



Active IQ Unified Managerのドキュメント

Active IQ Unified Manager

NetApp
October 15, 2025

目次

Active IQ Unified Managerのドキュメント	1
リリース ノート	2
始めましょう	3
インストールのクイック スタート手順 (VMware)	3
システム要件	3
Active IQ Unified Managerのインストール	3
インストールのクイック スタート手順 (Linux)	4
システム要件	4
Active IQ Unified Managerのインストール	4
インストールのクイック スタート手順 (Windows)	5
システム要件	5
Active IQ Unified Managerのインストール	6
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サーバの機能	7
インストール手順の概要	7
Unified Managerをインストールするための要件	8
仮想インフラおよびハードウェア システムの要件	8
VMwareソフトウェアとインストールの要件	10
サポートされるブラウザ	10
プロトコルとポートの要件	11
ワークシートへの記入	14
Unified Manager ソフトウェアのインストール、アップグレード、および削除	16
導入プロセスの概要	16
Unified Manager を導入する	17
Unified Manager のアップグレード	21
Unified Manager仮想マシンを再起動する	24
統合マネージャーを削除する	24
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サーバの機能	26
インストール手順の概要	26
Unified Managerをインストールするための要件	27
仮想インフラおよびハードウェア システムの要件	27
Linuxソフトウェアとインストールの要件	29
サポートされるブラウザ	32
プロトコルとポートの要件	32
ワークシートへの記入	35
Unified Manager ソフトウェアのインストール、アップグレード、および削除	37

インストール プロセスの概要	37
必要なソフトウェアリポジトリを設定する	38
NFS共有とCIFS共有におけるSELinuxの要件	40
LinuxシステムへのUnified Managerのインストール	43
Red Hat Enterprise Linux での Unified Manager のアップグレード	49
Unified Manager のインストール後にサードパーティ製品をアップグレードする	55
統合マネージャーを再起動します	55
統合マネージャーを削除する	56
カスタム umadmin ユーザーとメンテナンス グループを削除します	57
WindowsシステムへのUnified Managerのインストール	58
Active IQ Unified Managerの概要	58
Unified Managerサーバの機能	58
インストール手順の概要	58
Unified Managerをインストールするための要件	59
仮想インフラおよびハードウェア システムの要件	59
Windowsソフトウェアとインストールの要件	61
サポートされるブラウザ	62
プロトコルとポートの要件	63
ワークシートへの記入	66
Unified Manager ソフトウェアのインストール、アップグレード、および削除	68
インストール プロセスの概要	68
WindowsにUnified Managerをインストールする	69
JBossのパスワードを変更する	72
Unified Managerのバージョンとサポートされるアップグレード パス	73
Unified Manager のアップグレード	74
サードパーティ製品のアップグレード	75
サードパーティ製品をアンインストールする	76
統合マネージャーを再起動します	77
Unified Manager をアンインストールする	78
設定タスクと管理タスクの実行	79
Active IQ Unified Managerを構成する	79
設定手順の概要	79
Unified Manager Web UI にアクセスする	79
Unified Manager Web UIの初期セットアップを実行します	80
クラスターを追加する	82
アラート通知を送信するようにUnified Managerを構成する	84
ローカル ユーザのパスワードを変更	93
アクティブでないセッションのタイムアウトを設定	93
CLI経由でセッションタイムアウトを設定する	94
Unified Managerのホスト名を変更する	94
ポリシーベースのストレージ管理を有効または無効にする	99

Unified Manager バックアップを構成する	100
機能設定を管理します	100
ポリシーベースのストレージ管理を有効にする	100
API ゲートウェイを有効にする	101
非アクティブタイムアウトを指定する	102
Active IQ ポータル イベントを有効にする	102
コンプライアンスのためのセキュリティ設定を有効または無効にする	102
スクリプトのアップロードを有効または無効にする	103
ログインバナーを追加	104
メンテナンスコンソールを使用する	104
メンテナンス コンソールで提供される機能	104
メンテナンス ユーザの役割	105
診断ユーザの権限	105
メンテナンス コンソールへのアクセス	105
vSphere VM コンソールを使用してメンテナンス コンソールにアクセスする	106
メンテナンス コンソールのメニュー	106
Windowsでメンテナンスユーザーのパスワードを変更する	112
Linuxシステムでumadminパスワードを変更する	112
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	113
ネットワークインターフェースを追加する	113
Unified Managerデータベースディレクトリにディスクスペースを追加する	114
ユーザ アクセスの管理	118
ユーザーを追加する	118
ユーザー設定を編集する	119
ユーザーを表示	120
ユーザーまたはグループを削除する	120
RBACとは	121
ロールベース アクセス制御の機能	121
ユーザ タイプの定義	121
ユーザ ロールの定義	122
Unified Managerのユーザ ロールと機能	123
SAML認証設定を管理する	124
アイデンティティ プロバイダの要件	125
SAML認証の有効化	126
SAML認証に使用するIDプロバイダーを変更する	127
Unified Manager のセキュリティ証明書の変更後に SAML 認証設定を更新する	128
SAML認証を無効にする	129
メンテナンスコンソールからSAML認証を無効にする	130
[SAML認証]ページ	130
認証を管理する	131
認証サーバーを編集する	131

認証サーバーを削除する	132
Active DirectoryまたはOpenLDAPによる認証	132
監査ログ	133
[リモート認証]ページ	135
セキュリティ証明書を管理する	138
HTTPSセキュリティ証明書を表示する	138
HTTPS証明書署名要求をダウンロードする	139
CA署名済みのHTTPS証明書をインストールする	139
外部ツールを使用して生成されたHTTPS証明書をインストールする	140
証明書管理のページの説明	143
ストレージの監視と管理	145
Active IQ Unified Managerの概要	145
Active IQ Unified Managerの健全性監視の概要	145
Active IQ Unified Managerによるパフォーマンス監視の概要	146
Unified Manager REST APIを使用する	147
Unified Managerサーバの機能	147
ユーザーインターフェースを理解する	148
一般的なウィンドウ レイアウト	148
ウィンドウ レイアウトのカスタマイズ	149
Unified Managerヘルプを使用する	150
お気に入りのヘルプトピックをブックマークする	151
保管オブジェクトの検索	151
ストレージデータをレポートとしてエクスポート	153
在庫ページのコンテンツをフィルタリングする	154
通知ベルからアクティブなイベントを表示する	155
ダッシュボードからクラスターを監視および管理する	155
[ダッシュボード]ページ	156
ONTAPの問題や機能をUnified Managerから直接管理	159
クラスタを管理します。	166
クラスタ検出プロセスの仕組み	166
監視対象クラスターのリストを表示する	167
クラスターを追加する	168
クラスターを編集する	170
クラスターを削除する	171
クラスターを再発見	171
VMware仮想インフラストラクチャを監視する	172
サポートされていない機能	174
vCenter Server の表示と追加	175
vCenter Server を削除する	177
仮想マシンを監視する	177
災害復旧セットアップにおける仮想インフラストラクチャの表示	179

ワークロードのプロビジョニングと管理	181
ワークロードの概要	182
パフォーマンスサービスレベル	189
ストレージ効率ポリシーの管理	195
MetroCluster構成の管理と監視	197
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	197
MetroCluster over FC構成のクラスタ接続ステータスの定義	199
MetroCluster over FCのデータ ミラーリング ステータスの定義	200
MetroCluster構成の監視	201
MetroClusterレプリケーションを監視する	204
割り当てを管理する	205
クォータ制限とは	205
ユーザーとユーザー グループの割り当てを表示する	205
メールアドレスを生成するルールを作成する	205
ユーザーおよびユーザー グループのクォータに関する電子メール通知形式を作成する	206
ユーザーとグループのクォータのメールアドレスを編集する	207
クォータについてさらに詳しく	207
クォータのダイアログ ボックスの説明	208
トラブルシューティング	212
Unified Managerデータベースディレクトリにディスクスペースを追加する	212
パフォーマンス統計の収集間隔を変更する	215
Unified Manager がイベントとパフォーマンスデータを保持する期間を変更する	216
不明な認証エラー	217
ユーザが見つからない	217
その他の認証サービスを使用してLDAPを追加する場合の問題	218
Windows システムにおけるNetApp Manageability SDK のログローテーションの問題	218
イベントとアラートの管理	220
イベントを管理する	220
Active IQプラットフォーム イベントとは	220
イベント管理システム イベントとは	220
イベント受信時の動作	226
イベントとイベントの詳細を表示する	227
割り当てられていないイベントを表示する	228
イベントを認識して解決する	228
特定のユーザーにイベントを割り当てる	229
不要なイベントを無効にする	230
Unified Manager の自動修復を使用して問題を修正する	231
Active IQイベントレポートの有効化と無効化	232
新しいActive IQルールファイルをアップロードする	233
Active IQプラットフォーム イベントの生成方法	234
Active IQプラットフォームイベントを解決する	234

イベントの保持設定を構成する	235
Unified Managerのメンテナンスウィンドウとは	235
ホストシステムのリソースイベントを管理する	238
イベントについてもっと理解する	238
イベントおよび重大度タイプのリスト	244
イベントのウィンドウとダイアログ ボックスの説明	303
アラートを管理する	316
アラートとは	316
アラートEメールに含まれる情報	316
アラートを追加する	317
パフォーマンスイベントのアラートを追加する	320
アラートのテスト	321
解決済みおよび廃止されたイベントのアラートを有効または無効にする	321
災害復旧の宛先ボリュームをアラート生成から除外する	322
アラートを表示	323
アラートを編集する	323
アラートを削除する	324
アラートのウィンドウとダイアログ ボックスの説明	324
スクリプトを管理する	330
スクリプトとアラートの連携方法	330
スクリプトを追加する	331
スクリプトを削除する	332
テストスクリプトの実行	333
サポートされるUnified ManagerのCLIコマンド	333
スクリプトのウィンドウとダイアログ ボックスの説明	340
クラスタ パフォーマンスの監視と管理	342
Active IQ Unified Managerによるパフォーマンス監視の概要	342
Unified Managerのパフォーマンス監視機能	342
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のインターフェイス	343
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	343
データの継続性収集サイクルとは	345
収集されたデータとイベントのタイムスタンプの意味	346
Unified Manager GUIでパフォーマンスワークフローをナビゲートする	346
UIにログインする	346
グラフィカル インターフェイスと操作手順	347
保管オブジェクトの検索	352
在庫ページのコンテンツをフィルタリングする	353
ダッシュボードからクラスターのパフォーマンスを監視する	355
ダッシュボードのパフォーマンスパネルを理解する	355
パフォーマンスのバナー メッセージと説明	356

パフォーマンス統計の収集間隔を変更する	356
ワークロード アナライザーを使用してワークロードをトラブルシューティングする	357
Workload Analyzerで表示されるデータ	358
Workload Analyzerを使用するタイミング	359
ワークロードアナライザーを使用する	360
パフォーマンス クラスター ランディング ページからクラスターのパフォーマンスを監視します。	360
パフォーマンス クラスターのランディング ページを理解する	360
[パフォーマンス クラスター ランディング]ページ	361
パフォーマンスインベントリページを使用してパフォーマンスを監視する	366
すべてのストレージ オブジェクトのパフォーマンス インベントリ ページを表示します。	366
[パフォーマンス インベントリ]ページの内容の絞り込み	372
クラウドにデータを階層化するための Unified Manager の推奨事項を理解する	375
パフォーマンス エクスプローラー ページを使用してパフォーマンスを監視する	376
ルートオブジェクトを理解する	377
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	377
関連オブジェクトの時間範囲を指定する	377
比較グラフ化のための関連オブジェクトのリストを定義する	379
カウンターチャートを理解する	380
パフォーマンス カウンタ グラフのタイプ	381
表示するパフォーマンスチャートを選択	384
カウンターチャートペインを展開する	384
カウンターチャートの焦点をより短い期間に変更します	384
イベントタイムラインでイベントの詳細を表示する	385
カウンタ グラフ ズーム ビュー	386
クラスターコンポーネント別にボリュームのレイテンシを表示する	388
プロトコル別にSVM IOPSトラフィックを表示する	389
ボリュームとLUNのレイテンシチャートを表示してパフォーマンス保証を確認します	389
すべてのSANアレイクラスターのパフォーマンスを表示する	390
ローカルノードにのみ存在するワークロードに基づいてノードIOPSを表示する	391
[オブジェクト ランディング]ページの構成要素	391
QoSポリシーグループ情報を使用してパフォーマンスを管理する	397
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	397
すべてのクラスターで利用可能なすべての QoS ポリシー グループを表示します	398
同じQoSポリシーグループ内のボリュームまたはLUNを表示する	399
特定のボリュームまたはLUNに適用されたQoSポリシーグループ設定を表示する	400
パフォーマンス チャートを表示して、同じ QoS ポリシー グループ内のボリュームまたは LUN を比較します。	400
スループット グラフでの各種QoSポリシーの表示	401
パフォーマンス エクスプローラーでワークロード QoS の最小および最大設定を表示します。	402
パフォーマンス容量と利用可能なIOPS情報を使用してパフォーマンスを管理する	403
使用済みパフォーマンス容量とは	404

使用済みパフォーマンス容量の値の意味	405
使用可能なIOPSとは	406
ノードと集計パフォーマンス容量の使用値を表示する	407
ノードと集計の利用可能な IOPS 値を表示する	408
パフォーマンス容量カウンターチャートを表示して問題を特定します	408
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	410
パフォーマンス容量使用カウンタを使用してパフォーマンスを管理する	411
ノードフェイルオーバー計画ページを理解して使用する	411
ノードフェイルオーバー計画ページを使用して修正アクションを決定します	412
[ノード フェイルオーバー プラン]ページの構成要素	412
ノードフェイルオーバー計画ページでしきい値ポリシーを使用する	413
フェイルオーバー計画にはパフォーマンス使用容量の内訳チャートを使用します	414
データを収集し、ワークロードのパフォーマンスを監視する	415
Unified Managerで監視されるワークロードのタイプ	416
ワークロードパフォーマンス測定値	417
パフォーマンスの想定範囲とは	419
レイテンシ予測とパフォーマンス分析	420
Unified Manager がワークロードの遅延を使用してパフォーマンスの問題を特定する方法	421
クラスタでの処理によるワークロードのレイテンシへの影響	422
MetroCluster構成のパフォーマンス監視	422
パフォーマンスイベントとアラートを理解する	423
パフォーマンス イベントのソース	424
パフォーマンス イベントの重大度タイプ	424
Unified Managerで検出される構成の変更	425
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	426
パフォーマンス イベントの分析と通知	429
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	430
クラスタ コンポーネントとその競合要因	431
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	433
パフォーマンスしきい値を管理する	434
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	434
パフォーマンスしきい値ポリシーを超えた場合の動作	436
しきい値を使用して追跡可能なパフォーマンス カウンタ	436
組み合わせしきい値ポリシーで使用可能なオブジェクトとカウンタ	438
ユーザー定義のパフォーマンスしきい値ポリシーを作成する	439
ストレージオブジェクトにパフォーマンスしきい値ポリシーを割り当てる	440
パフォーマンスしきい値ポリシーを表示する	442
ユーザー定義のパフォーマンスしきい値ポリシーを編集する	442
ストレージ オブジェクトからパフォーマンスしきい値ポリシーを削除する	443
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	443
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	444

パフォーマンスイベントを分析する	445
パフォーマンスイベントに関する情報を表示する	445
ユーザー定義のパフォーマンスしきい値からイベントを分析する	446
システム定義のパフォーマンスしきい値からイベントを分析する	447
動的パフォーマンスしきい値からイベントを分析する	452
パフォーマンスイベントを解決する	460
レイテンシが予想範囲内であることを確認する	460
構成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	461
クライアント側からワークロード パフォーマンスを改善するためのオプション	461
クライアントまたはネットワークに問題がないかどうかの確認	461
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異常に高いかどうかを確認します	462
論理インターフェイス（LIF）の移動	462
負荷の低い時間帯でのStorage Efficiency処理の実行	463
ディスクの追加とデータの再配置	464
ノードでFlash Cacheを有効にしてワークロード パフォーマンスを改善する仕組み	464
ストレージ アグリゲートでFlash Poolを有効にしてワークロード パフォーマンスを改善する仕組み	465
MetroCluster構成の健全性チェック	465
MetroCluster構成の検証	465
ワークロードを別のアグリゲートに移動する	466
ワークロードを別のノードに移動する	467
ワークロードを別のノードのアグリゲートに移動する	469
ワークロードを別のHAペアのノードに移動する	471
ワークロードを別のHAペアの別のノードに移動する	472
QoSポリシーの設定を使用したノードでの作業の優先順位付け	474
非アクティブなボリュームとLUNの削除	475
ディスクの追加およびアグリゲート レイアウトの再構築	475
Unified Manager サーバーと外部データ プロバイダー間の接続を設定する	476
外部サーバに送信可能なパフォーマンス データ	476
Unified Managerからパフォーマンスデータを受信できるようにGraphiteを設定する	477
Unified Manager サーバから外部データ プロバイダへの接続を構成する	478
クラスタの健全性の監視と管理	481
Active IQ Unified Managerの健全性監視の概要	481
物理容量と論理容量	481
容量の測定単位	481
Unified Managerの健全性監視機能	482
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インターフェース	483
クラスターとクラスターオブジェクトの健全性の管理と監視	484
クラスター監視を理解する	484
クラスターのリストと詳細を表示する	485
MetroCluster構成内のクラスタの健全性をチェックする	486
すべてのSANアレイクラスタの健全性と容量ステータスを表示します	488

ノードリストと詳細を表示する	489
契約更新のためのハードウェア在庫レポートを生成する	490
ストレージVMのリストと詳細を表示する	490
集計リストと詳細を表示する	491
FabricPool の容量情報を表示する	492
ストレージプールの詳細を表示する	493
ボリュームリストと詳細を表示する	493
NFS共有の詳細を表示する	494
SMB/CIFS共有の詳細を表示する	495
スナップショットコピーのリストを表示する	496
Snapshotコピーを削除する	496
スナップショットコピーの再利用可能なスペースを計算する	497
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	498
Unified Managerの一般的な健全性関連のワークフローとタスク	498
データの可用性を監視およびトラブルシューティングする	499
容量の問題を解決する	506
健康閾値を管理する	508
クラスターのセキュリティ目標を管理する	513
バックアップと復元操作を管理する	526
スクリプトを管理する	542
グループの管理と監視	545
アノテーションを使用してストレージ オブジェクト イベントを優先順位付けする	554
Web UI とメンテナンス コンソールからサポート バンドルを送信する	563
複数のワークフローに関連するタスクと情報	570
データの保護とリストア	630
保護関係の作成、監視、トラブルシューティング	630
SnapMirror保護の種類	630
Unified Managerで保護関係を設定する	632
保護関係のフェイルオーバーとフェイルバックを実行する	634
保護ジョブの失敗を解決する	638
遅延問題を解決する	642
保護関係の管理と監視	643
ボリューム保護ステータスの表示	643
ボリューム保護関係の表示	645
整合性グループ関係のLUNを監視する	646
ヘルス: すべてのボリュームビューからSnapVault保護関係を作成します	647
ボリューム/ヘルスの詳細ページからSnapVault保護関係を作成します	648
ヘルス: すべてのボリュームビューからSnapMirror保護関係を作成します。	649
ボリューム/ヘルスの詳細ページからSnapMirror保護関係を作成します。	650
バージョンに柔軟性のあるレプリケーションでSnapMirror関係を作成する	651
バックアップ オプションを備えたバージョンに柔軟なレプリケーションで	

SnapMirror関係を作成する	652
宛先効率設定を構成する	653
SnapMirrorとSnapVaultのスケジュールを作成する	654
既存の保護関係から保護を拡張するためにカスケードまたはファンアウト関係を作成します	655
ボリューム関係ページから保護関係を編集する	655
ボリューム/健全性の詳細ページから保護関係を編集する	656
転送効率を最大化するためにSnapMirrorポリシーを作成する	657
転送効率を最大化するためのSnapVaultポリシーを作成する	657
ボリューム関係ページからアクティブなデータ保護転送を中止する	658
ボリューム/ヘルス詳細ページからアクティブなデータ保護転送を中止します	658
ボリューム関係ページから保護関係を静止する	659
ボリューム/ヘルスの詳細ページから保護関係を休止する	660
ボリューム関係ページからSnapMirror関係を解除する	661
ボリューム関係ページから保護関係を削除します	661
ボリューム関係ページから、休止関係でのスケジュールされた転送を再開します。	662
ボリューム/ヘルスの詳細ページから、休止関係でのスケジュールされた転送を再開します。	663
ボリューム関係ページから保護関係を初期化または更新します	663
ボリューム/ヘルスの詳細ページから保護関係を初期化または更新します	664
ボリューム関係ページから保護関係を再同期します	665
ボリューム関係ページから保護関係を反転する	666
ボリュームとボリューム/ヘルスの詳細ページを使用してデータを復元します	667
リソース プールとは	668
リソースプールを作成する	669
リソースプールを編集する	669
リソースプールのインベントリを表示する	670
リソースプールのメンバーを追加する	670
リソースプールから集約を削除する	671
リソースプールを削除する	671
ストレージ VM 災害復旧保護関係の監視	672
ストレージVMの関連付けを理解する	674
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	676
ジョブとは	677
ジョブの監視	677
求人の詳細を見る	677
ジョブを中止する	678
失敗した保護ジョブを再試行する	678
保護関係のウィンドウとダイアログ ボックスの説明	678
カスタム レポートの生成	722
Unified Managerレポート	722
レポートを生成するためのアクセス ポイント	722
レポートを理解する	724

ビューとレポートの関係を理解する	724
レポートの種類	725
レポート機能の制限事項	727
レポートの操作	727
レポート ワークフロー	727
レポートのクイック スタート	728
スケジュールされたレポートを検索する	731
レポートをカスタマイズする	731
レポートをダウンロード	735
スケジュールレポート	735
レポートをスケジュールする	735
レポートスケジュールを管理する	738
サンプルのカスタム レポート	740
クラスターストレージレポートをカスタマイズする	741
総容量レポートをカスタマイズする	744
ボリューム容量レポートをカスタマイズする	746
Qtree容量レポートをカスタマイズする	750
NFS共有レポートをカスタマイズする	750
ストレージVMレポートをカスタマイズする	752
ボリューム関係レポートをカスタマイズする	753
ボリュームパフォーマンスレポートをカスタマイズする	757
Microsoft Excelのサンプル レポート	758
総容量表とグラフを表示するレポートを作成する	758
合計合計と利用可能な容量のグラフを表示するレポートを作成します	761
利用可能なボリューム容量チャートを表示するレポートを作成します	765
利用可能なIOPSが最も高いアグリゲートを表示するレポートを作成する	767
REST APIを使用したストレージの管理	770
Active IQ Unified Manager REST APIの使用を開始する	770
このドキュメントの対象読者	770
Active IQ Unified Manager APIアクセスとカテゴリ	770
Active IQ Unified Managerで提供されるRESTサービス	772
Active IQ Unified ManagerでのAPIのバージョン管理	772
ONTAPのストレージ リソース	773
Active IQ Unified ManagerでのREST APIへのアクセスおよび認証	774
認証	776
Active IQ Unified Managerで使用されるHTTPステータスコード	777
Active IQ Unified ManagerのAPIの使用に関する推奨事項	778
トラブルシューティング用のログ	778
ジョブ オブジェクトの非同期プロセス	779
Hello API server	780
統合マネージャー REST API	784

APIを使用してデータセンター内のストレージオブジェクトを管理する	785
プロキシアクセスを介してONTAP APIにアクセスする	790
APIを使用して管理タスクを実行する	793
APIを使用してユーザーを管理する	795
APIを使用してパフォーマンス メトリックを表示する	796
ジョブとシステムの詳細を表示する	806
APIを使用してイベントとアラートを管理する	807
APIを使用してワークロードを管理する	810
ストレージ管理の一般的なAPIワークフロー	819
ワークフローで使用されるAPI呼び出しを理解する	819
APIを使用して集計のスペースの問題を特定する	819
イベント API を使用してストレージ オブジェクトの問題を特定する	821
ゲートウェイ API を使用してONTAPボリュームのトラブルシューティングを行う	822
APIによるワークロード管理のワークフロー	826
法律上の表示	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 9.16 の新機能、制限事項、既知の問題の概要を示します。

詳細については、"[Active IQ Unified Managerリリースノート](#)"。

始めましょう

インストールのクイック スタート手順 (VMware)

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

システム要件

- オペレーティング システム: VMware ESXi 8.0
- メモリ: 12 GB
- CPU: 合計9572MHz
- 空きディスク容量: 5 GB (シンプロビジョニング)、152 GB (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、"[Unified Managerをインストールするための要件](#)"そして"[Interoperability Matrix](#)"。

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. ダウンロード`.tar`ルート証明書を含むファイル、`README`ファイルと`OVA`ファイル。
2. vSphere Clientからアクセス可能なローカルまたはネットワークのディレクトリにファイルを保存します。
3. ダウンロードしたディレクトリで`.tar`ファイルに、`tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz`指示。+ 必要な`OVA`ファイル、ルート証明書、および`README`ファイルはターゲット ディレクトリに解凍されます。

整合性を検証する

整合性を検証することができます`OVA`ファイルに記述されている手順に従って`README`ファイル。

Unified Managerをインストールする

1. vSphere Client で、[ファイル]>[OVF テンプレートのデプロイ]をクリックします。
2. OVAファイルを検索し、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発行者セクションに、メッセージ`Entrust Code Signing - OVCS2 (Trusted certificate)`ダウンロードしたファイルの整合性を確認します`OVA`ファイル。メッセージについて`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. [Customize Template]ページの[Properties]タブで、実行しているインストールのタイプに必要なフィールドを入力します。
 - 静的な設定の場合、すべてのフィールドに必要な情報を入力します。セカンダリ **DNS** フィールドに情報を追加する必要はありません。

- IPv4を使用するDHCPの場合、すべてのフィールドを空にしてください。
- IPv6を使用するDHCPの場合、[Enable Auto IPv6 addressing]ボックスをオンにします。それ以外のフィールドはすべて空にしてください。

5. VMの電源をオンにします。
6. [Console]タブをクリックして最初のブート プロセスを確認します。
7. タイムゾーンを設定します。
8. Unified Manager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への接続方法が表示されます。

インストールのクイック スタート手順 (Linux)

Unified Managerのインストール パッケージをダウンロードして、Red Hat Enterprise Linux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 8.x および 9.4 (x86_64 アーキテクチャに基づく)、OS インストーラの ソフトウェア選択 オプションから「GUI 付きサーバー」ベース環境を使用してインストールされます。
- RAM: 12 GB、CPU: 合計9572 MHz
- 空きディスク容量: 100 GBのディスク容量 /opt/netapp/data`ディレクトリ、ルート パーティションに 50 GB。別途取り付けの場合、`/opt`そして `/var/log`ディレクトリについては、`/opt 15GB あり、/var/log 16GBあり、/tmp 10 GB の空き容量があります。

詳細なシステム要件と、製品をセキュリティ保護されたサイトにインストールする方法については、"[Unified Managerをインストールするための要件](#)"そして"[Interoperability Matrix](#)"。

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. ダウンロード ActiveIQUnifiedManager-`<version>`.zip`インストールパッケージとコード署名証明書(.pem)`とデジタル署名(.sig)。
2. インストール ファイルをダウンロードしたフォルダで、次のコマンドを実行します。

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

整合性を検証する

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検証します。

- 走る `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > `<public_key_file_name>``コード署名証明書の公開キーを含むファイルを作成します。
- 走る `openssl dgst -sha256 -verify `<public_key_file_name>` -signature `<signature_file_name>`

ActiveQUnifiedManager-<version>.zip`インストーラー パッケージの署名を検証します。

リポジトリ設定を確認する

Red Hat Enterprise Linuxのリポジトリの設定手順はサイトによって異なります。使用することができます`pre\_install\_check.sh`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 システムの構成を確認します。システムがインターネットに接続されている場合、Red Hat Enterprise Linuxのリポジトリのセットアップ方法が通知されます。

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

Unified Managerをインストールする

Unified Managerは`yum`ソフトウェアおよび依存ソフトウェアをインストールするためのユーティリティ。Red Hat Enterprise Linuxには複数のイメージがあるため、どのパッケージがインストールされるかはイメージに含まれているソフトウェアによって決まります。その`yum`ユーティリティは、インストールする依存ソフトウェア パッケージを決定します。依存ソフトウェアパッケージに関する詳細情報が必要な場合は、"[Linuxソフトウェアとインストールの要件](#)"。

