セキュリティ	Storage VM 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以前に付属の標準レポートをカスタマイズした場合、それらのカスタム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い、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をスケジュールする（推奨）
- レポートにカーソルを合わせてSQLをコピーし、外部ツールを使用してデータを取得します。

デフォルトビューは、カスタマイズを必要とせずにレポートとして生成できます。新しいレポートソリューションを使用して、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、複数のレポートでスケジュールを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、定期的なイベントレポートを生成して配信するようにスケジュールを設定することはできません。

### レポートの添付

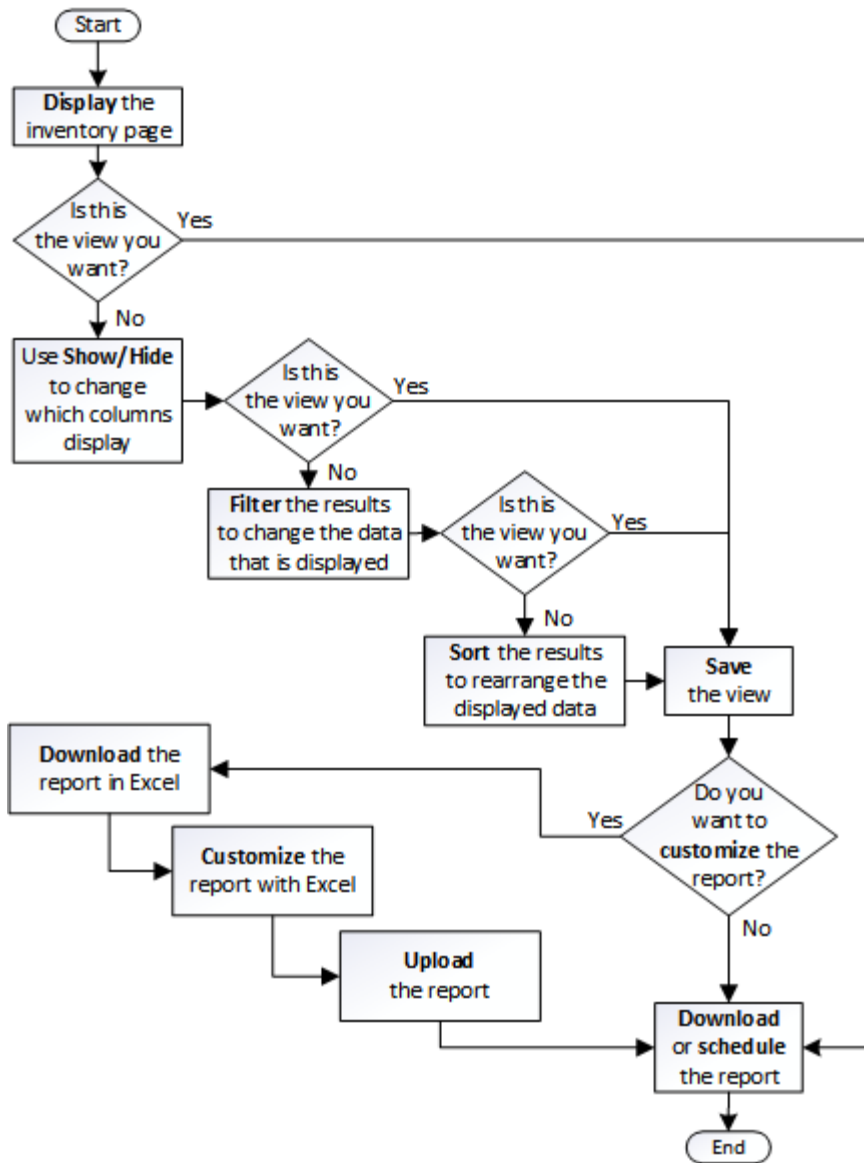
レポートをEメールの本文として送信することはできません。代わりに、レポートはPDF、Excel、またはCSVの添付ファイルとしてのみ送信されます。

## レポートの操作

インベントリページのビューを検索し、共有可能なスケジュール済みレポートに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、ビューを確認したり、レポートのスケジュールを設定したりできます。このクイックスタートレポートでは、アクセス頻度の低いコールドデータがかなりあるためにクラウド階層への移動が必要なボリュームのリストを特定します。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、それらのアグリゲートにボリュームを配置しておく必要があります。

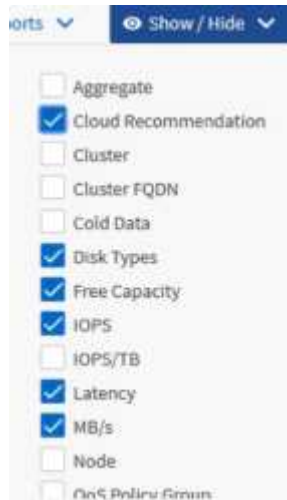
以下の手順に従って、次の操作を実行します。

- デフォルトビューを開く

- データのフィルタリングと並べ替えによる列のカスタマイズ
- ビューを保存する
- カスタムビューのレポートを生成するようにスケジュール設定する

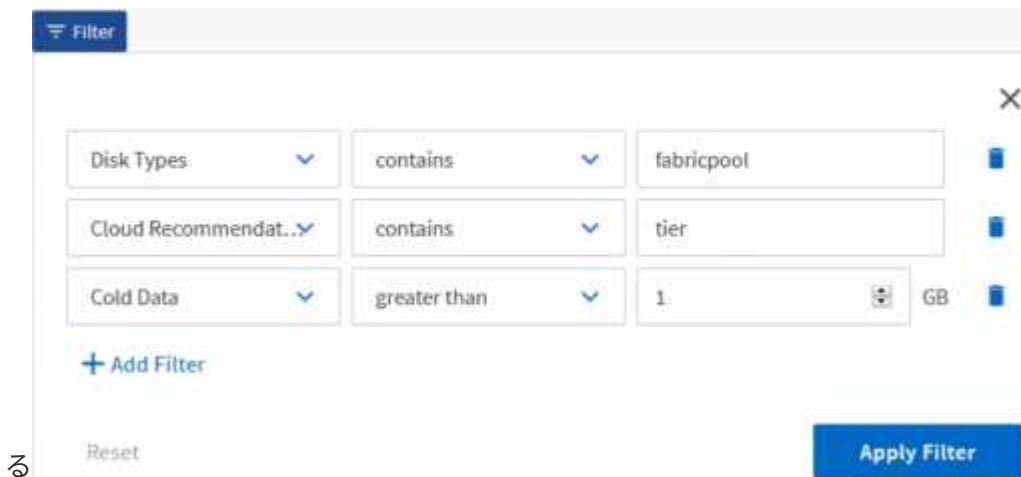
#### 手順

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、レポートに重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いる
  - コールドデータが10GBを超え



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。

- [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。
- 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 (Unsaved View)]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す保存します。

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 🏠

Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
rfs_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

- 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済み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ことで、複雑なフィルタ、並べ替え、ピボットテーブル、または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。このファイルとそのカスタマイズは、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。

- 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（ここではボリューム）に関連するスケジュール済みレポート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

Schedule Name	View	Recipients	Frequency	Format
Weekly / Vols c... tiering policy	Performance / V... tiering policy	user@company.com	Weekly - Monday 1:00 PM	CSV

- [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。
- レポートの名前を入力し、他のレポートフィールドに入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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。

Status	Volume	Volume Id	Tiering Policy	Cold Data	Free Capacity	Total Capacity	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id
Ok	kjagnfsd1	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040
Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141

PDF形式のサンプルレポートを次に示します。

Status	Volume	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	Cluster	Node	Aggregate
Ok	kjagnfsd1	Snapshot	28.01	121.32	150	ocum-mo	ocum-mo	aggr5_vs
Ok	nfs_vol4	Snapshot	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の検索

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、レポートをその列（スケジュール名や形式など）の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から開始し、列の追加または削除、列の順序の変更、データのフィルタリング、特定の列での昇順または降順でのソートなど、カスタマイズします。

Unified Manager 9.8以降では、Excelで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、カスタマイズされた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。



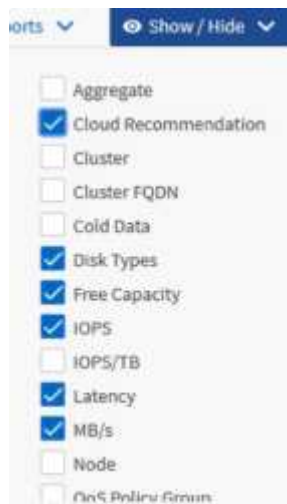
レポートを管理するには、アプリケーション管理者またはストレージ管理者のロールが必要です。

### 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。



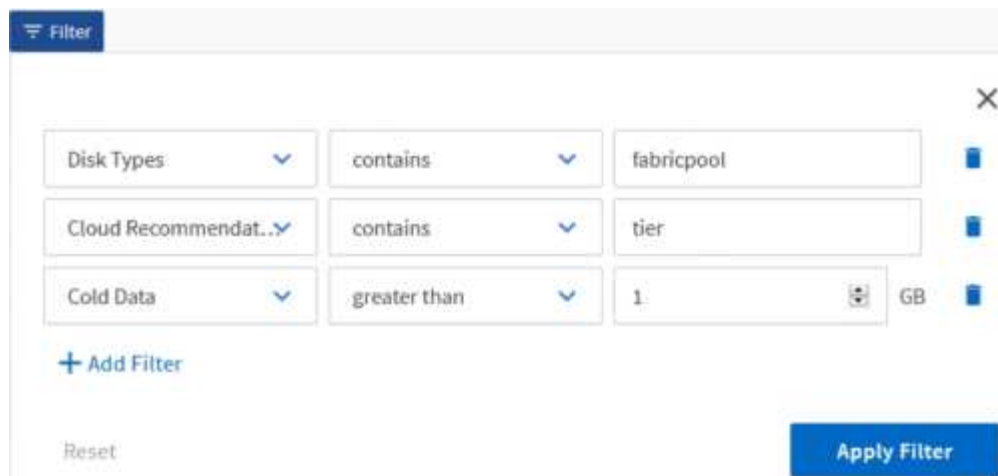
2. インベントリページで、列をドラッグしてレポートで希望する順序に並べ替えます。
3. 保存されていないビューに名前を付けて、変更を保存します。

### データのフィルタリング

データをフィルタリングして、結果がレポート要件に一致す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。



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。

### 検索を使用した表示の絞り込み

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結果をさらに絞り込み、レポートに含める結果に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 (Search) ]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的な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場合は、ノードの完全な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、スケジュールされた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を使用したレポートのカスタマイズ

ビューを保存したら、Excel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。

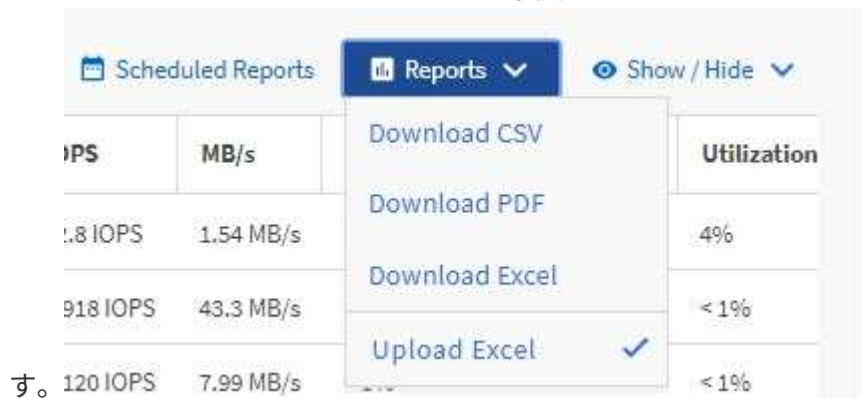
- 必要なもの \*

アップロードできるのは、.xlsx拡張子を持つExcelワーク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。