Unified Managerをインストールするには、rootユーザーとして、または`sudo`インストール ファイルを解凍したディレクトリから:

```
# 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への接続方法が表示されます。ウェブUIに接続できない場合は、`README`ポート 443 の制限に関する詳細については、ソフトウェアに同梱されているファイルを参照してください。

インストールのクイック スタート手順 (Windows)

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Windowsオペレーティング システムの次の言語版に対応しています。

- 英語
- 日本語
- 簡体字中国語

- メモリ: 12 GB
- 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、"[Unified Managerをインストールするための要件](#)"そして"[Interoperability Matrix](#)"。

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. ダウンロード `ActiveIQUnifiedManager-<version>.exe`インストール パッケージ。
2. インストール ファイルをターゲット システム上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ためには、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。Unified Managerのインストール時には、このほかにもいくつかの他社製パッケージが必要に応じて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、"[Windowsソフトウェアとインストールの要件](#)"。

1. デフォルトのローカル管理者アカウントでWindowsにログインします。
2. インストール ファイルをダウンロードしたディレクトリで、Unified Manager実行可能ファイル (.exe) を管理者権限で実行します。
3. 画面の指示に従ってユーザ名とパスワードを入力し、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. インストールの最後に「完了」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）では、ONTAPストレージシステムの健全性とパフォーマンスを一元的に監視および管理することができます。Unified Managerは、LinuxサーバやWindowsサーバに導入できるほか、VMwareホストに仮想アプライアンスとして導入することもできます。

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

関連情報

["NetApp Interoperability Matrix Tool"](#)

Unified Managerサーバの機能

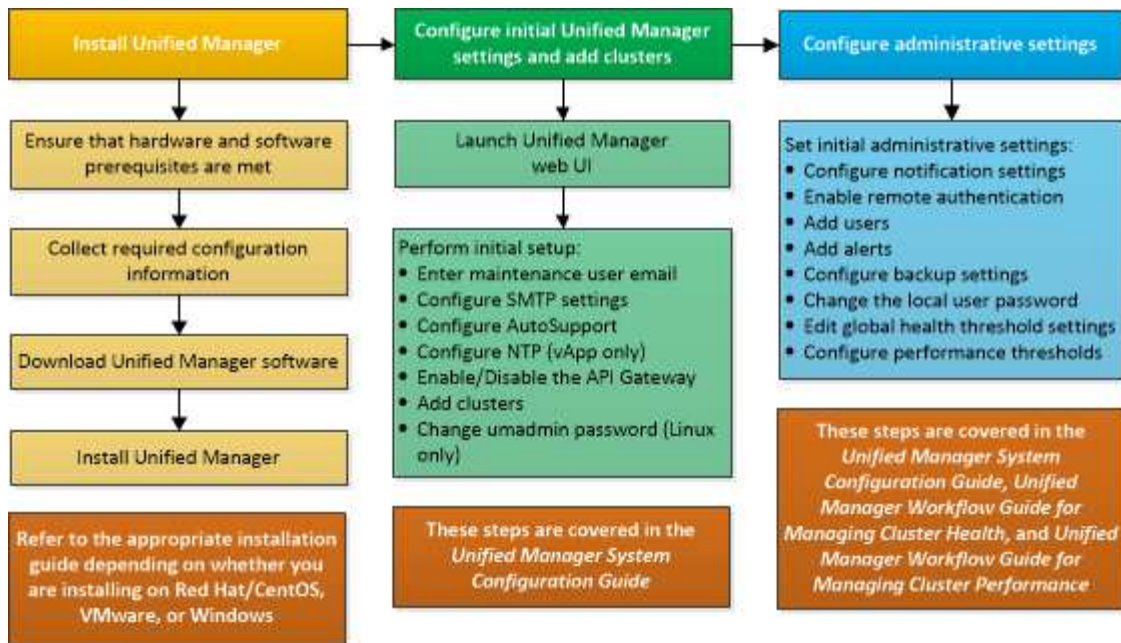
Unified Manager サーバー インフラストラクチャは、データ収集ユニット、データベース、およびアプリケーション サーバーで構成されます。検出、監視、ロールベース アクセス制御（RBAC）、監査、ロギングなどのインフラ サービスを提供します。

Unified Manager はクラスタ情報を収集し、そのデータをデータベースに保存し、そのデータを分析してクラスタに問題があるかどうかを確認します。

インストール手順の概要

インストール ワークフローでは、Unified Manager を使用する前に実行する必要があるタスクについて説明します。

以降の各セクションでは、このワークフローの各項目について説明します。



Unified Managerをインストールするための要件

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

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

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

["Supportability for Security Measures applied to Active IQ Unified Manager for Clustered Data ONTAP"](#)

関連情報

詳細については、["NetApp Interoperability Matrix Tool"](#)

仮想インフラおよびハードウェア 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ついて、推奨される値を示します。これらは、Unified Managerが許容されるパフォーマンス レベルを達成することが確認されている値です。

ハードウェア構成	推奨設定
RAM	12GB（最小要件は8GB）

ハードウェア構成	推奨設定
プロセッサ	CPU×4
CPUサイクル	合計9572MHz（最小要件は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）

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。

さらに、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、"[『Unified Manager Best Practices Guide』](#)"。

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

専用使用の要件

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

バックアップ用のスペース要件

Unified Manager のバックアップおよび復元機能を使用する予定の場合は、「data」ディレクトリまたはディスクに 150 GB のスペースが確保されるように追加の容量を割り当てます。バックアップはローカルにもリモートにも保存できますが、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、次の方法で正常に実行できるように構成する必要があります。`ping`ホスト自体からのホスト名。IPv6設定の場合は、次の点を確認する必要があります。`ping6`ホスト名への変更が成功し、Unified Manager のインストールが成功していることを確認します。

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

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

VMwareソフトウェアとインストールの要件

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

オペレーティング システム ソフトウェア

サポートされているオペレーティング システムは VMware ESXi 8.0 です。



VMware vSphere システム上の Unified Manager OVA は、内部で Debian OS 12 (bookworm) を実行します。サポート対象バージョンのESXiサーバでサポートされる仮想マシン ハードウェアのバージョンについては、VMwareのドキュメントを参照してください。

サポートされるvSphereのバージョンは次のとおりです。

- VMware vCenter Server 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動作するには、VMware ESXiサーバの時刻がNTPサーバの時刻と同じになっている必要があります。VMware ESXiサーバの時刻をNTPサーバの時刻と同期すると、時刻に関する障害は発生しなくなります。

インストールの要件

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

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

リソースが十分でないために導入環境でハイアベイラビリティを有効にできない場合は、[Cluster Features]の[Virtual Machine Options]の変更が必要な可能性があります。[VM Restart Priority]を無効にし、[Host Isolation Response]を[Leave Powered On]に設定します。



Unified Managerのインストールまたはアップグレード中、必要なサードパーティ製ソフトウェアとセキュリティ 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のインストールおよびアップグレード プロセスで制御されるため、サードパーティ製コンポーネントを単独でインストールまたはアップグレードすることは避けてください。

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は、Interoperability Matrixを参照してください。

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

アイデンティティ プロバイダ (IdP) でユーザが認証されるように、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

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

Unified Managerサーバへの接続

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

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

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

インターフェイス	プロトコル	ポート	説明
syslog	UDP	514	ONTAPシステムからのサブスクリプションベースのEMSメッセージにアクセスし、メッセージに基づいてイベントを作成する際に使用されます。
REST	HTTPS	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のEMSイベントにアクセスする際に使用されます。
MySQLデータベース	MySQL	3306	OnCommand Workflow AutomationおよびOnCommand API Services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）から受信する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）から受信する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は、TLS または SSL によって提供される暗号化をサポートします。



VMware vSphereシステムにUnified Managerをインストールしている間、MySQLのデフォルトポートである3306へのアクセスはlocalhostのみに制限されます。アップグレード シナリオでは以前の設定が維持されるため、このことによる影響はありません。この設定は変更可能であり、接続を他のホストに利用可能にするには、`Control access to MySQL port 3306` メンテナンス コンソールのオプション。詳細については、"[その他のメニュー オプション](#)"。HTTP通信とHTTPS通信に使用されるポート（ポート80と443）は、Unified Managerメンテナンス コンソールを使用して変更できます。詳細については、"[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	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。  このポート、または他のポートを使用してVMware vCenter Server やESXiサーバに接続する場合は、ポートが使用可能で、セキュアなサイト内で接続できることを確認してください。
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。

デスティネーション	プロトコル	ポート	説明
LDAPS	636	セキュアなLDAP通信に使用されます。	メール サーバ
SMTP	25	アラート通知Eメールの送信に使用されます。	SNMPトラップの送信元
SNMPv1またはSNMPv3	162 / UDP	アラート通知SNMPトラップの送信に使用されます。	外部データ プロバイダのサーバ
TCP	2003	外部のデータ プロバイダ（Graphiteなど）へのパフォーマンス データの送信に使用されます。	NTP サーバ
NTP	123 / UDP	Unified Managerサーバの時間を外部の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）。	syslog

ワークシートへの記入

Unified Manager をインストールして構成する前に、環境に関する具体的な情報をすぐに入手できるようにしておく必要があります。次のリストに情報をまとめておくとう便利です。

Unified Managerのインストール情報

Unified Manager をインストールするために必要な詳細。

ソフトウェアが展開されるシステム	あなたの価値
ESXiサーバのIPアドレス	
ホストの完全修飾ドメイン名	
ホストのIPアドレス	
ネットワーク マスク	
ゲートウェイのIPアドレス	
プライマリDNSアドレス	

ソフトウェアが展開されるシステム	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 ユーザのユーザ名	
メンテナンス ユーザのパスワード	

Unified Managerの設定情報

インストール後に Unified Manager を構成するための詳細。構成によっては省略可能な値もあります。

設定	あなたの価値
メンテナンス ユーザのEメール アドレス	
NTP サーバ	
SMTPサーバのホスト名またはIPアドレス	
SMTPのユーザ名	
SMTPのパスワード	
SMTP ポート	25（デフォルト値）
アラート通知の送信元Eメール アドレス	
認証サーバのホスト名またはIPアドレス	
Active Directoryの管理者名またはLDAPバインド識別名	
Active Directoryのパスワードまたは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）のメタデータ	

設定	あなたの価値
SNMPトラップの送信先ホストのIPアドレス	
SNMP ポート	

クラスタ情報

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

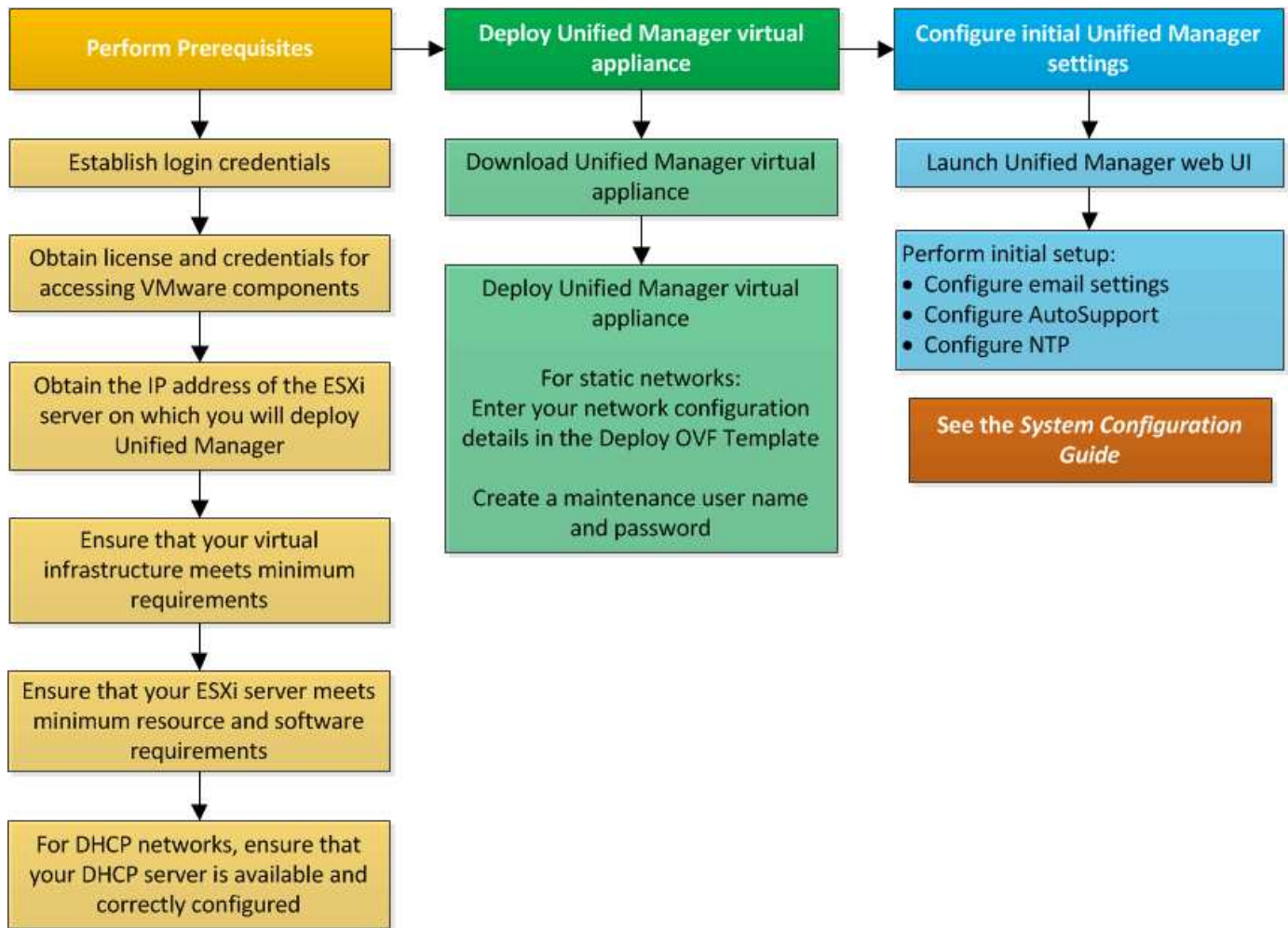
Nのクラスター1	あなたの価値
ホスト名またはクラスタ管理IPアドレス	
ONTAP管理者のユーザ名  管理者には「admin」ロールが割り当てられている必要があります。	
ONTAP管理者のパスワード	
プロトコル	HTTPS

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

VMware vSphereシステムで、Unified Managerのインストール、新しいバージョンのソフトウェア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

展開ワークフローでは、Unified Manager を使用する前に実行する必要があるタスクについて説明します。



Unified Manager を導入する

Unified Manager の展開には、ソフトウェアのダウンロード、仮想アプライアンスの展開、メンテナンス ユーザー名とパスワードの作成、Web UI での初期セットアップの実行が含まれます。

開始する前に

- 導入のためのシステム要件を確認し、完了しておく必要があります。

見る"[システム要件](#)".

- 次の情報が揃っていることを確認します。
 - NetAppサポート サイトのログイン資格情報
 - 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サーバーの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予定の場合は、ホストで IPv6 を有効にする必要があります。

Unified Manager を VMware ESXi サーバー上の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、VMware ToolsはOpen VM Toolsに置き換えられました。open-vm-tools)。VMware Toolsをインストールの一部としてインストールする必要はなくなりました。open-vm-tools Unified Manager インストール パッケージに含まれています。

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

手順

1. 以下の手順に従ってください"[Unified Managerをダウンロード](#)"。
2. さらに、以下の手順に従ってください。"[Unified Manager仮想アプライアンスを展開する](#)"。

Unified Managerのインストールファイルをダウンロードする

Unified Managerを仮想アプライアンスとして導入するには、Unified Managerインストール ファイルをNetAppサポート サイトからダウンロードします。

開始する前に

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

手順

1. NetApp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. ダウンロードして保存`.tar`VMware vSphere インストール用のファイルを、vSphere クライアントからアクセスできるローカル ディレクトリまたはネットワーク ディレクトリに保存します。
4. チェックサムをチェックして、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. ダウンロードしたディレクトリに移動します`.tar`ファイルを開き、ターミナル ウィンドウに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. の整合性を確認する`OVA`ファイルに記述されている手順に従って`README`ファイル。

Unified Manager仮想アプライアンスを展開する

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。ESXiサーバに仮想アプライアンスを導入するには、vSphere Web Clientを使用します。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。

開始する前に

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。

見る["仮想インフラストラクチャの要件"](#)。

見る["VMwareソフトウェアとインストールの要件"](#)。

動的ホスト構成プロトコル（DHCP）を使用する場合は、DHCPサーバが使用可能で、DHCPと仮想マシン（VM）のネットワーク アダプタが正しく構成されていることを確認します。デフォルトでは、DHCPを使用するように設定されています。

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、DNSサーバの適切なエントリが設定されていることを確認します。

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を使用しない場合は、接続先のネットワーク デバイスのIPv4またはIPv6アドレスを取得します。
 - ホストの完全修飾ドメイン名（FQDN）
 - ホストのIPアドレス
 - ネットワーク マスク
 - デフォルト ゲートウェイのIPアドレス
 - プライマリDNSとセカンダリDNSのアドレス
 - 検索ドメイン

Unified Manager 9.8以降、VMware ToolsはOpen VM Toolsに置き換えられました。 *open-vm-tools*）。インストールプロセスの一部としてVMware Toolsをインストールする必要はありません。 *open-vm-tools* Unified Manager インストール パッケージに含まれています。

仮想アプライアンスを導入すると、HTTPSアクセス用に独自の自己署名証明書が生成されます。Unified Manager Web UI にアクセスすると、信頼されていない証明書に関するブラウザ警告が表示される場合があります。

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、[ファイル]>[OVF テンプレートのデプロイ] をクリックします。
2. OVF テンプレートのデプロイ ウィザードを完了して、Unified Manager 仮想アプライアンスをデプロイします。

[Review Details]ページで次の操作を行います。

- ° 発行者セクションの詳細を確認します。 **Entrust**コード署名 - **OVCS2** (信頼された証明書) *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`ファイル。 + ***Entrust** コード署名 - **OVCS2** (無効な証明書) 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てください。

[Customize Template]ページで次の操作を行います。

- ° DHCPとIPv4アドレスを使用する場合は、すべてのフィールドを空白のままにします。
 - ° DHCP と IPv6 アドレス指定を使用する場合は、「自動 IPv6 アドレス指定を有効にする」ボックスをオンにし、他のすべてのフィールドを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、各フィールドに値を指定します。ここで指定した値が導入時に適用されます。導入先のホストで一意で、使用されておらず、有効なDNSエントリが割り当てられたIPアドレスを指定してください。
3. Unified Manager 仮想アプライアンスを ESXi サーバーに展開した後、VM を右クリックし、[電源オン] を選択して VM の電源をオンにします。



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

4. *コンソール*タブをクリックします。

初回のブート プロセスには数分かかります。

5. タイム ゾーンを構成するには、VM コンソール ウィンドウの指示に従って、地理的エリア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は、管理対象デバイスのタイムゾーン設定に関係なく、Unified Manager に設定されているタイムゾーンを使用します。ストレージ システムと管理サーバで同じNTPサーバが設定されている場合、違う時間が表示された場合でも、それぞれが表しているのは同じ時刻です。たとえば、管理サーバとは異なるタイム ゾーンが設定されたデバイスでSnapshotコピーを作成した場合も、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に誤りがある場合は、次のいずれかを実行します。

インターフェイス	操作
DHCP	*DHCPの再試行*を選択します。DHCPを使用する場合は、設定が正しいことを確認してください。 DHCP対応のネットワークを使用すると、FQDNとDNSサーバのエントリが仮想アプライアンスに自動的に割り当てられます。DHCP が DNS で適切に構成されていない場合、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、ネットワーク設定の情報を手動で入力する必要があります。

インターフェイス	操作
静的なネットワーク設定	a. *静的ネットワーク構成の詳細を入力*を選択します。 設定プロセスが完了するまでに数分かかります。 b. 入力した値を確認し、「Y」を選択します。

7. プロンプトでメンテナンス ユーザー名を入力し、[Enter] をクリックします。

メンテナンス ユーザの名前は、1文字目を小文字のアルファベット（a～z）、2文字目以降をハイフン（-）、a～z、0～9を任意に組み合わせて指定する必要があります。

8. プロンプトが表示されたら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。

ウェブUIにアクセスしてUnified Managerの初期セットアップを実行することができます。["Active IQ Unified Managerの設定"](#)。

Unified Manager のアップグレード

Active IQ Unified Managerリリース9.13または9.14からリリース9.16へのアップグレードのみ可能です。

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

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

手順

1. 以下の手順に従ってください["Unified Manager ISOイメージをダウンロードする"](#)。
2. さらに、以下の手順に従ってください。["Unified Manager のアップグレード"](#)。

Unified Managerのバージョンとサポートされるアップグレード パス

Active IQ Unified Managerでサポートされるアップグレード パスはバージョンごとに異なります。

すべてのバージョンのUnified Managerで、新しいバージョンへのインプレース アップグレードを実行できるわけではありません。Unified ManagerのアップグレードはN-2モデルに限定されています。つまり、すべてのプラットフォームにおいて、アップグレードできるのは2つ上のリリースまでです。たとえば、Unified Manager 9.16へのアップグレードはUnified Manager 9.13と9.14からのみ実行できます。

サポート対象よりも前のバージョンを実行している場合は、Unified Managerインスタンスを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、最新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、現在Unified Manager 9.9がインストールされていて、Unified Manager 9.14にアップグレードする場合、アップグレード手順は次のようになります。

アップグレード パスの例：

1. 9.11から9.13にアップグレードします。
2. 9.13から9.14にアップグレードします。
3. 9.13から9.16にアップグレードします。
4. 9.14から9.16にアップグレードします。

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

Unified Manager アップグレード ファイルをダウンロードする

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

開始する前に

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. ダウンロード \.iso\アップグレード用のイメージを作成し、vSphere Client からアクセスできるローカル ディレクトリまたはネットワーク ディレクトリに保存します。
4. チェックサムをチェックして、ソフトウェアが正しくダウンロードされたことを確認します。

Unified Manager仮想アプライアンスをアップグレードする

Active IQ Unified Manager仮想アプライアンスは、リリース9.13または9.14から9.16にアップグレードできます。

開始する前に

以下を確認してください。

- 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く必要があります。
- Unified Managerをアップグレードするシステムがシステムとソフトウェアの要件を満たしている必要があります。

見る["仮想インフラストラクチャの要件"](#)。

見る"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) をインストール済みであること。
- アップグレードの実行中に、パフォーマンス データの保持期間について、以前のデフォルト設定である13カ月のままにするか6カ月に変更するかを確認するプロンプトが表示されることがあります。変更を確認すると、6カ月を過ぎた過去のパフォーマンス データはパージされます。
- 次の情報を入手していること。
 - NetAppサポート サイトのログイン資格情報
 - 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メンテナンスユーザーの認証情報

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

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

手順

1. vSphere Client で、ホーム > インベントリ > **VM** とテンプレート 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 が実行中の場合は、[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. 選択してください `ActiveQUnifiedManager-<version>-virtual-update.iso` ファイルを選択し、[開く] をクリックします。
9. *コンソール*タブをクリックします。
10. Unified Managerメンテナンス コンソールにログインします。
11. メインメニューで、[アップグレード]を選択します。

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

12. タイプ `y` 続行します。

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

13. タイプ `y` 続行します。

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

14. いずれかのキーを押して次に進みます。

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、アップグレード後のバージョンのUnified Managerにログインします。UI でタスクを実行する前に、検出プロセスが完了するまで待つ必要があることに注意してください。

Unified Manager仮想マシンを再起動する

メンテナンス コンソールから Unified Manager 仮想マシン (VM) 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。

開始する前に

- 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。

仮想マシンを再起動することもできます。参照 ["Broadcom の VMware vSphere PowerCLI CMDLET リファレンスの Restart-VMGuest コマンドレット。"](#)

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。

統合マネージャーを削除する

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。

開始する前に

- 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、ホーム > インベントリ > **VM** とテンプレート をクリックします。
3. 削除する VM を選択し、[概要] タブをクリックします。
4. VM が実行中の場合は、[電源] > [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）では、ONTAPストレージシステムの健全性とパフォーマンスを一元的に監視および管理することができます。Unified Managerは、LinuxサーバやWindowsサーバに導入できるほか、VMwareホストに仮想アプライアンス（vApp）として導入することもできます。

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

関連情報

["NetApp Interoperability Matrix Tool"](#)

Unified Managerサーバの機能

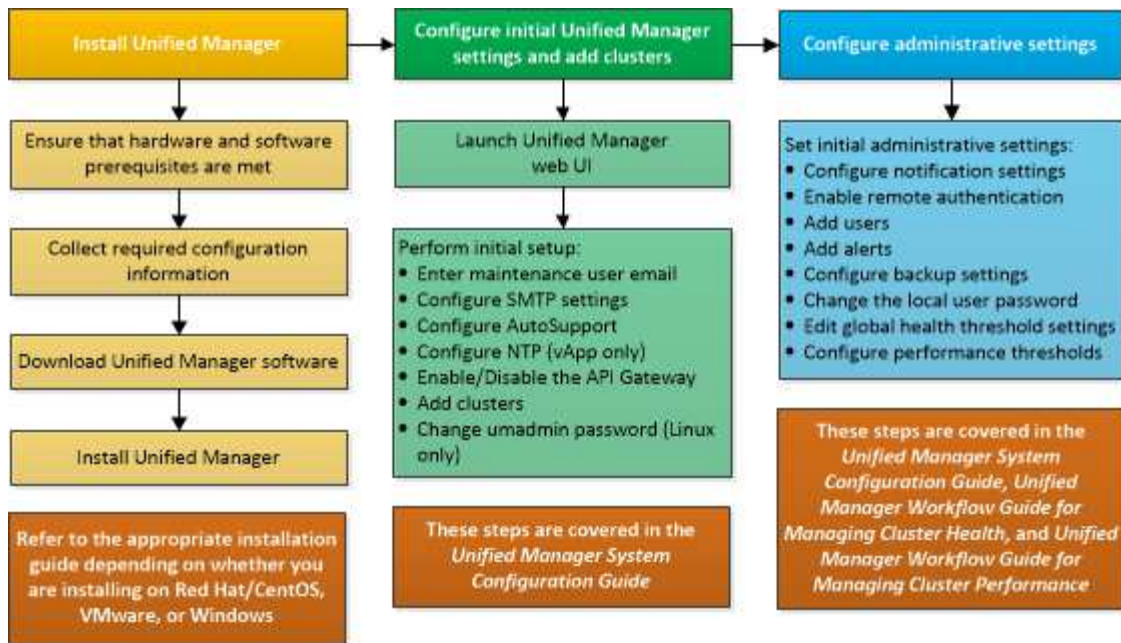
Unified Manager サーバー インフラストラクチャは、データ収集ユニット、データベース、およびアプリケーション サーバーで構成されます。検出、監視、ロールベース アクセス制御（RBAC）、監査、ロギングなどのインフラ サービスを提供します。

Unified Manager はクラスタ情報を収集し、そのデータをデータベースに保存し、そのデータを分析してクラスタに問題があるかどうかを確認します。

インストール手順の概要

インストール ワークフローでは、Unified Manager を使用する前に実行する必要があるタスクについて説明します。

以降の各セクションでは、このワークフローの各項目について説明します。



Unified Managerをインストールするための要件

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

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

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

["Supportability for Security Measures applied to Active IQ Unified Manager for Clustered Data ONTAP"](#)

関連情報

["NetApp Interoperability Matrix Tool"](#)

仮想インフラおよびハードウェア 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ついて、推奨される値を示します。これらは、Unified Managerが許容されるパフォーマンス レベルを達成することが確認されている値です。

ハードウェア構成	推奨設定
RAM	12GB（最小要件は8GB）

ハードウェア構成	推奨設定
プロセッサ	CPU×4
CPUサイクル	合計9572MHz（最小要件は9572MHz）
空きディスク スペース	150GB。割り当ては次のとおりです。 • 50GBをルート パーティションに割り当て • 100 GBの空きディスク容量が `/opt/netapp/data` LVMドライブまたはターゲット システムに接続された別のローカルディスクにマ ウントされたディレクトリ  別途取り付けの場合 /opt`そして `/var/log`ディレクトリについて は、`/opt` 15GBあり、`/var/log` 16 GB の空き容量があります。その `/tmp`ディレクトリには少なくとも 10 GB の空き容量が必要です。

Unified Managerはメモリの少ないシステムにもインストールできますが、推奨される12GBのRAMがあれば最適なパフォーマンスが保証されるだけでなく、拡張時にクラスタやストレージ オブジェクトの追加にも対応できます。Unified Managerを導入するVMにはメモリの上限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。

さらに、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 ベストプラクティスガイド"

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

専用使用の要件

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

バックアップ用のスペース要件

Unified Manager のバックアップおよび復元機能を使用する予定の場合は、「data」ディレクトリまたはディスクに 150 GB のスペースが確保されるように追加の容量を割り当てます。バックアップはローカルにもリモートにも保存できますが、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、次の方法で正常に実行できるように構成する必要があります。`ping`ホスト自体からのホスト名。IPv6設定の場合は、次の点を確認する必要があります。`ping6`ホスト名への変更が成功し、Unified Manager のインストールが成功していることを確認します。

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

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

Linuxソフトウェアとインストールの要件

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

オペレーティング システム ソフトウェア

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

- x86_64アーキテクチャに基づくRed Hat Enterprise Linuxバージョン8.xおよび9.4。

サポートされているRed Hat Enterprise Linux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のみを実行する専用のサーバを用意する必要があります。他のアプリケーションをサーバにインストールしないでください。社内の規定により、LinuxシステムにQualysなどの脆弱性スキャナがインストールされている可能性があります。Unified Managerのインストールが失敗しないように、インストール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）は、仮想マシン（VM）を内部的にスキャンする場合（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）または外部的にスキャンする場合（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、Unified ManagerがインストールされているVMを脆弱性スキャナがスキャンする場合）にCPU使用率が高くなる可能性があります。この問題が原因で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にはUnified Managerがバンドルされていて、設定済みです。

以下のサードパーティ 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、`yum` 次のセクションで説明するようにリポジトリを構成しておけば、インストール中にインストーラーが起動します。

- MySQL Community Edition バージョン 8.4.4 (MySQL リポジトリから)
- OpenJDKバージョン11.0.25 (Red Hat Extra Enterprise Linux Serverリポジトリから入手)
- Python 3.9.x (Red Hat Extra Enterprise Linux Serverリポジトリから入手)
- 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ユーザーまたは非rootユーザーが以下のコマンドを使用して実行できます。`sudo`指示。

さらに、デフォルトのUnified Managerインストールでは、umadminユーザー（デフォルトのメンテナンスユーザー）とjbossユーザーがsudoersファイルに含まれています。(ocum_sudoers`そして`ocie_sudoers)の`/etc/sudoers.d/`ディレクトリ。セキュリティ ポリシーまたはセキュリティ監視ツールのために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。

インストールの要件

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

- Red Hat のベスト プラクティスに従って Red Hat Enterprise Linux をインストールし、次のデフォルト オプションを選択する必要があります。そのためには、「GUI 付きサーバー」ベース環境を選択する必要があります。
- Red Hat Enterprise LinuxへのUnified Managerのインストール中にインストール プログラムが必要なすべてのソフトウェアにアクセスしてインストールできるように、システムには該当するリポジトリへのアクセスが必要です。
- のために`yum`インストーラーがRed Hat Enterprise Linux リポジトリ内の依存ソフトウェアを見つけるには、Red Hat Enterprise Linux のインストール中またはその後に有効なRed Hat サブスクリプションを使用してシステムを登録しておく必要があります。

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

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

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

見る["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は、システムにMySQLソフトウェアが正しくインストールされるようにMySQLリポジトリを有効にする必要があります。

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

見る["MySQLリポジトリの手動設定"](#)。

- Unified Manager ホストには Java の 1 つのバージョンのみをインストールする必要があります。そうでない場合、システムはどのバージョンを使用するかを判断できない可能性があります。見る ["Active IQ Unified ManagerホストでJavaを更新した後、サービスが開始されません"](#)。

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。その後、必要なソフトウェアをインターネットに接続されたシステムへダウンロードし、`.rpm` Unified Manager をインストールする予定のシステムにファイルを追加します。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、`'yum install'` 指示。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のサブスクリプション ライセンスがあることを確認してください。



必要なサードパーティ製ソフトウェアは、ここに記載されたりリポジトリ以外からはインストールしないでください。Red Hatリポジトリからインストールされるソフトウェアは、Red Hat Enterprise Linux用に特別に設計されたものであり、Red Hatのベストプラクティス（ディレクトリのレイアウトや権限など）に準拠しています。他の場所から入手したソフトウェアは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の汎用イメージは、ポート443への外部アクセスをブロックする場合があります。そのため、Unified Managerのインストール後に管理者Web UIに接続できなくなることがあります。次のコマンドを実行すると、汎用的なRed Hat Enterprise Linuxのすべての外部ユーザおよび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 は、「GUI 付きサーバー」ベース環境でインストールする必要があります。このベース環境は、Unified Managerのインストール手順で使用されるコマンドを提供します。他のベース環境では、インストールを検証または完了するために追加のコマンドのインストールが必要になる場合があります。もし `'firewall-cmd'` システムで利用できない場合は、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、会社のセキュリティ ポリシーに違反しないか（別の方法が必要でないか）をIT部門の担当者に確認してください。



Red HatシステムではTransparent Huge Pages (THP) を無効にします。有効にすると、特定のプロセスがメモリを大量に消費して終了した場合にUnified Managerがシャットダウンする可能性があります。

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は、Interoperability Matrixを参照してください。

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

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

アイデンティティ プロバイダ (IdP) でユーザが認証されるように、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

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

Unified Managerサーバへの接続

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

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

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

インターフェイス	プロトコル	ポート	説明
Linuxコマンドライン	SSH / SFTP	22	Red Hat Enterprise Linux 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 ServicesからUnified Managerへのアクセスで 使用されます。
syslog	UDP	514	ONTAPシステムからのサ ブスクリプションベース のEMSメッセージにアク セスし、メッセージに基 づいてイベントを作成す る際に使用されます。
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のEMS イベントにアクセスする 際に使用されます。
MySQLデータベース	MySQL	3306	OnCommand Workflow Automationおよ びOnCommand API Services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）から受信するメ ッセージをこのポートで リスンするために使用 されます。

インターフェイス	プロトコル	ポート	説明
AMQP QPIDブローカー	TCP経由のWebSocket	56443	ONTAP（クラウド エージェント）から受信する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は、TLS または SSL によって提供される暗号化をサポートします。



LinuxシステムにUnified Managerをインストールしている間、MySQLのデフォルト ポートである3306へのアクセスはlocalhostのみに制限されます。アップグレード シナリオでは以前の設定が維持されるため、このことによる影響はありません。この設定は変更可能であり、接続は`Control access to MySQL port 3306`メンテナンス コンソールのオプション。詳細については、"[その他のメニュー オプション](#)"。HTTP通信とHTTPS通信に使用されるポート（ポート80と443）は、Unified Managerメンテナンス コンソールを使用して変更できます。詳細については、"[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	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。

デスティネーション	プロトコル	ポート	説明
LDAPS	636	セキュアなLDAP通信に使用されます。	メール サーバ
SMTP	25	アラート通知Eメールの送信に使用されます。	SNMPトラップの送信元
SNMPv1またはSNMPv3	162 / UDP	アラート通知SNMPトラップの送信に使用されます。	外部データ プロバイダのサーバ
TCP	2003	外部のデータ プロバイダ（Graphiteなど）へのパフォーマンス データの送信に使用されます。	NTP サーバ
NTP	123 / UDP	Unified Managerサーバの時間を外部の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）。	syslog

ワークシートへの記入

Unified Manager をインストールして構成する前に、環境に関する具体的な情報をすぐに入手できるようにしておく必要があります。次のリストに情報をまとめておくとう便利です。

Unified Managerのインストール情報

Unified Manager をインストールするために必要な詳細。

ソフトウェアが展開されるシステム	あなたの価値
ホストの完全修飾ドメイン名	
ホストのIPアドレス	
ネットワーク マスク	
ゲートウェイのIPアドレス	
プライマリDNSアドレス	
セカンダリDNSアドレス	

ソフトウェアが展開されるシステム	あなたの価値
検索ドメイン	
メンテナンス ユーザのユーザ名	
メンテナンス ユーザのパスワード	

Unified Managerの設定情報

インストール後に Unified Manager を構成するための詳細。構成によっては省略可能な値もあります。

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

クラスタ情報

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

Nのクラスター1	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

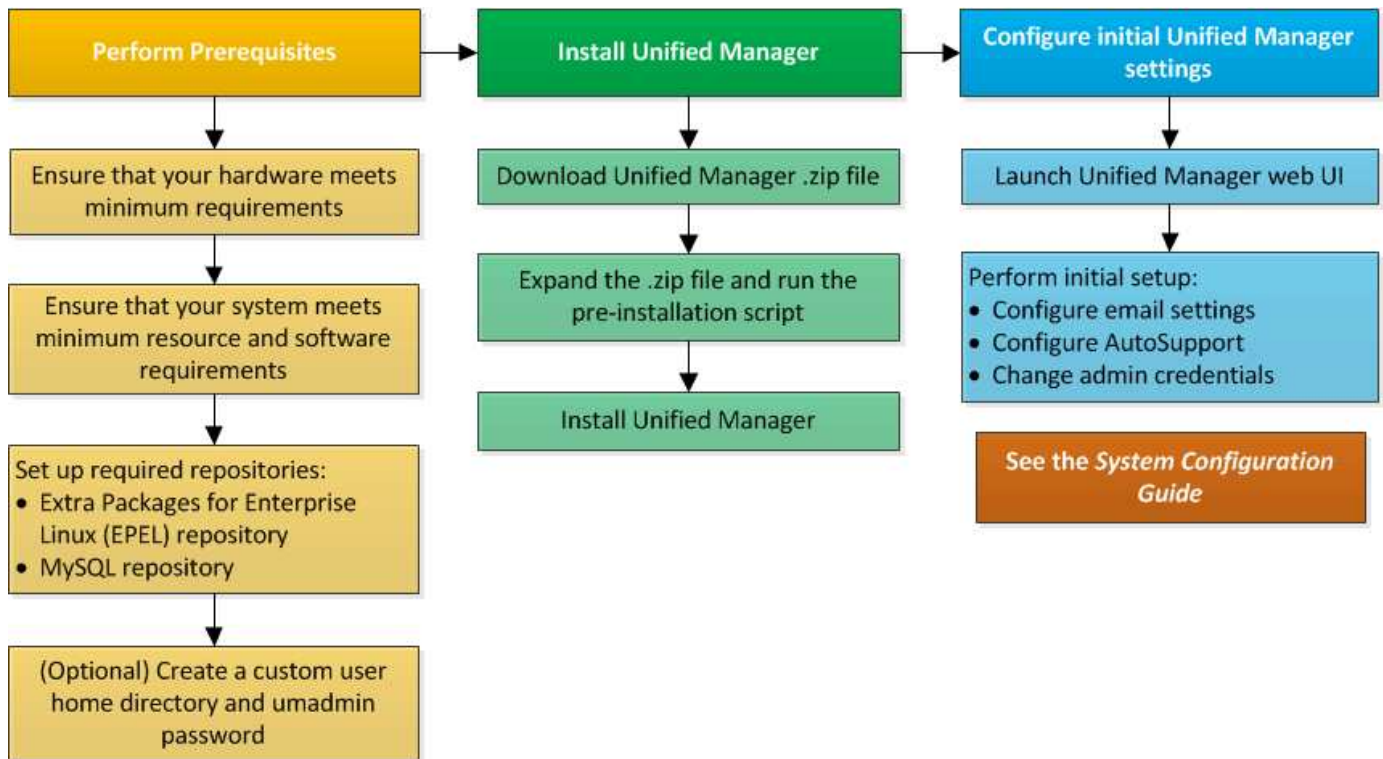
Unified Manager ソフトウェアのインストール、アップグレード、および削除

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

インストール ワークフローでは、Unified Manager を使用する前に実行する必要があるタスクについて説明します。



必要なソフトウェアリポジトリを設定する

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

EPELリポジトリを手動で設定する

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システムにインストールするには、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。バージョン8の場合は、次のサイトからダウンロードしてください。

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

バージョン9の場合は、次のサイトからダウンロードしてください。

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.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 システムでは、例えば、モジュール式 RPM パッケージを含む内部リポジトリがある場合、`javapackages-filesystem-<version>.module.rpm`、モジュラー パッケージのメタデータも同じリポジトリで使用できることを確認します。

MySQLリポジトリを手動で設定する

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

MySQLリポジトリは、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。



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

手順

1. インストールに対応するMySQLリポジトリをダウンロードします。バージョン8の場合は、次のサイトからダウンロードしてください。

```
wget http://repo.mysql.com/yum/mysql-8.4-community/el/8/x86_64/mysql84-community-release-el8-1.noarch.rpm
```

バージョン9の場合は、次のサイトからダウンロードしてください。

```
wget http://repo.mysql.com/yum/mysql-8.4-community/el/9/x86_64/mysql84-community-release-el9-1.noarch.rpm
```

2. MySQLリポジトリを設定します。

```
yum install mysql84-community-release-.noarch.rpm
```

Red Hat Enterprise Linux 8システムを使用していて、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
```

キーが見つからない、またはキーが一致しないというエラーが表示されて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は、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-2023
```

- ・インターネットに接続できないシステムでは、MySQLリポジトリファイルを更新して無効にします。
`gpgcheck`マークすることによって `gpgcheck=0`。

NFS共有とCIFS共有におけるSELinuxの要件

マウントする予定の場合 `/opt/netapp` または `/opt/netapp/data` NAS または SAN デバイス上で SELinux が有効になっている場合は、いくつかの考慮事項に注意する必要があります。

マウントする予定の場合 `/opt/netapp` または `/opt/netapp/data` ルート ファイル システム以外の場所からアクセスする場合、環境で SELinux が有効になっているときは、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。該当するシナリオに対応した手順に従って、正しいSELinuxコンテキストを設定および確認してください。

SELinuxコンテキストを設定する場合 `/opt/netapp/data` 搭載されている

マウントしている場合は `/opt/netapp/data` システムでSELinuxが設定されている `Enforcing`、SELinuxコンテキストタイプが `/opt/netapp/data` 設定されている `mysqld\_db\_t` 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
```

出力の例を次に示します。

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



この出力のコンテキストは default_t。この文脈を次のように変更する必要があります
mysqld_db_t。

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

- a. コンテキストを設定するには、次のコマンドを実行します。 mysqld_db_t:

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

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

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

- c. アンマウントと再マウント `/opt/netapp/data/` コンテキストを有効にするため。
- d. 直接NFSマウントの場合は、次のコマンドを実行してコンテキストを設定します。 `mysqld_db_t`:

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

3. コンテキストが正しく設定されているかどうかを確認します。

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

出力の例を次に示します。

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

SELinuxコンテキストを設定する場合 `/opt/netapp` 搭載されており、`/opt/netapp/data/` 別途マウント

このシナリオでは、まず、`/opt/netapp/data/` 前のセクションで説明したとおりです。適切なコンテキストを設定した後、`/opt/netapp/data/` 親ディレクトリが `/opt/netapp` SELinuxコンテキストが設定されていない `file\_t`。

手順

1. 次のコマンドを実行してコンテキストを確認します。

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

出力の例を次に示します。

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

この出力のコンテキストは `file_t` 変更する必要があります。次のコマンドはコンテキストを `usr\_t`。コンテキストは、以下の値以外に設定できます。`file\_t` セキュリティ要件に基づいて。

2. マウント方法に応じてコンテキストを設定するには、次の手順を実行します。 `/opt/netapp`。
 - a. 次のコマンドを実行してコンテキストを設定します。

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

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

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

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

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
```

出力の例を次に示します。

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

SELinuxコンテキストを設定する場合 `/opt/netapp` 搭載されており、`/opt/netapp/data/` 別途マウントされていない

マウントしている場合は `/opt/netapp` システムでSELinuxが設定されている `Enforcing`、SELinuxコンテキストタイプが `/opt/netapp` 設定されている `mysqld_db_t` 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
```

出力の例を次に示します。

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



この出力のコンテキストは `default_t`。この文脈を次のように変更する必要があります
`mysqld_db_t`。

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

a. コンテキストを設定するには、次のコマンドを実行します。 `mysqld_db_t` :

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

b. 設定した場合 `/opt/netapp` で `/etc/fstab`、編集 `/etc/fstab` ファイル。のために
`/opt/netapp/` マウント オプションで、MySQL ラベルを次のように追加します。

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

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

d. 直接NFSマウントの場合は、次のコマンドを実行してコンテキストを設定します。 `mysqld_db_t` :

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

3. コンテキストが正しく設定されているかどうかを確認します。


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

出力の例を次に示します。

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysql_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。

インストール前にカスタムユーザーホームディレクトリと**umadmin**パスワードを作成します

Unified Managerをインストールする前に、カスタムのホーム ディレクトリを作成し、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。

開始する前に

- ・ システムは、以下に記載されている要件を満たす必要があります。["ハードウェアシステム要件"](#)。
- ・ Red Hat Enterprise Linux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ユーザーを作成します `/home/umadmin` ホームディレクトリとして。
- ・ umadmin ユーザー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アクセスが制限されるため、/home、インストールは失敗します。この場合、ホーム ディレクトリを別の場所に作成する必要があります。また、サイトによっては、パスワードの複雑さに関するルールが設定されている場合や、インストール プログラムではなくローカルの管理者が設定したパスワードが必要な場合があります。

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

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

さらに、Unified Managerのデフォルトのインストールでは、sudoersファイルにumadminユーザーが含まれています。(ocum_sudoers`そして `ocie_sudoers) の`/etc/sudoers.d/`ディレクトリ。セキュリティ ポリシーや一部のセキュリティ監視ツールに従ってこの項目を環境から削除した場合は、再度追加する必要があります。Unified Managerの一部の処理ではsudo権限が必要なため、sudoersの設定を維持する必要があります。

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

```
sudo systemctl status ocie
```

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

手順

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

```
groupadd maintenance
```

3. 任意のホーム ディレクトリの下のメンテナンス グループにユーザー アカウント “umadmin” を作成します。

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

4. umadminのパスワードを定義します。

```
passwd umadmin
```

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

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

Unified Managerをダウンロード

Unified Managerをダウンロードする必要があります。`.zip`NetAppサポート サイトからファイルをダウンロードして、Unified Manager をインストールします。

開始する前に

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。

Red Hat Enterprise Linuxシステム用のUnified Managerのインストール パッケージをダウンロードします。

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"](#)

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、`.zip`ファイルをターゲット システム上のディレクトリにコピーします。



- 使用しているRed Hat Enterprise Linuxシステムに対応した正しいバージョンのインストーラ ファイルをダウンロードします。Red Hat Enterprise Linux 8 または 9 がインストールされているかどうかに応じて、適切なバージョンの Unified Manager をダウンロードしてください。`.zip`ファイル。
- NetAppはコード署名証明書をダウンロードすることを推奨しています(.pem) とデジタル署名(.sig) とともに`.zip`ファイル。

4. ダウンロードしたソフトウェアの整合性をチェックサムで検証します。
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検証するには、次のコマンドを使用します。
 - 次のコマンドは、コード署名証明書の公開鍵を含む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、コード署名証明書が含まれているファイルです。
- 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
```

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

Unified Managerをインストールする

Unified Managerは、Red Hat Enterprise Linux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。

開始する前に

- 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。

見る["ハードウェアシステム要件"](#)。

見る["Linuxソフトウェアとインストールの要件"](#)。

- Unified Managerをダウンロードしておく必要があります `zip` NetAppサポート サイトからターゲット システムにファイルをコピーします。
- ダウンロードしたファイルの整合性を確認する必要があります `zip` ファイル。
- サポートされているWebブラウザが必要です。
- ターミナル エミュレーション ソフトウェアでスクロールバックを有効にする必要があります。

Red Hat Enterprise Linuxシステムには、必要なソフトウェア（Java、MySQL、追加ユーティリティ）の必要なバージョンがすべてインストールされている場合もあれば、必要なソフトウェアが一部しかインストールされていない場合もあります。また、新規にインストールされたシステムの場合、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こともあります。

手順

1. Unified Managerをインストールするサーバにログインします。
2. 該当するコマンドを入力し、インストールを実施する前にターゲット システムで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特定します。

必要なソフトウェアと最小バージョン	ソフトウェアとバージョンを確認するコマンド
OpenJDKバージョン11.0.25	<code>java -version</code>
MySQL 8.4.4 Community Edition	<code>`rpm -qa</code>
<code>grep -i mysql`</code>	<code>p7zip 16.02</code>
<code>`rpm -qa</code>	<code>grep p7zip`</code>

- MySQL 8.4.4 Community Editionより前のMySQLバージョンがインストールされている場合、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、`--nodeps`コンポーネントをアンインストールするオプション。

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

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

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

- ディレクトリに次のモジュールが展開されたことを確認します。

```
ls *.rpm
```

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

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

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

インストール前スクリプトは、システムに有効なRed Hat Enterprise Linuxサブスクリプションが存在すること、およびシステムが必要なソフトウェア リポジトリにアクセスできることをチェックします。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システムを使用していて、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。インターネットにアクセス可能で、必要なすべてのパッケージがある場合は、手順8に進んでください。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調べ、足りない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、利用可能なパッケージと利用できないパッケージのリストを表示します。+

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

「Installing:」セクションの項目は現在のディレクトリで使用可能なパッケージであり、「Installing for dependencies:」セクションの項目はシステムに不足しているパッケージです。

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

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



プラグイン「yum-plugin-downloadonly」は Red Hat Enterprise Linux システムで常に有効になっているわけではないので、パッケージをインストールせずにダウンロードする機能を有効にする必要がある場合があります。

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

- a. インターネットに接続したシステムからインストール先のシステムに足りないパッケージをコピーします。

8. ルートユーザーとして、または `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、その他の必要なすべてのサポート 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。

GPG NOKEYエラーでインストールに失敗した場合は、`rpm --import URL` からキーをインポートするには:

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2023
```



代替コマンド（`rpm -ivh`）。Red Hat Enterprise LinuxシステムにUnified Managerを正常に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が、特定の順序で、システムによって自動的に適用される特定のディレクトリ構造にインストールされている必要があります。`yum install netapp-um<version>.x86\_64.rpm` 指示。

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

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

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

メッセージは次のようになります。

```
Active IQ Unified Manager installed successfully.  
Use a web browser and one of the following URL(s) to configure and  
access the Unified Manager GUI.
```

```
https://default_ip_address/      (if using IPv4)
```

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

```
https://fully_qualified_domain_name/
```

```
Log in to Unified Manager in a web browser by using following details:
```

```
username: umadmin
```

```
password: admin
```

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

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

Web UIにアクセスして、umadminユーザーのデフォルトパスワードを変更し、Unified Managerの初期セットアップを実行します。["Active IQ Unified Managerの設定"](#)。umadminユーザのデフォルト パスワードは必ず変更してください。

Unified Managerのインストール時に作成されるユーザ

Red Hat Enterprise Linux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ており、「メンテナンス ユーザー」タイプとして構成されています。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 クエリの実行に使します。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のパスワードを変更する

インストール時に設定されたインスタンス固有のJBossパスワードをリセットできます。サイトでUnified Managerのインストール設定と違うパスワードが必要な場合、リセットできます。この処理を実行すると、MySQLへのアクセス時にJBossで使用するパスワードも変更になります。

- Unified ManagerがインストールされているRed Hat Enterprise Linuxシステムへのrootユーザ アクセスが必要です。
- NetAppが提供する password.sh`ディレクトリ内のスクリプト ` /opt/netapp/essentials/bin。

手順

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

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

関連付けられているMySQLソフトウェアは停止しないでください。

3. 次のコマンドを入力して、パスワードの変更プロセスを開始します。

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

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

パスワードは8~16文字で指定し、数字、大文字、小文字、および次の特殊文字をそれぞれ1文字以上含める必要があります。

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

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

```
systemctl start ocie
```

```
systemctl start ocieau
```

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

Red Hat Enterprise Linux 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NetAppから提供されたときは、新規リリースと同じ手順でインストールします。

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

Unified Managerのバージョンとサポートされるアップグレード パス

Active IQ Unified Managerでサポートされるアップグレード パスはバージョンごとに異なります。

すべてのバージョンのUnified Managerで、新しいバージョンへのインプレース アップグレードを実行できるわけではありません。Unified ManagerのアップグレードはN-2モデルに限定されています。つまり、すべてのプラットフォームにおいて、アップグレードできるのは2つ上のリリースまでです。たとえば、Unified Manager 9.16へのアップグレードはUnified Manager 9.13と9.14からのみ実行できます。

サポート対象よりも前のバージョンを実行している場合は、Unified Managerインスタンスを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、最新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、現在Unified Manager 9.9がインストールされていて、Unified Manager 9.14にアップグレードする場合、アップグレード手順は次のようになります。

アップグレード パスの例：

1. 9.11から9.13にアップグレードします。
2. 9.13から9.14にアップグレードします。
3. 9.13から9.16にアップグレードします。
4. 9.14から9.16にアップグレードします。

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

Unified Manager のアップグレード

LinuxプラットフォームでUnified Manager 9.13または9.14から9.16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。

開始する前に

- 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。

見る["ハードウェアシステム要件"](#)。

見る["Linuxソフトウェアとインストールの要件"](#)。

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

は適切なバージョンにアップグレードする必要があります。

見る["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は、バックアップファイルを`/opt/netapp/data`ディレクトリを外部の場所にコピーします。
- アップグレードの実行中に、パフォーマンス データの保持期間について、以前のデフォルト設定である13カ月のままにするか6カ月に変更するかを確認するプロンプトが表示されることがあります。変更を確認すると、6カ月を過ぎた過去のパフォーマンス データはパージされます。
- アップグレード プロセスの実行中はUnified Managerを使用できなくなるため、実行中の処理がある場合は完了しておいてください。
- MySQL Community Editionは、Unified Managerのアップグレード時に自動的にアップグレードされます。システムにインストールされているMySQLのバージョンが8.4.4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8.4.4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サーバにログインします。
2. サーバにUnified Managerのバンドルをダウンロードします。

見る["Linux用Unified Managerのダウンロード"](#)。

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

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

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

4. ディレクトリに次のモジュールが展開されたことを確認します。

```
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存在すること、およびシステムが必要なソフトウェア リポジトリにアクセスできることをチェックします。問題が検出された場合は、修正してからアップグレードに進む必要があります。

不足しているパッケージが検出された場合は、["パッケージが不足している場合の追加手順"](#)。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かどうか確認されます。問題が検出された場合は、Unified Managerをアップグレードする前に修正する必要があります。Unified Manager をアップグレードする前に、*net-snmp*などのパッケージをインストールしていた場合、アップグレード中にMySQL 依存関係によってパッケージがアンインストールされる可能性があります。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。

メッセージは次のようになります。

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

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

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

パッケージが不足している場合の追加手順

アップグレード中にサイトでパッケージが不足していることが検出された場合、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揃っているかどうかを調べ、足りないパッケージをダウンロードします。



これらの手順は、メイン手順のステップ 5 の後に実行する必要があります。この手順によりUnified Managerがアップグレードされるため、それ以上アップグレードのため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で使用可能なパッケージであり、「Installing for dependencies:」セクションの項目はシステムに不足しているパッケージです。

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

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

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

プラグイン「yum-plugin-downloadonly」はRed Hat Enterprise Linux システムで常に有効になって

いるわけではないので、パッケージをインストールせずにダウンロードする機能を有効にする必要がある場合があります。

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

3. インストール先システムのUnified Managerのバンドルを解凍したディレクトリに、ダウンロードしたパッケージをコピーします。
4. 前述のディレクトリに移動し、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
```

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

```
systemctl start ocie
```

```
systemctl start ocieau
```

これで、Unified Managerのアップグレード プロセスは完了です。サポートされているWebブラウザの新しいウィンドウに、表示されたIPアドレスまたはURLを入力してUnified Manager Web UIを起動し、前に設定したメンテナンス 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。

ホスト **OS** を **Red Hat Enterprise Linux 7.x** から **8.x** にアップグレードします。

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8.0～8.10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サーバで実行するか同じサーバで実行するかです。

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。

見る["バックアップとリストア処理の管理"](#)バックアップおよび復元プロセスの詳細な手順を確認する必要があります。

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、次の手順に従います。

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

見る["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。

見る["LinuxへのUnified Managerのインストール"](#)。

インストールが完了しても、UIを起動したり、クラスタ、ユーザ、または認証設定を設定したりしないでください。これらの情報は、リストア プロセスでバックアップ ファイルから取り込みます。

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

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

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

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

同じサーバー上のホスト**OS**のアップグレード

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

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

見る["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。

見る["LinuxへのUnified Managerのインストール"](#)。

インストールが完了しても、UIを起動したり、クラスタ、ユーザ、または認証設定を設定したりしないでください。これらの情報は、リストア プロセスでバックアップ ファイルから取り込みます。

5. バックアップファイルをコピーする(.7z`外部の場所からファイル (ファイル) を /opt/netapp/data/ocum-backup/ データベースリポジトリファイルを /database-dumps-repo`サブディレクトリの下 /ocum-backup`ディレクトリ。
6. 次のコマンドを入力してバックアップ ファイルからUnified Managerデータベースをリストアします。

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

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

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

Unified ManagerがLinuxシステムにすでにインストールされている場合は、JREなどのサードパーティ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の開発元では、定期的にセキュリティ脆弱性が報告されています。これらのソフトウェアは、新しいバージョンに随時アップグレードすることができます。

Linux で OpenJDK をアップグレードする

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。

開始する前に

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は同一リリース ファミリー内でのみ更新可能です。たとえば、OpenJDK 11.0.14からOpenJDK 11.0.17には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. 該当するバージョンの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
```

統合マネージャーを再起動します

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

開始する前に

Unified ManagerがインストールされているRed Hat Enterprise Linux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` MySQL サーバーの起動と停止に必要なデーモン プログラムです。

統合マネージャーを削除する

Unified Managerは、Red Hat Enterprise Linux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。

開始する前に

- 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。SELinuxランタイムモードを「Permissive」に変更します。`setenforce 0`指示。
- 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目的で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。このファイアウォール 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
```

これにより、関連するNetAppのRPMパッケージがすべて削除されます。Java、MySQL、p7zipなど、前提条件のソフトウェア モジュールは削除されません。

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

```
rpm -e p7zip mysql-community-client mysql-community-server mysql-community-
```

```
common mysql-community-libs java-x.y
```

この処理が完了すると、ソフトウェアは削除されます。すべてのデータは `/opt/netapp/data` ディレクトリは `/opt/netapp/data/BACKUP` アンインストール後のフォルダー。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（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 **umadmin** ユーザーとメンテナンス グループを削除します

Unified Manager をインストールする前に、独自の umadmin ユーザーとメンテナンス アカウントを定義するカスタム ホーム ディレクトリを作成した場合は、Unified Manager をアンインストールした後にこれらの項目を削除する必要があります。

標準の Unified Manager アンインストールでは、カスタム定義された umadmin ユーザーとメンテナンス 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）では、ONTAPストレージシステムの健全性とパフォーマンスを一元的に監視および管理することができます。Unified Managerは、LinuxサーバやWindowsサーバに導入できるほか、VMwareホストに仮想アプライアンスとして導入することもできます。

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

関連情報

["NetApp Interoperability Matrix Tool"](#)

Unified Managerサーバの機能

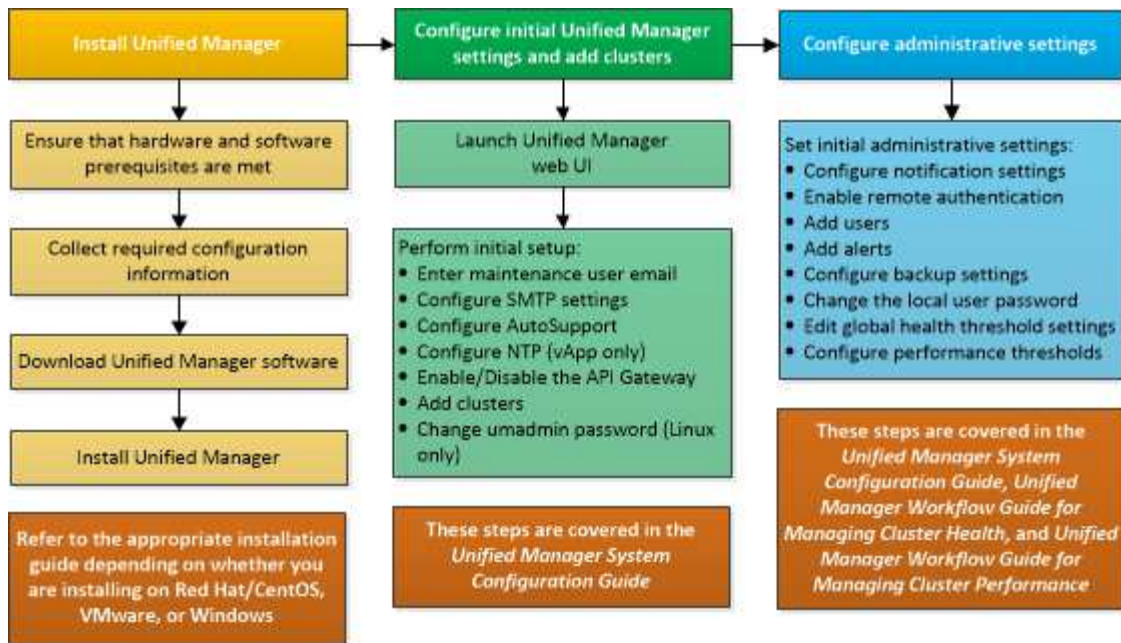
Unified Manager サーバー インフラストラクチャは、データ収集ユニット、データベース、およびアプリケーション サーバーで構成されます。検出、監視、ロールベース アクセス制御（RBAC）、監査、ロギングなどのインフラ サービスを提供します。

Unified Manager はクラスタ情報を収集し、そのデータをデータベースに保存し、そのデータを分析してクラスタに問題があるかどうかを確認します。

インストール手順の概要

インストール ワークフローでは、Unified Manager を使用する前に実行する必要があるタスクについて説明します。

以降の各セクションでは、このワークフローの各項目について説明します。



Unified Managerをインストールするための要件

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

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

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

["Supportability for Security Measures applied to Active IQ Unified Manager for Clustered Data ONTAP"](#)

関連情報

["NetApp Interoperability Matrix Tool"](#)

仮想インフラおよびハードウェア 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ついて、推奨される値を示します。これらは、Unified Managerが許容されるパフォーマンス レベルを達成することが確認されている値です。

ハードウェア構成	推奨設定
RAM	12GB（最小要件は8GB）

ハードウェア構成	推奨設定
プロセッサ	CPU×4
CPUサイクル	合計9572MHz（最小要件は9572MHz）
空きディスク スペース	150GB。割り当ては次のとおりです。 • 100GB - インストール ディレクトリ用 • 50G - MySQLのデータ ディレクトリ用

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（バレーニングなど）は有効にしないでください。

さらに、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 ベストプラクティスガイド"

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

専用使用の要件

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

バックアップ用のスペース要件

Unified Manager のバックアップおよび復元機能を使用する予定の場合は、「data」ディレクトリまたはディスクに 150 GB のスペースが確保されるように追加の容量を割り当てます。バックアップはローカルにもリモートにも保存できますが、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、次の方法で正常に実行できるように構成する必要があります。`ping`ホスト自体からのホスト名。IPv6設定の場合は、次の点を確認する必要があります。`ping6`ホスト名への変更が成功し、Unified Manager のインストールが成功していることを確認します。

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

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

Windowsソフトウェアとインストールの要件

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

オペレーティング システム ソフトウェア

Unified Managerは次の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Windowsオペレーティング システムの次の言語版に対応しています。

- 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のインストールをサポートしていません。

Unified Managerのみを実行する専用のサーバを用意する必要があります。他のアプリケーションをサーバにインストールしないでください。社内の規定により、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可能性があります。Unified Managerのインストールが失敗しないように、インストール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、以下のサードパーティ 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は、Unified Managerのインストール時にインストールされます。

- Visual Studio 2015 用 Microsoft Visual C++ 再頒布可能パッケージ バージョン 14.26.28720.3
- MySQL Community Editionバージョン8.4.4
- Python 3.12.4
- OpenJDKバージョン11.0.25
- 7-zip バージョン 23.01 以降



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

MySQLが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ること。
- サンプル データベースがインストールされていないこと。
- サービス名は「MYSQL84」です。

Unified ManagerはWildFly Webサーバに導入されます。WildFly 26.1.3にはUnified Managerがバンドルされていて、設定済みです。



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。
- その temp`インストール ファイルを抽出するために、ディレクトリには 2 GB のディスク領域を構成する必要があります。ディレクトリが作成されたかどうかを確認するには、コマンドライン インターフェイスで次のコマンドを実行します。 ``echo %temp%`
- Unified ManagerのMSIファイルのキャッシュ用に、Windowsドライブに2GBのディスク スペースを確保しておく必要があります。
- Unified ManagerをインストールするMicrosoft Windows Serverは、次のように完全修飾ドメイン名 (FQDN) で設定する必要があります。 ``ping`` ホスト名と FQDN への応答は成功します。
- Microsoft IIS World Wide Web発行サービスを無効にして、ポート80および443を空けておく必要があります。
- 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する必要があります。
- 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する必要があります。
- Unified Managerをインストールする前に、システムのウイルス対策ソフトウェアをすべて無効にしてください。インストールが完了したら、ウイルス対策スキャンの対象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、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データディレクトリ、例えば、 `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は、Interoperability Matrixを参照してください。

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

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

アイデンティティ プロバイダ (IdP) でユーザが認証されるように、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

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

Unified Managerサーバへの接続

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

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

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

インターフェイス	プロトコル	ポート	説明
syslog	UDP	514	ONTAPシステムからのサブスクリプションベースのEMSメッセージにアクセスし、メッセージに基づいてイベントを作成する際に使用されます。
REST	HTTPS	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のEMSイベントにアクセスする際に使用されます。
MySQLデータベース	MySQL	3306	OnCommand Workflow AutomationおよびOnCommand API Services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）から受信する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）から受信する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。



WindowsシステムにUnified Managerをインストールしている間、MySQLのデフォルト ポートである3306へのアクセスはlocalhostのみに制限されます。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MySQLポート3306へのアクセスを制限してください。アップグレードシナリオでは以前の設定が維持されるため、このことによる影響はありません。この設定は変更可能であり、接続を他のホストに利用可能にするには、`Control access to MySQL port 3306` メンテナンス コンソールのオプション。詳細については、["その他のメニュー オプション"](#)。HTTP通信とHTTPS通信に使用されるポート（ポート80と443）は、Unified Manager メンテナンス コンソールを使用して変更できます。詳細については、["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	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トラップの送信元
SNMPv1またはSNMPv3	162 / UDP	アラート通知SNMPトラップの送信に使用されます。	外部データ プロバイダのサーバ
TCP	2003	外部のデータ プロバイダ（Graphiteなど）へのパフォーマンス データの送信に使用されます。	NTP サーバ

デスティネーション	プロトコル	ポート	説明
NTP	123 / UDP	Unified Managerサーバの時間を外部の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）から受信する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）から受信する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。	syslog

ワークシートへの記入

Unified Manager をインストールして構成する前に、環境に関する具体的な情報をすぐに入手できるようにしておく必要があります。次のリストに情報をまとめておくとう便利です。

Unified Managerのインストール情報

Unified Manager をインストールするために必要な詳細。

ソフトウェアが展開されるシステム	あなたの価値
ホストの完全修飾ドメイン名	
ホストのIPアドレス	
ネットワーク マスク	
ゲートウェイのIPアドレス	
プライマリDNSアドレス	

ソフトウェアが展開されるシステム	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 ユーザのユーザ名	
メンテナンス ユーザのパスワード	

Unified Managerの設定情報

インストール後に Unified Manager を構成するための詳細。構成によっては省略可能な値もあります。

設定	あなたの価値
メンテナンス ユーザのEメール アドレス	
SMTPサーバのホスト名またはIPアドレス	
SMTPのユーザ名	
SMTPのパスワード	
SMTP ポート	25 (デフォルト値)
アラート通知の送信元Eメール アドレス	
認証サーバのホスト名またはIPアドレス	
Active Directoryの管理者名またはLDAPバインド識別名	
Active Directoryのパスワードまたは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) のメタデータ	
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 システムの情報を記入します。

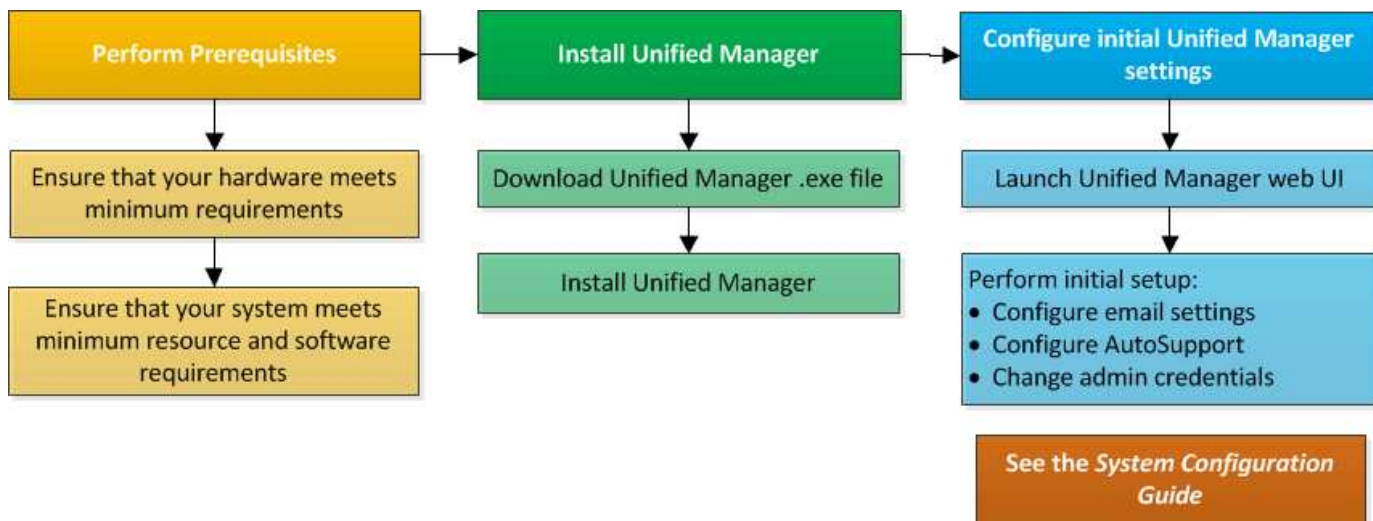
Nのクラスター1	あなたの価値
ホスト名またはクラスタ管理IPアドレス	
ONTAP管理者のユーザ名  管理者には「admin」ロールが割り当てられている必要があります。	
ONTAP管理者のパスワード	
プロトコル	HTTPS

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

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

インストール ワークフローでは、Unified Manager を使用する前に実行する必要があるタスクについて説明します。



WindowsにUnified Managerをインストールする

Windows に Unified Manager をダウンロードしてインストールするための一連の手順を理解することが重要です。

Unified Managerをインストールする

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。

開始する前に

- 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。

見る["ハードウェアシステム要件"](#)。

見る["Windowsソフトウェアとインストールの要件"](#)。



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

- Windowsの管理者権限が必要です。ユーザー名が感嘆符「」で始まっ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 "!"。
- ASA r2システムを除くすべてのクラスタがサポートされます。
- 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、および特殊文字を含める必要があります。
- メンテナンス ユーザまたはMySQLのrootユーザのパスワードに次の特殊文字は使用できません。" ' ` % , = & < > | ^ \ / () [] ; :

次の特殊文字は使用できます。~ ! @ # \$ * - ? . + { }

手順

1. デフォルトのローカル管理者アカウントでWindows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. 必要に応じて、zipファイルを展開し、インストール ファイルがあるディレクトリに移動します。
6. Unified Managerインストーラの実行ファイル（.exe）を右クリックし、管理者として実行します。

Unified Managerにより、不足しているサードパーティ パッケージとインストールされているパッケージ

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

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

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

11. *次へ*をクリックします。
12. Shield のインストール準備ウィザードで、[インストール] をクリックします。
13. インストールが完了したら、[完了] をクリックします。
14. Windowsシステムにウイルス対策ソフトウェアがインストールされて有効になっている場合は、インストールの完了後にウイルス対策スキャンの対象から次のパスを手動で除外します。
 - Unified Managerデータ ディレクトリ
 - Unified Managerインストール ディレクトリ
 - MySQLデータ ディレクトリ

インストールが完了すると、次のディレクトリが作成されます。

- インストール ディレクトリ

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

- MySQLデータ ディレクトリ

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

- Javaディレクトリ

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

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

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

C:\ProgramData\NetApp\OnCommandAppData\

ウェブUIにアクセスしてUnified Managerの初期セットアップを実行することができます。["Active IQ Unified Managerの設定"](#)。

Unified Managerの無人インストールを実行する

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

手順

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

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	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" 例： 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"

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	<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> 例： <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>

その `/qr` オプションにより、ユーザー インターフェイスを縮小した静音モードが有効になります。インストールの進捗を示す基本的なユーザ インターフェイスのみが表示され、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プリインストールされていない場合は、`/qr` オプション。インストールが失敗する場合は、`/qn` このオプションは、サードパーティのパッケージがインストールされていないサーバーで使用されます。

その `/qn` オプションは、ユーザー インターフェイスのない静音モードを有効にします。インストールの実行中にユーザ インターフェイスも進捗も表示されません。使用しないでください `/qn` サードパーティのパッケージがインストールされていない場合のオプション。

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

`https://IP address`

JBossのパスワードを変更する

インストール時に設定されたインスタンス固有のJBossパスワードをリセットできます。サイトでUnified Managerのインストール設定と違うパスワードが必要な場合、リセットできます。この処理を実行すると、MySQLへのアクセス時にJBossで使用するパスワードも変更になります。

開始する前に

- 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。
- NetAppが提供する `password.bat` ディレクトリ内のスクリプト

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

手順

1. Unified Managerホスト マシンにadminユーザとしてログインします。
2. Windows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 Acquisition Service (Ocie-au)
 - NetApp Active IQ Management Server Service (Oncommandsvc)
3. 起動する `password.bat` パスワード変更プロセスを開始するスクリプト:

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

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

パスワードは8～16文字で指定し、数字、大文字、小文字、および次の特殊文字をそれぞれ1文字以上含める必要があります。

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

6. スクリプトが完了したら、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 Management Server Service (Oncommandsvc)
 - NetApp Active IQ Acquisition Service (Ocie-au)
7. すべてのサービスが開始されたら、Unified Manager UIにログインできます。

Unified Managerのバージョンとサポートされるアップグレード パス

Active IQ Unified Managerでサポートされるアップグレード パスはバージョンごとに異なります。

すべてのバージョンのUnified Managerで、新しいバージョンへのインプレース アップグレードを実行できるわけではありません。Unified ManagerのアップグレードはN-2モデルに限定されています。つまり、すべてのプラットフォームにおいて、アップグレードできるのは2つ上のリリースまでです。たとえば、Unified Manager 9.16へのアップグレードはUnified Manager 9.13と9.14からのみ実行できます。

サポート対象よりも前のバージョンを実行している場合は、Unified Managerインスタンスを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、最新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、現在Unified Manager 9.9がインストールされていて、Unified Manager 9.14にアップグレードする場合、アップグレード手順は次のようになります。

アップグレード パスの例：

1. 9.11から9.13にアップグレードします。
2. 9.13から9.14にアップグレードします。
3. 9.13から9.16にアップグレードします。
4. 9.14から9.16にアップグレードします。

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

Unified Manager のアップグレード

WindowsプラットフォームでUnified Manager 9.13または9.14から9.16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。