- 複数列のソート
- 複雑なフィルタリング
- ピボットテーブル
- グラフ

- ダウンロードされたExcelファイルは、保存された名前ではなく、ビューにデフォルトのファイル名を使用します。
  - 形式は次のとおりです。 <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 `Volumes-not online` には、その日と時刻に保存された場合にというファイル名が付けられ `health-volumes-05-May-2020-19-18-00.xlsx` ます。
- Excelファイルにシートを追加することはできますが、既存のシートを変更することはできません。
  - 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、または保存済みビューを開きます。
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う場合は、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元の場所にファイルを保存し直します。

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の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のドキュメント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。最後にダウンロードしたファイルは、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、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。

選択	目的
CSVをダウンロード	レポートをカンマ区切り値（CSV）ファイルとして保存します。
PDFのダウンロード	レポートを.pdfファイルとして保存します。
Excelをダウンロード	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を管理し、各レポートスケジュールの受信者と配信頻度を変更できます。

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、イベントは例外で、CSVファイルとしてダウンロードできますが、再生成と共有のためにイベントをスケジュール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、グラフなどの高度なExcel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、レポートをスケジュールして共有するたびにExcelファイルをアップロードして使用できます。

ビルトイン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。送信するファイルタイプは、CSV、PDF、またはXSLXのいずれかを選択できます。レポートを初めてスケジュールする場合は、レポートをダウンロードし、自分自身を唯一の受信者として割り当て、受信者がレポートを表示するように設定できます。

## レポートのスケジュール設定

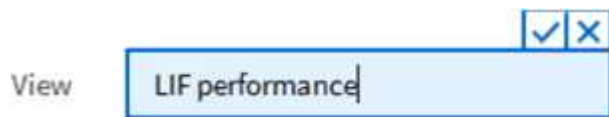
定期的な生成と配信のスケジュールを設定するビューまたはExcelファイルが作成されたら、レポートのスケジュールを設定できます。

- 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 の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。

ビューに対して生成されるレポートをテストおよびスケジュール設定するには、次の手順を実行します。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ています。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. Unified Managerの組み込みの機能を使用して、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、を参照してください ["Excelを使用したレポートのカスタマイズ"](#)。
5. 出力をスケジュールまたは共有する前に確認するには、次の手順を実行します。

オプション	製品説明
• 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) などのインストールされた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、レポートスケジュールを保存します。

LIFs - Scheduled Reports View all Scheduled Reports

Schedule Name	View	Recipients	Frequency			Format
Weekly / LIF performar	Performance / LIF pe	test@netapp.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、レポートが生成され、スケジュールされた頻度を使用してリストされた受信者にEメールで送信されます。

#### インポートされた.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設定できます。

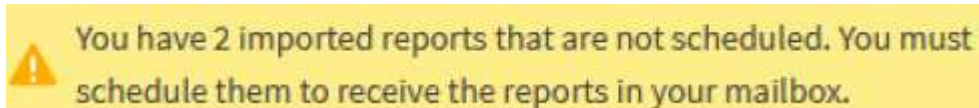
インポートされたレポートのスケジュールを設定するには、

- 以前のUnified Managerリリースで設計された.rptdesignファイルレポートをインポートしたBIRT
- Unified Manager 9.6 GA以降にアップグレードする場合に適用

Unified Manager 9.6 GA以降にアップグレードすると、[Report Schedules]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。そうしないと、これらのレポートをUnified Manager UIで編集または表示できません。

#### 手順

1. [Report Schedules]ページを開きます。レポートをインポートした場合は、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 、\*[編集]\*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

[Report Schedules]ページでは、レポートスケジュールを管理できます。既存のスケジュールを表示、変更、または削除できます。

- 必要なもの \*



[Report Schedules]ページでは、新しいレポートのスケジュールを設定できません。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]ページで、次の手順を実行します。

状況	そしたら...
既存のスケジュールを表示する	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	そしたら...
既存のスケジュールを編集する	<ol style="list-style-type: none"> <li>使用するスケジュールの詳細アイコンをクリックし  ます。</li> <li>[編集 (Edit) ] をクリックします。</li> <li>必要な変更を行います。</li> <li>チェックマークをクリックして変更を保存します。</li> </ol>
既存のスケジュールを削除する	<ol style="list-style-type: none"> <li>使用するスケジュールの詳細アイコンをクリックし  ます。</li> <li>[削除 (Delete) ] をクリックします。</li> <li>操作を確定します。</li> </ol>

## スケジュール済みレポートの編集

スケジュールが設定されたレポートは、[Report Schedules]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	<a href="#">Performance / Tom_test</a>	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	<a href="#">Health / my view</a>	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	<a href="#">Performance / LIF performance</a>	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. 変更するスケジュールの詳細アイコンをクリックし  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

スケジュールを設定したレポートは、[Report Schedules]ページで削除できます。

- 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.

Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	<a href="#">Performance / Tom_test</a>	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	<a href="#">Health / my view</a>	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	<a href="#">Performance / LIF performance</a>	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. 削除するスケジュールの詳細アイコンをクリックし  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、潜在的な問題を未然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のリストはすべてを網羅しているわけではなく、時間の経過とともに増えていきます。ドキュメントに関するフィードバックを提供することで、このセクションに追加するカスタムレポートを提案できます。



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

このセクションのサンプルクラスタストレージレポートは、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理解するのに役立つサンプルです。

### 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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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容量が最も多い（0.5TBを超える）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. ビューの内容を表す名前をビューを保存し（例：「未割り当てのLUN容量」）、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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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、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. ビューの内容を表す名前で見えを保存し（例：「Least used aggregate capacity」）、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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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応じて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見えを保存します ( 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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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、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に関するレポートの作成方法を理解するのに役立つサンプルです。

### 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特定するレポートを作成して、容量を追加したり、他のアグリゲートにワークロードを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、容量がフルに達し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. ビューの内容を表す名前前でビューを保存し（例：「Days to full aggregate capacity」）、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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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、「フルまでの日数」容量のしきい値をデフォルトの7日より長くして、イベントを受信してアグリゲートのスペースが少なくなった場合に対応できるようにすることもできます。

### 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%を超えている
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. ビューの内容を表す名前前でビューを保存し（例：「Aggregates nearing full」）、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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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%を超えている
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. ビューの内容を表す名前でビューを保存し（例：「Aggregates overcommitted」）、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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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**の自動削除がオフになっている容量がほぼフルになっ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る状態で容量がフルに近づいているボリュームのリストを含むレポートを作成できます。この結果は、**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っています

- 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。
- 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。
- 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。
- 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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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、利用可能なスペースを増やす方法を見つけたりできます。

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と、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

- 左側のナビゲーションペインで、 \* Storage \* > \* Volumes \* をクリックします。
- 表示メニューで、 \* 容量 \* > \* すべてのボリューム \* を選択します。
- 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。
- [ 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
- 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。
- 「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。
- 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」）。
- 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。
- [ \* 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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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。

クラウド階層にデータを移動する必要がある**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アグリゲートに存在し、クラウド階層に関する推奨事項があり、コールドデータを大量に含むボリュームのリストを含む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、それらのアグリゲートにボリュームを配置しておく必要があります。

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いる
  - コールドデータが10GBを超える

- [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がビューの上部に表示されるようにします。
- ビューの内容を表す名前でもビューを保存します（例：「Vols change tiering policy」）。

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

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

change tiering policy (階層化ポリシーの変更) ページが表示され、必要な列が正しい順序で表示されます。"]

- 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。
- [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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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の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し、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. ビューの内容を表す名前前でビューを保存し（例：「Qtrees nearing full」）、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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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間でデータを分散したりできます。

## NFS共有レポートのカスタマイズ

ストレージシステム上のボリュームに対するNFSエクスポートのポリシーとルールに関する情報を分析できるように、NFS共有レポートをカスタマイズできます。たとえば、アクセスできないマウントパスの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、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ない
4. ビューの内容を表す名前で見え方を保存し（例："`Volumes with an inaccessible mount path`"）、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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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デフォルトが含まれている

5. ビューの内容を表す名前で見出しを保存し（例：“Volumes with a default export policy”）、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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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、ボリューム数が上限に達している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. ビューの内容を表す名前で見出しを保存し（例：“S VMs reaching max volumes”）、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入力して、行の最後にあるチェックマーク ( ) 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、指定した受

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に割り当てられているボリュームを分散したり、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したりできます。

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。
  - 状態が停止しています
6. ビューの内容を表す名前前でビューを保存し（例：「Stopped SVMs」）、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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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したり、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「State」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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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、問題のタイプごとに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 \* > \* 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 (過去7日間)
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称でビューを保存しますたとえば 'デュー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入力し、行の最後にあるチェックマーク ( ) 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、指定した受信者に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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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見出し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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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にある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。これは、FabricPoolアグリゲートに移動す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、FabricPool対応でないアグリゲート上にあるコールドデータを大量に含む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 \* > \* 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を超える
  - ディスクタイプにSSDが含まれる
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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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

これらのサンプルMicrosoft Excelレポートは、Excelの高度な機能を使用して使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、ニーズに応じたさまざまなレポートを作成できます。Excelの使用法の詳細については、製品ドキュメント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。

### アグリゲート容量の表とグラフを表示するレポートの作成

合計の合計とクラスタ化された縦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。



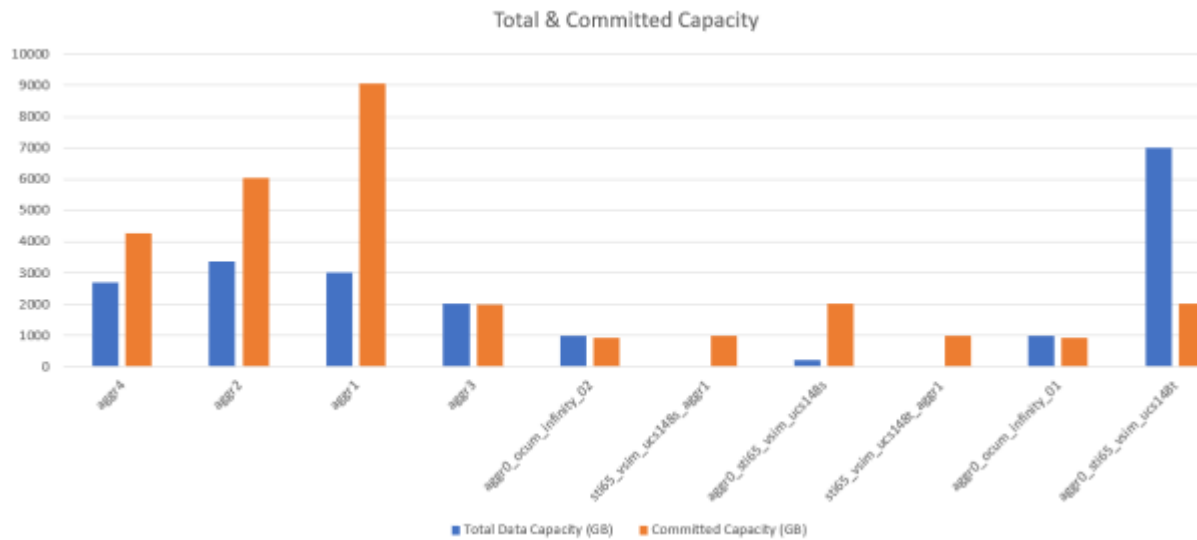
ブラウザによっては、ファイルを保存するために \* OK \* をクリックする必要があります。

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. シートの後に新しいシート() `data`を作成し 、\* Total Data Capacity \*という名前を付けます。
6. 新しい[Total Data Capacity]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!) を参照し、取得したデータの正しい列および行指定子を参照していることを確認します (Total Data Capacityは、列E、行2~20からデータを取得します)。
  - a. = SUM (DATA ! E\$2 : DATA ! E\$20)
  - b. = SUM (DATA ! F\$2 : DATA ! F\$50)
  - c. = SUM (DATA ! G\$2 : DATA ! G\$50)
  - d. = SUM (DATA ! H\$2 : DATA ! H\$50)

計算式では、現在のデータに基づいて各列の合計が計算されます。

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て\*[グラフの移動]\*を選択し、グラフをシートに移動し `Total Data Capacity` ます。
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. 問題がなければ、変更したファイルを保存します。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ビューと同じビューに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。

Scheduled Reports		Reports	Show / Hide
IOPS	MB/s		Utilization
1.8 IOPS	1.54 MB/s	Download CSV	4%
918 IOPS	43.3 MB/s	Download PDF	< 1%
120 IOPS	7.99 MB/s	Download Excel	< 1%
		Upload Excel	

- [スケジュール済みレポート] をクリックします。
- [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。

- 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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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適に使用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の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。

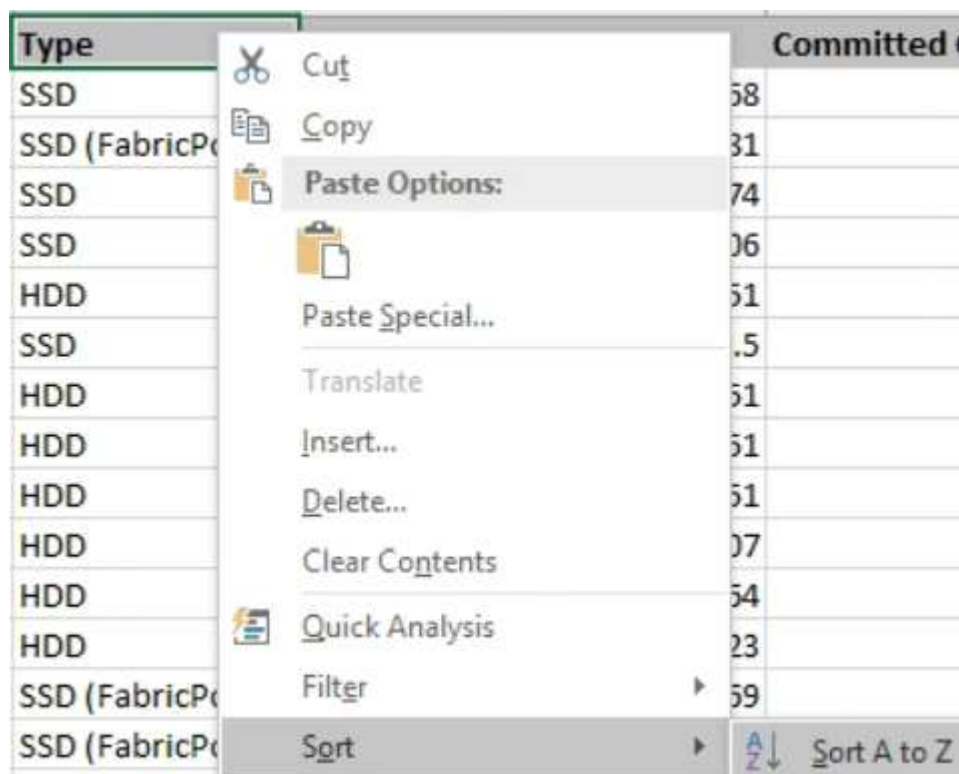
### 手順

- 左側のナビゲーションペインで、\* Storage \* > \* Aggregates \* をクリックします。
- [\* 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。

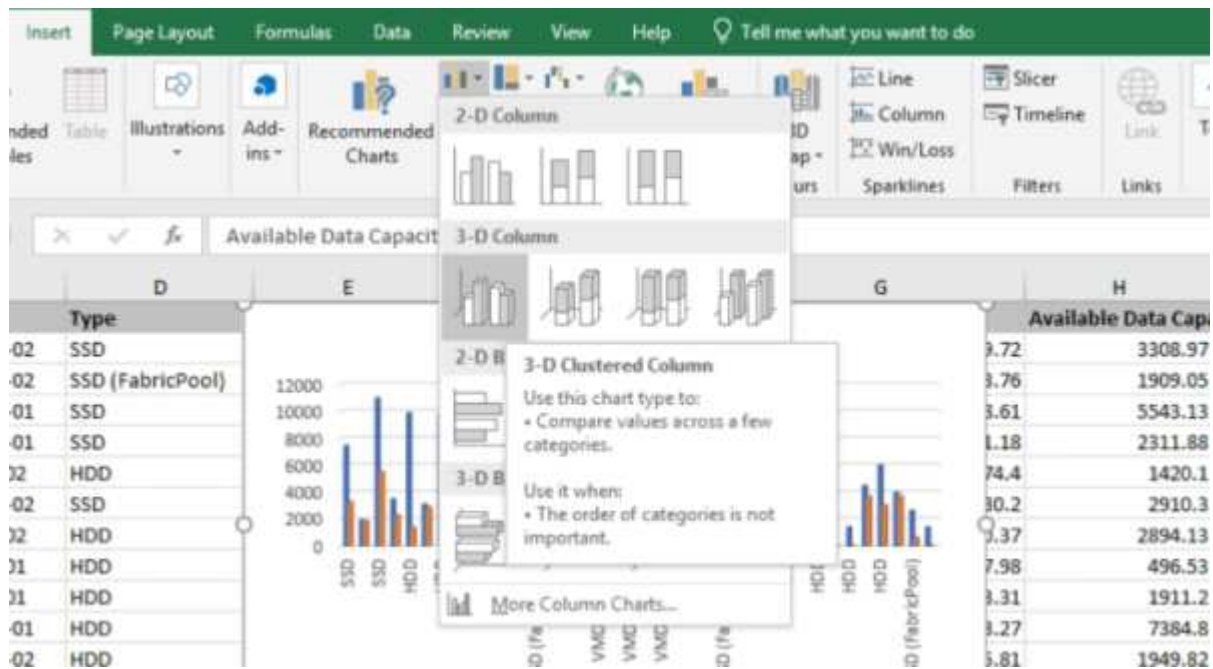
- HDD
- ハイブリッド
- SSD
- SSD (FabricPool)



6. 列と `Available Data Capacity`列を選択し `Type, Total Data Capacity,` ます。

7. [挿入]メニューで、グラフを選択し `3-D column` ます。

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。



情報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. 問題がなければ、変更したファイルを保存します。ファイルの名前や場所を変更しないでください。





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、指定した受信者に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

使用可能なボリューム容量をExcelグラフ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。

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. data `シートで、列と `Available Data%列で使用するデータを選択します Volume。
6. [挿入 (Insert) ]メニューで、3-D piechart.

グラフには、使用可能なスペースが最も多いボリュームが表示されます。グラフがデータシートに表示されます。

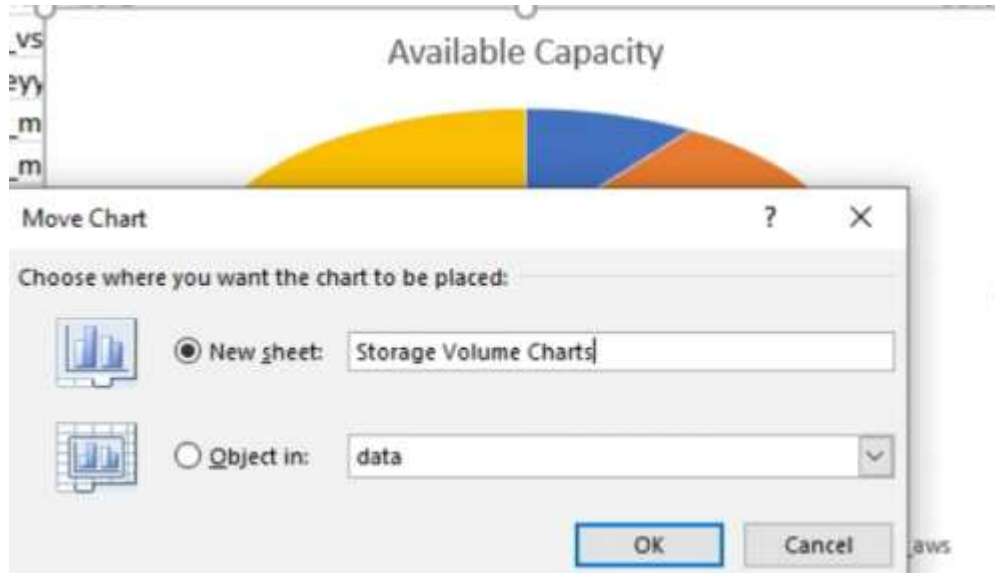


ネットワーク設定によっては、列全体を選択するか、データ行が多すぎると円グラフが読み取れなくなることがあります。このサンプルでは3D円グラフを使用しますが、任意の種類のグラフを使用できます。収集するデータに最も適したグラフを使用してください。

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。



情報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。



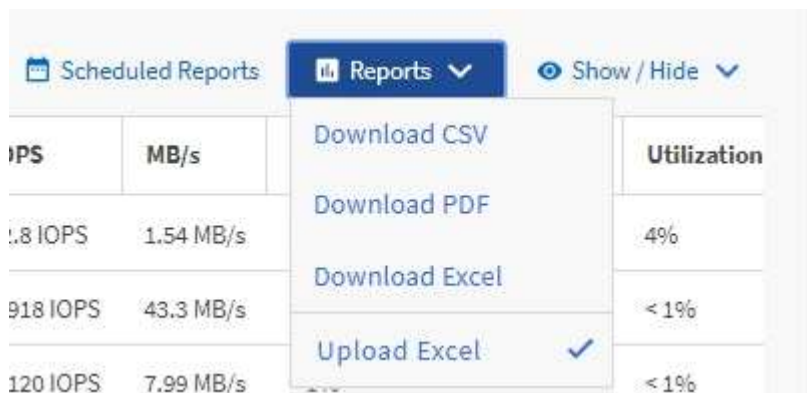
10. グラフを選択したときに使用できる \* デザイン \* および \* フォーマット \* メニューを使用して、グラフの外観をカスタマイズできます。
11. 問題がなければ、変更したファイルを保存します。
12. Unified Manager で、\* Reports \* > \* Upload Excel \* を選択します。



Excelファイルをダウンロードしたビューと同じビューに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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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、ボリュームの負荷を分散できます。

## 使用可能な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あたりのIOPSが最も高い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. 列を表示し、列と `Threshold Policy` 列を非表示にするには、\*[表示/非 `Cluster FQDN, Inactive Data Reporting,` 表示]\*を選択し `Available IOPS` ます。
4. 列と `Free Capacity` 列を列の横に `Type` ドラッグアンドドロップし `Available IOPS` ます。
5. カスタムビューに名前を付けて保存する 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. データシートで、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、Sort & Filter area.
11. 次のソートレベルを設定します。
  - a. Sort by \* As (IOPS) 、 \* Sort On \* As、 \* Cell Values, Order \* Asを Largest to Smallest. `指定します。 `Available IOPS
  - b. [レベルの追加] をクリックします。
  - c. \* Sort by \* As、 \* Sort on \* As、 \* Order \* As Cell Values, `を `Z to A. `指定します。 `Type
  - d. [レベルの追加] をクリックします。
  - e. 「\* Sort by」を「Sort on \* as」 Cell Values, `に、「\* Order \* as」を `Largest to Smallest. `指定します。 `Free Capacity (GB),
  - 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ビューと同じビューに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。ここでは、 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。