開始する前に

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

見る["ハードウェアシステム要件"](#)。

見る["Windowsソフトウェアとインストールの要件"](#)。



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



アップグレードを開始する前に、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8.4.4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8.4.4に自動的にアップグレードされます。MySQLを単体で旧バージョンから8.4.4へアップグレードしないでください。
- ASA r2システムを除くすべてのクラスタがサポートされます。
- Windowsの管理者権限が必要です。ユーザー名が感嘆符「`!`」で始まっ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、データ ディレクトリのサイズに加え、2.5GBの使用可能なスペースが追加で必要になります。十分な空きスペースがないと、アップグレードが中止され、追加に必要なスペース量がエラー メッセージに表示されます。

- アップグレードの実行中に、パフォーマンス データの保持期間について、以前のデフォルト設定である13カ月のままにするか6カ月に変更するかを確認するプロンプトが表示されることがあります。変更を確認すると、6カ月を過ぎた過去のパフォーマンス データはパージされます。
- アップグレードする前に、`<InstallDir>\JDK` および `MySQL Data Directory` 内の開いているファイルまたはフォルダーを閉じる必要があります。
- Windowsシステムにウイルス対策ソフトウェアがインストールされて有効になっていると、Unified Managerのアップグレードに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してください。

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

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

手順

1. NetApp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. 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。必要に応じて、zipファイルを展開し、インストール ファイルがあるディレクトリに移動します。Unified Managerインストーラの実行ファイル（.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?
```

4. [はい] をクリックし、[次へ] をクリックします。
5. インストール中に設定した MySQL84 のルートパスワードを入力し、[次へ] をクリックします。
6. 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にログインします。
7. Windowsシステムにウイルス対策ソフトウェアがインストールされて有効になっている場合は、アップグレードの完了後にウイルス対策スキャンの対象から次のパスを手動で除外します。
 - Unified Managerデータ ディレクトリ
 - Unified Managerインストール ディレクトリ
 - MySQLデータ ディレクトリ



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の開発元では、定期的にセキュリティ脆弱性が報告されています。これらのソフトウェアは、新しいバージョンに随時アップグレードすることができます。

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。

開始する前に

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

OpenJDKは同一リリース ファミリー内でのみ更新可能です。たとえば、OpenJDK 11.0.16からOpenJDK 11.0.18にはアップグレードできますが、OpenJDK 11からOpenJDK 12に直接更新することはできません。

手順

1. Unified Managerホスト マシンにadminユーザとしてログインします。
2. OpenJDKのWebサイトから、該当するバージョンの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。

たとえば、ダウンロード `jdk-11.0.18_windows-x64_bin.zip` from <https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html>。



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、"[Oracleアカウントのサインイン](#)"作成するためのページです。

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 Acquisition Service (Ocie-au)
 - NetApp Active IQ Management Server Service (Oncommandsvc)
4. 拡大する `zip` ファイル。
5. 結果からディレクトリとファイルをコピーします `jdk`ディレクトリ`（例： ``jdk-11.0.18 Java` がインストールされている場所）に移動します。例： `C:\Program Files\NetApp\JDK\`
6. Windows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 Management Server Service (Oncommandsvc)
 - NetApp Active IQ Acquisition Service (Ocie-au)

サードパーティ製品をアンインストールする

Unified Manager をアップグレードした後、Python や Microsoft Visual C++ 2013 などのサードパーティ製品をアンインストールできます。これはオプションです。

Pythonをアンインストールする

手順

1. コントロール パネル から プログラム > プログラムと機能 を選択します。
2. プログラムのリストからPythonを選択します。
3. *このプログラムをアンインストール*を選択します。3.12以外のPythonのすべてのバージョンをアンイン

ストールします。Pythonバージョン3.12を保持していることを確認します。

Microsoft Visual C++ 2013 をアンインストールする

手順

1. コントロール パネル から プログラム > プログラムと機能 を選択します。
2. プログラムのリストから*Microsoft Visual C++ 2013*を選択します。
3. *このプログラムをアンインストール*を選択します。

統合マネージャーを再起動します

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

開始する前に

Windowsの管理者権限が必要です。

手順

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

...から	次の順序でサービスを停止します...
コマンドライン	a. <code>sc stop ocie-au</code> b. <code>sc stop Oncommandsvc</code>
Microsoftサービス マネージャ	a. NetApp Active IQ Acquisition Service (Ocie-au) b. NetApp Active IQ Management Server Service (Oncommandsvc)

3. Unified Managerのサービスを開始します。

...から	次の順序でサービスを開始します...
コマンドライン	a. <code>sc start Oncommandsvc</code> b. <code>sc start ocie-au</code>
Microsoftサービス マネージャ	a. NetApp Active IQ Management Server Service (Oncommandsvc) b. NetApp Active IQ Acquisition Service (Ocie-au)

Unified Manager をアンインストールする

Unified Managerをアンインストールする場合は、[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。

開始する前に

- Windowsの管理者権限が必要です。
- ソフトウェアをアンインストールする前に、Unified Managerサーバからすべてのクラスタ（データ ソース）を削除しておく必要があります。
- MySQLポート3306を許可またはブロックする目的で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。このファイアウォール 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。

- プログラムと機能 ウィザードから 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. 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、[アンインストール] をクリックします。
- コマンドラインからUnified Managerをアンインストールする場合は、次の手順を実行します。
 - i. 管理者権限でWindowsのコマンドラインにログインします。
 - ii. Active IQ Unified Managerディレクトリに移動し、次のコマンドを実行します。

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

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

Unified Managerがシステムからアンインストールされます。

2. Unified Managerのアンインストール時に削除されない次のサードパーティ パッケージとデータをアンインストールします。
- サードパーティ製パッケージ: JRE、MySQL、Microsoft Visual C++ 2015 再頒布可能パッケージ、Python、7zip
 - Unified Manager によって生成された MySQL 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 ディレクトリのデータ

設定タスクと管理タスクの実行

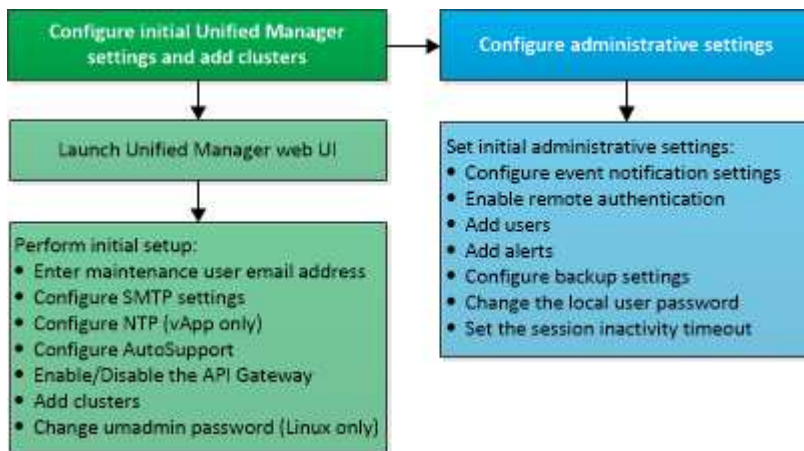
Active IQ Unified Managerを構成する

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

このマニュアルで説明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に必要です。それ以外の手順は新しいインスタンスをセットアップする際に推奨される設定か、またはONTAPの定期的な監視を開始する前に把握しておくことが推奨される設定です。

設定手順の概要

設定ワークフローでは、Unified Manager を使用する前に実行する必要があるタスクについて説明します。



Unified Manager Web UI にアクセスする

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。

開始する前に

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

手順

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

リンクの形式は次のとおりです。 `https://URL`。

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



1時間以内にWeb UIへのログインに3回連続して失敗すると、システムからロックアウトされ、システム管理者への連絡が必要になります。これはローカル ユーザにのみ該当します。

Unified Manager Web UIの初期セットアップを実行します

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

開始する前に

次の作業を完了しておきます。

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

Active IQ Unified Managerの[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環境の場合の例を示したものです。

≡

Active IQ Unified Manager

All ▾

Search All Storage Objects and Actions 🔍

Getting Started

1

2

3

4

5

EmailAutoSupportAPI GatewayAdd ONTAP ClustersFinish

Notifications

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

Maintenance User Email

Emailmgo@eng.netapp.com

SMTP Server

Host Name or IP Addressemail.eng.netapp.com

Port25

User Nameadmin

Password

☐ Use STARTTLS ⓘ ☐ Use SSL ⓘ

Continue

これらのオプションをあとで変更する場合は、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専用です。この設定はあとからUnified Managerメンテナンスコンソールを使用して変更できます。

手順

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



STARTTLS を使用する または **SSL** を使用する オプションを選択した場合は、続行 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を続行します。

2. AutoSupportページで「同意して続行」をクリックし、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コンテンツを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する必要がある場合、またはAutoSupportを無効にする場合は、Web UI から 全般 > * AutoSupport* オプションを使

用します。

3. Red Hat システムでは、umadmin ユーザーのパスワードをデフォルトの「admin」文字列から個人用の文字列に変更します。
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Unified ManagerでONTAP REST APIを使用して管理できるようにAPIゲートウェイ機能を使用するかどうかを選択します。次に、[続行] をクリックします。

この設定は、Web UI の 一般 > 機能設定 > **API** ゲートウェイ から後で有効または無効にすることができます。APIの詳細については、以下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、[次へ] をクリックします。管理する予定のクラスタごとに、ユーザー名とパスワードの資格情報とともに、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。ユーザーには「admin」ロールが必要です。

この手順はオプションです。後で Web UI の ストレージ管理 > クラスタ設定 からクラスタを追加できます。

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。

クラスタを追加する

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

開始する前に

- アプリケーショ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完全修飾ドメイン名 (FQDN) または短縮名です。ホスト名は、クラスタ管理IPアドレスに解決できる必要があります。

クラスタ管理IPアドレスは、管理用Storage Virtual Machine (SVM) のクラスタ管理LIFであることが必要です。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* ロールが必要です。

- HTTPSプロトコルを使用してクラスタに接続するポート番号 (通常はポート443)

- 必要な証明書を用意しておきます。

SSL (HTTPS) 証明書: この証明書は Unified Manager が所有します。Unified Managerの新規インストール時に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、この証明書をCA署名証明書にアップグレードすることを推奨します。サーバ証明書の有効期限が切れた場合は、証明書を再生成する必要があります。その後Unified Managerを再起動すると、新しい証明書がサービスに組み込まれます。SSL証明書の再生成の詳細については、以下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通知の認証に使用されます。

相互 TLS 通信用の証明書: Unified Manager とONTAP間の相互 TLS 通信中に使用されます。証明書ベースの認証は、クラスタのONTAPバージョンに基づいて有効になります。ONTAP 9.5よりも前のバージョンを実行しているクラスタでは、証明書ベースの認証は有効ではありません。

古いバージョンのUnified Managerを更新しても、クラスタの証明書ベースの認証は自動では有効になりません。ただし、クラスタの詳細を変更して保存すれば、認証を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、証明書を再生成して新しい証明書を組み込む必要があります。証明書の表示と再生成の詳細については、以下を参照してください。"[クラスタの編集](#)"。



- クラスタはWeb UIから追加でき、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することもできますが、証明書ベースの認証はデフォルトでは有効になりません。Unified ManagerのCLIを使用してクラスタを追加した場合、クラスタを編集するにはUnified Manager UIを使用する必要があります。見ることができます"[サポートされるUnified ManagerのCLIコマンド](#)"Unified Manager CLI を使用してクラスターを追加します。
- 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、あるサーバからUnified Managerのバックアップを作成し、ホスト名またはIPアドレスが異なる別のUnified Managerサーバにリストアすると、クラスタの監視に失敗することがあります。このエラーを回避するには、クラスタの詳細を編集して保存します。クラスタの詳細編集の詳細については、以下を参照してください。"[クラスタの編集](#)"。

+

クラスタ証明書: この証明書はONTAPが所有します。有効期限が切れた証明書でUnified Managerにクラスタを追加することはできません。クラ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) の記事を参照してください。"[System ManagerユーザーインターフェイスでONTAP自己署名証明書を更新する方法](#)"。

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

MetroCluster構成では、ローカル クラスタとリモート クラスタの両方を追加し、追加した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、ストレージ管理 > クラスター セットアップ をクリックします。
2. クラスター設定ページで、[追加] をクリックします。
3. [クラスタの追加]ダイアログ ボックスで、クラスタのホスト名またはIPアドレス、ユーザ名、パスワード、ポート番号など、必要な値を指定します。

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

4. *送信*をクリックします。
5. [ホストの承認] ダイアログ ボックスで、[証明書の表示] をクリックして、クラスター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したあとに相互TLS通信用の証明書を表示できます。

証明書ベースの認証が有効になっていない場合、Unified Managerではクラスタの初回追加時にのみ証明書がチェックされます。ONTAPへのAPI呼び出しのたびに証明書がチェックされることはありません。

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日間のパフォーマンス データの収集を開始します。これらの統計は、データの継続性収集機能を使用して収集されます。この機能では、クラスタが追加された直後から2週間分のクラスタのパフォーマンス情報を入手できます。データの継続性収集サイクルが完了すると、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（デフォルトでは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、新しいクラスタを複数追加する場合は、データの継続性収集のポーリングが同時に多数のクラスタで実行されないように、時間差をつけて追加するようにしてください。また、データの継続性収集期間にUnified Managerを再起動すると、収集が停止し、その間のデータがパフォーマンス グラフに表示されません。



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

関連情報

["CAの署名を受けて返されたHTTPS証明書のインストール"](#)

アラート通知を送信するようにUnified Managerを構成する

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。

開始する前に

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設定することを検討する必要があります。

手順

1. ["イベント通知を設定"](#)。

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

2. "リモート認証を有効にする"。

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"。

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

4. "ユーザーを追加する"。

さまざまなタイプのローカル ユーザやリモート ユーザを追加し、特定のロールを割り当てることができます。アラートを作成する際に、アラート通知を受信するユーザを指定します。

5. "アラートを追加する"。

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

イベント通知を設定

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サーバの設定や、さまざまな通知メカニズムの設定が可能です。たとえば、アラート通知はEメールやSNMPトラップとして送信できます。

開始する前に

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

送信されたアラート通知の「From」フィールドに電子メール アドレスが表示されます。何らかの理由でEメールを配信できない場合の不達メールの送信先としても使用されます。

- SMTPサーバのホスト名とアクセスに使用するユーザ名およびパスワード
- 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

トラップの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、[全般] > [通知] をクリックします。

2. [通知] ページで、該当する項目を設定します。

注記:

- 送信元アドレスに「ActiveIQUnifiedManager@localhost.com」というアドレスが事前に入力されている場合は、すべての電子メール通知が正常に配信されるように、実際に機能する電子メール アドレスに変更する必要があります。
- SMTPサーバのホスト名を解決できない場合は、SMTPサーバのホスト名の代わりにIPアドレス（IPv4 またはIPv6）を指定できます。

3. *保存*をクリックします。

4. **STARTTLS** を使用する または **SSL** を使用する オプションを選択した場合は、保存 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てください。既存の証明書の有効期限が切れている場合は、[**STARTTLS** を使用する] または [**SSL** を使用する] ボックスのチェックを外し、通知設定を保存し、[**STARTTLS** を使用する] または [**SSL** を使用する] ボックスを再度チェックして新しい証明書を表示します。

リモート認証を有効にする

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。

開始する前に

アプリケーション管理者のロールが必要です。



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

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

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



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

手順

1. 左側のナビゲーション ペインで、[全般] > [リモート認証] をクリックします。

2. *リモート認証を有効にする...*のボックスをチェックします。

3. [認証サービス] フィールドで、サービスの種類を選択し、認証サービスを設定します。

認証タイプの場合...	次の情報を入力してください...
Active Directory	• 認証サーバの管理者の名前（次のいずれかの形式を使用） ◦ domainname\username ◦ username@domainname ◦ Bind Distinguished Name（適切なLDAP表記を使用） • 管理者のパスワード • ベース識別名（適切なLDAP表記を使用）
オープンLDAP	• バインド識別名（適切なLDAP表記を使用） • パスワードをバインドする • ベース識別名

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

認証サーバの設定で[セキュアな接続を使用]オプションを選択すると、Unified Managerと認証サーバの間の通信にSecure Sockets Layer（SSL）プロトコルが使用されます。

4. オプション: 認証サーバーを追加し、認証をテストします。
5. *保存*をクリックします。

リモート認証からネストされたグループを無効にする

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。

開始する前に

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

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

手順

1. 左側のナビゲーション ペインで、[全般] > [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*のボックスをチェックします。
3. *保存*をクリックします。

認証サービスを設定する

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

開始する前に

- 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、[全般] > [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。

選択した場合...	操作
Active Directory	a. 管理者の名前とパスワードを入力します。 b. 認証サーバのベース識別名を指定します。 たとえば、認証サーバーのドメイン名が <code>ou@domain.com</code> の場合、基本識別名は <code>cn=ou,dc=domain,dc=com</code> になります。
OpenLDAP	a. バインド識別名とバインド パスワードを入力します。 b. 認証サーバのベース識別名を指定します。 たとえば、認証サーバーのドメイン名が <code>ou@domain.com</code> の場合、基本識別名は <code>cn=ou,dc=domain,dc=com</code> になります。
その他	a. バインド識別名とバインド パスワードを入力します。 b. 認証サーバのベース識別名を指定します。 たとえば、認証サーバーのドメイン名が <code>ou@domain.com</code> の場合、基本識別名は <code>cn=ou,dc=domain,dc=com</code> になります。 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。 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。



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*をクリックします。

認証サーバを追加する

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。

開始する前に

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

追加する認証サーバがハイアベイラビリティ（HA）ペアを構成している（同じデータベースを使用している）場合は、パートナーの認証サーバも追加できます。これにより、どちらかの認証サーバが到達不能になったときに、管理サーバはパートナーと通信できます。

手順

1. 左側のナビゲーション ペインで、[全般] > [リモート認証] をクリックします。
2. *安全な接続を使用する*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	a. *安全な接続を使用する*オプションを選択します。 b. 認証サーバー領域で、[追加] をクリックします。 c. [認証サーバの追加]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。 d. [ホストの承認]ダイアログ ボックスで、[証明書を表示]をクリックします。 e. [証明書の表示] ダイアログ ボックスで証明書情報を確認し、[閉じる] をクリックします。 f. [ホストの承認] ダイアログ ボックスで、[はい] をクリックします。  *セキュア接続認証を使用する*オプションを有効にする と、Unified Manager は認証サーバと通信し、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。
無効にする	a. *安全な接続を使用する*オプションをオフにします。 b. 認証サーバー領域で、[追加] をクリックします。 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）を指定し、ポートの詳細を指定します。 d. *[追加]*をクリックします。

追加した認証サーバが[サーバ]領域に表示されます。

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

認証サーバーの構成をテストする

認証サーバの設定を検証し、管理サーバと通信できるかどうかを確認することができます。具体的には、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、設定されている情報を使用して認証を実行します。

開始する前に

- リモート ユーザまたはリモート グループをUnified Managerサーバで認証できるように、リモート認証を有効にし、認証サービスを設定しておく必要があります。
- 認証サーバのリモート 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、認証サーバのプライマリ グループに属するリモートユーザの認証の検証では、認証結果にプライマリ グループに関する情報は表示されません。

手順

1. 左側のナビゲーション ペインで、[全般] > [リモート認証] をクリックします。
2. *認証テスト*をクリックします。
3. [ユーザーのテスト] 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、[テスト] をクリックします。

リモート グループを認証する場合、パスワードは入力しないでください。

アラートを追加する

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。

開始する前に

- イベントが生成されたときに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。

アラートは、ここで説明する手順に従って[アラート セットアップ] ページで作成できるほか、イベントを受け取ったあとに[イベントの詳細] ページで直接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、ストレージ管理 > アラート設定 をクリックします。
2. アラート設定ページで、[追加] 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、アラートの名前と説明を入力します。
4. *リソース* をクリックし、アラートに含めるまたはアラートから除外するリソースを選択します。

*名前に含まれる*フィールドにテキスト文字列を指定してフィルターを設定し、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利用可能 なリソースのリストに表示されます。テキスト文字列の指定では、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. *イベント*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. アクション をクリックし、通知するユーザーを選択し、通知頻度を選択し、トラップ受信者に SNMP ト ラップを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。



該当するユーザのEメール アドレスを変更し、その後アラートを編集するために開くと、[名前]フィールドは空欄になります。これは、Eメールが変更されたことでユーザとのマッ ピングが無効になったためです。また、選択したユーザのEメール アドレスを[ユーザ]ペー ジで変更した場合、変更後のEメール アドレスは反映されません。

SNMPトラップを使用してユーザに通知することもできます。

7. *保存*をクリックします。

アラートの追加例

ここでは、次の要件を満たすアラートを作成する例を示します。

- 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が含まれ、名前に「xyz」が含まれるすべてのボ リュームが除外されます
- イベント: 健全性に関するすべての重大なイベントを対象に含める
- アクション: 「sample@domain.com」と「Test」 スクリプトが含まれており、ユーザーに15分ごとに通 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. 名前に「abc」が含まれるボリュームを表示するには、「名前を含む」フィールドに **abc** と入力しま す。
 - b. を選択<<All Volumes whose name contains 'abc'>> を [使用可能なリソース] 領域から選択し、[選 択したリソース] 領域に移動します。
 - c. *除外*をクリックし、*名前に含まれる*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、イベントの重大度フィールドから*重大*を選択します。
4. [一致するイベント] 領域から すべての重要なイベント を選択し、[選択したイベント] 領域に移動します。

5. アクション*をクリックし、【これらのユーザーに警告】フィールドに ***sample@domain.com** と入力します。
6. ユーザーに 15 分ごとに通知するには、**[15 分ごとに通知]** 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*をクリックします。

ローカル ユーザのパスワードを変更

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。

開始する前に

ローカル ユーザとしてログインする必要があります。

リモート ユーザとメンテナンス ユーザのパスワードについては、この手順では変更できません。リモート ユーザのパスワードを変更するには、パスワードの管理者に連絡してください。メンテナンスユーザーのパスワードを変更するには、"[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. 上部のメニューバーから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 ユーザーの場合、[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*をクリックします。

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

アクティブでないセッションのタイムアウトを設定

Unified Manager の非アクティブ タイムアウト値を指定して、一定時間非アクティブになった後にセッションが自動的に終了されるようにすることができます。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。

開始する前に

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。



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

手順

1. 左側のナビゲーション ペインで、[全般] > [機能の設定*] 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 タイムアウトを指定します。

状況	操作
タイムアウトを設定しない（セッションを自動的に閉じない）	*「非アクティブ タイムアウト」パネルで、スライダー 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（分）を設定する	*[非アクティブ タイムアウト] パネルで、スライダー ボタンを右 (オン) に移動し、非アクティブ タイムアウト値を分単位で指定して、[適用] をクリックします。

CLI経由でセッションタイムアウトを設定する

CLI を使用して Unified Manager の最大セッション タイムアウト値を設定すると、一定時間後にセッションが自動的に終了されます。デフォルトでは、セッション タイムアウトは最大値の 4,320 分 (72 時間) に設定されています。つまり、ログインして Unified Manager をアクティブに使用している場合でも、セッションは 72 時間後に自動的に終了します。

タスク概要

アプリケーション管理者のロールが必要です。

セッション タイムアウト設定は、ログインしているすべてのユーザー セッションに影響します。

手順

1. 次のコマンドを入力してUnified Manager CLIにログインします。`um cli login`指示。認証には有効なユーザー名とパスワードを使用してください。
2. 入力してください `um option set max.session.timeout.value=<in mins>`セッション タイムアウト値を変更するコマンド。

Unified Managerの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ー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、Microsoft Windowsサーバのいずれで実行しているかによって異なります。

Unified Manager仮想アプライアンスのホスト名を変更する

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

開始する前に

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

Unified Manager Web UIには、ホスト名（またはホストのIPアドレス）を使用してアクセスできます。導入時に静的IPアドレスを使用してネットワークを設定した場合は、指定したネットワーク ホストの名前を使用します。DHCPを使用してネットワークを設定した場合は、DNSからホスト名を取得します。DHCP または DNS が適切に構成されていない場合、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、ホスト名の変更時に新しい証明書を生成する必要はありません。ただし、証明書のホスト名が実際のホスト名と同じになるように証明書を更新することを推奨します。

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

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

手順

1. HTTPSセキュリティ証明書を生成する

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

2. Unified Manager仮想マシンを再起動する

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を生成する

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、既存の証明書を置き換えることができます。

開始する前に

アプリケーション管理者のロールが必要です。

証明書を再生成する理由はいくつもあります。たとえば、識別名（DN）をより適切な値に変更する場合、キーのサイズを大きくする場合、有効期限を延長する場合、現在の証明書の有効期限が切れた場合などです。

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。を使用する場合 `Reset Server Certificate` メンテナンス コンソールからオプションを選択すると、397 日間有効な新しい HTTPS 証明書が作成されます。また、RSAキーのサイズは2048ビットに設定されます。

手順

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

[HTTPS証明書の再生成]ダイアログ ボックスが表示されます。

- 3. 証明書を生成する方法に応じて、次のいずれかを実行します。

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*オプションをクリックします。

状況	操作
別の値で証明書を生成する	*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。 [共通名]フィールドと[別名]フィールドについては、新しい値を入力しなければ既存の証明書の値が使用されます。「Common Name」はホストの FQDN に設定する必要があります。それ以外のフィールドの値は必須ではありませんが、必要に応じて[Eメール]、[会社]、[部門]、[市町村]、[都道府県]、[国]などの値を入力し、証明書に表示することができます。利用可能なキー サイズ (キー アルゴリズムは「RSA」です) と有効期間を選択することもできます。  • キーサイズの許容値は次のとおりです。2048、3072、そして4096。 • 有効期間は1日～36500日です。 ただし、推奨される有効期間は397日（13カ月）以内です。397日を超える有効期間を選択しても、CSRをエクスポートして既知のCAから署名を受ける場合にCAからは有効期間が397日に削減され署名済み証明書が返されます。 • 証明書の[別名]フィールドにローカルの識別情報を含めない場合は、[ローカルの識別情報を除外する（ローカルホストなど）]チェックボックスを選択します。このチェックボックスを選択すると、このフィールドで入力した情報だけが[別名]フィールドで使用されます。このフィールドを空白にした場合は、[別名]フィールドのない証明書が生成されます。

4. 証明書を再生成するには、[はい] をクリックします。
5. 新しい証明書を有効にするためにUnified Managerサーバを再起動します。
6. HTTPS証明書を表示して新しい証明書の情報を確認します。

Unified Manager仮想マシンを再起動する

仮想マシンは、Unified Managerのメンテナンス コンソールから再起動できます。新しい

セキュリティ証明書を生成した場合や仮想マシンで問題が発生した場合、仮想マシンの再起動が必要になります。

開始する前に

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。

ゲストの再起動 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 の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。

開始する前に

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

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

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

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

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

手順

1. 変更するUnified Managerシステムにrootユーザとしてログインします。
2. 次のコマンドを入力して、Unified Managerソフトウェアと関連するMySQLソフトウェアを停止します。

```
systemctl stop ocieau ocie mysqld
```

3. Linuxを使用してホスト名を変更する `hostnamectl` 指示：

```
hostnamectl set-hostname new_FQDN
```



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

4. サーバのHTTPS証明書を再生成します。

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

5. ネットワーク サービスを再起動します。

```
systemctl restart NetworkManager.service
```

6. 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
```

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

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

```
systemctl start mysqld ocie ocieau
```

ポリシーベースのストレージ管理を有効または無効にする

Unified Manager 9.7 以降では、ONTAPクラスタ上でストレージ 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 レベルに基づいてそれらの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、QoS ポリシーをアタッチする機能に似ていますが、Unified Manager を使用して適用すると、Unified Manager インスタンスが監視しているすべてのクラスタにわたって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することができます。

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

新しいコンテンツ	Location
新しいワークロードのプロビジョニング ページ	共通タスク > *プロビジョニング*から利用可能
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 レベルから利用できます
パフォーマンス ストレージ効率ポリシーの作成ページ	設定 > ポリシー > ストレージ効率 から利用できます

新しいコンテンツ	Location
現在のワークロード パフォーマンスとワークロード IOPS を説明するパネル	ダッシュボード

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

手順

1. 左側のナビゲーション ペインで、[全般] > [機能の設定*] 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、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、スライダー ボタンを左に移動します。
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、スライダー ボタンを右に移動します。

Unified Manager バックアップを構成する

ホスト システムで実行される一連の設定手順とメンテナンス コンソールを通じて、Unified Manager のバックアップ機能を設定できます。

設定手順については、以下を参照してください。["バックアップとリストア処理の管理"](#)。

機能設定を管理します

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



[機能設定]ページは、アプリケーション管理者ロールが割り当てられたユーザだけが使用できません。

スクリプトのアップロードについては、以下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を有効にする

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) に基づいたストレージ管理が可能になります。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るONTAPクラスタのストレージワークロードをプロビジョニングし、割り当てられたパフォーマンス サービス レベルとストレージ効率化ポリシーに基づいてワークロードを管理できます。

この機能は、一般 > 機能設定 > ポリシーベースのストレージ管理 から有効または無効にすることができます。この機能を有効にすると、次のページを操作および監視できるようになります。

- [プロビジョニング]ページ（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
- クラスタ設定ページの「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」列
- *ダッシュボード*のワークロードパフォーマンスパネル

これらのページを使用して、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、割り当てられたパフォーマンス サービス レベルに準拠したストレージワークロードと準拠しないストレージワークロードを監視することもできます。ワークロード パフォーマンス パネルとワークロード IOPS パネルでは、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、データセンター全体のクラスタの合計、使用可能、使用済みの容量とパフォーマンス (IOPS) を評価することもできます。

この機能を有効にすると、メニュー バー > ヘルプ ボタン > **API** ドキュメント > ストレージ プロバイダー カテゴリから、Unified Manager REST API を実行して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URLを+https://<hostname>/docs/api/+の形式で入力してREST APIページにアクセスすることもできます。

APIの詳細については、以下を参照してください。"[Active IQ Unified Manager REST APIでの作業の開始](#)"。

API ゲートウェイを有効にする

API ゲートウェイ機能を使用すると、Active IQ Unified Manager を単一のコントロールプレーンとして使用し、個別にログインすることなく複数のONTAPクラスタを管理できるようになります。

この機能は、Unified Manager に初めてログインしたときに表示される構成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 はONTAP REST API とは異なり、Unified Manager REST API を使用しても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 に公開されていない特定の機能を管理するためにONTAP API にアクセスするという特定のビジネス要件がある場合は、API ゲートウェイ機能を有効にしてONTAP API を実行できます。ゲートウェイは、ヘッダーと本文の形式をONTAP APIと同じにすることで、API要求をトンネリングするプロキシとして機能します。Unified Manager の認証情報を使用して特定の API を実行し、個々のクラスタ認証情報を渡すことなくONTAPクラスタにアクセスして管理できます。Unified Manager は、Unified Manager インスタンスによって管理されるONTAPクラスタ全体で 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から返される応答は、対応するONTAP REST APIをONTAPから直接実行した場合と同じです。

この機能を有効にすると、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REST APIページにアクセ

スするためのURLを次の形式で入力することもできます。 <https://<hostname>/docs/api/>

APIの詳細については、以下を参照してください。"[Active IQ Unified Manager REST APIでの作業の開始](#)"。

非アクティブタイムアウトを指定する

Active IQ Unified Managerの非アクティブ タイムアウト値を指定できます。操作がない状態で指定した時間が経過すると、アプリケーションから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。

この機能を無効にしたり、一般 > 機能設定 > 非アクティブタイムアウト から時間を変更したりできます。この機能を有効にしたら、**LOGOUT AFTER** フィールドに非アクティブ時間の制限 (分単位) を指定する必要があります。この時間が経過すると、システムは自動的にログアウトします。デフォルト値は4320分（72時間）です。



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

Active IQ ポータル イベントを有効にする

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。この設定により、Active IQポータルはシステム構成やケーブル接続などに関する追加イベントを検出して表示できるようになります。このオプションはデフォルトで有効になっています。

この機能を有効にすると、Active IQ Unified Manager はActive IQポータルによって検出されたイベントを表示します。イベントはすべての監視対象ストレージ システムから生成されたAutoSupportメッセージに対して一連のルールを実行することによって作成されます。これらのイベントは他の Unified Manager 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またはリスクを識別します。

この機能は、一般 > 機能設定 > **Active IQ**ポータル イベント から有効または無効にすることができます。外部ネットワークにアクセスできないサイトでは、ストレージ管理 > イベント設定 > ルールのアップロード からルールを手動でアップロードする必要があります。

この機能はデフォルトで有効になっています。この機能を無効にすると、Active IQイベントが Unified Manager で検出または表示されなくなります。無効になっている場合は、この機能を有効にすると、Unified Manager はクラスタのタイムゾーンの定義済み時刻である 00:15 にクラスタ上のActive IQイベントを受信できるようになります。

コンプライアンスのためのセキュリティ設定を有効または無効にする

機能設定ページの セキュリティ ダッシュボード パネルの カスタマイズ ボタンを使用すると、Unified Manager でのコンプライアンス監視のセキュリティ パラメータを有効または無効にすることができます。

このページでどの設定を有効または無効にするかで、クラスタとStorage VMのUnified Managerでの全体的なコンプライアンス ステータスが決まります。選択内容に応じて、クラスター インベントリ ページの セキュリティ: すべてのクラスター ビューと、ストレージ VM インベントリ ページの セキュリティ: すべてのストレージ **VM** ビューに、対応する列が表示されます。



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、ストレージVM、ボリュームのセキュリティ基準は、"[NetApp ONTAP 9セキュリティ設定ガイド](#)"。ダッシュボードの[セキュリティ]パネル、および[セキュリティ]ページに、クラスタ、Storage VM、およびボリュームのデフォルトのセキュリティ コンプライアンス ステータスが表示されます。また、セキュリティ違反があるクラスタとStorage VMに対してセキュリティ イベントが生成され、管理操作を実行できるようになります。

セキュリティ設定をカスタマイズする

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. [全般] > [機能設定] > [セキュリティ ダッシュボード] > [カスタマイズ] をクリックします。*セキュリティ ダッシュボード設定のカスタマイズ*ポップアップが表示されます。



有効または無効にしたセキュリティ コンプライアンス パラメータは、[クラスタ]ページと[Storage VM]ページ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します。これらのページからExcelレポートをアップロードしたあとにセキュリティ パラメータを変更した場合、ダウンロードしたExcelレポートに誤った情報が含まれることがあります。

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、クラスタ の下に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、以下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. ストレージ VM のカスタム設定を有効または無効にするには、ストレージ **VM** の下に必要な一般設定を選択します。ストレージVMコンプライアンスをカスタマイズするためのオプションについては、以下を参照してください。"[Storage VMのコンプライアンス カテゴリ](#)"。

AutoSupportと認証設定をカスタマイズする

- AutoSupport設定* セクションでは、ONTAPからAutoSupportメッセージを送信するために HTTPS トランSPORTを使用するかどうかを指定できます。

*認証設定*セクションから、デフォルトのONTAP管理者ユーザーに対して Unified Manager アラートを発生させることができます。

スクリプトのアップロードを有効または無効にする

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操作を禁止したい場合は、この機能を無効にすることができます。