Scheduled Reports		Reports	Show / Hide
IOPS	MB/s		Utilization
1.8 IOPS	1.54 MB/s	Download CSV	4%
918 IOPS	43.3 MB/s	Download PDF	< 1%
120 IOPS	7.99 MB/s	Download Excel	< 1%
		Upload Excel <input checked="" type="checkbox"/>	

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入力して、行の最後にあるチェックマーク ( ) 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、指定した受信者に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を使用したストレージの管理

## Active IQ Unified Manager REST APIでの作業の開始

Active IQ Unified Managerには、サポートされている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使用して管理するための一連のAPIが用意されています。これにより、サードパーティ製品との統合が可能になります。

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、NetAppシステムを管理するためのNetAppマネージャビリティソフトウェアソリューションのRESTfulクライアントを作成できます。APIは、Representational State Transfer (REST) のアーキテクチャスタイルに基づいています。Create、Read、Update、Delete (CRUDとも呼ばれる) の4つのREST処理がすべてサポートされます。

についてActive IQ Unified Manager REST APIのその他のリソースおよび利点の詳細、を参照してください"[Active IQ Unified Manager](#)"は。

### このコンテンツの対象者

このトピックは、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。

ストレージ管理者およびストレージアーキテクトは、この情報を参照して、Unified Manager REST APIを使用してNetAppストレージシステムを管理および監視するクライアントアプリケーションを構築する方法について基本的な知識を得ることができます。

この情報は、ストレージプロバイダ、ONTAPクラスタ、および管理管理APIを使用してストレージを管理する場合に使用します。



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。REST APIにアクセスするためのホスト名またはIPアドレスとURLを次の形式で入力します。

+ 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へのアクセス

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、次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（カテゴリ）に基づいて機能別に分類されています。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、データセンター内のクラスター、ノード、アグリゲート、ボリューム、LUN、ファイル共有、ネームスペースなどの要素に関する情報を提供します。

- \* management-server \*

management-server \*カテゴリのAPIには、APIと`events`APIが含まれていて`jobs, system,`ます。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からデータセンター内のイベントが返され、`system`APIからUnified Managerインスタンスの詳細が返されます。

- \* 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、このAPIを使用して、アクセスエンドポイントと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、バックアップ設定の管理、Unified Managerデータソースの信頼ストア証明書の表示、Unified ManagerのデータソースとしてのONTAPクラスターの管理など、管理タスクを実行するためのAPIが含まれています。

- \* 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、DELETEの各処理の例を次に示します。

- GETの例：`GET /datacenter/cluster/clusters`は、データセンター内のクラスタの詳細を取得します。操作によって返されるレコードの最大数`GET`は1000です。



APIを使用すると、サポートされている属性に基づいてレコードをフィルタリング、ソート、および順序付けできます。

- POSTの例：は、`POST /datacenter/svm/svms`カスタムのStorage Virtual Machine (SVM) を作成します。
- PATCHの例：は、`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。
- DELETEの例：は `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のユーザーロールによって異なります。

ユーザーロール	サポートされている REST メソッド
運用者	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、DELETE要求を実行するため) があります。
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、すべての機能に対してGET、PATCH、POST、DELETEの各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。たとえば `/v2/datacenter/svm/svms.`、の ``v2/datacenter/svm/svms`` バージョン番号 ``v2`` は、特定のリリースで使用されているAPIバージョンを示します。バージョン番号を指定すると、クライアントが処理できる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、将来のリリースで下位互換性を維持する一貫したインターフェイスが提供されます。また、同じAPIにバージョンがない場合もあります。たとえば `/datacenter/svm/svms.`、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では、(増分整数に関して) Unified Managerインスタンスで使用可能な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要求する必要があります。バージョン番号を指定すると、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、`version`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、いくつかのリリース後に最終的に廃止されます。このリリースでは、``v1``バージョンのAPIは廃止されています。

## 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 \*

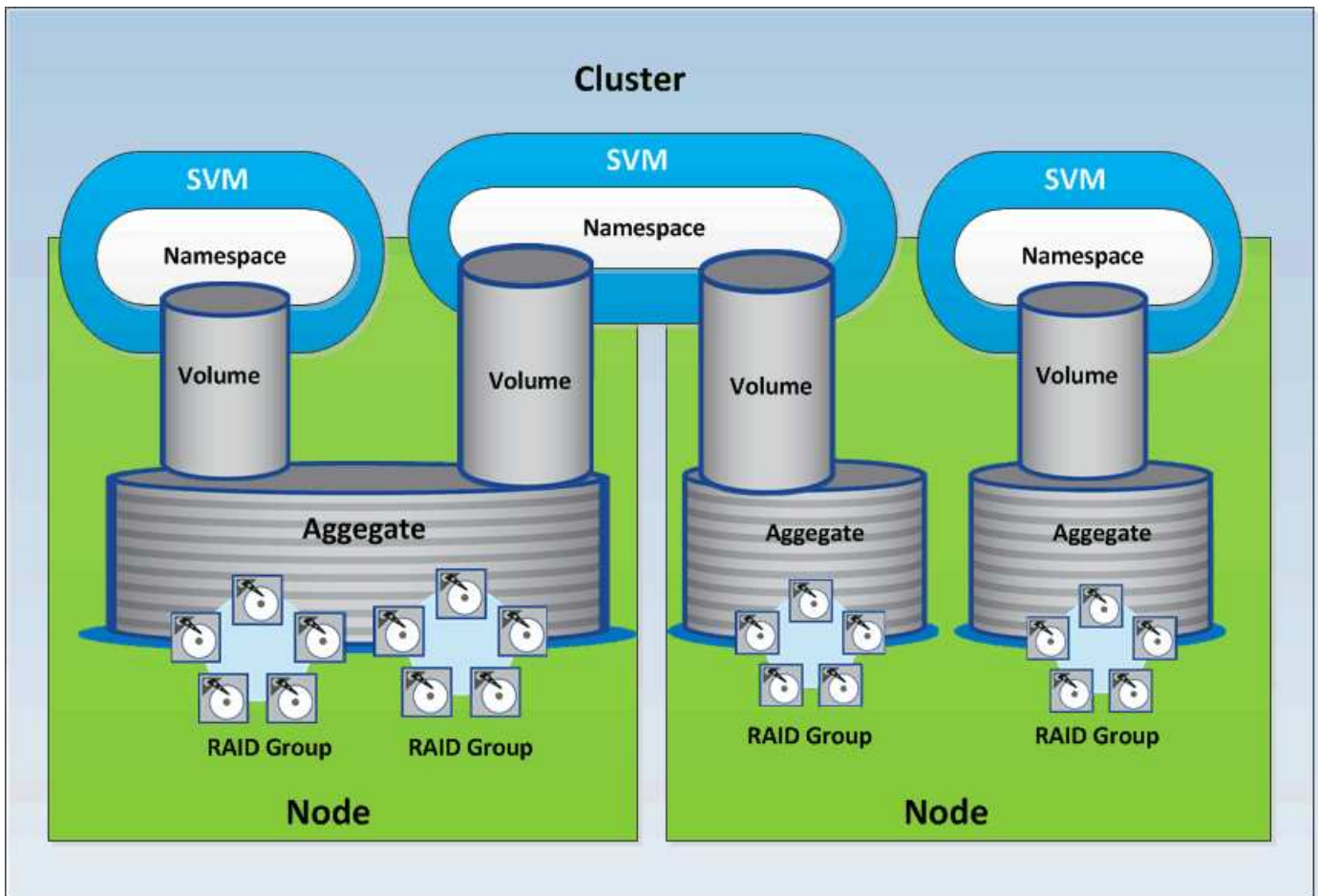
ONTAPが提供する物理ストレージオブジェクトです。物理ストレージリソースには、ディスク、クラスタ、ストレージコントローラ、ノード、アグリゲートがあります。

### \* 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からは独立して存在します。

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のほか、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と設定が含まれます。

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アクセスと認証

Active IQ Unified Manager REST APIには、基本的なHTTP認証メカニズムを使用してHTTP要求を発行できる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

デフォルトのHTTPSポートは443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HTTP要求を発行するには、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のベーシックHTTP認証方式がサポートされています。情報のフロー（要求と応答）を保護するために、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（CA証明書）に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	製品説明
200	OK	同期API呼び出しの実行が成功した場合に返されます。
201	作成済み	Active Directoryの設定など、同期呼び出しによる新しいリソースの作成。
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が正常に実行された場合に返されます。
400	無効な要求	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など、入力を修正する必要があります。
401	未許可の要求	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	禁止されている要求	アクセスしようとしている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たリソースが見つかりません。
405	許可されていないメソッド	許可されていないメソッドです。
429	要求が多すぎます	ユーザが特定の時間内に大量の要求を送信した場合に返されます。

HTTPステータスコード	ステータスコードタイトル	製品説明
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、処理または GET ALL`処理を実行してこのエラーが表示された場合は `GET、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は、ステータスコード500が引き続き返されます。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。

- 有効な実行を行うには、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を使用してアレイ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、値に文字が含まれていないことを確認して `?` ください。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。
- すべてのAPIの(all)要求は、最大1000レコードを返すことに注意してください GET。パラメータを1000より大きい値に設定してクエリを実行しても、`max\_records`1000レコードだけが返されます。
- 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すると、APIの実行中に発生する可能性が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	APIを呼び出しているユーザのユーザ名、開始時刻、実行時刻、ステータス、URLなど、API呼び出しのすべての詳細が格納されます。  このログファイルを使用して、頻繁に使用する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。
/var/log/ocum/ocumserver.log	すべてのAPI実行ログが含まれます。  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。
/var/log/ocie/server.log	すべてのWildflyサーバー展開とサービスの開始/停止に関連するログが含まれます。  このログファイルを使用して、Wildflyサーバーの起動、停止、または展開中に発生した問題の根本原因を見つけることができます。
/var/log/ocie/au.log	Acquisition Unit関連のログが含まれます。  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。

## ジョブオブジェクトの非同期プロセス

Active IQ Unified Managerには、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が用意されて `jobs` があります。ジョブオブジェクトを使用した非同期処理の仕組み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する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た非同期要求の説明

非同期で実行されるAPI呼び出しを実行すると、HTTP応答コード202が返されます。これは、要求が正常に検証されて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、一意の識別子を含む、要求をアンカーするジョブオブジェクトが含まれます。



## API要求に関連付けられている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してタスクの最終状態（成功または失敗）を検出するには、次の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。
- 長時間のポーリング要求：ジョブの状態がまた PARTIAL\_FAILURES. に移行したとき `NORMAL, ERROR,

## 非同期要求の手順

非同期API呼び出しを完了する手順の概要は次のとおりです。

1. 非同期API呼び出しを実行します。
2. 要求が正常に受け入れられたことを示す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 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サアハ

`_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。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がJSON形式で表示されます（サーバでは形式のみがサポートされ `application/json` ます）。