開始する前に

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、[全般] > [機能の設定*] 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、スライダーボタンを左に移動します。
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、スライダーボタンを右に移動します。

ログインバナーを追加

ログイン バナーを追加して、システムへのアクセスを許可されているユーザや利用条件などの情報をログインとログアウトの際に表示することができます。

このログイン バナーのポップアップは、ストレージのオペレータや管理者などのすべてのユーザに対して、ログイン、ログアウト、セッション タイムアウトの際に表示されます。

メンテナンスコンソールを使用する

メンテナンス コンソールを使用すると、ネットワーク設定を構成したり、Unified Manager がインストールされているシステムを構成し管理したり、発生する可能性のある問題を防止およびトラブルシューティングするのに役立つその他のメンテナンス タスクを実行したりできます。

メンテナンス コンソールで提供される機能

Unified Manager メンテナンス コンソールを使用すると、Unified Manager システムの設定を維持し、問題の発生を防ぐために必要な変更を加えることができます。

Unified Manager がインストールされているオペレーティング システムに応じて、メンテナンス コンソールは次の機能を提供します。

- 仮想アプライアンスに関する問題のトラブルシューティング（特にUnified Manager Webインターフェイスが利用できない場合）
- Unified Manager の新しいバージョンにアップグレードする
- 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
- パフォーマンス統計の送信を目的とした外部データ プロバイダへの接続
- 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 Unified Manager データベースと構成設定を復元します。

メンテナンス ユーザの役割

Unified ManagerをRed Hat Enterprise Linux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 ユーザー名は「umadmin」ユーザーです。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を割り当てられ、他のユーザを作成してロールを割り当てることができます。

メンテナンス ユーザまたはumadminユーザは、Unified Managerのメンテナンス コンソールにもアクセスできます。

診断ユーザの権限

診断アクセスの目的は、テクニカル サポートからトラブルシューティングのサポートを受けられるようにすることです。このため、テクニカル サポートから指示された場合にのみ診断アクセスを使用する必要があります。

診断ユーザは、テクニカル サポートからの指示を受けて、トラブルシューティングの目的でOSレベルのコマンドを実行できます。

メンテナンス コンソールへのアクセス

Unified Managerユーザ インターフェイスが動作状態でない場合、またはこのユーザ インターフェイスにない機能を実行する必要がある場合は、メンテナンス コンソールにアクセスしてUnified Managerシステムを管理できます。

開始する前に

Unified Managerをインストールして設定しておく必要があります。

15分間操作しないと、メンテナンス コンソールからログアウトされます。



VMwareにインストールした場合、VMwareコンソールからメンテナンス ユーザとしてすでにログインしているときは、Secure Shellを使用して同時にログインできません。

手順

1. 次の手順に従ってメンテナンス コンソールにアクセスします。

このオペレーティング システムでは...	次の手順に従ってください...
VMware	a. Secure Shellを使用して、Unified Manager仮想アプライアンスのIPアドレスまたは完全修飾ドメイン名に接続します。 b. メンテナンス ユーザ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。

このオペレーティング システムでは...	次の手順に従ってください...
Linux	a. Secure Shellを使用して、Unified ManagerシステムのIPアドレスまたは完全修飾ドメイン名に接続します。 b. メンテナンス ユーザ（umadmin）の名前とパスワードでシステムにログインします。 c. コマンドを入力してください `maintenance_console` Enter キーを押します。
Windows	a. 管理者のクレデンシャルでUnified Managerシステムにログインします。 b. Windows管理者としてPowerShellを起動します。 c. コマンドを入力してください `maintenance_console` Enter キーを押します。

Unified Managerメンテナンス コンソール メニューが表示されます。

vSphere VM コンソールを使用してメンテナンス コンソールにアクセスする

Unified Managerユーザ 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。

開始する前に

- メンテナンス ユーザー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見つけます。
2. *コンソール*タブをクリックします。
3. コンソール ウィンドウ内をクリックしてログインします。
4. ユーザ名とパスワードを使用してメンテナンス コンソールにログインします。

15分間操作しないと、メンテナンス コンソールからログアウトされます。

メンテナンス コンソールのメニュー

メンテナンス コンソールは、Unified Manager サーバーの特別な機能と構成設定を保守および管理できるさまざまなメニューで構成されています。

Unified Manager がインストールされているオペレーティング システムに応じて、メンテナンス コンソールは次のメニューで構成されます。

- Upgrade Unified Manager (VMwareのみ)
- Network Configuration (VMwareのみ)
- System Configuration (VMwareのみ)
 - a. Support/Diagnostics
 - b. Reset Server Certificate
 - c. External Data Provider
 - d. Backup Restore
 - e. Performance Polling Interval Configuration
 - f. SAML認証を無効にする
 - g. View/Change Application Ports
 - h. Debug Log Configuration
 - i. Control access to MySQL port 3306
 - j. 出口

希望するメニュー オプションの番号をリストから選択します。たとえば、バックアップと復元の場合は、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することができます。このメニューは、Unified Managerユーザ インターフェイスを使用できない場合に使用してください。



Unified ManagerがRed Hat Enterprise Linux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。

表示されるメニュー項目は次のとおりです。

- **IPアドレス設定を表示**

仮想アプライアンスの現在のネットワーク設定が表示されます (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)。

- **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を変更することができます (IPアドレス、ネットマスク、ゲートウェイ、DNSサーバなど)。メンテナンス コンソールでネットワーク設定をDHCPから静的ネットワークに切り替えた場合は、ホスト名を編集できません。変更を反映するには、[変更をコミット]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を変更**

ホスト名を解決する際に検索するドメイン名を変更することができます。変更を反映するには、[変更をコミット]を選択する必要があります。

- 静的ルートを表示

現在の静的ネットワーク ルートが表示されます。

- 静的ルートを変更する

静的ネットワーク ルートを追加または削除することができます。変更を反映するには、[変更をコミット]を選択する必要があります。

- ルートを追加

静的ルートを追加することができます。

- ルートを削除

静的ルートを削除することができます。

- 戻る

メイン メニュー に戻ります。

- 出口

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ースを無効にする

使用可能なネットワーク インターフェースを無効にします。使用可能なネットワーク インターフェースが1つしかない場合は、それを無効にすることはできません。変更を反映するには、[変更をコミット]を選択する必要があります。

- ネットワークインターフェースを有効にする

使用可能なネットワーク インターフェースを有効にします。変更を反映するには、[変更をコミット]を選択する必要があります。

- 変更をコミット

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、必ずこのオプションを選択します。そうしないと、変更は適用されません。

- ホストにpingを送信

IPアドレスの変更やDNS設定を確認するために、ターゲット ホストにpingを実行します。

- デフォルト設定に戻す

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。変更を反映するには、[変更をコミット]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。

- 出口

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]メニューには、仮想アプライアンスを管理するためのさまざまなオプションが用意されています（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）。



Unified Manager が Linux または Microsoft Windows システムにインストールされている場合、このメニューからは「Unified Manager バックアップからの復元」オプションのみが使用できません。

表示されるメニュー項目は次のとおりです。

- サーバステータスの表示

現在のサーバ ステータスを表示します。ステータスには「Running」と「Not Running」があります。

サーバが実行されていない場合は、テクニカル サポートに連絡することを推奨します。

- 仮想マシンを再起動

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。

- 仮想マシンをシャットダウン

すべてのサービスを停止して仮想マシンをシャットダウンします。

このオプションは、仮想マシン コンソールからのみ選択できます。

- <ログインユーザー>のユーザーパスワードを変更する

現在ログインしているユーザ（メンテナンス ユーザ）のパスワードを変更します。

- データディスクサイズの増加

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。

- スワップディスクのサイズを増やす

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の場所に変更します。

- **NTPサーバーの変更**

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

- **NTPサービスの変更**

切り替える `ntp` として `systemd-timesyncd` サービス。

- **Unified Manager** バックアップからの復元

以前にバックアップしたバージョンから Unified Manager データベースと構成設定を復元します。

- **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。

- **ホスト名を変更する**

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]メニューを終了して[Main Menu]に戻ります。

- **出口**

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

「サポートと診断」メニューを使用すると、トラブルシューティングの支援のためにテクニカル サポートに送信できるサポート バンドルを生成できます。

表示されるメニュー オプションは次のとおりです。

- **ライトサポートバンドルを生成する**

30日分のログと構成データベース レコードのみを含む軽量のサポート バンドル（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）を作成できます。

- **サポートバンドルの生成**

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、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。

ファイルには、AutoSupportメッセージによって生成された情報、Unified Manager データベースの内容、Unified Manager サーバ内部の詳細データ、およびAutoSupportメッセージや軽量サポート バンドルに通常は含まれない詳細レベルのログが含まれます。

その他のメニュー オプション

次のメニュー オプションを使用すると、Unified Manager サーバー上でさまざまな管理タスクを実行できます。

表示されるメニュー項目は次のとおりです。

- 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 GUI で [一般] > [HTTPS 証明書] > [HTTPS 証明書の再生成] をクリックすると、サーバ証明書を再生成できます。

- **SAML**認証を無効にする

SAML 認証を無効にして、アイデンティティ プロバイダー (IdP) が Unified Manager GUI にアクセスするユーザーに対してサインオン認証を提供しないようにします。このコンソール オプションは通常、IdP サーバーまたは SAML 構成の問題によりユーザーが Unified Manager GUI にアクセスできない場合に使用されます。

- 外部データプロバイダー

Unified Manager を外部データ プロバイダーに接続するためのオプションを提供します。接続が確立されると、パフォーマンス データが外部サーバに送信されて、ストレージ パフォーマンスのエクスポートがサードパーティ 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。

- サーバー構成の表示 - 外部データ プロバイダーの現在の接続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 プロバイダー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できます。
- サーバー構成の変更 - 外部データ プロバイダーの新しい構成設定を入力したり、既存の設定を変更したりできます。
- サーバー接続の削除 - 外部データ プロバイダーへの接続を削除します。

接続を削除すると、Unified Managerは外部サーバから切断されます。

- バックアップの復元

詳細については、以下のトピックを参照してください。"[バックアップとリストア処理の管理](#)"。

- 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構成する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ためのオプション

ョンを提供します（セキュリティ上必要である場合）。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する**

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、Linux、Windows、およびVMware vSphereシステムへのUnified Managerの新規インストール中は、このポートを使用したアクセスはローカル ホストに限定されます。このオプションを使用すると、このポートの認識をローカル 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、このオプションをローカル ホストに対してのみ有効にすると、リモート ホストでポート3306を使用できるようにすることができます。逆に、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ローカル ホストに限定できます。アップグレード前にリモート ホストでアクセスが有効になっていれば、アップグレード後もその設定が維持されます。ポートの認識を切り替えたら、Windowsシステムのファイアウォール設定を確認し、MySQLポート3306へのアクセスが制限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。

- **出口**

メンテナンス コンソール メニューを終了します。

Windowsでメンテナンスユーザーのパスワードを変更する

必要に応じて、Unified Manager メンテナンス ユーザーのパスワードを変更できます。

手順

1. Unified Manager Web UI ログイン ページで、[パスワードを忘れた場合] をクリックします。

パスワードをリセットするユーザの名前を入力するように求めるページが表示されます。

2. ユーザー名を入力し、「送信」をクリックします。

入力したユーザ名に定義されているEメール アドレスに、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メールが送信されます。

3. メール内の*パスワードリセットリンク*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umadminパスワードを変更する

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。このパスワードは、必要に応じてあとからいつでも再変更できます。

開始する前に

- Unified ManagerがRed Hat Enterprise 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、インストール後に変更できます（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。

開始する前に

Unified Managerサーバのメンテナンス コンソールへのログインが許可されているユーザIDとパスワードが必要です。



Mozilla FirefoxまたはGoogle Chromeブラウザでは、安全でないとみなされるポートがいくつかあります。HTTPトラフィックとHTTPSトラフィックに新しいポート番号を割り当てる前にブラウザで確認してください。安全でないポートを選択すると、システムにアクセスできなくなる可能性があります。その場合、カスタマー サポートに連絡して解決を依頼する必要があります。

ポートを変更するとUnified Managerのインスタンスが自動的に再起動されるため、システムを短時間停止しても問題のないタイミングであることを確認してください。

1. SSHを使用して、Unified Managerホストにメンテナンス ユーザとしてログインします。

Unified Managerメンテナンス コンソールのプロンプトが表示されます。

2. アプリケーション ポートの表示/変更 というメニュー 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した場合は、プロトコルのデフォルトの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. ポートを変更して Unified Manager を再起動するには、「y」と入力します。
6. メンテナンス コンソールを終了します。

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

ネットワークインターフェースを追加する

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。

開始する前に

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、システム構成 > オペレーティング システムの再起動 を選択します。

再起動すると、新たに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 > ネットワーク インターフェースの有効化 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** を押します。

eth1 を選択し、**Enter** を押します。

5. ネットワーク インターフェイスを有効にするには、**y** と入力します。
6. ネットワークの設定を入力します。

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、ネットワークの設定を入力するよう求められます。

ネットワーク設定を入力すると、自動的に*ネットワーク構成*メニューに戻ります。

7. *変更をコミット*を選択します。

ネットワーク インターフェイスを追加するには、変更をコミットする必要があります。

Unified Managerデータベースディレクトリにディスクスペースを追加する

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は、すべてUnified Managerデータベース ディレクトリに格納されます。状況によっては、データベース ディレクトリのサイズの拡張が必要になることがあります。

たとえば、Unified Managerで多数のクラスタからデータを収集している場合、各クラスタに大量のノードがあると、データベース ディレクトリがいっぱいになることがあります。データベース ディレクトリの容量の95%に達すると警告イベントが生成され、95%に達すると重大イベントが生成されます。



ディレクトリの容量の95%に達すると、クラスタからデータが収集されなくなります。

データ ディレクトリの容量を追加する手順は、Unified ManagerをVMware ESXiサーバ、Red Hatサー

バ、Microsoft Windowsサーバのいずれで実行しているかによって異なります。

Linuxホストのデータディレクトリにスペースを追加する

十分なディスク容量がない場合は、`/opt/netapp/data` Linuxホストを最初にセットアップしてUnified ManagerをインストールしたときにUnified Managerをサポートするためにディレクトリを作成した場合、インストール後にディスク容量を増やすことでディスク容量を追加できます。`/opt/netapp/data`ディレクトリ。`

開始する前に

Unified ManagerがインストールされているRed Hat Enterprise Linuxマシンへのrootユーザ アクセスが必要です。

データ ディレクトリのサイズを拡張する前にUnified Managerデータベースをバックアップすることを推奨します。

手順

1. ディスク スペースを追加するLinuxマシンにrootユーザとしてログインします。
2. Unified Managerサービスと関連するMySQLソフトウェアを次の順序で停止します。

```
systemctl stop ocieau ocie mysqld
```

3. 一時的なバックアップフォルダを作成します（例：`/backup-data`）現在のデータを格納するのに十分なディスク容量を持つ`/opt/netapp/data`ディレクトリ。`
4. 既存のコンテンツと権限設定をコピーします`/opt/netapp/data`ディレクトリをバックアップデータディレクトリに変更します。`

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

5. SE Linuxが有効になっている場合は、次の手順を実行します。

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

```
se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |  
head -1
```

次のような情報が返されます。

```
echo $se_type  
mysqld_db_t
```

- a. `chcon`コマンドを実行して、バックアップ ディレクトリに対してSE Linuxタイプを設定します。

```
chcon -R --type=mysqld_db_t /backup-data
```

6. 内容を削除する`/opt/netapp/data`ディレクトリ：`

- a. `cd /opt/netapp/data`

b. `rm -rf *`

7. サイズを拡大する `/opt/netapp/data` LVM コマンドまたはディスクの追加によって、ディレクトリを最低 150 GB まで拡張します。



作成した場合は `/opt/netapp/data` ディスクからマウントしようとしないでください `/opt/netapp/data` NFS または CIFS 共有として。この場合、ディスクスペースを拡張しようとする、次のようなLVMコマンドが実行される可能性があるためです。`resize`そして`extend`期待通りに動作しない可能性があります。

8. 確認する `/opt/netapp/data` ディレクトリの所有者 (mysql) とグループ (root) は変更されません。

```
ls -ltr /opt/netapp/ | grep data
```

次のような情報が返されます。

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. SE Linuxが有効になっている場合は、`/opt/netapp/data` ディレクトリは引き続き `mysqld_db_t` に設定されています:

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

10. ファイルabcを削除して、この無駄なファイルがデータベース エラーの原因にならないようにします。

11. バックアップデータの内容を拡張されたファイルにコピーします。 `/opt/netapp/data` ディレクトリ:

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

12. SE Linuxが有効になっている場合は、次のコマンドを実行します。

```
chcon -R --type=mysqld_db_t /opt/netapp/data
```

13. MySQLサービスを開始します。

```
systemctl start mysqld
```

14. MySQLサービスが開始されたら、ocieサービスとocieauサービスを次の順序で開始します。

```
systemctl start ocie ocieau
```

15. すべてのサービスが開始されたら、バックアップフォルダを削除します。 `/backup-data`:

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

VMware仮想マシンのデータディスクにスペースを追加する

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メンテナンス コンソールを使用して容量を追加できます。

開始する前に

- vSphere Clientへのアクセス権が必要です。
- 仮想マシンにスナップショットがローカルに格納されていない必要があります。
- 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拡張する前に仮想マシンをバックアップすることを推奨します。

手順

1. vSphereクライアントで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 の展開で、データ ディスクとして「ハード ディスク 3」ではなく「ハード ディスク 2」が使用されることがあります。その場合は、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 ディスクのスペースは、常に他のディスクより大きくなります。

2. vSphere クライアントで、Unified Manager 仮想マシンを選択し、[コンソール] 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」オプションの番号を入力します。

Microsoft Windows サーバーの論理ドライブにスペースを追加します

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。

開始する前に

Windowsの管理者権限が必要です。

ディスク スペースを追加する前にUnified Managerデータベースをバックアップすることを推奨します。

手順

1. ディスク スペースを追加するWindowsサーバに管理者としてログインします。
2. スペースを追加する方法に応じて、該当する手順を実行します。

オプション	説明
物理サーバで、Unified Manager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する。	Microsoftの次のトピックの手順に従います。 "Extend a Basic Volume"
物理サーバで、ハード ディスク ドライブを追加する。	Microsoftの次のトピックの手順に従います。 "Adding Hard Disk Drives"
仮想マシンで、ディスク パーティションのサイズを拡張する。	VMwareの次のトピックの手順に従います。 "Increasing the size of a disk partition"

ユーザ アクセスの管理

Active IQ Unified Managerへのユーザ アクセスを制御するために、ロールを作成し、権限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。これらのロールと権限を持つユーザのみがUnified Managerでオブジェクトを管理できます。

ユーザーを追加する

[ユーザ]ページを使用して、ローカル ユーザまたはデータベース ユーザを追加できます。また、認証サーバに属するリモート ユーザやリモート グループを追加することもできます。追加したユーザにロールを割り当てることで、ユーザはロールの権限に基づいてUnified Managerでストレージ オブジェクトやデータを管理したり、データベースのデータを参照したりすることができます。

開始する前に

- アプリケーション管理者のロールが必要です。
- リモート ユーザまたはリモート グループを追加する場合は、リモート認証を有効にし、認証サーバを設定しておく必要があります。
- アイデンティティ プロバイダー (IdP) がグラフィカル インターフェイスにアクセスするユーザーを認証するように SAML 認証を構成する場合は、これらのユーザーが「リモート」ユーザーとして定義されていることを確認してください。

SAML 認証が有効になっている場合、タイプが「local」または「maintenance」のユーザーは UI にアクセスできません。

Windows Active Directoryのグループを追加した場合、そのグループの直接のメンバーに加え、ネストされたサブグループも（無効になっていなければ）すべてUnified Managerで認証されます。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、[全般] > [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。

ユーザに固有なEメール アドレスを指定する必要があります。複数のユーザで共有しているEメール アドレスは指定しないでください。

4. *[追加]*をクリックします。

データベースユーザーを作成する

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、統合スキーマ ロールまたはレポート スキーマ ロールを割り当てたデータベース ユーザを作成する必要があります。

開始する前に

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えます。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、[全般] > [ユーザー] をクリックします。
2. [ユーザー] ページで、[追加] をクリックします。
3. [ユーザーの追加] ダイアログ ボックスで、[タイプ] ドロップダウン リストから [データベース ユーザー] を選択します。
4. データベース ユーザの名前とパスワードを入力します。
5. *役割*ドロップダウンリストで、適切な役割を選択します。

状況	この役割を選択
Unified ManagerをWorkflow Automationに接続する場合	統合スキーマ
レポートおよびその他のデータベース ビューにアクセスする場合	レポート スキーマ

6. *[追加]*をクリックします。

ユーザー設定を編集する

ユーザごとに指定されたEメール アドレスやロールなどの設定を編集することができます。たとえば、ストレージ オペレータのユーザのロールを変更して、そのユーザにストレージ管理者の権限を割り当てることができます。

開始する前に

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した場合、次のいずれかの時点で変更内容が反映されます。

- ユーザがUnified Managerからログアウトして再度ログインしたとき
- セッションの開始から24時間が経過してタイムアウトしたとき

手順

1. 左側のナビゲーション ペインで、[全般] > [ユーザー] をクリックします。
2. 「ユーザー」 ページで、設定を編集するユーザーを選択し、「編集」をクリックします。
3. [ユーザの編集]ダイアログ ボックスで、ユーザに対して指定されている設定を編集します。
4. *保存*をクリックします。

ユーザーを表示

[ユーザ]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表示できます。ユーザに関する詳細（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）を参照できます。

開始する前に

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、[全般] > [ユーザー] をクリックします。

ユーザーまたはグループを削除する

管理サーバ データベースから1人または複数のユーザを削除して、それらのユーザが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、グループを削除すると、そのグループのすべてのユーザによる管理サーバへのアクセスを禁止できます。

開始する前に

- リモート グループを削除するときは、リモート グループのユーザに割り当てられているイベントを再割り当てしておく必要があります。

ローカル ユーザまたはリモート ユーザを削除する場合は、それらのユーザに割り当てられていたイベントの割り当てが自動的に解除されます。

- アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーション ペインで、[全般] > [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. 削除を確認するには、[はい] をクリックします。

RBACとは

RBAC（ロールベース アクセス制御）を使用すると、Active IQ Unified Managerサーバのさまざまな機能および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により、ユーザのグループを管理できます。特定の機能のアクセスを選択した管理者に制限する必要がある場合は、その管理者用の管理者アカウントを設定してください。その管理者が表示できる情報と、実行できる処理を制限する場合は、作成した管理者アカウントにロールを適用する必要があります。

管理サーバでは、ユーザ ログインとロールの権限に対してRBACを使用します。管理サーバで管理ユーザ アクセスのデフォルト設定を変更していない場合は、ログインして設定を表示する必要はありません。

特定の権限を必要とする処理を開始すると、管理サーバによってログインが求められます。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

ユーザは、アカウントの種類に基づいて、リモート ユーザ、リモート グループ、ローカル ユーザ、データベース ユーザ、およびメンテナンス ユーザの各タイプに分類されます。それぞれのタイプには、管理者ロールを持つユーザによって独自のロールが割り当てられます。

Unified Managerには次のユーザ タイプがあります。

- メンテナンスユーザー

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、他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が Red Hat Enterprise Linux システムにインストールされると、メンテナンス ユーザーに「umadmin.」というユーザー名が付与されます。

- 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。このグループの名前は、認証サーバに保存されているグループの名前と同じに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基づいて操作を実行できます。

- 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。ロールにはそれぞれ特定の権限が含まれています。Unified Manager で実行できるアクティビティの範囲は、割り当てられているロールと、そのロールに含まれる権限によって異なります。

Unified Manager には、次の定義済みのユーザー ロールが含まれています。

- オペレーター

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 システム情報やその他のデータを表示します。このロールを割り当てられたストレージ オペレータは、イベントについて、表示、割り当て、応答、解決、メモの追加などの操作が可能です。

- ストレージ管理者

Unified Manager 内でストレージ管理操作を構成します。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の設定が可能です。



Unified Manager が Linux システムにインストールされると、アプリケーション管理者ロールを持つ初期ユーザーの名前は自動的に「umadmin」になります。

- 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

このロールにより、Unified Manager データベースからのレポートやその他のデータベース ビューへの読み取り専用アクセスが直接可能になります。表示できるデータベースは次のとおりです。

- netapp_model_view
- netapp_performance
- ocum
- ocum_report
- ocum_report_birt
- opm
- scalemonitor

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	オペレーター	ストレージ管理者	アプリケーション管理者	統合スキーマ	レポートスキーマ
ストレージ システムの情報の表示	•	•	•	•	•
その他のデータ（履歴や容量の使用状況）の表示	•	•	•	•	•
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	•	•	•		
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		•	•		

機能	オペレーター	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
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 ポリシーの管理		•	•		
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との統合の 管理とデータベ ースビューへの アクセス				•	
レポートのスケ ジュール設定と 保存		•	•		
管理アクション から「Fix It」操 作を実行する		•	•		
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認証設定を管理する

リモート認証を設定したあと、Security Assertion Markup Language（SAML）認証を有効にして、Unified ManagerのWeb UIにアクセスするリモート ユーザをセキュアなアイデンティティ プロバイダ（IdP）で認証するように設定できます。

SAML認証を有効にした場合、Unified Managerのグラフィカル ユーザ インターフェイスにアクセスできるのはリモート ユーザのみです。ローカル ユーザとメンテナンス ユーザはUIにアクセスできません。この設定は、メンテナンス コンソールにアクセスするユーザには影響しません。

アイデンティティ プロバイダの要件

すべてのリモート ユーザに対して SAML 認証を実行するために ID プロバイダ (IdP) を使用するように Unified Manager を構成する場合は、Unified Manager への接続が成功するために必要な構成設定に注意する必要があります。

Unified Manager URI とメタデータを IdP サーバーに入力する必要があります。この情報は、Unified Manager の[SAML 認証]ページからコピーできます。 Unified Manager は、Security Assertion Markup Language (SAML) 標準のサービス プロバイダー (SP) と見なされます。

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) : 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

- Unified Manager がこの証明書利用者信頼エントリの ADFS SAML 応答を解析するために必要な 3 つのクレーム ルールを次の順序で定義する必要があります。

要求規則	Value
SAM-account-name	Name ID
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Token groups – Unqualified Name	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。そうしないと、Unified Manager からログアウトするときにエラーが発生する可能性があります。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[認証ポリシー]フォルダをクリックします。
 - c. 右側の[操作]で、[グローバル プライマリ認証ポリシーの編集]をクリックします。
 - d. イン트라ネット認証方法を、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 セキュリティ証明書が CA 署名されている場合、IdP 経由のログインが拒否されることがあります。この問題の対処方法は2つあります。

- 次のリンクの手順に従って、CA証明書チェーンの関連する証明書利用者についてのADFSサーバでの失効確認を無効にします。

"証明書利用者信頼ごとに失効チェックを無効にする"

- Unified Manager サーバーの証明書要求に署名するには、CA サーバーを ADFS サーバー内に配置します。

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 サーバーと Unified Manager サーバー間の時間差は 5 分を超えることはできません。5 分を超えると認証が失敗します。

SAML認証の有効化

Security Assertion Markup Language (SAML) 認証を有効にして、Unified Manager のWeb UIにアクセスするリモート ユーザをセキュアなアイデンティティ プロバイダ (IdP) で認証するように設定できます。

開始する前に

- リモート認証を設定し、正常に動作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、両方で接続の準備を完了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、[全般] > [SAML 認証] をクリックします。
2. **SAML** 認証を有効にする チェックボックスを選択します。

IdPの接続の設定に必要なフィールドが表示されます。

3. IdPのURIとUnified ManagerサーバをIdPに接続するために必要なIdPメタデータを入力します。

IdP サーバが Unified Manager サーバから直接アクセスできる場合は、IdP URI を入力した後に **[IdP メタ**

データの取得] ボタンをクリックして、IdP メタデータ フィールドに自動的に入力することができます。

4. Unified Managerのホスト メタデータURIをコピーするか、ホスト 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*をクリックします。

設定を完了してUnified Managerを再起動するかどうかの確認を求めるメッセージ ボックスが表示されます。

6. *確認してログアウト*をクリックすると、Unified Manager が再起動します。

許可されたリモート ユーザがUnified Managerのグラフィカル インターフェイスにアクセスする際にクレデンシャルを入力するページが、次回からUnified Managerのログイン ページではなくIdPのログイン ページに変わります。

まだ完了していない場合は、IdPにアクセスし、Unified ManagerサーバのURIとメタデータを入力して設定を完了します。



アイデンティティ プロバイダにADFSを使用している場合は、Unified Manager GUIでADFSのタイムアウトが考慮されず、Unified Managerのセッション タイムアウトに達するまでセッションが続行されます。一般 > 機能設定 > 非アクティブ タイムアウト をクリックすると、GUI セッション タイムアウトを変更できます。

SAML 認証に使用するIDプロバイダーを変更する

Unified Managerでリモート ユーザの認証に使用するアイデンティティ プロバイダ (IdP) を変更することができます。

開始する前に

- 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、[全般] > [SAML 認証] 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。

IdP が Unified Manager サーバーから直接アクセスできる場合は、IdP URL を入力した後に **IdP** メタデータの取得 ボタンをクリックすると、IdP メタデータ フィールドに自動的に入力されます。

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. *[構成を保存]*をクリックします。

設定を変更するかどうかの確認を求めるメッセージ ボックスが表示されます。

5. [OK]をクリックします。

新しいIdPにアクセスし、Unified ManagerサーバのURIとメタデータを入力して設定を完了します。

許可されたリモート ユーザがUnified Managerのグラフィカル インターフェイスにアクセスする際にクレデンシャルを入力するページが、次回から古いIdPのログイン ページではなく新しいIdPのログイン ページに変わります。

Unified Manager のセキュリティ証明書の変更に SAML 認証設定を更新する

Unified Manager サーバーにインストールされている HTTPS セキュリティ証明書を変更する場合は、SAML 認証構成設定を更新する必要があります。証明書が更新されるのは、ホスト システムの名前を変更した場合、ホスト システムに新しいIPアドレスを割り当てた場合、システムのセキュリティ証明書を手動で変更した場合です。

セキュリティ証明書が変更され、Unified Manager サーバーが再起動されると、SAML 認証は機能しなくなり、ユーザーは Unified Manager 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。ユーザー インターフェイスへのアクセスを再度有効にするには、IdP サーバーと Unified Manager サーバーの両方で SAML 認証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 ユーザー インターフェイスを起動し、更新されたサーバー証明書をブラウザで受け入れ、メンテナンス ユーザーの資格情報を使用してログインします。
4. *セットアップ/認証*ページで、***SAML 認証***タブを選択し、IdP 接続を構成します。
5. Unified Managerのホスト メタデータURIをコピーするか、ホスト メタデータをXMLテキスト ファイルに保存します。
6. *保存*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 サーバーにアクセスし、Unified Manager サーバーの URI とメタデータを入力して構成を完了します。

アイデンティティプロバイダー	設定手順
ADFS	a. ADFS管理GUIで、既存の証明書利用者信頼エントリを削除します。 b. 新しい証明書利用者信頼エントリを追加するには、`saml_sp_metadata.xml`更新された Unified Manager サーバーから。 c. Unified Manager がこの証明書利用者信頼エントリの ADFS SAML 応答を解析するために必要な3つのクレームルールを定義します。 d. ADFS Windowsサービスを再開します。
Shibboleth	a. Unified Managerサーバーの新しいFQDNを`attribute-filter.xml`そして`relying-party.xml`ファイル。 b. Apache Tomcat Webサーバを再起動し、ポート8005がオンラインになるまで待ちます。

9. Unified Managerにログインし、IdP経由のSAML認証が想定どおりに機能することを確認します。

SAML認証を無効にする

リモート ユーザーが Unified Manager Web UI にログインする前に、セキュア ID プロバイダー (IdP) を介した認証を停止する場合は、SAML 認証を無効にすることができます。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 プロバイダによるサインオン認証が行われます。

SAML認証を無効にすると、設定されているリモート ユーザに加え、ローカル ユーザとメンテナンス ユーザもグラフィカル ユーザ インターフェイスにアクセスできるようになります。

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、SAML認証はUnified Managerメンテナンスコンソールからも無効にすることができます。



SAML認証を無効にしたあと、Unified Managerが自動的に再起動されます。

手順

1. 左側のナビゲーション ペインで、[全般] > [SAML 認証] をクリックします。
2. **SAML 認証を有効にする** チェックボックスをオフにします。
3. *保存*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 サーバーの URI とメタデータを削除します。

メンテナンスコンソールから**SAML**認証を無効にする

Unified Manager GUIにアクセスできない場合は、必要に応じてメンテナンス コンソールからSAML認証を無効にすることができます。この状況は、設定に誤りがある場合やIdPにアクセスできない場合に発生します。

開始する前に

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 プロバイダによるサインオン認証が行われます。設定されているリモート ユーザに加え、ローカル ユーザとメンテナンス ユーザもグラフィカル ユーザ インターフェイスにアクセスできるようになります。

SAML認証は、UIの[セットアップ / 認証]ページからも無効にできます。



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URIとメタデータを削除します。

[SAML認証]ページ

[SAML 認証]ページでは、Unified ManagerのWeb UIにログインするリモート ユーザを、セキュアなアイデンティティ プロバイダ (IdP) 経由でSAMLを使用して認証するようにUnified Managerを設定することができます。

- 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 ユーザの設定後、[SAML認証を有効にする]チェックボックスを選択し、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 サーバーから IdP にアクセスするための URI。URIの例を次に示します。