使用される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する次の考慮事項に注意してください。

- 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。
- URI接続にを使用します。 `javax.net.ssl.HttpURLConnection`
- サードパーティライブラリを使用(`org.apache.commons.codec.binary.Base64`) を使用して、HTTPベーシック認証で使用される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.HttpURLConnection;
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 {
    HttpURLConnection 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 HttpURLConnection
getAllTrustingHttpsURLConnection() {
    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());
HttpsURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));
    URL url = new URL(server_url);
    conn =
(HttpsURLConnection) 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呼び出しを検索したら、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呼び出しを見つけ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のAPI呼び出しは、機能に関連する領域（カテゴリ）に分類されています。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されるアクションを示します。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、呼び出しの実行時にアクションが使用する特定のリソースを決定します。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を使用したデータセンター内のストレージオブジェクトの管理

カテゴリのREST APIを `datacenter` 使用すると、クラスタ、ノード、アグリゲート、Storage VM、ボリューム、LUN、ファイル共有、ネームスペースなど、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。これらのAPIはオブジェクトの設定の照会に使用できますが、一部のAPIではオブジェクトの追加、削除、変更の処理を実行できます。

これらのAPIのほとんどは、フィルタリング、ソート、およびページネーションをサポートするクラスタ間集約を提供するGET呼び出しです。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場合は、そのオブジェクトの一意のIDを入力して詳細を表示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と分析の情報については、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使用できます。Swaggerに示されているように、特定のパラメータで結果をフィルタおよび順序付けることができます。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対して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API

HTTP動詞	パス	製品説明
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から返される情報には、クラスタのIPv4アドレスまたはIPv6アドレス、ノードに関する情報（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）、クラスタがオールSANアレイかどうかが含まれます。

HTTP動詞	パス	製品説明
GET	<pre>/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}</pre>	<p>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が返されます。必要な条件に基づいて結果をフィルタリングできます。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して、特定のライセンスの詳細を取得できます。</p>
GET	<pre>/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}</pre>	<p>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。</p>
GET	<pre>/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}</pre>	<p>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とは別に、アクセス制御リスト (ACL) に関する情報も返されます。</p>
GET	<pre>/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}</pre>	<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>クラスタまたはStorage VMのエクスポートポリシーを照会し、そのエクスポートポリシーキーをNFSファイル共有のプロビジョニングに再利用できます。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	製品説明
GET	<pre>/datacenter/storage/aggregates</pre> <pre>/datacenter/storage/aggregates/{key}</pre>	このメソッドを使用して、データセンター内の一連のアグリゲートや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に使用できます。クラスタとノードの詳細、使用済みパフォーマンス容量、使用可能スペースと使用済みスペース、Storage Efficiencyなどの情報が返されます。
GET	<pre>/datacenter/storage/luns</pre> <pre>/datacenter/storage/luns/{key}</pre>	このメソッドを使用して、データセンター全体の一連のLUNを表示できます。LUNに関する情報（クラスタとSVMの詳細、QoSポリシー、igroupなど）を確認できます。
GET	<pre>/datacenter/storage/qos/policies</pre> <pre>/datacenter/storage/qos/policies/{key}</pre>	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されるすべての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	<pre>/datacenter/storage/qtrees</pre> <pre>/datacenter/storage/qtrees/{key}</pre>	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 volume、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	製品説明
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。ボリュームに関する情報（SVMとクラスタの詳細、QoS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）が返されます。</p> <p>FlexVolボリュームと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、コンスティテュエントアグリゲートのリストが返されます。</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がある場合は割り当てることができます。igroupを作成してLUNに割り当てることもできます。</p> <p>これらのメソッドを使用して、igroupの照会、作成、削除、および変更をそれぞれ実行できます。</p> <p>注意事項：</p> <ul style="list-style-type: none"> <li>• `POST:`igroupの作成時に、アクセスを割り当てるStorage VMを指定できます。</li> <li>• `DELETE:`特定のigroupを削除するには、igroupキーを入力パラメータとして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。</li> <li>• `PATCH:`特定のigroupを変更するには、igroupキーを入力パラメータとして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。</li> </ul>

HTTP動詞	パス	製品説明
GET	/datacenter/svm/svms	<p>これらのメソッドを使用し、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"> <li>・`POST`: 作成するStorage VMオブジェクトを入力パラメータとして入力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。</li> <li>・`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。</li> <li>・`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。</li> </ul>
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は、Storage VMの作成時に、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（CIFS、SMB、NFS、FCP、iSCSIなど）がサポートされていることを確認してください。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。それぞれの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サーバまたはSMBサーバが設定されているStorage VMを削除すると、CIFSサーバまたはSMBサーバとローカルのActive Directory設定も削除されます。ただし、CIFSサーバまたはSMBサーバ名は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。

#### データセンターのネットワーク要素用API

datacenter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、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	製品説明
GET	<pre>/datacenter/network/ethernet/ports</pre> <pre>/datacenter/network/ethernet/ports/{key}</pre>	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。ポートキーを入力パラメータとして使用すると、その特定のポートの情報を表示できます。取得される情報は、クラスタの詳細、ブロードキャストドメイン、ポートの詳細（状態、速度、タイプなど）、ポートが有効かどうかなどです。
GET	<pre>/datacenter/network/fc/interfaces</pre> <pre>/datacenter/network/fc/interfaces/{key}</pre>	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。インターフェイスキーを入力パラメータとして使用すると、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	<pre>/datacenter/network/fc/ports</pre> <pre>/datacenter/network/fc/ports/{key}</pre>	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。ポートキーを入力パラメータとして使用すると、その特定のポートの情報を表示できます。クラスタの詳細、ポートの説明、サポートされるプロトコル、ポートの状態などの情報が取得されます。
GET	<pre>/datacenter/network/ip/interfaces</pre> <pre>/datacenter/network/ip/interfaces/{key}</pre>	このメソッドを使用して、データセンター環境のIPインターフェイスの詳細を表示できます。インターフェイスキーを入力パラメータとして使用すると、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。

## プロキシアクセスによるONTAP APIへのアクセス

ゲートウェイAPIには、Active IQ Unified Managerクレデンシャルを使用してONTAP REST APIを実行したり、ストレージオブジェクトを管理したりできるという利点があります。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した場合に使用できます。

Unified Manager REST APIでは、Unified Managerデータソース（ONTAPクラスタ）に対して実行され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として使用して、Unified Managerが管理するONTAPクラスタで実行されるすべての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。Unified Managerインスタンスで管理されるONTAPクラスタ間でAPIを実行するための単一の管理ポイントとして機能します。APIゲートウェイ機能を使用すると、Unified Managerを単一のコントロールプレーンとして使用して、複数のONTAPクラスタに個別にログインすることなく管理できます。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。



すべてのユーザが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、ONTAP RESTのすべての処理を実行できます。

ゲートウェイは、ヘッダーと本文の要求をONTAP APIと同じ形式で維持することで、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と、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るようにリダイレクトされます。APIから返される応答は、ONTAPから直接実行された対応するONTAP REST APIから返される応答と同じです。

HTTP動詞	パス（URL）	製品説明
GET	/gateways	<p>このGET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 style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>ゲートウェイAPIは、ONTAP 9.5以降でサポートされていて、HTTPS経由でUnified Managerに追加されたクラスタのみを取得します。</p> </div>

HTTP動詞	パス (URL)	製品説明
GET POST DELETE PATCH OPTIONS (Swaggerでは使用できません) HEAD (Swaggerでは使用できません)	<p>/gateways/{uuid}/{path}</p> <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、ONTAP 9.5以降でサポートされているクラスタのUUIDで、HTTPS経由でUnified Managerに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。URLから削除する必要があります。 \ /api/ ます。</p>	<p>これはシングルポイントプロキシAPIであり、すべてのONTAP REST APIでPOST、DELETE、PATCH操作、GETをサポートしています。ONTAPでサポートされている限り、どのAPIにも制限はありません。トンネリング機能またはプロキシ機能はディセーブルにできません。</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p>\ `OPTIONS` メソッドは、ONTAP REST APIでサポートされるすべての処理を返します。たとえば、ONTAP APIが処理のみをサポートしている場合</p> <p>\ `GET` は、このゲートウェイAPIを使用してメソッドを実行すると、</p> <p>\ `OPTIONS` が応答として返されます</p> <p>\ `GET`。このメソッドはSwaggerではサポートされていませんが、他のAPIツールでも実行できます。</p> </div> <p>メソッドは、\ `OPTIONS` リソースが使用可能かどうかを判断します。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。このメソッドはSwaggerではサポートされていませんが、他のAPIツールでも実行できます。</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で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、要求をONTAP RESTエンドポイントにリダイレクトします。ゲートウェイAPIは、ヘッダーと応答の本文にあるアプリケーション状態のエンジン(HATEOAS)リンクとしてURLと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ベースURLとして機能します。



APIゲートウェイ経由でONTAP APIを正常に実行するには、APIが実行されているONTAPクラスタの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）は次のとおりです。 `/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、“add/” symbol at the beginning of the URL. For the API `/storage/volumes`, `storage/volumes`.

追加されるURLは次のとおりです。 `/gateways/{uuid}/storage/volumes`

処理の実行時に GET 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のタグは追加された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/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

APIは、その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を実行したときに受け取る形式と同じです。返されるステータスコードは、ONTAP RESTステータスコードです。

#### APIスコープノセッティ

すべてのAPIには、クラスタの範囲内にコンテキストが設定されています。Storage VMを基に動作するAPIには、スコープとしてクラスタも含まれます。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。APIを実行するときは `/gateways/{uuid}/{path}`、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）を入力してください。クラスタ内の特定のStorage VMにコンテキストを設定するには、X-Dot-svm-UUIDパラメータにStorage VMキーを入力するか、X-Dot-svm-NameパラメータにStorage VM名を入力します。パラメータが文字列ヘッダーにフィルタとして追加され、そのクラスタ内のその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自動化"]

## APIを使用した管理タスクの実行

のAPIを使用してカテゴリことができます administration、バックアップ設定の変更、バックアップファイルの情報とクラスタ証明書の検証、およびONTAPクラスタのActive IQ Unified Managerデータソースとしての管理を行う。



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。これらの設定は、Unified Manager Web UIを使用して行うこともできます。

HTTP動詞	パス	製品説明
GET	/admin/backup-settings	<p>メソッドを使用すると、Unified Managerでデフォルト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できます GET。次のことを確認できます。</p> <ul style="list-style-type: none"> <li>• スケジュールが有効か無効か</li> <li>• スケジュールされたバックアップの頻度（毎日または毎週）</li> <li>• バックアップの時刻</li> <li>• アプリケーションで保持するバックアップファイルの最大数</li> </ul> <p>バックアップの時刻はサーバのタイムゾーンです。</p> <p>Unified Managerではデータベースのバックアップ設定をデフォルトで使用でき、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、メソッドを使用すると、デフォルト設定を変更できます PATCH。</p>
PATCH	/admin/backup-settings	

HTTP動詞	パス	製品説明
GET	/admin/backup-file-info	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たかどうか、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。
GET	/admin/datasource-certificate	このメソッドを使用すると、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。
GET POST PATCH DELETE	/admin/datasources/clusters  /admin/datasources/clusters/{key}	メソッドを使用すると、Unified Managerで管理されているデータソース（ONTAPクラスタ）の詳細を取得できます GET。  また、新しいクラスタをデータソースとしてUnified Managerに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、ユーザー名、パスワードが必要です。  Unified Managerでデータソースとして管理されてい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。

## APIを使用したユーザの管理

カテゴリのAPIを使用して、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できます `security`。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。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Privileges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。これらの設定は、Unified Manager Web UIを使用して行うこともできます。

カテゴリのAPI `security` では、ユーザエンティティの一意の識別子としてキーパラメータではなく、usersパラメータ（ユーザ名）を使用します。



HTTP動詞	パス	製品説明
GET POST	/security/users	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。  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。
GET PATCH DELETE	/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メソッドを使用すると、詳細を更新できます。deleteメソッドを使用すると、ユーザを削除できます。