ADFSのURIの例：

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml
```

ShibbolethのURIの例：

```
https://centos7.ntap2016.local/idp/shibboleth
```

- **IdPメタデータ**

XML形式のIdPメタデータ。

IdP URL が Unified Manager サーバーからアクセスできる場合は、**[IdP メタデータの取得]** ボタンをクリックしてこのフィールドに入力できます。

- **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。

認証を管理する

Unified ManagerサーバでLDAPまたはActive Directoryのいずれかを使用して認証を有効にし、サーバと連携してリモート ユーザを認証するように設定することができます。

リモート認証の有効化、認証サービスの設定、認証サーバーの追加については、前のセクションの「**Unified Manager** を設定してアラート通知を送信する」を参照してください。

認証サーバーを編集する

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。

開始する前に

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、**[全般] > [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*ボックスをチェックします。

3. *認証サーバー*領域で、編集する認証サーバーを選択し、*編集*をクリックします。
4. 認証サーバーの編集 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*をクリックします。

認証サーバーを削除する

Unified Managerサーバと認証サーバの間の通信を中止する場合は、認証サーバを削除できます。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、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。

開始する前に

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 ユーザとリモート 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、[全般] > [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. 削除要求を確認するには、[はい] をクリックします。

安全な接続を使用する オプションが有効になっている場合、認証サーバーに関連付けられている証明書は認証サーバーとともに削除されます。

Active DirectoryまたはOpenLDAPによる認証

管理サーバーでリモート認証を有効にし、管理サーバーが認証サーバーと通信するように設定して、認証サーバー内のユーザーが Unified Manager にアクセスできるようにすることができます。

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のライトウェイト ディレクトリ サービスは使用できません。

- OpenLDAP

必要な認証サービスを選択し、適切な認証サーバを追加して、認証サーバ内のリモート ユーザーが Unified Manager にアクセスできるようにすることができます。リモートのユーザまたはグループのクレデンシャルは、認証サーバで管理されます。管理サーバでは、設定された認証サーバ内のリモート ユーザの認証にLightweight Directory Access Protocol (LDAP) を使用します。

Unified Manager で作成されたローカル ユーザーの場合、管理サーバーはユーザー名とパスワードの独自のデータベースを維持します。管理サーバで認証が実行され、Active Directory認証またはOpenLDAP認証が使用されることはありません。

監査ログ

[監査ログ]を使用して、監査ログが侵害されていないかどうかを検出できます。ユーザが実行するアクティビティはすべて監視され、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。

監査ログ: ファイル ビュー を使用すると、Active IQ Unified Managerで使用可能なすべての監査ログ ファイルを表示およびアクセスできます。監査ログ: ファイル ビュー内のファイルは、作成日に基づいてリストされます。このビューには、インストールまたはアップグレードされてから現在までにシステムで取得されたすべての監査ログの情報が表示されます。Unified Managerで何らかの操作を実行すると、そのたびに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、「File Integrity Status」属性を使用してキャプチャされ、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ます。システムで使用可能な監査ログは、次のいずれかのステータスになります。

州	説明
ACTIVE	ログを記録中のファイル。
NORMAL	圧縮されてシステムに格納されている、アクティブでないファイル。
TAMPERED	侵害されたファイル（権限のないユーザによって手動で編集された）。
MANUALL_DELETE	権限のあるユーザ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ルオフで削除されたファイル。
UNEXPECTED_DELETE	不明な理由で削除されたファイル。

[監査ログ]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

削除 ボタンを使用すると、監査ログ ビューにリストされている監査ログを削除できます。監査ログを削除する際、あとで適切な削除だったことがわかるように、必要に応じてファイルの削除理由を指定することができます。この理由は、削除処理を実行したユーザの名前とともに[理由]列に表示されます。



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テーブル内のエントリは削除されません。

監査ログ セクションの ダウンロード ボタンを使用してActive IQ Unified Managerから監査ログをダウンロードし、監査ログ ファイルをエクスポートできます。「NORMAL」または「TAMPERED」とマークされたファイ

ルは圧縮された形式でダウンロードされます。`.gzip`形式。

監査ログ ファイルは定期的にアーカイブされ、参照できるよう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、アーカイブ前に監査ログはデジタル署名されます。

完全なAutoSupportバンドルには、アーカイブされた監査ログ ファイルとアクティブな監査ログ ファイルの両方が含まれます。一方、軽量なサポート バンドルには、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。

監査ログを構成する

監査ログ セクションの **構成** ボタンを使用して、監査ログ ファイルのローリング ポリシーを構成し、監査ログのリモート ログ記録を有効にすることもできます。

システムに保存するデータの希望量と頻度に応じて、最大ファイル サイズ と 監査ログ保持日数 の値を設定できます。フィールド **TOTAL AUDIT LOG SIZE** の値は、システム内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 **TOTAL AUDIT LOG SIZE** 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。ただし、ファイル エントリはデータベース内で引き続き使用可能であり、「Rollover Delete」としてマークされます。 **AUDIT LOG RETENTION DAYS** の値は、監査ログ ファイルが保存される日数です。このフィールドで設定された値よりも古いファイルはロールオーバーされます。

手順

1. 監査ログ > > ***構成***をクリックします。
2. 最大ファイル サイズ、監査ログの合計サイズ、および***監査ログの保持日数***に値を入力します。

リモート ログを有効にする場合は、[リモート ログを有効にする] を選択する必要があります。 /// 2025-6-11、OTHERDOC-133

監査ログのリモートログを有効にする

監査ログの構成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すると、リモート監査ログを有効にすることができます。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 ロギングは、Active IQ Unified Managerサーバ上の監査ログ ファイルが改ざんされた場合のバックアップとしても機能します。

手順

1. ***監査ログの構成***ダイアログボックスで、***リモートログの有効化***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フィールドが表示されます。

2. 接続するリモート サーバーの **HOSTNAME** と **PORT** を入力します。
3. **SERVER CA CERTIFICATE** フィールドで、**BROWSE** をクリックして、対象サーバーの公開証明書を選択します。

証明書は、.pem形式。ターゲットのsyslogサーバから取得した、有効期限内の証明書を使用してください。証明書には、選択した「hostname」がSubjectAltName(SAN)属性。

4. 次のフィールドに値を入力します: **CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

ミリ秒単位の値を指定してください。

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 バージョンを選択します。
6. 対象の 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オンにします。

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を作成する必要があります。

例: syslog-ngでは、コマンドを使用して証明書の<ハッシュ>を作成する必要があります。`openssl x509 -noout -hash -in cert.pem`次に、クライアント認証証明書を <ハッシュ>.0 という名前のファイルにシンボリック リンクする必要があります。

7. 保存 をクリックして、サーバーとの接続を構成し、リモート ログを有効にします。

[監査ログ]ページにリダイレクトされます。



接続タイムアウト*の値は構成に影響する可能性があります。定義された値よりも応答に時間がかかると、接続エラーが発生して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、構成を再度試してください。

[リモート認証]ページ

[リモート認証]ページでは、Unified Manager Web UIにログインするリモート ユーザを認証できるように、Unified Managerと認証サーバの通信を設定することができます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

[リモート認証を有効化する]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することができます。

• 認証サービス

Active DirectoryやOpenLDAPなどのディレクトリ サービス プロバイダでユーザを認証するように管理サーバを設定するか、または独自の認証メカニズムを指定できます。認証サービスは、リモート認証を有効にした場合にのみ指定できます。

◦ アクティブディレクトリ

▪ 管理者名

認証サーバの管理者の名前を指定します。

▪ パスワード

認証サーバにアクセスするためのパスワードを指定します。

- ベース識別名

認証サーバでのリモート ユーザの場所を指定します。たとえば、認証サーバーのドメイン名が `ou@domain.com` の場合、基本識別名は `cn=ou,dc=domain,dc=com` になります。

- 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。

- セキュアな接続を使用

認証サーバとの通信に使用される認証サービスを指定します。

- オープンLDAP

- バインド識別名

認証サーバでリモート ユーザを検出する際にベース識別名とともに使用されるバインド識別名を指定します。

- バインド パスワード

認証サーバにアクセスするためのパスワードを指定します。

- ベース識別名

認証サーバでのリモート ユーザの場所を指定します。たとえば、認証サーバーのドメイン名が `ou@domain.com` の場合、基本識別名は `cn=ou,dc=domain,dc=com` になります。

- セキュアな接続を使用

LDAP認証サーバとの通信に使用されるセキュアなLDAPを指定します。

- その他

- バインド識別名

設定した認証サーバでリモート ユーザを検出する際にベース識別名とともに使用されるバインド識別名を指定します。

- バインド パスワード

認証サーバにアクセスするためのパスワードを指定します。

- ベース識別名

認証サーバでのリモート ユーザの場所を指定します。たとえば、認証サーバーのドメイン名が `ou@domain.com` の場合、基本識別名は `cn=ou,dc=domain,dc=com` になります。

- 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 バージョンを自動検出するか、またはバージョン2か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ている属性と値に基づいて管理サーバのグループ メンバーシップをリモート ユーザに割り当てる値を指定します。

- UGID

リモート ユーザがGroupOfUniqueNamesオブジェクトのメンバーとして認証サーバに含まれている場合は、このオプションを使用して、GroupOfUniqueNamesオブジェクトで指定されている属性を基に管理サーバのグループ メンバーシップをリモート ユーザに割り当てることができます。

- ネストされたグループの検索を無効化

ネストされたグループの検索を有効にするか無効にするかを指定します。デフォルトでは、このオプションは無効になっています。Active Directoryを使用する場合は、ネストされたグループのサポートを無効にすることで認証を高速化できます。

- メンバー

認証サーバがグループの個々のメンバーに関する情報を格納するために使用する属性の名前を指定します。

- ユーザ オブジェクト クラス

リモート認証サーバ内のユーザのオブジェクト クラスを指定します。

- グループ オブジェクト クラス

リモート認証サーバ内のすべてのグループのオブジェクト クラスを指定します。



Member、*User Object Class*、および *Group Object Class* 属性に入力する値は、Active Directory、OpenLDAP、および LDAP 構成に追加された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される認証サービスを指定します。



認証サービスを変更する場合は、既存の認証サーバをすべて削除してから新しい認証サーバを追加するようにしてください。

【認証サーバ】領域

【認証サーバ】領域には、管理サーバがリモート ユーザの検出と認証を行う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

認証サーバの追加、編集、削除を行うことができます。

- 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 ペアを構成している（同じデータベースを使用している）場合は、パートナーの認証サーバも追加できます。これにより、どちらかの認証サーバが到達不能になったときに、管理サーバはパートナーと通信できます。

- 編集

選択した認証サーバの設定を編集できます。

- 削除

選択した認証サーバを削除します。

- 名前またはIPアドレス

管理サーバでユーザの認証に使用される認証サーバのホスト名またはIPアドレスが表示されます。

- ポート

認証サーバのポート番号が表示されます。

- テスト認証

このボタンでは、リモートのユーザまたはグループを認証することで認証サーバの設定を検証します。

テストの際にユーザ名のみを指定すると、管理サーバは認証サーバでリモート ユーザを検索しますが、ユーザの認証は行いません。ユーザ名とパスワードを指定すると、管理サーバはリモート ユーザの検索と認証を行います。

リモート認証が無効になっている場合は、認証をテストできません。

セキュリティ証明書を管理する

Unified Manager サーバーで HTTPS を設定すると、安全な接続を介してクラスターを監視および管理できます。

HTTPSセキュリティ証明書を表示する

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。

開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

証明書を表示すると、再生成された証明書の内容を検証したり、Unified Managerへのアクセスに使用できるSubject Alt Name (SAN)を確認したりできます。

手順

1. 左側のナビゲーション ペインで、全般 > **HTTPS 証明書** 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ついて、[HTTPS 証明書]ページの情報よりも詳しい情報を表示する必要がある場合は、ブラウザで接続証明書を表示します。

HTTPS証明書署名要求をダウンロードする

認証局にファイルを送信して署名を求めるために、現在のHTTPSセキュリティ証明書の証明書署名要求をダウンロードできます。CA署名証明書は、中間者攻撃を阻止するのに役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

開始する前に

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、全般 > **HTTPS 証明書** 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. 保存する `.csr` ファイル。

認証局にファイルを送信して署名を求め、署名済み証明書をインストールできます。

CA署名済みのHTTPS証明書をインストールする

認証局から署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。アップロードしてインストールするファイルは、既存の自己署名証明書の署名済みバージョンである必要があります。CA署名証明書は、中間者攻撃の阻止に役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

*始める前に

次の操作を完了しておきます。

- 証明書署名要求ファイルをダウンロードし、認証局の署名を受けます。
- 証明書チェーンをPEM形式で保存します。
- すべての証明書（Unified Managerサーバ証明書からルート署名証明書まで。存在する中間証明書もすべて含む）をチェーンに組み込みます。

アプリケーション管理者のロールが必要です。



CSRを作成した証明書の有効期間が397日より長い場合、CAは証明書に署名して返信する前に有効期間を397日に短縮します。

手順

1. 左側のナビゲーション ペインで、全般 > **HTTPS 証明書** 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見つけます。
4. ファイルを選択し、「インストール」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、"[外部ツールを使用して生成されたHTTPS証明書のインストール](#)"。

証明書チェーンの例

証明書チェーン ファイルの内容の例を次に示します。

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

外部ツールを使用して生成されたHTTPS証明書をインストールする

自己署名またはCA署名の証明書に加え、OpenSSL、BoringSSL、LetsEncryptなどの外部ツールを使用して生成された証明書をインストールできます。

これらの証明書は外部で生成された公開鍵と秘密鍵のキー ペアであるため、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。許可されるキーペアアルゴリズムは「RSA」と「EC」です。 **HTTPS** 証明書のインストール オプションは、HTTPS 証明書ページの [全般] セクションにあります。アップロードするファイルは、以下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. 上記の証明書への署名に使用された、ルートまでのCAの証明書

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「secp384r1」です。外部で生成されたECペアを含む証明書の例を次に示します。

```
-----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

RSAキー ペアを含む証明書のロード形式

ホスト証明書に属する RSA キー ペアの許可されるキー 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反映する必要があります。

ります。

外部で生成された証明書のアップロード チェック

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、システムでいくつかのチェックが実行されます。チェックに1つでも失敗すると、証明書は拒否されます。また、製品内のCSRから生成された証明書、および外部ツールを使用して生成された証明書の検証も実施されます。

- 入力で指定された秘密鍵が入力で指定されたホスト証明書と照合して検証されます。
- ホスト証明書の共通名 (CN) がホストのFQDNと照合してチェックされます。
- ホスト証明書の共通名 (CN) を空または空白にしたり、ローカル ホストに設定したりすることはできません。
- 証明書の有効期間の開始日を将来の日付にしたり、有効期限を過去の日付にしたりすることはできません。
- 中間CAまたはCAが存在する場合、証明書有効期間の開始日を将来の日付にしたり、有効期限を過去の日付にしたりすることはできません。



入力で指定する秘密鍵は暗号化しないでください。暗号化された秘密鍵はシステムで拒否されます。

例1

```
-----BEGIN ENCRYPTED PRIVATE KEY-----  
<Encrypted private key>  
-----END ENCRYPTED PRIVATE KEY-----
```

例2

```
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4, ENCRYPTED  
<content here>  
-----END RSA PRIVATE KEY-----
```

例3

```
-----BEGIN EC PRIVATE KEY-----  
Proc-Type: 4, ENCRYPTED  
<content here>  
-----END EC PRIVATE KEY-----
```

証明書のインストールに失敗した場合は、次のナレッジベース (KB) の記事を参照してください。 [https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate\[\"ActiveIQ Unified Manager が外部で生成された証明書のインストールに失敗する\"\]](https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate[\)

証明書管理のページの説明

[HTTPS 証明書]ページでは、現在のセキュリティ証明書を表示し、新しいHTTPS証明書を生成することができます。

[HTTPS 証明書]ページ

[HTTPS 証明書]ページでは、現在のセキュリティ証明書の表示、証明書署名要求のダウンロード、新しい自己署名HTTPS証明書の生成、新しいHTTPS証明書のインストールを行うことができます。

新しい自己署名HTTPS証明書を生成していない場合は、インストール時に生成された証明書がこのページに表示されます。

コマンド ボタン

各コマンド ボタンを使用して次の処理を実行できます。

- **HTTPS**証明書署名要求をダウンロード

現在インストールされているHTTPS証明書の署名要求をダウンロードします。ブラウザに、<hostname>.csr ファイルを保存するように求められます。これにより、証明機関にファイルを提供して署名を受けることができます。

- **HTTPS**証明書をインストールする

認証局の署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。新しい証明書は、管理サーバを再起動すると有効になります。

- **HTTPS**証明書の再生成

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 を再起動した後に有効になります。

[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証明書を生成することができます。

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、現在の情報を使用して証明書を再生成したり、新しい情報を使用して証明書を生成したりできます。

- 一般名

必須。保護する対象の完全修飾ドメイン名 (FQDN)。

Unified Manager の高可用性構成では、仮想 IP アドレスを使用します。

- メールアドレス

オプション。組織の連絡先のEメール アドレス。証明書の管理者またはIT部門のEメール アドレスが一般的です。

- 会社

オプション。通常は会社の法人名。

- 部門

オプション。社内の部署の名前。

- 市

オプション。会社の所在地の市区町村。

- 州

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。通常はISOの2文字の国コードです。

- 別名

必須。このサーバにアクセスするために既存のローカルホストやその他のネットワーク アドレスに加えて使用できる、プライマリ ドメイン以外の追加の名前。別名はそれぞれカンマで区切ります。

証明書の代替名フィールドからローカル識別情報を削除する場合は、「ローカル識別情報 (例: localhost) を除外する」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、フィールドに入力した内容のみが「別名」フィールドで使用されます。このフィールドを空白にした場合は、[別名]フィールドのない証明書が生成されます。

- キーサイズ (キーアルゴリズム: **RSA**)

キー アルゴリズムはRSAに設定されています。キー サイズは 2048 ビット、3072 ビット、4096 ビットから選択できます。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期間がそのまま表示される可能性があります。

詳細については、"[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）では、ONTAPストレージシステムの健全性とパフォーマンスを一元的に監視および管理することができます。

Unified Manager は次の機能を提供します。

- 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、通知を行います。
- 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 (操作)、MBps (スループット)、レイテンシ (応答時間)、使用率、パフォーマンス容量、キャッシュ比率など、時間の経過に伴うワークロード アクティビティをプロットする詳細なグラフを表示します。
- クラスター コンポーネントを過剰に使用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るワークロードを識別します。
- 特定のインシデントやイベントに対し、実行できる対処方法を提案します。一部のイベントには[修正]ボタンが表示され、問題をただちに解決できます。
- OnCommand Workflow Automationと統合して、自動保護ワークフローを実行します。
- 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にパフォーマンスとストレージの目標を定義することができます。

Active IQ Unified Managerの健全性監視の概要

Active IQ Unified Manager（旧OnCommand Unified Manager）では、ONTAPソフトウェアを実行する多数のシステムを一元化されたユーザ インターフェイスで監視できます。Unified Managerサーバ インフラは拡張性とサポート性に優れ、高度な監視および通知機能を備えています。

Unified Managerの主な機能は、クラスターの可用性と容量の監視 / 通知 / 管理、保護機能の管理、診断データの収集とテクニカル サポートへの送信です。

Unified Managerを使用してクラスターを監視できます。クラスターで問題が発生すると、Unified Managerのイベントを通じて問題の詳細が通知されます。一部のイベントでは、問題を解消するための対応策も提示されます。問題が発生したときにEメールやSNMPトラップで通知されるように、イベントに対してアラートを設定できます。

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ー、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ー オブジェクトについて、容量や健全性のグラフに表示される情報を使用してストレージ要件を計画することもできます。

物理容量と論理容量

Unified Managerは、ONTAPストレージ オブジェクトに使用される物理容量と論理容量の概念を利用します。

- **物理容量:** 物理スペースとは、ボリュームで使用されるストレージの物理ブロックを指します。Storage Efficiency機能（重複排除や圧縮など）によるデータの削減により、一般に「使用済み物理容量」は使用済み論理容量よりも小さくなります。
- **論理容量:** 論理スペースとは、ボリューム内の使用可能なスペース (論理ブロック) を指します。論理スペースとは、重複排除や圧縮の結果を考慮せずに、理論上のスペースの使用方法を指します。「使用済み論理容量」とは、使用済み物理容量に、設定されているStorage Efficiency機能（重複排除や圧縮など）による削減量を加えたものです。物理スペースの削減が反映されないため、通常は使用済み物理容量よりも大きくなります。したがって、合計論理容量はプロビジョニング済みスペースよりも大きくなる場合があります。

容量の測定単位

Unified Manager は、1024 (2¹⁰) 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、これらの単位がKB、MB、GB、TB、PBと表示されていました。ONTAP 9.10.1以降では、KiB、MiB、GiB、TiB、PiBと表示されます。



スループットに使用される単位は、すべてのリリースのONTAPについて、引き続きキロバイト/秒 (Kbps)、メガバイト/秒 (Mbps)、ギガバイト/秒 (Gbps)、テラバイト/秒 (Tbps) などになります。

ONTAP 9.10.0 以前の Unified Manager に表示される容量単位	ONTAP 9.10.1 の Unified Manager に表示される容量単位	計算式	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によるパフォーマンス監視の概要

Active IQ Unified Manager (旧OnCommand Unified Manager) は、NetApp ONTAPソフトウェアを実行するシステムを対象に、パフォーマンス監視機能とパフォーマンス イベントの根本原因分析機能を提供します。

Unified Manager は、クラスタ コンポーネントを過剰に使用し、クラスタ上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するのに役立ちます。パフォーマンスしきい値ポリシーを定義して特定のパフォーマンス カウンタの最大値を指定し、しきい値を超えた場合にイベントが生成されるようにすることも可能です。Unified Manager は、これらのパフォーマンス イベントについて警告を発し、修正アクションを実行してパフォーマンスを通常の操作レベルに戻すことができるようにします。Unified Manager UI でイベントを表示および分析できます。

Unified Manager は、次の 2 種類のワークロードのパフォーマンスを監視します。

- ユーザ定義のワークロード

このワークロードは、クラスタに作成したFlexVolとFlexGroupボリュームで構成されます。

- システム定義のワークロード

このワークロードは、内部のシステム アクティビティで構成されます。

Unified Manager REST APIを使用する

Active IQ Unified Managerには、ストレージ環境の監視と管理に関する情報を表示するためのREST APIが用意されています。また、ポリシーに基づいてストレージ オブジェクトをプロビジョニングおよび管理できるAPIもあります。

Unified ManagerでサポートされるAPIゲートウェイを使用して、ONTAPのすべての管理対象クラスタに対して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、以下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 サーバー インフラストラクチャは、データ収集ユニット、データベース、およびアプリケーション サーバーで構成されます。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。

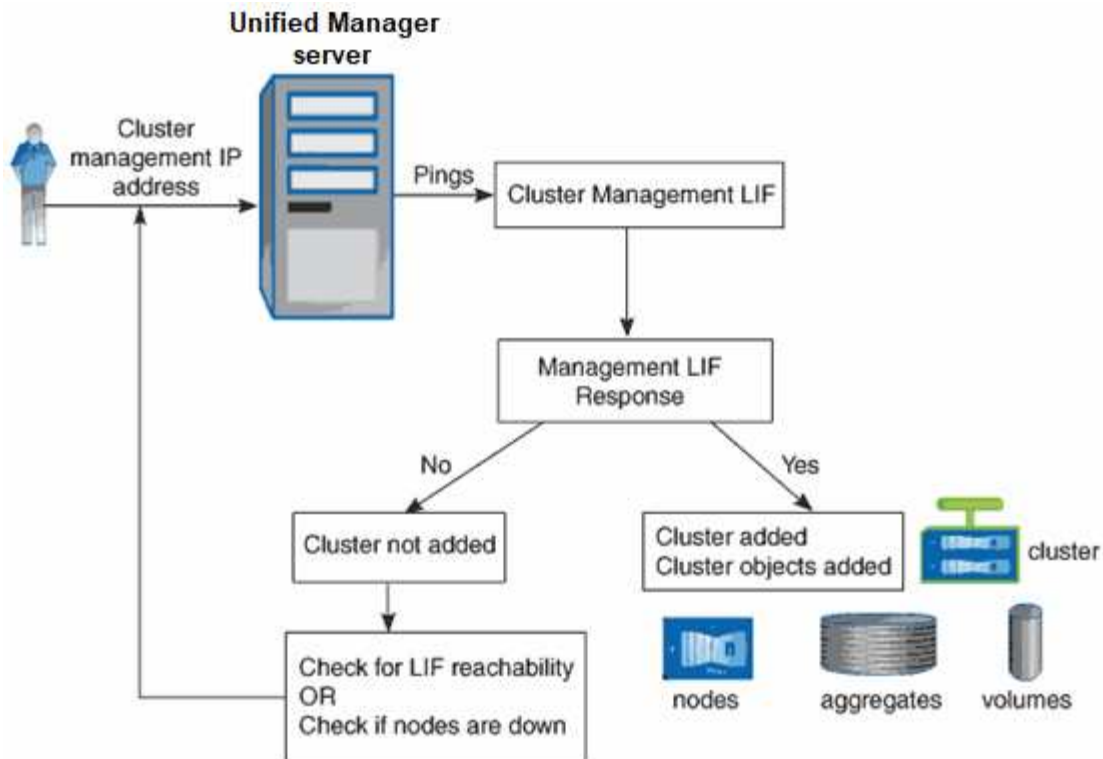
Unified Manager はクラスタ情報を収集し、そのデータをデータベースに保存し、そのデータを分析してクラスタに問題があるかどうかを確認します。

検出プロセスの仕組み

クラスタを Unified Manager に追加すると、サーバはクラスタ オブジェクトを検出し、それをデータベースに追加します。検出プロセスの仕組みを理解しておくと、使用するクラスタとそのオブジェクトを管理する際に役立ちます。

デフォルトの監視間隔は 15 分です。Unified Manager サーバーにクラスタを追加した場合、Unified Manager UI にクラスタの詳細が表示されるまでに 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。



ユーザーインターフェースを理解する

Unified Manager ユーザー インターフェイスは主に、監視対象のオブジェクトを一目で確認できるダッシュボードで構成されています。また、ユーザ インターフェイスを使用して、すべてのクラスタ オブジェクトを表示できます。

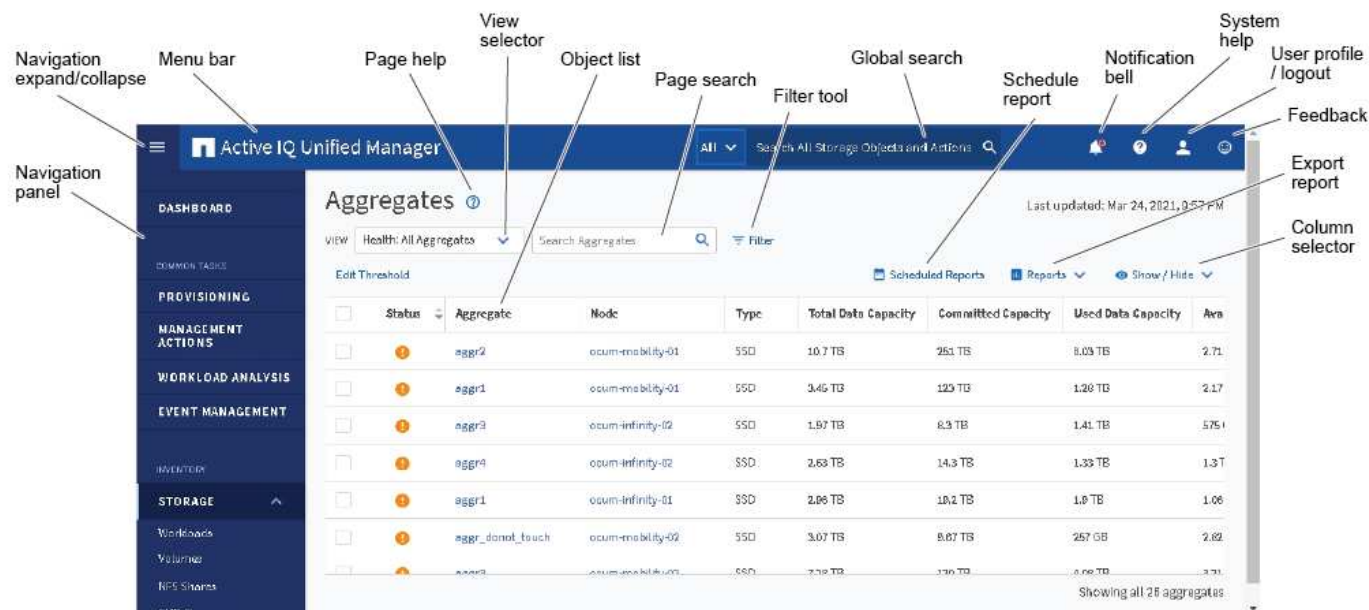
必要に応じて、優先するビューを選択したり、操作ボタンを使用したりできます。画面構成はワークスペースに保存されるため、Unified Manager を起動すると必要な機能がすべて利用できるようになります。ただし、別のビューに移動してから元のビューに戻ると、表示内容が変わる可能性があります。

一般的なウィンドウ レイアウト

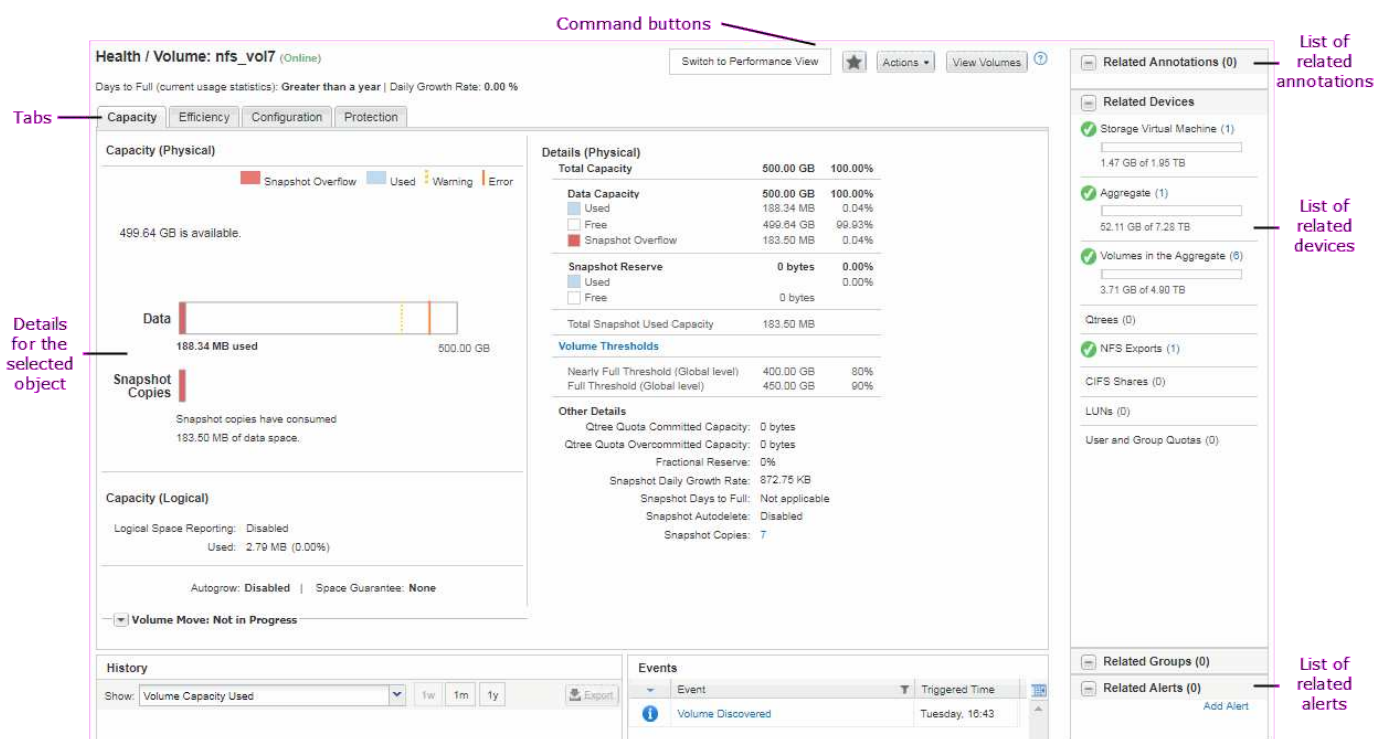
一般的なウィンドウ レイアウトを理解しておく、Active IQ Unified Managerを効果的に操作して使用できるようになります。ほとんどの Unified Manager ウィンドウは、オブジェクト リストまたは詳細という 2 つの一般的なレイアウトのいずれかに似ています。推奨される表示設定は1280×1024ピクセル以上です。

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

オブジェクト リスト ウィンドウのレイアウト



オブジェクト詳細ウィンドウのレイアウト



ウィンドウ レイアウトのカスタマイズ

Active IQ Unified Managerを使用して、ストレージ オブジェクトとネットワーク オブジェクトのページに表示される情報のレイアウトをカスタマイズできます。ウィンドウをカスタマイズすることによって、表示するデータやその表示方法を制御できます。

- 並べ替え

列エントリのソート順序を変更するには、列見出しをクリックします。列ヘッダーをクリックすると、並べ替え矢印 (▲そして▼) がその列に表示されます。

- フィルタリング

フィルターアイコン () を使用すると、フィルターを適用して、ストレージ オブジェクト ページおよびネットワーク オブジェクト ページの情報の表示をカスタマイズし、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なります。フィルタは[フィルタ]ペインから適用します。

[フィルタ]ペインでは、ほとんどの列を選択したオプションに基づいてフィルタリングできます。たとえば、[ヘルス: すべてのボリューム] ビューでは、[フィルター] ペインを使用して、[状態] の下にある適切なフィルター オプションを選択することで、オフラインになっているすべてのボリュームを表示できます。

容量関連の列に表示される容量データは小数点以下2桁に四捨五入され、適切な単位で表示されます。これは、容量の列をフィルタするときにも適用されます。たとえば、[ヘルス: すべての集計] ビューの [合計データ容量] 列のフィルターを使用して 20.45 GB を超えるデータをフィルタすると、実際の容量 20.454 GB は 20.45 GB として表示されます。同様に、20.45 GB 未満のデータをフィルタリングすると、実際の容量 20.449 GB が 20.45 GB として表示されます。

「ヘルス: すべての集計」ビューの「使用可能なデータ %」列のフィルターを使用して 20.45% を超えるデータをフィルタすると、実際の容量 20.454% が 20.45% として表示されます。同様に、20.45% 未満のデータをフィルタリングすると、実際の容量 20.449% が 20.45% として表示されます。

- 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。列を選択したら、マウスでドラッグして列を並べ替えることができます。

- 検索中

検索ボックスを使用して特定のオブジェクト属性を検索し、インベントリ ページ内の項目リストを絞り込むことができます。たとえば、「cloud」と入力してボリューム インベントリ ページ内のボリュームのリストを絞り込むと、「cloud」という単語が含まれているすべてのボリュームを表示できます。

- データのエクスポート

*レポート*ボタン (または*エクスポート*ボタン) をクリックして、データをカンマ区切りの形式でエクスポートできます。`.csv` ファイル、`.pdf` ドキュメント、またはMicrosoft Excel `(.xlsx)` ファイルを作成し、エクスポートしたデータを使用してレポートを作成します。

Unified Managerヘルプを使用する

このヘルプは、Active IQ Unified Managerに含まれているすべての機能に関する情報を提供します。目次、索引、または検索ツールを使用すると、機能に関する情報と機能の使用方法を検索できます。

ヘルプは、Unified Manager ユーザー インターフェイスの各タブおよびメニュー バーから利用できます。

ヘルプの検索ツールは一部の単語だけを入力しても機能しません。

- 特定のフィールドまたはパラメータの詳細については、。

- すべてのヘルプコンテンツを表示するには、をクリックしてください。❓ * > メニューバーの *ヘルプドキュメント。

ナビゲーション ペインで目次の一部を展開すると、より詳細な情報を参照できます。

- ヘルプ コンテンツを検索するには、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単語の列を入力して [実行] をクリックします。
- ヘルプ トピックを印刷するには、プリンタのアイコンをクリックします。

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。ブックマークに登録すると、よく見るヘルプトピックにすばやくアクセスできます。

手順

1. お気に入りに登録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。

保管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 オブジェクトを検索] フィールドを使用できます。すべてのオブジェクトをグローバルに検索できるので、特定のタイプのオブジェクトが簡単に見つかります。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。

開始する前に

- 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必要です。
- 検索キーワードは3文字以上入力する必要があります。

ドロップダウン メニューで[すべて]を選択すると、グローバル検索によって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）。ドロップダウン メニューで特定のオブジェクト タイプを選択すると、検索の対象をそのオブジェクト タイプに絞り込むことができます。この場合、結果のリストに表示されるオブジェクトの数は上位25個に限定されません。

検索対象として選択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 / 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
- Initiators
- 整合性グループ

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]カテゴリの下にワークロードの一覧が表示されます。

検索結果でいずれか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対応する[健全性]ページがない場合は、親オブジェクトの[健全性]ページが表示されます。たとえば、特定のLUNを検索する場合は、そのLUNが配置されているSVMの詳細ページが表示されます。

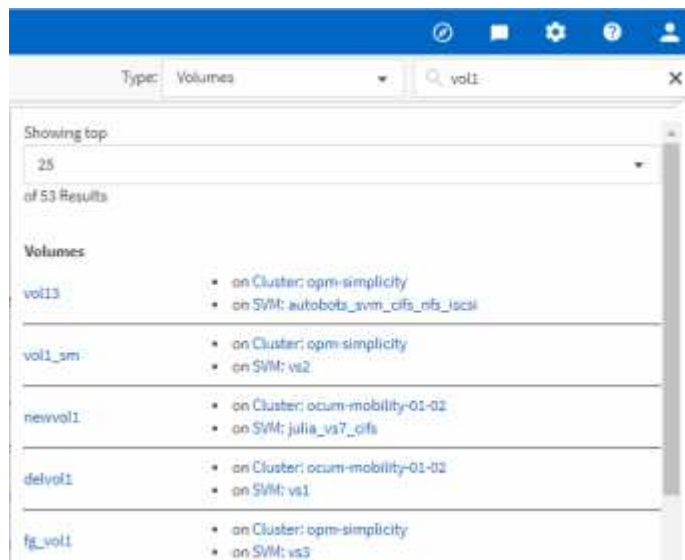


ポートとLIFはグローバル検索バーでは検索できません。

手順

1. メニューでオブジェクト タイプを選択して、検索結果を特定のオブジェクト タイプに絞り込みます。
2. すべてのストレージ オブジェクトを検索 フィールドにオブジェクト名の少なくとも 3 文字を入力します。

次の例では、ドロップダウン ボックスで[ボリューム]オブジェクト タイプが選択されています。すべてのストレージ オブジェクトを検索 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るすべてのボリュームのリストが表示されます。



ストレージデータをレポートとしてエクスポート

ストレージ データをさまざまな出力形式でエクスポートし、エクスポートしたデータを使用してレポートを作成できます。たとえば、未解決の重大イベントが10件ある場合、[イベント管理]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そのレポートを送信することができます。

データをエクスポートすることができます。`.csv`ファイル、`.xlsx`ファイル、または`.pdf`ストレージ*および*ネットワーク*インベントリ ページからドキュメントを取得し、エクスポートしたデータを使用してレポートを作成します。製品には他にも、`.csv`または`.pdf`ファイルを生成できます。

手順

1. 次のいずれかを実行します。

エクスポートしたい場合...	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 ストレージ または ネットワーク 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 [ストレージ] > [QoS ポリシー グループ] 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、単一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 > クラスター > パフォーマンス:すべてのクラスター*をクリックし、クラスターを選択して*トップ パフォーマー 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. レポート ボタン (または一部の UI ページでは エクスポート 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。

「トップ パフォーマー」タブでは、表示している単一のクラスターまたはデータセンター内のすべてのクラスターの統計レポートをダウンロードすることを選択できます。

ファイルがダウンロードされます。

4. ファイルを適切なアプリケーションで開きます。

["\[健全性/クラスタインベントリ ページ\]"](#)

["レポートのスケジュール設定"](#)

在庫ページのコンテンツをフィルタリングする

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、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。

*フィルタリング*を使用して、好みに応じてグリッド ビューをカスタマイズします。使用可能なフィルタ オプションは、グリッドで表示しているオブジェクト タイプによって異なります。現在フィルタが適用されている場合は、適用されているフィルタの数が[フィルタ]ボタンの右側に表示されます。

次の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、含む、で始まる、で終わる、*含まない*です。
数値	演算子は、より大きい、より小さい、最後、および*間*です。
列挙 (テキスト)	演算子は is と is not です。

それぞれのフィルタに、[列]、[演算子]、[値]の各フィールドが必要です。使用可能なフィルタは、現在のページのフィルタ可能な列に基づいて決まります。適用できるフィルタは4つまでです。フィルタ パラメータの組み合わせに基づいてフィルタされた結果が表示されます。フィルタされた結果は、現在表示しているページだけでなく、フィルタで検索するすべてのページに適用されます。

フィルタは[フィルタ]パネルで追加できます。

1. ページの上部にある*フィルター*ボタンをクリックします。[フィルタ]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、オブジェクト (たとえば、*Cluster* またはパフォーマンス カウンター) を選択します。
3. 中央のドロップダウン リストをクリックし、使用する演算子を選択します。
4. 最後のリストで、値を選択または入力してそのオブジェクトのフィルタを完成させます。
5. 別のフィルターを追加するには、[フィルターを追加] 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。上記と同じ手順で追加のフィルタを設定します。4 番目のフィルターを追加すると、[フィルターを追加] ボタンが表示されなくなることに注意してください。
6. *フィルターを適用*をクリックします。フィルタ オプションがグリッドに適用されて、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、[フィルタ]パネルで、削除するフィルタの右にあるごみ箱のアイコンを

クリックします。

- すべてのフィルターを削除するには、フィルタリング 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

この図では、[フィルタ]パネルで3つのフィルタを設定しています。フィルターの数が増加した場合、最大 4 個より少ない場合、「+ フィルターを追加」ボタンが表示されます。

MBps	greater than	5	MBps	✕
Node	name starts with	test		✕
Type	is	FCP Port		✕

+ Add Filter

Cancel Apply Filter

*フィルターを適用*をクリックすると、フィルタリングパネルが閉じ、フィルターが適用され、適用されたフィルターの数が表示されます (3)。

通知ベルからアクティブなイベントを表示する

通知ベル () を使用すると、Unified Manager が追跡している最も重要なアクティブイベントをすばやく表示できます。

アクティブ イベントのリストでは、すべてのクラスターの重大イベント、エラー イベント、警告イベント、アップグレード イベントの総数を確認できます。このリストには過去7日間のイベントが含まれ、情報イベントは含まれていません。リンクをクリックすることで、関心のあるイベントのリストを表示できます。

クラスターに到達できない場合、Unified Manager はこのページにこの情報を表示することに注意してください。詳細 ボタンをクリックすると、到達できないクラスターの詳細情報を表示できます。[イベントの詳細] ページが開きます。このページには、拡張監視の問題（管理ステーションにおけるスペースやRAMの不足など）も表示されます。

手順

- メニューバーからクリック 。
- アクティブ イベントの詳細を表示するには、「2 容量」や「4 パフォーマンス」などのイベント テキストのリンクをクリックします。

ダッシュボードからクラスターを監視および管理する

ダッシュボードには、監視対象のONTAPシステムの現在の健全性に関する累積的な情報が一目でわかります。ダッシュボードには、監視対象のクラスターの全体的な容量、パフォーマンス、セキュリティの健全性を評価できる「パネル」が用意されています。

さらに、ONTAP System Manager またはONTAP CLI を使用する代わりに、Unified Manager ユーザー イン

ターフェイスから直接修正できる特定のONTAPの問題もあります。

ダッシュボードの上部では、監視対象のすべてのクラスターの情報を表示するか、個々のクラスター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ー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ーにドリルダウンできます。



以下にリストされているパネルの一部は、設定によってはページに表示されない場合があります。

パネル	説明
管理操作	Unified Manager が問題を診断して単一の解決策を決定できる場合、それらの解決策は [修正] ボタンとともにこのパネルに表示されます。
容量	ローカル層とクラウド層の合計容量と使用容量、およびローカル容量が上限に達するまでの日数を表示します。
パフォーマンス容量	各クラスターのパフォーマンス容量値と、パフォーマンス容量が上限に達するまでの日数を表示します。
ワークロード IOPS	特定の IOPS 範囲で現在実行中のワークロードの合計数を表示します。
ワークロード パフォーマンス	定義された各パフォーマンス サービス レベルに割り当てられている準拠ワークロードと非準拠ワークロードの総数が表示されます。
セキュリティ	準拠しているクラスターまたは準拠していないクラスターの数、準拠している SVM または準拠していない SVM の数、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を表示します。
保護	SVM-DR関係で保護されているStorage VMの数、SnapMirror関係で保護されているボリュームの数、Snapshotで保護されているボリュームの数、およびMetroClusterで保護されているクラスターの数が表示されます。
使用状況	最高の IOPS、最高のスループット (MBps)、または最高の使用済み物理容量で並べ替えられたクラスターを表示します。

【ダッシュボード】ページ

【ダッシュボード】ページには、監視しているクラスターの容量、パフォーマンス、セキュリティ

ティの健全性の概要が表示される「パネル」があります。また、このページには、Unified Managerが特定のイベントを解決するために実行できる修正が表示される[管理操作]パネルがあります。

ほとんどのパネルには、そのカテゴリのアクティブ イベントの数および過去24時間に追加された新しいイベントの数が表示されます。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[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の情報を表示するか（[すべてのクラスタ]）、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。



次のパネルの一部は、設定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

問題によっては、Unified Managerの詳細な診断の結果、単一の解決策が提示されることがあります。利用可能な場合、それらの解決策は、修正 または すべて修正 ボタンとともにこのパネルに表示されます。問題はUnified Managerから直接解決できます。ONTAP System ManagerやONTAP CLIを使用する必要はありません。すべての号を見るには、「見る」をクリックしてください["ONTAPの問題をUnified Managerから直接修正"](#)詳細についてはこちらをご覧ください。

[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によって実現可能な削減効果を含まない）、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コピーを含まない）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、ローカル階層上の各データ アグリゲート（ディスクタイプ別にソート）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な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[ノード]インベントリ ページが表示されます。[ノード]インベントリ ページには、過去72時間の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、そのノード名をクリックすると詳細が表示されます。

単一のクラスタを表示している場合、このパネルには、そのクラスタの使用済みパフォーマンス容量（%）、合計IOPS、合計スループット（MBps）、およびこれらの3つの指標が上限に達するまでの想定日数が表示されます。

[ワークロード 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IOPS範囲で実行中のワークロードの総数が表示され、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) ポリシーが割り当てているワークロードのうち、準拠しているワークロードと準拠していないワークロードの総数が表示されます。また、PSLが割り当てられていないアグリゲートの数も表示されます。棒グラフをクリックすると、そのポリシーが割り当てられ、準拠しているワークロードが[ワークロード]ページに表示されます。棒グラフ上の数をクリックすると、そのポリシーが割り当てられていて、準拠しているワークロードと準拠していないワークロードが表示されます。

[セキュリティ]パネル

[セキュリティ]パネルには、現在のビューに応じてすべてのクラスタまたは単一のクラスタのセキュリティ ステータスの概要が表示されます。このパネルには次の情報が表示されます。

- 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、詳細が[イベントの詳細]ページに表示されます。
- クラスターのセキュリティ ステータス (準拠クラスターと非準拠クラスターの数)
- ストレージ VM のセキュリティ ステータス (準拠ストレージ VM と非準拠ストレージ VM の数)
- 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と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)

準拠しているクラスタとしていないクラスタ、Storage VM、暗号化されているボリュームとされていないボリューム、およびボリュームのランサムウェア対策ステータスの棒グラフをクリックすると、該当するページに移動して該当するクラスタ、Storage VM、ボリュームのセキュリティの詳細が表示されます。

コンプライアンスは、"[NetApp ONTAP 9 セキュリティ強化ガイド](#)"。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、"[クラスタとストレージVMの詳細なセキュリティステータスの表示](#)"。

[データ保護]パネル

このパネルには、データセンター内の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で過去24時間に生成されたデータ保護イベントとMetroClusterイベントの総数、および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、イベント管理インベントリ ページでアクティブな保護イベントをすべて表示できます。このパネルには次の情報が表示されます。

- Snapshotコピーで保護されているデータセンター内の1つまたはすべてのクラスタのボリューム数。
- SnapMirror関係で保護されているデータセンター内の1つまたはすべてのクラスタのボリューム数。SnapMirror関係については、ソース クラスタのボリューム数がカウントされます。
- MetroCluster over IP構成とMetroCluster over FC構成で保護されているデータセンター内のクラスタの数または全クラスタ。
- SnapMirror目標復旧時点 (RPO) 遅延のあるボリューム関係の数 (遅延ステータスに基づく)。

カーソルを合わせると、それぞれの数と凡例を確認できます。パネル上部の右矢印をクリックすると、[データ保護]ページに単一またはすべてのクラスタの詳細が表示されます。また、次の操作を行うこともできます。

- Snapshotコピーで保護されていないボリュームおよびされているボリュームの棒グラフをクリックすると、[ボリューム]ページに移動して詳細を確認できます。
- MetroCluster構成で保護されているクラスタまたはされていないクラスタの棒グラフをクリックすると、[クラスタ]ページに移動して詳細を確認できます。
- すべての関係の棒グラフをクリックすると、ソース クラスタに基づいてフィルタされた詳細が[関係]ページに表示されます。

詳細については、"[ボリュームの保護ステータスの表示](#)"。

【使用状況】パネル

すべてのクラスタを表示している場合、IOPS、スループット（MBps）、または使用済み物理容量が大きい順にクラスタを表示できます。

単一のクラスタを表示している場合は、IOPS、スループット（MBps）、または使用済み論理容量が大きい順にワークロードを表示できます。

関連情報

["Unified Managerの自動修正措置を使用した問題の修正"](#)

["パフォーマンス イベントに関する情報の表示"](#)

["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"](#)

["クラスターのセキュリティ目標を管理する"](#)

["パフォーマンス クラスター ランディング ページからクラスターのパフォーマンスを監視します。"](#)

["パフォーマンスインベントリページを使用してパフォーマンスを監視する"](#)

ONTAPの問題や機能をUnified Managerから直接管理

ONTAPの一部の問題または機能については、ONTAP System ManagerやONTAP CLIを使用しなくても、Unified Managerユーザ インターフェイスから直接修正または管理することができます。「管理アクション」オプションは、Unified Manager イベントをトリガーしたいいくつかのONTAP の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 [管理アクション] オプションを選択すると、[管理アクション] ページから直

接問題を修正できます。[管理操作]オプションは、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]からも使用できます。

問題によっては、Unified Managerの詳細な診断の結果、単一の解決策が提示されることがあります。ONTAPの一部の機能（ランサムウェア対策監視など）については、Unified Managerで内部チェックが実行されて特定の操作が提案されます。利用可能な場合、それらの解決策は[管理アクション]に[修正]ボタンとともに表示されます。問題を解決するには、[修正]ボタンをクリックします。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 は、要求された修正を行うためにクラスタにONTAPコマンドを送信します。修正が完了すると、イベントは廃止状態になります。

一部の管理アクションでは、[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、「ボリュームの自動拡張を有効にする」のすべて修正 管理アクションをクリックすることで解決できる「ボリューム領域がいっぱい」イベントが発生しているボリュームが5つある場合があります。1回のクリックで5つのボリュームに対してまとめて問題を修正できます。

自動修復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、以下を参照してください。["Unified Managerで解決可能な問題"](#)。

[修正] / [すべて修正]ボタンが表示されたときの処理

[管理アクション] ページには、Unified Manager がイベントを通じて通知した問題を修正するための [修正] ボタンまたは [すべて修正] ボタンが用意されています。

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推奨します。ただし、Unified Manager の推奨に従って問題を解決するかどうか分からない場合は、次の操作を実行できます。

希望する処理	アクション
特定されたすべてのオブジェクトについて、Unified Managerで問題を修正する。	*すべて修正*ボタンをクリックします。
特定されたどのオブジェクトについても現時点では問題を修正せず、再度イベントが生成されるまでの管理操作を非表示にする。	下矢印をクリックし、「すべて閉じる」をクリックします。
特定されたオブジェクトの一部についてのみ、問題を修正する。	管理アクションの名前をクリックすると、リストが展開され、すべての個別の*修正*アクションが表示されます。次に、個別の管理アクションを修正または却下するための手順に従います。

希望する処理	アクション
Unified Manager に問題を修正してもらってください。	*[修正]*ボタンをクリックします。
現時点では問題を修正せず、再度イベントが生成されるまでこの管理操作を非表示にする。	下矢印をクリックし、[閉じる] をクリックします。

希望する処理	アクション
問題について詳しく確認するために、このイベントの詳細を表示する。	• [修正] ボタンをクリックし、表示されるダイアログ ボックスで適用される修正を確認します。 • 下矢印をクリックし、[イベントの詳細を表示] をクリックして、イベントの詳細ページを表示します。 問題を修正したい場合は、表示されたページのいずれかから「修正」をクリックします。
問題について詳しく確認するために、このストレージ オブジェクトの詳細を表示する。	ストレージ オブジェクトの名前をクリックすると、パフォーマンス エクスプローラーまたはヘルス詳細ページに詳細が表示されます。

修正は、次の15分間に実施される構成ポーリングで反映されることもあれば、構成の変更が検証されてイベントが廃止状態になるまでに何時間もかかることもあります。

完了した、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、フィルター アイコンをクリックし、「完了」または「進行中」を選択します。

修正すべての操作は順番に実行されるため、「進行中」パネルを表示すると、一部のオブジェクトのステータスは「進行中」になり、他のオブジェクトのステータスは「スケジュール済み」になります。つまり、これらのオブジェクトはまだ実装を待機中です。

修正するために選択した管理アクションのステータスを表示します

修正することを選択したすべての管理操作のステータスは、[管理操作]ページで確認できます。ほとんどのアクションは、Unified Manager がクラスタにONTAPコマンドを送信した後、すぐに「完了」と表示されます。ただし、ボリュームの移動などの一部の操作には時間がかかることがあります。

[管理操作]ページでは、次の3つのフィルタを使用できます。

- 完了 には、正常に完了した管理アクションと失敗した管理アクションの両方が表示されます。*失敗した*アクションでは失敗の理由が提供されるため、手動で問題に対処できます。
- 進行中 には、実装中の管理アクションと実装が予定されている管理アクションの両方が表示されます。
- 推奨 では、監視対象のすべてのクラスターに対して現在アクティブなすべての管理アクションが表示されます。

手順

1. 左側のナビゲーション ペインで [管理アクション] をクリックします。または、クリック  *ダッシュボード*の*管理アクション*パネルの上部にある  をクリックし、表示するビューを選択します。

[管理操作]ページが表示されます。

2. 説明 フィールドの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すると、問題の詳細と、問題を解決するために使用されているコマンドが表示されます。

3. 失敗した*アクションを表示するには、[*完了] ビューの [ステータス] 列で並べ替えます。同じ目的で*フィルター*ツールを使用することもできます。
4. 失敗した管理アクションに関する詳細情報を表示する場合、または推奨された管理アクションを修正することにした場合は、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後、展開された領域から [イベントの詳細を表示] をクリックできます。そのページから「修正」ボタンを利用できます。

Unified Managerで解決可能な問題

Active IQ Unified Managerの自動修正機能を使用すると、Unified ManagerからONTAPの特定の問題を解決したり、特定の機能（ランサムウェア対策の監視など）を管理したりできます。

この表では、Unified Manager Web UI の **Fix It** または **Fix All** ボタンから直接管理できるONTAP の問題または機能について説明します。

イベント名と説明	管理操作	「Fix It」 作戦
ボリューム スペースがフル ボリュームにスペースがほとんど残っておらず、容量の「フル」しきい値を超えています。このしきい値は、デフォルトではボリューム サイズの90%に設定されています。	ボリュームの自動拡張を有効にする	Unified Managerはこのボリュームにボリュームの自動拡張が設定されていないと判断し、必要に応じてボリュームが拡張されるようにこの機能を有効にします。
iノードがいっぱい このボリュームにはinodeが残っていないため、新しいファイルを受け付けることができません。	ボリュームのinodeの数を増やす	ボリュームのinodeの数を2%増やします。
ストレージ階層のポリシーの不一致を検出 ボリュームにアクセス頻度の低いデータが大量にあり、階層化ポリシーが「Snapshot のみ」または「なし」に設定されています。	クラウドへの自動階層化を有効にする	ボリュームはすでにFabricPoolに配置されているため、階層化ポリシーを「自動」に変更して、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るようになります。
ストレージ階層の不一致を検出 ボリュームにアクセス頻度の低いデータが大量にありますが、ボリュームがクラウド対応のストレージ階層（FabricPool）に配置されていません。	ボリュームのストレージ階層を変更する	ボリュームをクラウド対応のストレージ階層に移動して階層化ポリシーを「自動」に設定し、アクセス頻度の低いデータをクラウド階層に移動します。

イベント名と説明	管理操作	「Fix It」 作戦
監査ログが無効 Storage VMの監査ログが有効になっていません。	Storage VMの監査ログを有効にする	Storage VMの監査ログを有効にします。 Storage VMにローカルまたはリモートの監査ログの場所が設定されている必要があります。
ログイン バナーが無効 アクセス制限を明確にしてセキュリティを強化するためには、クラスタのログイン バナーを設定する必要があります。	クラスタのログイン バナーを設定する	クラスタのログイン バナーを「アクセスは許可されたユーザーに制限されています」に設定します。
ログイン バナーが無効 アクセス制限を明確にしてセキュリティを強化するためには、Storage VMのログイン バナーを設定する必要があります。	Storage VMのログイン バナーを設定する	Storage VMのログイン バナーを「権限のあるユーザだけがアクセスできます」に設定します。
SSHでセキュアでない暗号を使用 サフィックスが「-cbc」の暗号はセキュアでないといみなされます。	セキュアでない暗号をクラスタから削除する	セキュアでない暗号（aes192-cbc、aes128-cbcなど）をクラスタから削除します。
SSHでセキュアでない暗号を使用 サフィックスが「-cbc」の暗号はセキュアでないといみなされます。	セキュアでない暗号をStorage VMから削除する	セキュアでない暗号（aes192-cbc、aes128-cbcなど）をStorage VMから削除します。
AutoSupport HTTPS 転送が無効 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は、暗号化されている必要があります。	AutoSupportメッセージの転送プロトコルとしてHTTPSを設定する	クラスタ上のAutoSupportメッセージの転送プロトコルとしてHTTPSを設定します。
クラスタ負荷の不均衡しきい値を超過 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。	クラスタのワークロードのバランスをとる	Unified Managerは別のノードに移動することで不均衡が最も解消されるボリュームを特定し、そのボリュームを移動します。

イベント名と説明	管理操作	「Fix It」 作戦
クラスタ容量の不均衡しきい値を超過 クラスタのアグリゲート間で容量が不均衡になっています。このイベントは、アグリゲート間の使用済み容量の差が70%を超えた場合に生成されます。	クラスタ容量のバランスをとる	Unified Managerは別のアグリゲートに移動することで不均衡が最も解消されるボリュームを特定し、そのボリュームを移動します。
使用済みパフォーマンス容量しきい値を超過 いくつかの非常にアクティブなワークロードによる使用率を下げないと、ノードの負荷が高くなりすぎる可能性があります。このイベントは、ノードの使用済みパフォーマンス容量の値が12時間以上100%を超えている場合に生成されます。	ノードの高負荷を制限する	Unified ManagerはIOPSが最も高いボリュームを特定し、過去の想定IOPSとピークIOPSのレベルを使用してQoSポリシーを適用し、ノードの負荷を軽減します。
動的イベントの警告しきい値を超過 一部のワークロードの負荷が異常に高いため、ノードはすでに過負荷状態です。	ノードの過負荷を軽減	Unified ManagerはIOPSが最も高いボリュームを特定し、過去の想定IOPSとピークIOPSのレベルを使用してQoSポリシーを適用し、ノードの負荷を軽減します。
テイクオーバーを実行不可 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。	ノード フェイルオーバーを有効にする	Unified Manager は、クラスタ内のすべてのノードでフェイルオーバーを有効にするために適切なコマンドを送信します。
オプションcf.takeover.on_panicの設定がOFF ノードシェル オプション「cf.takeover.on_panic」がオフに設定されているため、HA 構成のシステムで問題が発生する可能性があります。	パニック時のテイクオーバーを有効にする	Unified Manager は、この設定をオンに変更するための適切なコマンドをクラスタに送信します。

イベント名と説明	管理操作	「Fix It」 作戦
ノードシェル オプションsnapmirror.enableを無効化 古いノードシェル オプション「snapmirror.enable」が on に設定されているため、ONTAP 9.3 以降にアップグレードした後、起動時に問題が発生する可能性があります。	snapmirror.enableオプションをoffに設定する	Unified Manager は、この設定をオフ に変更するための適切なコマンドをクラスタに送信します。
Telnetが有効 Telnetは安全性が高くなく、暗号化されていない方法でデータが渡されるため、潜在的なセキュリティの問題があります。	Telnetを無効にする	Unified Managerがクラスタに該当するコマンドを送信し、Telnetを無効にします。
Storage VMのランサムウェア対策の学習を設定 ランサムウェア対策監視のライセンスのあるクラスタを定期的にチェックします。該当するクラスタ内でStorage VMがNFSボリュームまたはSMBボリュームのみをサポートしているかどうかを検証します。	ストレージVMを `learning` ランサムウェア対策監視モード	Unified Managerはランサムウェア対策監視を設定します `learning` クラスター管理コンソールを通じてストレージ VM の状態を確認します。Storage VM上に作成されたすべての新しいボリュームで、ランサムウェア対策監視が自動的に学習モードに切り替わりま す。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、潜在的な悪意ある攻撃による異常を検出することができます。
ボリュームのランサムウェア対策の学習を設定 ランサムウェア対策監視のライセンスのあるクラスタを定期的にチェックします。該当するクラスタ内でボリュームがNFSサービスまたはSMBサービスのみをサポートしているかどうかを検証します。	ボリュームを入れる `learning` ランサムウェア対策監視モード	Unified Managerはランサムウェア対策監視を設定します `learning` クラスター管理コンソールを通じてボリュームの状態を確認します。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、潜在的な悪意ある攻撃による異常を検出することができます。

イベント名と説明	管理操作	「Fix It」 作戦
ボリュームのランサムウェア対策の有効化 ランサムウェア対策監視のライセンスのあるクラスタを定期的にチェックします。ボリュームが`learning`ランサムウェア対策監視モードを 45 日間以上使用し、アクティブ モードに移行する可能性を判断します。	ボリュームを入れる `active` ランサムウェア対策監視モード	Unified Managerはランサムウェア対策監視を設定します `active` クラスタ管理コンソールを通じてボリューム上で。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、潜在的な悪意ある攻撃による異常を検出して、データ保護操作のアラートを作成します。
ボリュームのランサムウェア対策の無効化 ランサムウェア対策監視のライセンスのあるクラスタを定期的にチェックします。ボリュームのランサムウェア対策監視がアクティブな場合に繰り返し表示される通知を検出します（潜在的なランサムウェア攻撃の警告が30日以上にわたって返される場合など）。	ボリュームのランサムウェア対策監視を無効にする	Unified Managerは、クラスタ管理コンソールから、ボリュームのランサムウェア対策監視を無効にします。

スクリプトによる管理アクションの上書き

カスタム スクリプトを作成してアラートに関連付けると、特定のイベントに対して、[管理操作] ページやUnified Managerダッシュボードに表示されるデフォルトの管理操作ではなく特定の操作を実行できます。

あるイベント タイプに対して、Unified Managerの管理機能を使用して修正するのではなく特定の操作を実行するには、希望する操作のカスタム スクリプトを設定します。設定したスクリプトをそのイベント タイプのアラートに関連付けると、イベントに対して個別に対処できます。この場合、[管理操作] ページやUnified Managerのダッシュボードでそのイベント タイプに対する管理操作は生成されません。

クラスタを管理します。

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。

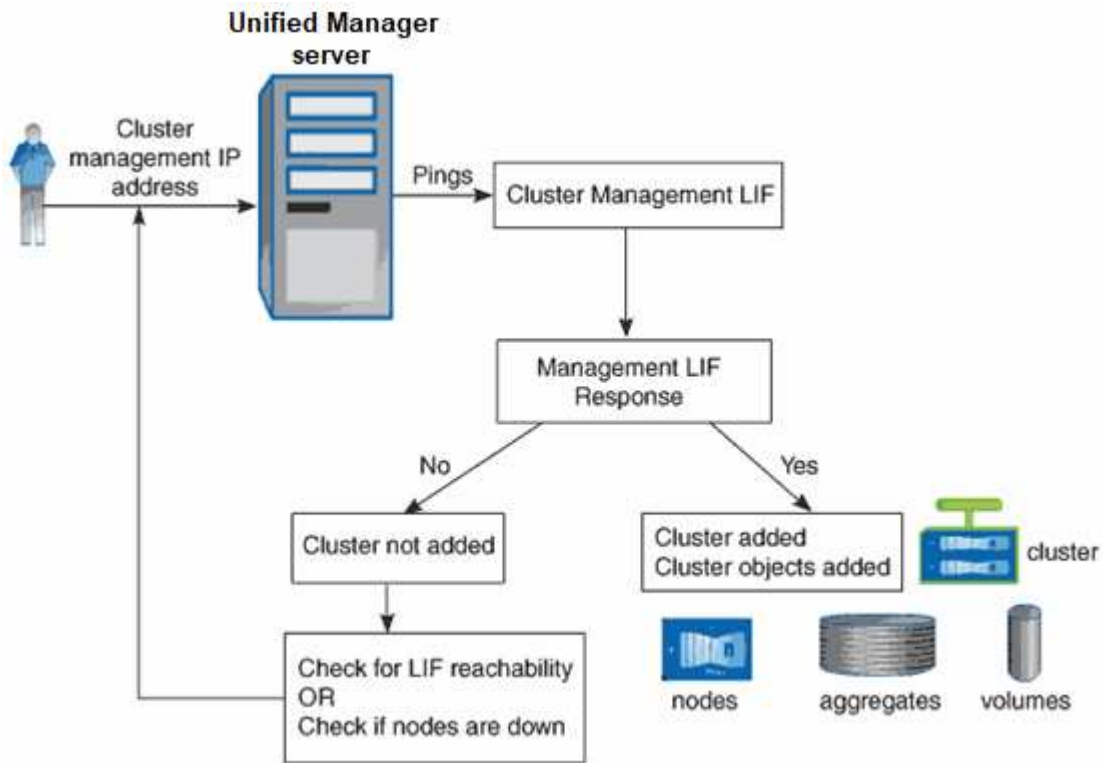
クラスタ検出プロセスの仕組み

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、使用するクラスタとそのオブジェクトを管理する際に役立ちます。

クラスタ構成情報を収集する監視間隔は15分です。たとえば、クラスターを追加した後、Unified Manager UI にクラスター オブジェクトが表示されるまでに 15 分かかります。この時間は、クラスタに変更を加えた場合

も同様です。たとえば、クラスター内の SVM に 2 つの新しいボリュームを追加すると、次のポーリング間隔（最大 15 分）後にそれらの新しいオブジェクトが UI に表示されます。

次の図は検出プロセスを示しています。



新しいクラスターのオブジェクトがすべて検出されると、Unified Managerは過去15日間のパフォーマンスデータの収集を開始します。これらの統計は、データの継続性収集機能を使用して収集されます。この機能では、クラスターが追加された直後から2週間分のクラスターのパフォーマンス情報を入手できます。データの継続性収集サイクルが完了すると、リアルタイムのクラスターパフォーマンスデータが収集されます（デフォルトでは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、新しいクラスターを複数追加する場合は、データの継続性収集のポーリングが同時に多数のクラスターで実行されないように、時間差をつけて追加するようにしてください。

監視対象クラスターのリストを表示する

[クラスター セットアップ]ページを使用して、クラスターのインベントリを表示できます。クラスターに関する詳細（名前またはIPアドレス、通信ステータスなど）を参照できます。

開始する前に

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、ストレージ管理 > クラスター セットアップ をクリックします。

ストレージ環境内の、Unified Managerで管理されているクラスターがすべて表示され、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。

クラスターを追加する

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

開始する前に

- アプリケーショ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クラスター、ONTAP Select、Cloud Volumes ONTAP をサポートします。
 - 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* ロールが必要です。

- 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9.9以降が実行されている必要があります。
- Unified Managerサーバに十分なスペースが必要です。スペースの使用率が90%を超えている場合、サーバにクラスタを追加することはできません。
- 必要な証明書を用意しておきます。

SSL (HTTPS) 証明書: この証明書は Unified Manager が所有します。Unified Managerの新規インストール時に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、この証明書をCA署名証明書にアップグレードすることを推奨します。サーバ証明書の有効期限が切れた場合は、証明書を再生成する必要があります。その後Unified Managerを再起動すると、新しい証明書がサービスに組み込まれます。SSL証明書の再生成の詳細については、以下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通知の認証に使用されます。

相互 TLS 通信用の証明書: Unified Manager とONTAP間の相互 TLS 通信中に使用されます。証明書ベースの認証は、クラスタのONTAPバージョンに基づいて有効になります。ONTAP 9.5よりも前のバージョンを実行しているクラスタでは、証明書ベースの認証は有効ではありません。

古いバージョンのUnified Managerを更新しても、クラスタの証明書ベースの認証は自動では有効になりません。ただし、クラスタの詳細を変更して保存すれば、認証を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、証明書を再生成して新しい証明書を組み込む必要があります。証明書の表示と再生成の詳細については、以下を参照してください。"[クラスタの編集](#)"。



- クラスタはWeb UIから追加でき、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することもできますが、証明書ベースの認証はデフォルトでは有効になりません。Unified ManagerのCLIを使用してクラスタを追加した場合、クラスタを編集するにはUnified Manager UIを使用する必要があります。見ることができます"[サポートされるUnified ManagerのCLIコマンド](#)"Unified Manager CLI を使用してクラスタを追加します。
- 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、あるサーバからUnified Managerのバックアップを作成し、ホスト名またはIPアドレスが異なる別のUnified Managerサーバにリストアすると、クラスタの監視に失敗することがあります。このエラーを回避するには、クラスタの詳細を編集して保存します。クラスタの詳細編集の詳細については、以下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インターフェイスによって、認証方式「cert」に対して2つの新しいユーザ グループ エントリが追加されます。

+

クラスタ証明書: この証明書はONTAPが所有します。有効期限が切れた証明書でUnified Managerにクラスタを追加することはできません。クラ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) の記事を参照してください。"[System ManagerユーザーインターフェイスでONTAP自己署名証明書を更新する方法](#)"。