## APIを使用したパフォーマンス指標の表示

Active IQ Unified Managerには、カテゴリの一連のAPIが用意されています。このAPIを`/datacenter`を使用して、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ます。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、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インターフェイスなど、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。

`/metrics` APIと

`/analytics` APIでは、パフォーマンス指標がさまざまに表示されます。これを使用すると、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 VM
- アグリゲート
- 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

次の表に、取得したパフォーマンスデータの詳細に関するAPIと `/analytics`API`の比較を示します  
``/metrics。`

指標	分析
単一オブジェクトのパフォーマンスの詳細。たとえば、APIで <code>`/datacenter/cluster/clusters/{key}/metrics`</code> は、その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cluster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、 <code>`/datacenter/cluster/clusters/analytics`API</code> はデータセンター内のすべてのクラスタの総合的な指標を取得します。
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のサンプル。	特定のタイプのストレージオブジェクトの一定期間（72時間以上）のパフォーマンスの集計値の概要。
オブジェクトの基本的な詳細（ノードやクラスタの詳細など）が読み出されます。	特定の詳細は取得されません。
1つのオブジェクトについて、最小値、最大値、95パーセンタイル値、一定期間の平均パフォーマンス値などの累積カウンタ（読み取り、書き込み、合計、その他のカウンタなど）が読み出されます。	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。例としては、1h、12h、1d、2d、3d、15d、1w、1m、2m、3m、6mがあります。範囲が3日（72時間）を超える場合は、1時間のサンプルが取得されます。それ以外の場合は、5分のサンプルが取得されます。各時間範囲の期間は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 1M：最近1時間でサンプリングされた月のメトリックス。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul> <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。このサンプルが計算される期間は、ISO-8601標準形式で表されます。</p>

### 指標APIの出力例

たとえば、`/datacenter/cluster/nodes/{key}/metrics` APIは（特に）ノードについて次の詳細を取得します。



要約値の95パーセンタイルは、その期間に収集されたサンプルの95%が、95パーセンタイルとして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

たとえば `/datacenter/cluster/nodes/analytics`、すべてのノードについて（とりわけ）次の値が取得されます。

```

{
  "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

次の表に、と `/analytics` のAPIの詳細を示し `/metrics` ます。



これらのAPIから返されるIOPSとパフォーマンスの指標は、のように2倍の値です 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	製品説明
GET	/datacenter/cluster/clusters/{key}/metrics	クラスタキーの入力パラメータで指定され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	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リングできます。集計されたIOPS、スループット、収集期間（時間）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されたノードのパフォーマンスデータ（サンプルと概要）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、使用率などの情報が返されます。
GET	/datacenter/cluster/nodes/analytics	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リングできます。ノードキーやクラスタキーなどの情報と、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	アグリゲートキーの入力パラメータで指定されたアグリゲートのパフォーマンスデータ（サンプルと概要）を取得します。期間、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	製品説明
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を取得します。必要な条件に基づいて結果をフィルタリングできます。アグリゲートキーやクラスターキーなどの情報と、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（サンプルと概要）を取得します。読み取り、書き込み、合計の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、各カウンタで収集されたサンプル数などの情報が返されます。
GET	/datacenter/storage/luns/analytcs  /datacenter/storage/volumes/analytcs	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リングできます。Storage VMやクラスターのキーなどの情報と、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された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。サポートされる各プロトコルに基づくIOPSの概要（や、`nfs`スループット、レイテンシ、収集されたサンプル数など）`nvmf, fcp, iscsi`が返されます。
GET	/datacenter/svm/svms/analytcs	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リングできます。Storage VM UUID、集約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	製品説明
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は一定期間のパフォーマンスの最小値、最大値、平均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について、パフォーマンス指標の概要を取得します。クラスタとノードのキーと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され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は一定期間のパフォーマンスの最小値、最大値、平均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について、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	製品説明
GET	/datacenter/network/fc/ports/{key}/metrics	ポートキーの入力パラメータで指定された特定の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は一定期間のパフォーマンスの最小値、最大値、平均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ポートについて、パフォーマンス指標の概要を取得します。クラスタとノードのキーと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したネットワーク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、送受信された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インターフェイスについて、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と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の表示

カテゴリのAPIを `management-server`` 使用して、非同期処理の実行の詳細を確認できます。`jobs`。`system`カテゴリのAPIを`management-server`使用すると、Active IQ Unified Manager環境でインスタンスの詳細を確認できます。

## 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。非同期実行が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を返します。このURIを使用すると、ジョブの進捗状況にアクセスして追跡できます。このAPIを使用して、各実行の詳細を取得できます。

このAPIを使用すると、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。デフォルトでは、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。また、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一連の処理を実行することもできます。

カテゴリ	HTTP動詞	パス	製品説明
management-server	取得	/management-server/jobs	すべてのジョブのジョブの詳細を返します。並べ替え順序が指定されていない場合、最後に送信されたジョブオブジェクトが上に返されます。
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、そのジョブの特定の詳細を表示します。	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

APIを使用する`/management-server/system`と、Unified Manager環境のインスタンス固有の詳細を照会できます。APIから、製品とサービスに関する情報が返されます。これには、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のほか、Unified Managerインスタンスで実行されているサービスの名前、説明、ステータスなどの情報が含まれます。

カテゴリ	HTTP動詞	パス	製品説明
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を使用したイベントとアラートの管理

`alerts`カテゴリのAPI、`management-server`、および`scripts`を使用して、`events` Active IQ Unified Manager環境内のイベント、アラート、およびアラートに関連付けられているスクリプトを管理できます。

## イベントの表示と変更

Unified Managerは、Unified Managerによって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け取ります。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、解決および更新できます。

APIのメソッドを`/management-server/events`実行すると、`GET`履歴データを含むデータセンター内のイベントを照会できます。組み込みのフィルタ（名前、影響レベル、影響領域、重大度、状態、リソース名、リソースタイプなど）を使用して、特定のイベントを表示します。リソースタイプと領域の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、影響領域はイベントが発生した問題に関する情報（可用性、容量、構成、セキュリティ、保護、パフォーマンスなど）を返します。

このAPIに対してPATCH処理を実行することで、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。自分または別のユーザにイベントを割り当て、イベントの受信を確認することができます。イベントをトリガーした問題を解決するための手順をリソースに対して実行すると、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	製品説明
management-server	取得	/management-server/events /management-server/events/{key}	GET ALLメソッドを実行すると、応答の本文はデータセンター内のすべてのイベントの詳細で構成されます。特定のキーで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一連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	management-server/events/{key}	このAPIを実行してイベントを割り当てるか、状態をacknowledgedまたはresolved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にイベントを割り当てることもできます。これは同期処理です。

## 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。APIを使用する`/management-server/alerts`と、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ように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	製品説明
management-server	取得	/management-server/alerts /management-server/alerts/{key}	alert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。アラートの説明、アクション、通知の送信先EメールID、イベントや重大度など、環境で生成されたアラートに関する情報を確認できます。
management-server	投稿	/management-server/alerts	このメソッドを使用すると、特定のイベントのアラートを追加できます。アラート名、アラートを適用する物理リソースまたは論理リソース、またはイベント、アラートが有効になっているかどうか、SNMPトラップを発行しているかどうかを追加する必要があります。アクション、通知EメールID、スクリプトの詳細、アラートスクリプトを追加する場合のスクリプトの詳細など、アラートを生成する詳細を追加できます。
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。説明や名前、アラートの有効化と無効化など、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すると、クラスタの重大イベントに対するアラートのみが送信されます。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

APIを使用する `/management-server/scripts` と、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実行をテストすることができます。Unified Manager でイベントに対してアラートが生成され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	製品説明
management-server	取得	/management-server/scripts	このAPIを使用して、環境内のすべての既存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、標準のフィルタおよび順序指定操作を使用します。
management-server	投稿	/management-server/scripts	このAPIを使用して、スクリプトの説明を追加し、アラートに関連付けられているスクリプトファイルをアップロードします。

## APIを使用したワークロードの管理

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への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を使用して、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の表示

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の表示

使用済み容量、使用可能容量、使用済みIOPS、使用可能IOPS、および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の表示

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の追加

カスタムアクセスエンドポイントを作成し、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入力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プロトコルと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	/storage-provider/access-endpoints

## アクセスエンドポイントの削除

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の変更

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

ここに記載されている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を使用して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マッピングの表示

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マッピングの追加

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	/storage-provider/active-directories-mappings

#### APIを使用したファイル共有の管理

APIを使用して、データセンター環境でCIFSおよびNFSファイル共有ボリュームを表示、追加、変更、削除できます /storage-provider/file-shares。

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てください。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、プロビジョニング時に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。

#### ファイル共有の表示

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}

#### ファイル共有の追加

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	/storage-provider/file-shares



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パラメータのどちらか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と、CIFS共有は作成されず、デフォルトでNFS共有が作成されてすべてのアクセスが許可されます。

データ保護ボリュームを作成する：SVMにファイル共有を追加する場合、マウントされるボリュームのタイプは、デフォルトで（読み取り/書き込み）です `rw`。データ保護（DP）ボリュームを作成する場合は、パラメータの値として `type`` を指定します ``dp`。

#### ファイル共有の削除

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}

#### ファイル共有の変更

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。複数の更新を行う場合は、このAPIを何度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

APIを使用して、データセンター環境のLUNを表示、追加、変更、削除できます  
/storage-provider/luns。

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。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、プロビジョニング時に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の表示

Unified Manager環境では、次のメソッドを使用してLUNを表示できます。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の追加

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	/storage-provider/luns



cURL要求で、オプションのパラメータvolume\_name\_tagの値を入力に指定すると、その値がLUNの作成時にボリュームの命名に使用されます。このタグを使用すると、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、タギングはスキップされます。

## LUNの削除

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}

## LUNの変更

LUN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。複数の更新を行う場合は、このAPIを何度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の表示

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リストし、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の追加

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、次のメソッドを使用してカスタムの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	/storage-provider/performance-service-levels

### パフォーマンスサービスレベルの削除

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、または使用可能な唯一のパフォーマンスサービスレベルである場合、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、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/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できる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することができます。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の表示

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場合は、ポリシーの一意的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	<code>/storage-provider/storage-efficiency-policies</code>  <code>/storage-provider/storage-efficiency-policies/{key}</code>

#### ストレージ効率化ポリシーの追加

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、次のメソッドを使用して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	<code>/storage-provider/storage-efficiency-policies</code>

#### ストレージ効率化ポリシーの削除

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的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	<code>/storage-provider/storage-efficiency-policies/{key}</code>

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

一般的なワークフローでは、クライアントアプリケーション開発者が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の例を紹介します。ここでは、いくつかのサンプルワークフローについて説明します。

以下のワークフローでは、ストレージ管理でよく使用されるいくつかのユースケースとサンプルコードについて説明します。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されるAPI呼び出しの概要

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のみが含まれています。特定のAPI呼び出しを検索したら、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呼び出しを見つけ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**：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。

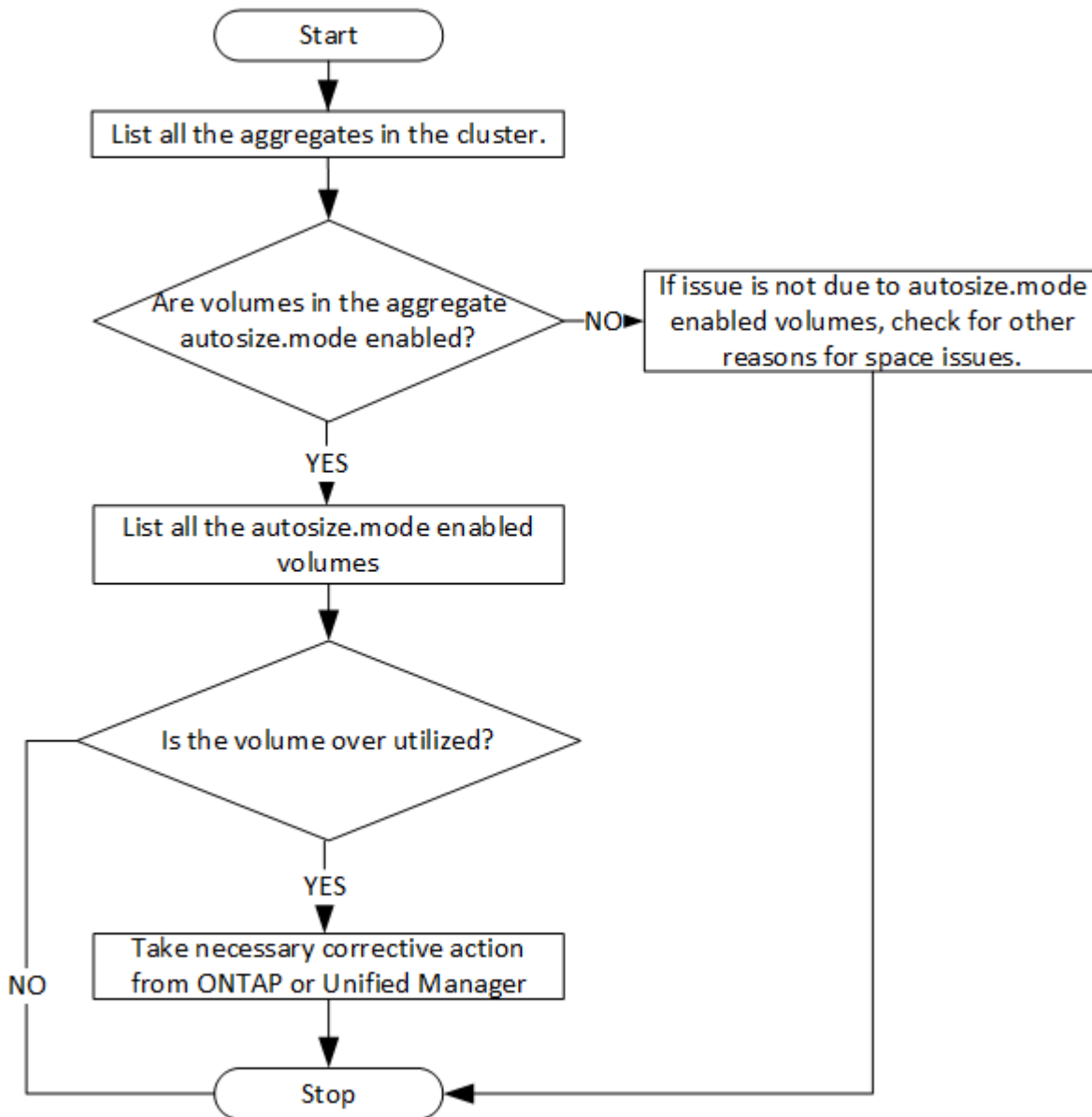
### APIを使用したアグリゲート内のスペースの問題の特定

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、利用率が高いストレージリソースや利用率が低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効率の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。

アグリゲートのスペース不足を確認する方法の1つは、環境にオートサイズモードが有効になっているボリュームがあるかどうかを確認することです。次に、利用率の高いボリュームを特定し、対処方法を実行します。

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ONTAPで作成されてUnified Managerに追加されていることを前提としています。

1. 値がわからない場合は、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、そのクラスター上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。スペースに問題があ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パラメータの値がとなっているすべてのボリュームを次のようにフィルタリングします。 grow.

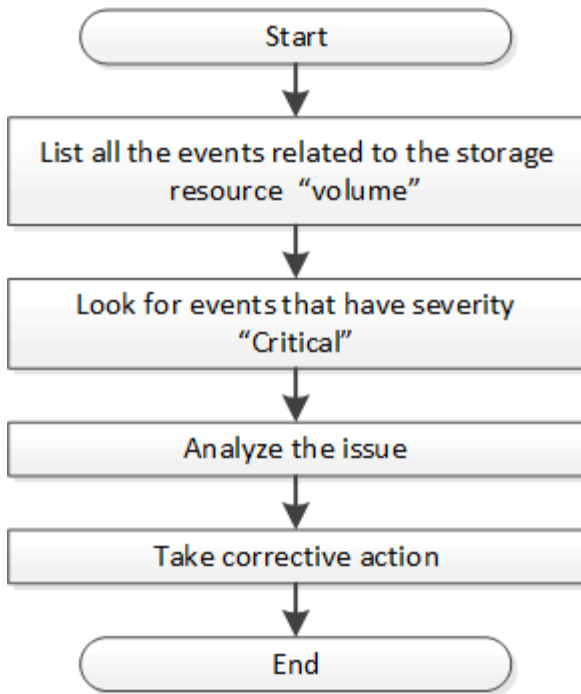
カテゴリ	HTTP動詞	パス
データセンター	取得	/datacenter/storage/volumes

5. 利用率の高いボリュームを分析します。
6. ボリューム内のスペースの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、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のWeb UIから実行できます。

## イベントAPIを使用したストレージオブジェクトの問題の特定

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届きます。この通知を使用して、APIを使用して問題を分析し、対処することができます events。

このワークフローでは、ボリュームをリソースオブジェクトとして使用する例を示します。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、問題を修正するための対処方法を実行できます events。



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Active IQ Unified Managerの重大イベント通知を分析します。
2. /management-server/events APIで次のパラメータを使用して、ボリュームに関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/events

3. 出力を表示して、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、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対策を講じるためのゲートウェイとして機能します。

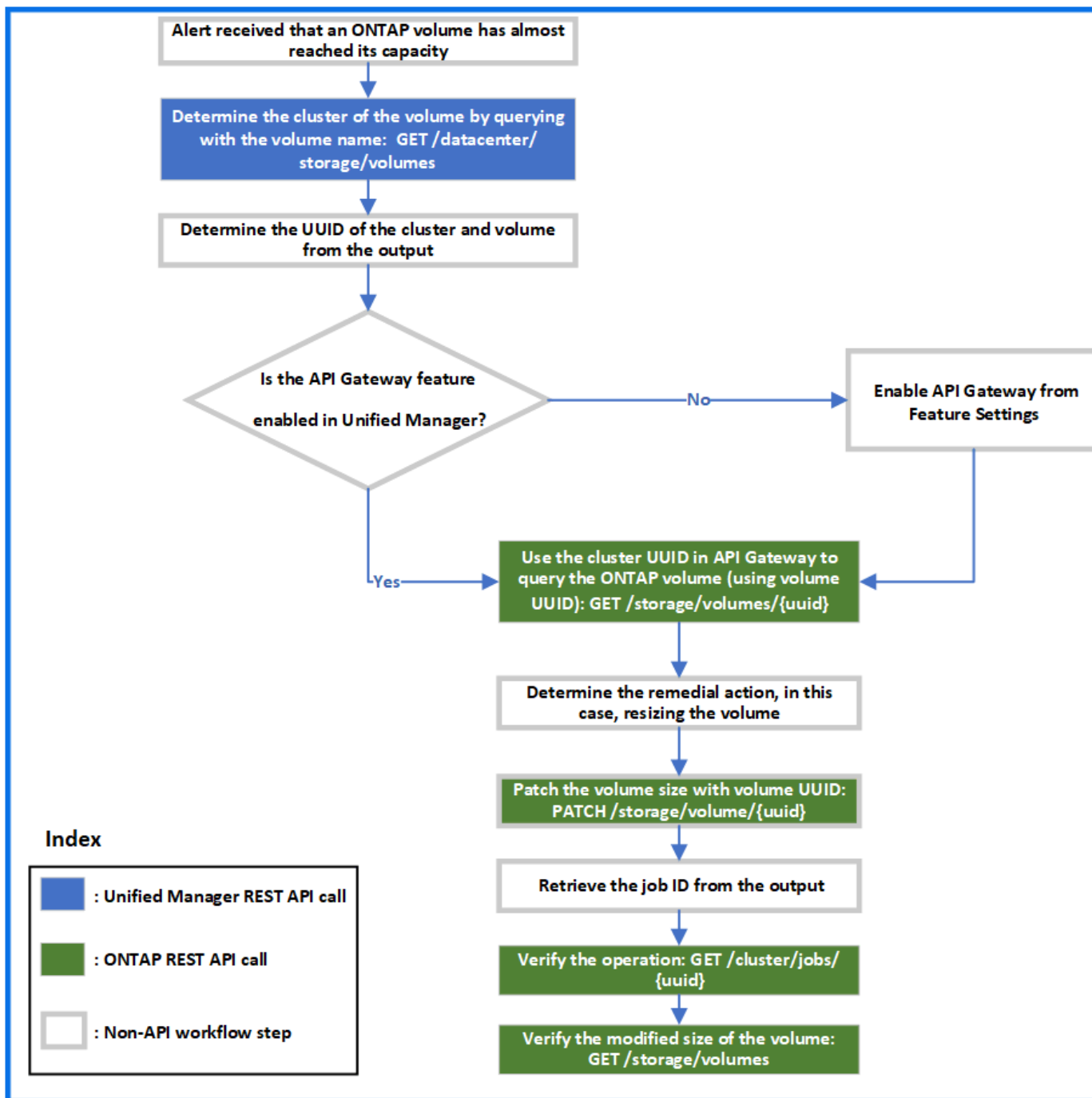
このワークフローでは、ONTAPの容量がほぼ上限に達したときにイベントが生成されるユースケースを取り上げます。また、Active IQ Unified ManagerとONTAP REST APIを組み合わせることでこの問題に対処する方法についても説明します。

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APIとその使用方法について理解しておく必要があります。詳細については、[を参照してください "プロキシアクセスによるONTAP APIへのアクセス"](#)。
- ONTAP REST APIの使用方法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](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、HTTPS経由でUnified Managerに追加されています。

次の図は、ONTAPボリュームの容量使用に関する問題をトラブルシューティングするための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の両方の呼び出しポイントについて説明します。

1. ボリュームの容量利用率を通知するイベントのボリューム名をメモします。
2. nameパラメータの値にボリューム名を使用して、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

- 出力からクラスタUUIDとボリュームUUIDを取得します。
- 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。無効になっている場合は、この機能を有効にします。
- クラスタUUIDを使用して、APIゲートウェイ経由でONTAP APIを実行し、`/storage/volumes/{uuid}` ます。APIパラメータとしてボリュームUUIDを指定すると、ボリュームの詳細が返されます。

APIゲートウェイを介してONTAP APIを実行する場合は、Unified Managerのクレデンシャルが認証用に内部的に渡されるため、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	取得	ゲートウェイAPI： <code>/gateways/{uuid}/{path}</code>
ONTAP：ストレージ		ONTAP API： <code>/storage/volumes/{uuid}</code>



`/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>"
```

- 出力から、実行するサイズ、使用量、修復方法を確認します。このワークフローでは、ボリュームのサイズ変更を修正します。
- クラスタUUIDを使用し、APIゲートウェイ経由で次のONTAP APIを実行してボリュームのサイズを変更します。ゲートウェイAPIとONTAP APIの入力パラメータについては、手順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}



ボリュームのサイズを変更するには、クラスタUUIDとボリュームUUIDに加えて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size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出力からジョブ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APIとONTAP APIの入力パラメータについては、手順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、サイズが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APIとONTAP APIの入力パラメータについては、手順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、ボリュームサイズが120GBに拡張されたことが表示されます。

## ワークロード管理の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）について、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、関連する概念と参考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の作成時には、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（CIFS、NFS、FCP、iSCSIなど）をサポートするようにしてください。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	/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入力します。

```
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\" ] }, \"fcp\": { \"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。

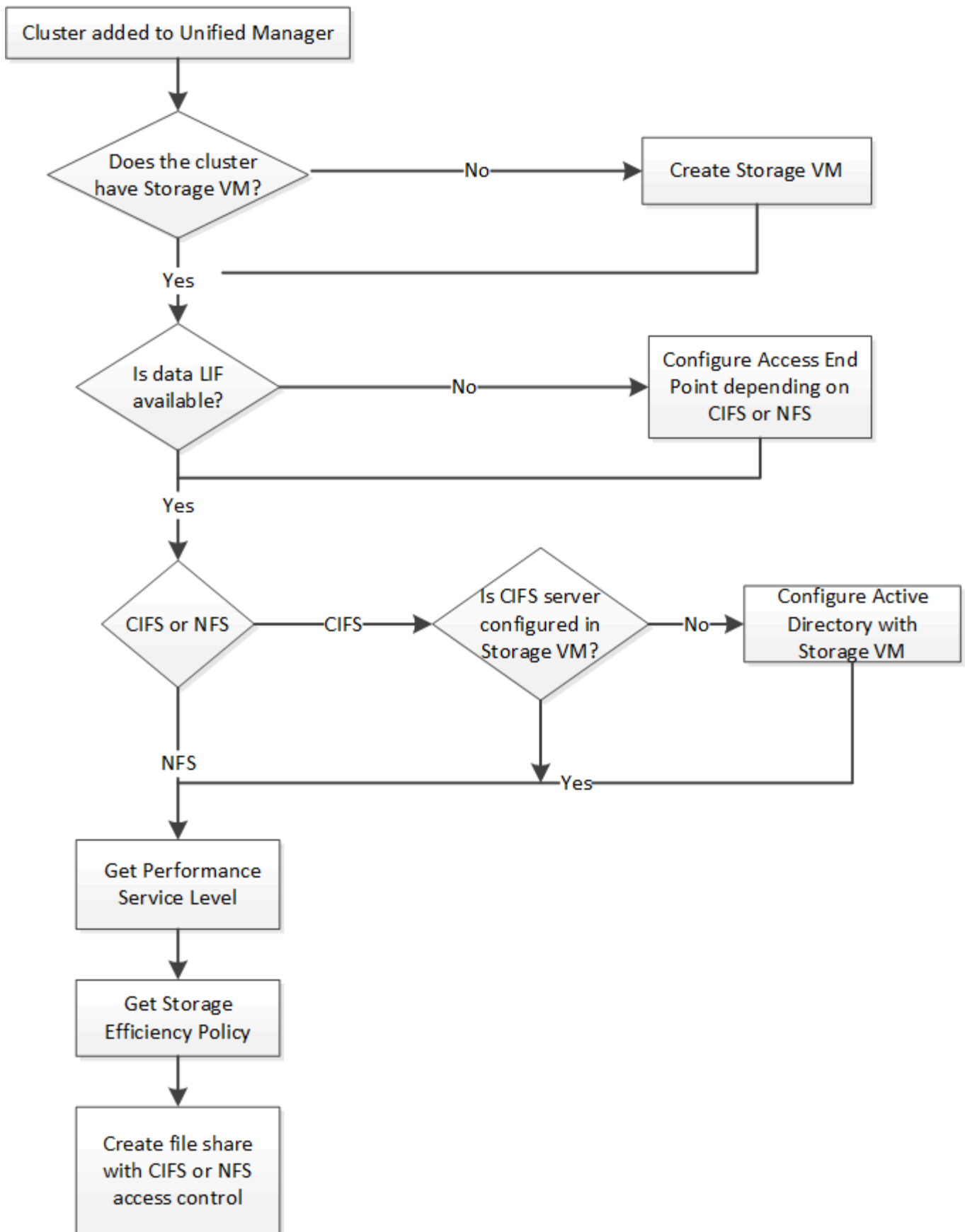
4. ジョブオブジェクトキーを使用してクエリを実行し、SVMの作成を確認します。SVMが正常に作成されると、SVMキーが応答に返されます。

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。これには、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。
- SVMでCIFSサービスとNFSサービスがサポートされます。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ポートはポートプロビジョニング用にオンラインになっています。

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. 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プロトコルが有効になっている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いないと、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	/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入力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確認します。

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決定します。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。つまり、SVMにActive Directoryマッピング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
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	/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入力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,uid=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、トラブルシューティングを行っ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、「クラスターの 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、入力パラメータを `true` 設定し `system\_defined` ます。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ことで、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て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、Access Control List (ACL; アクセス制御リスト) 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 / 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。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共有をプロビジョニングする際に、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。キーがわからない場合は、API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。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。入力したルールに対して、APIはホスト、Storage VM、およびルールを照合することで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の両方のファイル共有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	/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。です。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メソッドは、`/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、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APIを呼び出し`/storage-provider/performance-service-levels/`ます。

```

{
  "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"
        }
      ]
    }
  }
}

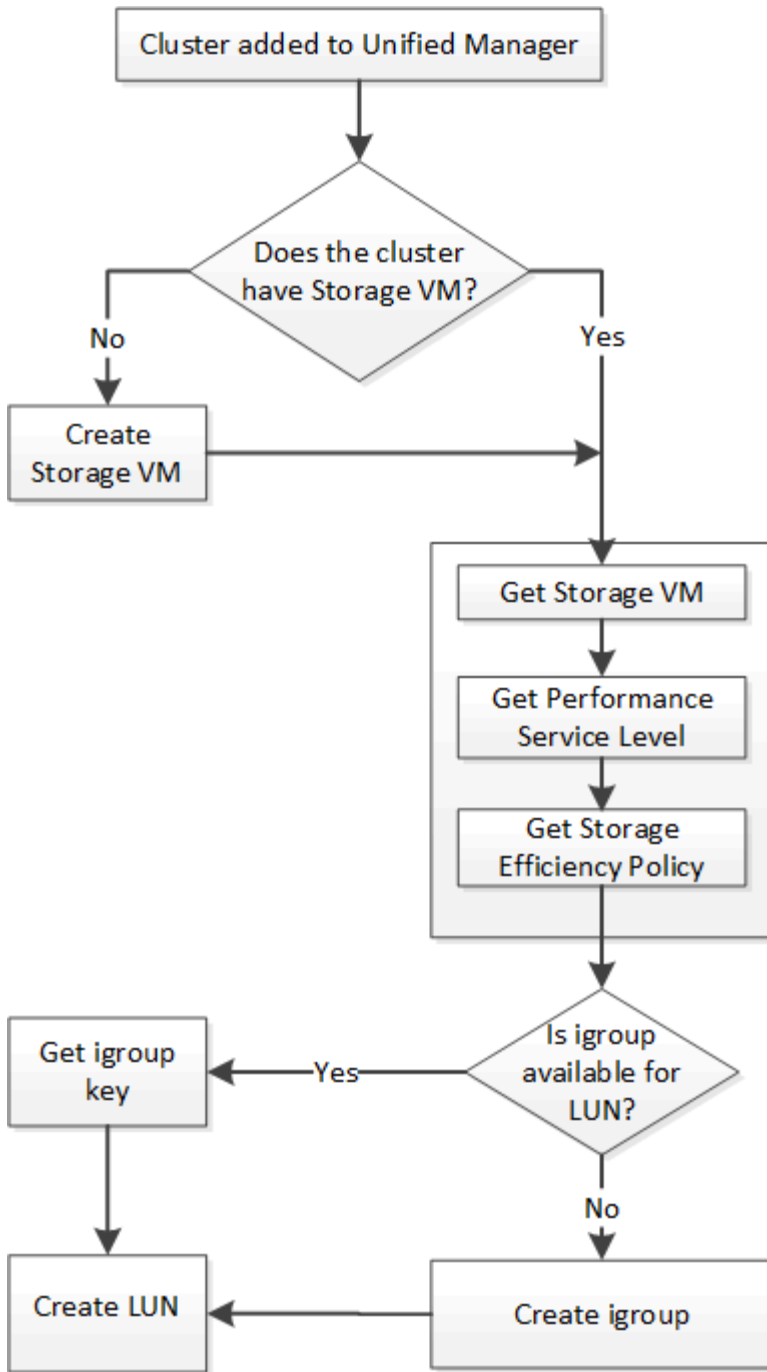
```

```

    }
  ],
  "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"
        ]
      }
    ]
  }
}

```





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がクラスタに作成済みであ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 ノサクシヨ\_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、入力パラメータを `true` 設定し `system\_defined` ます。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がアクセスを許可するSVMをパラメータ値で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が出力に表示されたら、キーを取得します。それ以外の場合は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	/datacenter/protocols/san/igroups

作成するigroupの詳細を入力パラメータとして入力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、トラブルシューティングしてAPIを再実行するように求めるメッセージが表示されます。

- LUNを作成

カテゴリ	HTTP動詞	パス
ストレージプロバイダ	投稿	/storage-provider/luns

LUNを作成する場合は、取得した値を必須パラメータとして追加しておきます。



ストレージ効率化ポリシーは、LUNを作成する場合のオプションパラメータです。

◦ 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入力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}

応答の最後に、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メソッドは、`/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、LUNにパフォーマンスサービスレベルを割り当てるAPIを呼び出し`/storage-provider/performance-service-levels/`ます。

= 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の作成に成功した場合でも、LUNを作成するノードにSAN LIFまたはアクセスエンドポイントがないことが原因で、igroupとのLUNマッピングが失敗することがあります。障害が発生した場合は、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	/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入力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が追加されていることを確認します。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 \*

出力の最後に、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確認に使用できません。

4. LUNキーを指定して照会して、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 \*

出力から、LUNのプロビジョニング時に使用したigroup (key d19ec2fa-fec7-11E8-b23d-00a098e32c28) 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、パラメータが指定されていない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。



このワークフローは、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：
- Access Control List (ACL;アクセスコントロールリスト) 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、入力パラメータを `true` 設定し `system\_defined` ます。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。この場合は、パフォーマンスサービスレベルのキーです。

◦ 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、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が表示されます。障害が発生した場合は、障害をトラブルシューティングして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の更新

LUNの更新時に変更できるパラメータは次のとおりです。

- 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。他のLUNプロパティも同じ手順で更新できます。

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、この手順をスキップします。

カテゴリ	HTTP動詞	パス
ストレージプロバイダ	取得	/storage-provider/luns

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}

の出力で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ません。

- 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、入力パラメータを `true` 設定し `system\_defined` ます。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キーと一緒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です。

##### ° 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}

の出力で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。ファイル共有の作成時に、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そのファイル共有の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。

これは、ACLパラメータではなく、エクスポートポリシーのみを追加して作成したNFSファイル共有に該当します。ACLパラメータを追加するようにNFSファイル共有を変更します。

#### 手順

1. NFSファイル共有で、CIFSアクセスを許可するACLの詳細を指定して処理を実行し `PATCH` 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

#### ◦ 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Privileges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エクスポートポリシーと一緒にACLが割り当てられていることを確認できます。

# 法的通知

法的通知では、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。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## 特許

NetAppが所有する特許の最新リストは、次のサイトで参照できます。

<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 9.14の場合の注意事項"](#)

## 著作権に関する情報

Copyright © 2024 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。