- 1つのUnified Managerインスタンスでサポートできるノードの数には上限があります。ノードの数がサポートされる最大数を超える環境を監視する必要がある場合は、Unified Managerインスタンスを追加でインストールし、一部のクラスタをそのインスタンスで監視する必要があります。サポートされているノード数のリストを表示するには、"[『Unified Manager Best Practices Guide』](#)"。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > クラスタ セットアップ をクリックします。
2. クラスタ設定ページで、[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、必要に応じて値を指定し、[送信] をクリックします。
4. [ホストの承認] 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したあとに相互TLS通信用の証明書を表示できます。

証明書ベースの認証が有効になっていない場合、Unified Managerではクラスタの初回追加時にのみ証明書がチェックされます。ONTAPへのAPI呼び出しのたびに証明書がチェックされることはありません。

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日間のパフォーマンス データの収集を開始します。これらの統計は、データの継続性収集機能を使用して収集されます。この機能では、クラスタが追加された直後から2週間分のクラスタのパフォーマンス情報を入手できます。データの継続性収集サイクルが完了すると、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 (デフォルトでは5分間隔)。



- 15 日間のパフォーマンス データの収集には CPU 負荷がかかります。NetApp、データ継続性収集ポーリングが同時に多くのクラスターで実行されないように、新しいクラスターの追加を段階的に行うことを推奨しています。さらに、データ継続性収集期間中に Unified Manager を再起動すると、収集が停止し、欠落した期間のパフォーマンス チャートにギャップが表示されます。
- バージョン 9.14.1 以降のONTAPクラスターを追加すると、クラウド エージェント機能を通じて通信が行われます。ONTAP は、読み取り専用権限を持つ内部サービス アカウント ユーザー (clus-agent-xxxx など) を自動的に作成します。Unified Managerは、以下の場合、これらのクラスターからのデータ収集を停止します。`clus-agent` ユーザーは削除されます。

エラー メッセージが表示されてクラスターを追加できない場合は、次の問題がないかどうかを確認してください。



- 2つのシステムのクロックが同期されておらず、Unified ManagerのHTTPS証明書の開始日がクラスターの日付よりもあとの日付になっている。この場合、NTPなどのサービスを使用してクロックを同期する必要があります。
- クラスターのEMS通知の送信先が最大数に達しており、Unified Managerのアドレスを追加できない。デフォルトでは、クラスターで定義できるEMS通知の送信先は20個までです。

関連情報

["ユーザの追加"](#)

["クラスター リストおよび詳細の表示"](#)

["CAの署名を受けて返されたHTTPS証明書のインストール"](#)

クラスターを編集する

[クラスターを編集]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、ユーザー名、パスワード、ポートなど、既存のクラスターの設定を変更することができます。

開始する前に

アプリケーショ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、クラスターを追加する際に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、ストレージ管理 > クラスター セットアップ をクリックします。
2. *クラスター設定*ページで、編集するクラスターを選択し、*編集*をクリックします。
3. クラスターの編集 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 に追加されたクラスター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、["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、[再生成] ボタンをクリックして新しい証明書を組み込みます。
4. *送信*をクリックします。

5. [ホストの承認] ダイアログ ボックスで、[証明書の表示] をクリックして、クラスター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"](#)

クラスターを削除する

[クラスタ セットアップ]ページを使用してUnified Managerからクラスタを削除することができます。たとえば、クラスタの検出が失敗した場合やストレージ システムを運用停止する場合に、クラスタを削除できます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

このタスクでは、選択したクラスタをUnified Managerから削除します。削除したクラスタは監視されなくなります。削除したクラスタに登録されていたUnified Managerのインスタンスは、クラスタから登録解除されます。

クラスタを削除すると、そのストレージ オブジェクト、履歴データ、ストレージ サービス、関連するイベントもすべてUnified Managerから削除されます。この変更は、次のデータ収集サイクルのあとでインベントリ ページと詳細ページに反映されます。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > クラスター セットアップ をクリックします。
2. クラスター設定ページで、削除するクラスターを選択し、「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認します。

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"](#)

クラスターを再発見

[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ことで、クラスタの健全性、監視ステータス、パフォーマンス ステータスに関する最新情報を得られます。

クラスタを更新し（スペースが不足しているためにアグリゲートのサイズを増やす場合など）、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とOnCommand Workflow Automation（WFA）を連携させている場合は、WFAでキャッシュされたデータの再取得がトリガーされます。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > クラスター セットアップ をクリックします。
2. *クラスターのセットアップ*ページで、*再検出*をクリックします。

Unified Manager は選択したクラスターを再検出し、最新の健全性とパフォーマンス ステータスを表示します。

関連情報

["クラスター リストおよび詳細の表示"](#)

VMware仮想インフラストラクチャを監視する

Active IQ Unified Managerでは、仮想インフラ内の仮想マシン（VM）を可視化し、仮想環境内のストレージやパフォーマンスの問題を監視してトラブルシューティングできます。この機能を使用すると、ストレージ環境におけるレイテンシの問題や、vCenter Serverでパフォーマンス イベントが報告されたタイミングを特定できます。

ONTAPの一般的な仮想インフラ環境には、さまざまなコンポーネントがコンピューティング レイヤ、ネットワーク レイヤ、ストレージ レイヤに分散して配置されています。VM アプリケーションのパフォーマンスの遅延は、それぞれのレイヤーのさまざまなコンポーネントが直面する遅延の組み合わせにより発生する可能性があります。この機能は、ストレージまたはvCenter Serverの管理者およびITゼネラリストが、仮想環境におけるパフォーマンスの問題を分析したり、問題が発生したコンポーネントを特定したりするのに役立ちます。

[VMware]セクションの[vCenter]メニューからvCenter Serverにアクセスできるようになりました。リストされている各仮想マシンのピーク ビューには、トポロジ ビューに **VCENTER SERVER** リンクがあり、新しいブラウザーで vCenter Server を起動します。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 は、仮想環境の基盤となるサブシステムをトポロジ ビューで表示し、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遅延の問題が発生しているかどうかを判断します。このビューでは、パフォーマンスの低下の原因となっている特定のオブジェクトも強調表示されるので、改善策を講じて根本的な問題に対処することができます。

ONTAPストレージ上の仮想インフラには次のオブジェクトが含まれます。

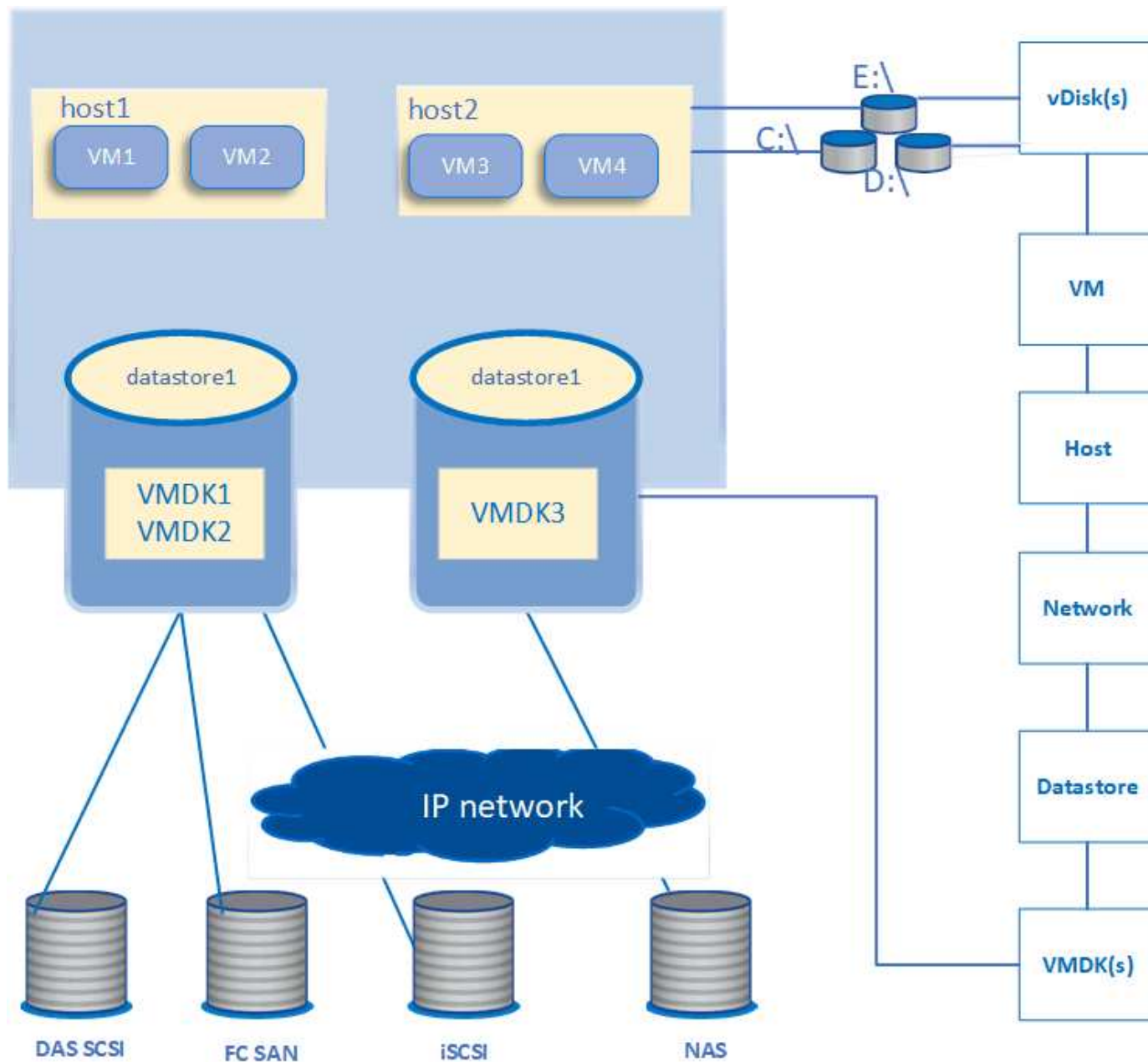
- vCenter Server: 仮想環境内の VMware VM、ESXi ホスト、および関連するすべてのコンポーネントを管理するための集中制御プレーン。vCenter Serverの詳細については、VMwareのドキュメントを参照してください。
- ホスト: VMware の仮想化ソフトウェアである ESXi を実行し、VM をホストする物理システムまたは仮想システム。
- データストア: データストアは、ESXi ホストに接続された仮想ストレージ オブジェクトです。LUNやボリュームなどのONTAPの管理可能なストレージ エンティティであり、ログ ファイル、スクリプト、構成ファイル、仮想ディスクなどのVMファイルのリポジトリとして使用され、SANまたはIPネットワーク接続を介して環境内のホストに接続されます。vCenter ServerにマッピングされているONTAP外部のデータストアは、Unified Managerではサポートされず、表示もされません。
- VM: VMware仮想マシンです。
- 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。仮想ディスクごとに対応するVMDKがあります。

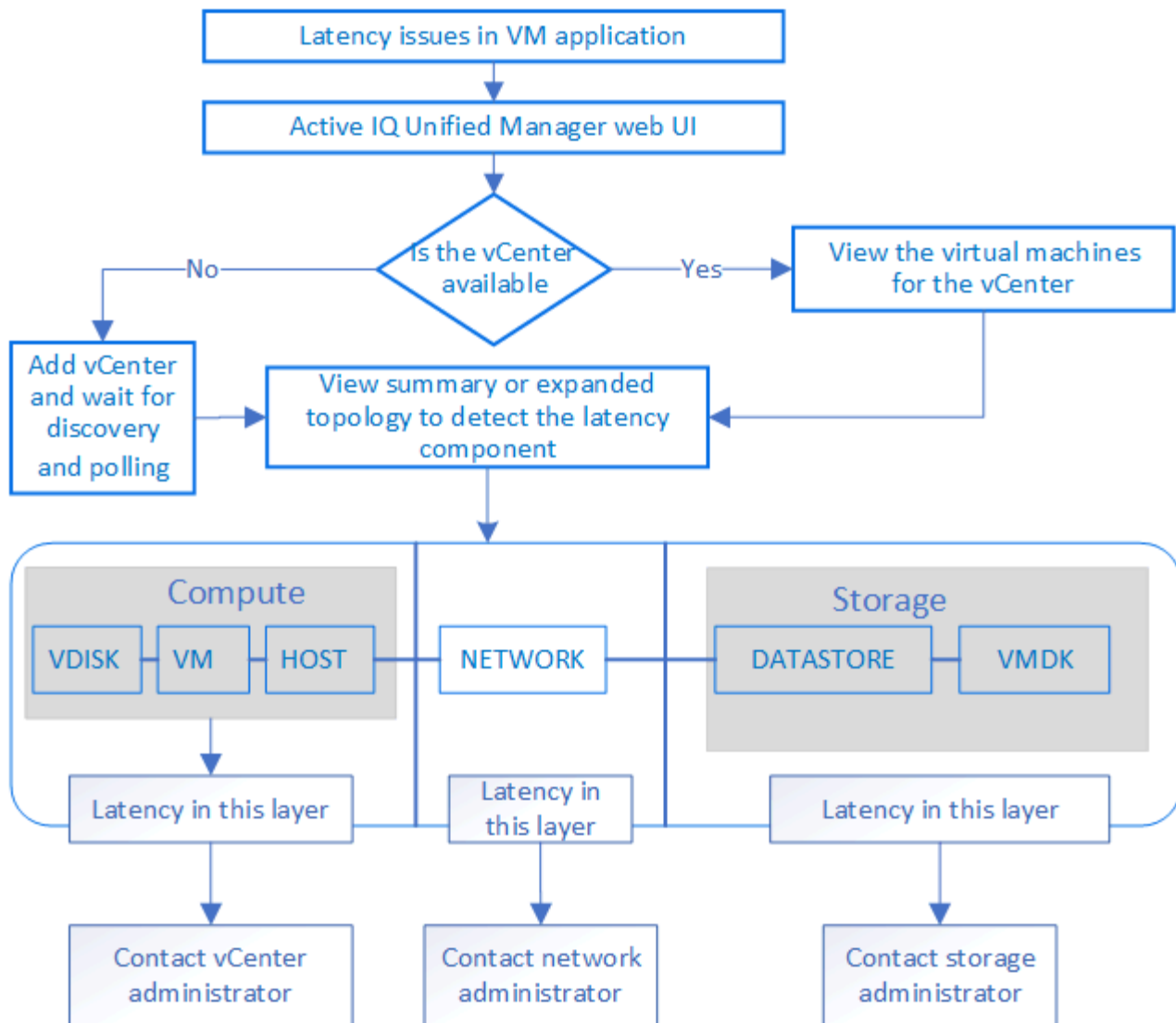
これらのオブジェクトはVMトポロジ ビューに表示されます。

- ONTAP上の VMware 仮想化 *



ユーザーワークフロー

次の図は、VMトポロジ ビューを使用する一般的なユースケースを示しています。



サポートされていない機能

- vCenter ServerインスタンスにマッピングされているONTAP外部のデータストアは、Unified Managerではサポートされません。これらのデータストアに仮想ディスクがあるVMもサポートされません。
- 複数のLUNにまたがるデータストアはサポートされません。
- ネットワーク アドレス変換（NAT）を使用してデータLIF（アクセス エンドポイント）をマッピングするデータストアはサポートされません。
- 複数のLIFがある構成で、ボリュームまたはLUNを同じIPアドレスを使用して異なるクラスタ上の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では、どのデータストアがどのクラスタに属しているかを特定できないためです。

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 は同じ IP アドレス xxxx を持つデータ LIF 経由でエクスポートされ、このデータストア上に VM A が作成されます。同様に、クラスタ B にはデータストア B があります。データストア B は、IP アドレスが同じ x.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 を対応する 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 および FC）だけです。仮想ボリューム（vVol）はサポートされません。

- iSCSI仮想ディスクのみがサポートされます。NVMeタイプとSATAタイプの仮想ディスクはサポートされません。
- 各コンポーネントのパフォーマンスを分析するレポートは生成できません。
- Unified Manager上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) 構成の場合、スイッチオーバーとスイッチバックのシナリオでは、アクティブなLUNを参照するようにvCenter Serverで設定を手動で変更する必要があります。手動で変更しないと、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してトラブルシューティングを行うには、関連するvCenter ServerをActive IQ Unified Managerインスタンスに追加する必要があります。

開始する前に

vCenter Serverを追加または表示する前に、次の項目を確認します。

- vCenter Serverの名前。
- vCenter ServerのIPアドレスと必要なクレデンシャル。vCenter Server管理者、またはvCenter Serverに読み取り専用でアクセスできるルート 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のサポートは、英語と日本語に対応しています。

- vCenter Serverのデータ収集設定は、統計レベルに設定されています。 *Level 3* すべての監視対象オブジェクトに対して必要なレベルのメトリック収集が確実に行われるようにします。間隔の長さは *5 minutes* 保存期間は *1 day*。

詳細については、VMware ドキュメントの『vSphere 監視およびパフォーマンス ガイド』の「データ収集レベル」セクション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。
- vCenter Serverにデータストアを追加するときにホストのIPアドレスと完全修飾ドメイン名 (FQDN) の両方を使用できる。FQDNを追加する場合は、Unified Managerサーバがドメイン名を解決できることを確認してください。たとえば、Linuxインストールの場合は、ドメイン名が `/etc/resolv.conf` ファイル。
- vCenter Serverの現在時刻がvCenter Serverのタイムゾーンと同期されている。
- vCenter Serverが到達可能で正しく検出される。
- Unified ManagerにvCenter Serverを追加するときにVMware SDKへの読み取りアクセス権がある。これは設定情報を取得するために必要です。

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および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の数などの設定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、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が表示されない場合は、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、デバイスに到達可能であることを確認します。
- c. 管理者またはvCenter Serverに読み取り専用でアクセスできるルート ユーザのユーザ名とパスワードを追加します。
- d. デフォルトの443以外のポートを使用している場合は、カスタム ポート番号を追加します。
- e. *保存*をクリックします。

検出に成功したら、表示されたサーバ証明書を承認します。

証明書を承認すると、vCenter Serverが使用可能なvCenter Serverのリストに追加されます。デバイスを追加しても、関連付けられたVMのデータ収集は開始されません。収集はスケジュールされた間隔で行われます。

2. **vCenters** ページで vCenter Server が利用できる場合は、ステータス フィールドにマウスを移動してステータスを確認し、vCenter Server が期待どおりに動作しているかどうか、または警告やエラーがあるかどうかを表示します。



vCenter Serverを追加すると、次のステータスが表示されます。ただし、vCenter Server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は最長で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 メトリックが正常に収集されたことを示します。
 - 黄色: 「警告」(たとえば、各オブジェクトの統計情報を取得するために vCenter Server の統計レベルが 3 以上に設定されていない場合)
 - オレンジ: 「エラー」(例外、構成データ収集の失敗、vCenter Server にアクセスできないなどの内部エラーを示します) 列表示アイコン (* 表示/非表示*) をクリックすると、vCenter Server のステータスのステータス メッセージが表示され、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 にアクセスできない場合、または資格情報が変更された場合は、[vCenter] > [編集] 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加えます。
 5. *保存*をクリックします。

vCenter Server データ収集が開始されます

vCenter Serverは、リアルタイムのパフォーマンス データのサンプルを20秒間収集して5分ごとのサンプルに集計します。Unified Managerのパフォーマンス データの収集スケジュールは、vCenter Serverのデフォルトの設定に基づきます。Unified Managerは、vCenter Serverから取得した5分ごとのサンプルを処理し、仮想ディスク、VM、およびホストのIOPSとレイテンシの1時間の平均を計算します。データストアの場合、Unified ManagerはONTAPから取得したサンプルに基づいてIOPSとレイテンシの1時間の平均を計算します。これらの値は毎時00分に更新されます。パフォーマンス指標はvCenter Serverを追加した直後には収集されず、次の1時間の開始時にのみ収集されます。パフォーマンス データのポーリングは、構成データ収集のサイクルが完了すると開始されます。

Unified Managerは、クラスタの構成データの収集と同じスケジュールでvCenter Serverの構成データをポーリングします。vCenter Serverの構成データ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」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 を削除する

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に、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）とその構成データも削除されます。削除したvCenter Serverは、その関連オブジェクトおよび履歴データも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。

開始する前に

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. vCenter 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 ダイアログで、**OK** をクリックして削除要求を確認します。

仮想マシンを監視する

仮想マシン（VM）のアプリケーションでレイテンシの問題が発生した場合、原因の分析とトラブルシューティングのためにVMの監視が必要になることがあります。VMを監視できるのは、vCenter ServeとVMストレージをホストしているONTAPクラスタがUnified Managerに追加されている場合です。

VMの詳細は、**VMWARE >> 仮想マシン** ページに表示されます。可用性、ステータス、使用済み容量と割り当て容量、ネットワーク レイテンシ、およびVM、データストア、ホストのIOPSとレイテンシなどの情報が表示されます。複数のデータストアをサポートする VM の場合、グリッドには、レイテンシが最も悪いデータストアのメトリックが表示され、追加のデータストアを示すアスタリスク アイコン (*) が表示されます。このアイコンをクリックすると、その他のデータストアの指標が表示されます。これらの列の一部はソートおよびフィルタリングできません。



VMとその詳細を表示するには、ONTAPクラスタの検出（ポーリングまたは指標の収集）が完了している必要があります。クラスタがUnified Managerから削除されると、次の検出サイクル後、VMを表示できなくなります。

このページでは、VMの詳細なトポロジを表示して、VMに関連するコンポーネント（ホスト、仮想ディスク、

接続されているデータストアなど)を確認することもできます。トポロジビューには、基礎となるコンポーネントが特定のレイヤーに次の順序で表示されます: 仮想ディスク > **VM** > ホスト > ネットワーク > データストア > **VMDK**。

トポロジの観点から I/O パスとコンポーネントレベルのレイテンシを特定し、ストレージがパフォーマンスの問題の原因であるかどうかを特定できます。トポロジの概要ビューには I/O パスが表示され、トラブルシューティング手順を決定できるように IOPS と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、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表示するトポロジの拡張ビューも表示できます。コンポーネントを選択するとレイヤ内の対応する I/O パスが強調表示されます。

概要トポロジを表示

トポロジのサマリビューで VM を表示してパフォーマンスの問題を特定するには、次の手順を実行します。

1. **VMWARE** > 仮想マシン 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。フィルター ボタンをクリックすると、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 では、VM、クラスタ、データストア、フォルダ、ファイルなどの vSphere エンティティの名前に特殊文字 (%、&、\$、#、@、!、\、/、:、?、"、<、>、|、;、' など) を使用できます。VMware vCenter Server および ESX/ESXi Server は、表示名で使用する特殊文字をエスケープしません。ただし、Unified Manager で名前が処理されると、異なる表示になります。たとえば、次のような名前の VM %\$VC_AIQUM_clone_191124% vCenter Server では次のように表示されます `%25\$VC\_AIQUM\_clone\_191124%25` Unified Manager で。名前に特殊文字が含まれる VM を照会する場合は、この問題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。
 - 平常時
 - 警告
 - アラート
 - 監視なし
 - 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 レイヤー全体のコンポーネントのトポロジの概要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最もレイテンシの高い仮想ディスクが表示されます。
5. 一定期間にわたるデータストアのレイテンシとスループットを分析するには、データストアオブジェクトアイコンの上にあるワークロードアナライザー 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、時間範囲を選択して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。ワークロードアナライザーの詳細については、「ワークロードアナライザー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。

拡張トポロジを表示

VM の拡張トポロジを表示することで、各コンポーネントを個別にドリルダウンできます。

手順

1. 概要トポロジ ビューから、[トポロジの展開] をクリックします。各オブジェクトのレイテンシ数値とともに、各コンポーネントの詳細なトポロジを個別に確認できます。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、最もレイテンシの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、それぞれの 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を解決することができます。



VMDKについては指標は報告されません。トポロジでは、VMDK名のみ表示され、指標は表示されません。

関連情報

["Workload Analyzerを使用したワークロードのトラブルシューティング"](#)

災害復旧セットアップにおける仮想インフラストラクチャの表示

MetroCluster構成またはStorage Virtual Machine (Storage VM) ディザスタ リカバリ (DR) 構成でホストされているデータストアについて、その構成とパフォーマンス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を表示する

MetroCluster構成のデータストアを表示する前に、次の前提条件を確認してください。

- 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がUnified Managerで管理されている必要があります。
- ONTAPとvCenter Serverで必要なセットアップを完了しておく必要があります。詳細については、ONTAPと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** > 仮想マシン 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。ワークロード アナライザー またはデータストア オブジェクト リンクをクリックします。ボリュームまたはLUNをホストしているプライマリ サイトが正常に機能している標準的なシナリオでは、プライマリ サイトのvServer クラスタの詳細が表示されます。
2. 災害が発生してセカンダリ サイトにスイッチオーバーしているシナリオでは、データストアのリンクをクリックするとセカンダリ 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表示されます。情報は、クラスタと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は、再びプライマリ 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表示されます。情報は、クラスタとvServerの検出が完了したあとに反映されます。

ストレージ **VM** の災害復旧構成内のデータストアを表示する

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、次の前提条件を確認してください。

- スイッチオーバーとスイッチバックが発生した場合は、HAペアのプライマリ クラスタとセカンダリ クラスタ、およびvCenter Serverの検出が完了している必要があります。
- ソース クラスタとデスティネーション クラスタ、およびStorage VMピアの両方がUnified Managerで管理されている必要があります。
- ONTAPとvCenter Serverで必要なセットアップを完了しておく必要があります。

- NAS (NFS および VMFS) データストアの場合、災害発生時の手順には、セカンダリ ストレージ VM の起動、データ LIF とルートの検証、vCenter Server での失われた接続の確立、VM の起動が含まれます。

プライマリ サイトへのスイッチバックでは、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でデータを同期する必要があります。

- SAN (VMFS の場合は iSCSI および FC) 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。災害発生時には、セカンダリ Storage VMの起動、データLIFとルートの確認の各手順が実行されます。iSCSIターゲットのIPがプライマリLIFと異なる場合は、IPを手動で追加する必要があります。新しいLUNが、ホストのストレージ アダプタのiSCSIアダプタの下にデバイスとして表示される必要があります。以降は、新しいVMFSデータストアは新しいLUNを使用して作成し、古いVMは新しい名前に登録する必要があります。また、VMが動作している必要があります。

リカバリ時には、ボリューム間でデータを同期する必要があります。同様に、新しいVMFSデータストアはLUNを使用して作成し、古いVMを新しい名前に登録する必要があります。

設定については、ONTAPと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** > 仮想マシン ページで、データストアをホストする VM インベントリをクリックします。データストア オブジェクトのリンクをクリックします。標準的なシナリオでは、プライマリ Storage VMのボリュームとLUNのパフォーマンス データが表示されます。
2. 災害が発生してセカンダリ サイトにスイッチオーバーしているシナリオでは、データストアのリンクをクリックするとセカンダリ Storage VM内のボリュームまたはLUNのパフォーマンス指標が表示されます。情

報は、クラスタと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は、再びプライマリStorage VM内のボリュームまたはLUNのパフォーマンス指標が表示されます。情報は、クラスタとvServerの検出が完了したあとに反映されます。

サポート対象外のシナリオ

- MetroCluster構成では次の制限があります。
 - クラスタは `NORMAL`、そして `SWITCHOVER` 状態が取り上げられます。他の州、例えば `PARTIAL_SWITCHOVER`、`PARTIAL_SWITCHBACK`、そして `NOT_REACHABLE` 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場合、プライマリ クラスタがダウンすると、セカンダリ クラスタを検出できず、トポロジは引き続きプライマリ クラスタ内のボリュームまたはLUN を指します。
- Storage VMディザスタ リカバリ構成では次の制限があります。
 - SAN ストレージ環境で Site Recovery Manager (SRM) または Storage Replication Adapter (SRA) が有効になっている構成はサポートされていません。

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では、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を使用して、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、管理することができます。



Unified Manager はデフォルトでこの機能を提供します。この機能を使用しない場合は、ストレージ管理 > 機能設定 から無効にすることができます。

有効にすると、Unified Manager のインスタンスによって管理されるONTAPクラスタ上で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。

これにより、次の機能を実行できるようになります。

- 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て、ストレージ ワークロードを容易に評価して導入できるようにする
- NFSおよびCIFSプロトコルをサポートするNASワークロードをプロビジョニングする
- iSCSIおよびFCPプロトコルをサポートするSANワークロードをプロビジョニングする
- 同じファイル共有でNFSとCIFSの両プロトコルをサポートする
- 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を管理する
- 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をストレージ ワークロードに割り当てる

UI の左側のペインにある プロビジョニング、ストレージ > ワークロード、および ポリシー オプションを使用すると、さまざまな構成を変更できます。

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 ページでストレージ ワークロードを表示します。
- [ワークロードのプロビジョニング]ページからストレージ ワークロードを作成する
- [ポリシー]からパフォーマンス サービス レベルを作成、管理する
- [ポリシー]からストレージ効率化ポリシーを作成、管理する
- [ワークロード]ページからストレージ ワークロードにポリシーを割り当てる

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

ワークロードとは、ボリュームやLUNなどのストレージ オブジェクトの入出力 (I/O) 処理のことです。ストレージのプロビジョニング方法は、想定されるワークロード要件に基づいています。ワークロード統計は、ストレージ オブジェクトとの間でトラフィックが発生した後にのみ、Active IQ Unified Managerによって追跡されます。たとえば、ユーザがデータベースまたはEメール アプリケーションの使用を開始した時点で、ワークロードのIOPSとレイテンシを取得できるようになります。

[ワークロード]ページには、Unified Managerで管理されているONTAPクラスタのストレージ ワークロードの概要が表示されます。このページには、パフォーマンス サービス レベルに準拠したストレージ ワークロードと準拠しないストレージ ワークロードに関して、その履歴情報が一目でわかるように表示されます。また、データセンター内のクラスタの合計容量、使用可能容量、使用済み容量、およびパフォーマンス (IOPS) を評価することもできます。



非準拠、利用不可、またはパフォーマンス サービス レベルで管理されていないストレージ ワークロード数を調べ、それらが準拠条件を満たし、推奨される使用済み容量、IOPSが確保されるために必要な操作を実行す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 によって管理されるONTAPクラスタ上のストレージ ワークロードの数の概要を示します。
- データセンターの概要: データセンター内のストレージ ワークロードの容量とIOPSを表示します。関連するデータは、データセンター レベルおよび個別に表示されます。

[ワークロードの概要]セクション

[ワークロードの概要]セクションには、ストレージ ワークロード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、パフォーマンス サービス レベルの割り当て状況に基づいて表示されます。

- 割り当て済み: パフォーマンス サービス レベルが割り当てられたストレージ 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。
 - 適合: ストレージ ワークロードのパフォーマンスは、割り当てられたパフォーマンス サービス レベルに基づいています。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のレイテンシ内である場合、それらは「適合」としてマークされます。準拠

しているワークロードは青で表示されます。

- ・ 非適合: パフォーマンス監視中に、ストレージ ワークロードのレイテンシが、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を超えると、ストレージ ワークロードは「非適合」としてマークされます。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 ワークロードは、オフラインの場合、または対応するクラスターにアクセスできない場合は、「利用不可」としてマークされます。利用不可の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」として報告されます。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合計数をクリックすると、ワークロード ページでそれらを表示できます。

パフォーマンス サービス レベル別の適合サブセクションには、使用可能なストレージ ワークロードの合計数が表示されます。

- ・ 各タイプのパフォーマンス サービス レベルに準拠している
- ・ パフォーマンス サービス レベルが割り当てられているが推奨のものと一致していない

[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は、データ センター内のすべてのクラスターの使用可能な容量と使用済み容量、および IOPS がグラフィカルに表示されます。このデータを使用して、ストレージ ワークロードの容量とIOPSを管理します。このセクションには、すべてのクラスターのストレージ 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ーの合計容量、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ーの合計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合計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、クラスター内のすべてのストレージ ワークロードの総使用済み容量とパフォーマンスに関して取得されます。

使用可能IOPSは、ノードでの想定レイテンシと推奨されるパフォーマンス サービス レベルに基づいて計算されます。これには、想定レイテンシがノード独自の想定レイテンシ以下であるすべてのパフォーマンス サービス レベルの使用可能IOPSが含まれます。

使用可能容量は、アグリゲートでの想定レイテンシと推奨されるパフォーマンス サービス レベルに基づいて計算されます。これには、想定レイテンシがアグリゲート独自の想定レイテンシ以下であるすべてのパフォーマンス サービス レベルの使用可能容量が含まれます。

ワークロードを表示

Unified Managerにクラスタを追加すると、各クラスタのストレージ ワークロードが自動的に検出されて[ワークロード]ページに表示されます。

Unified Managerは、ストレージ ワークロードでI/O処理が開始された時点で、推奨事項（推奨されるPSL）に対するワークロードの分析を開始します。

FlexGroupボリュームとそのコンスチチュエントは対象外です。

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:** ワークロードの合計数と、PSL が割り当てられているワークロードと割り当てられていないワークロードの数を表示します。また、PSLごとのワークロード数の内訳も表示されます。カウントをクリックすると、フィルタリングされたワークロードを含む「すべてのワークロード」ビューが表示されます。また、システム推奨事項に準拠していないワークロードの数を表示し、[システム推奨 **PSL** の割り当て] ボタンをクリックして、それらのワークロードにシステム推奨 PSL を割り当てることもできます。
- **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および使用済みスペース (TiB) とパフォーマンス (IOPS) を表示します。すべてのワークロードの使用可能スペースと使用済みスペース (TiB) およびパフォーマンス (IOPS) の、各PSL別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 によって管理されるONTAPクラスタに関連付けられているストレージ ワークロードが一覧表示されます。

I/O 操作が行われていない新しく検出されたストレージ ワークロードの場合、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 操作が開始されると、Unified Manager は分析を開始し、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。

このページを使用して、ストレージ ワークロードにストレージ効率化ポリシー（SEP）とパフォーマンス サービス レベル（PSL）を割り当てることもできます。次のような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
- ストレージ ワークロードにSEPを割り当てる

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

サポートされている LUN (iSCSI プロトコルと FCP プロトコルの両方をサポート)、NFS ファイル共有、および 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. ワークロードを作成します。詳細については、"[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確認したり、PSLや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。フィルター アイコンを使用して、検索の特定の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 単位) でフィルタリングできます。ただしこの場合、合計容量はバイト レベルで比較されるため、返されるワークロードの数が変わることがあります。

各ワークロードについて、ホスト クラスタとStorage VMなどの情報、および割り当てられているPSLとSEPが表示されます。

また、このページではワークロードのパフォーマンスの詳細を確認することもできます。列の選択/順序付け ボタンをクリックし、表示する特定の列を選択すると、ワークロードの IOPS、容量、およびレイテンシに関する詳細情報を表示できます。パフォーマンス ビュー列には、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 アナライザー アイコンをクリックすると、詳細な IOPS 分析を表示できます。

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に移動し、時間範囲を選択して、選択したワークロードのレイテンシ、スループット、容量の傾向を表示できます。ワークロードアナライザーの詳細については、以下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。オブジェクトを分析するためにワークロード分析ページでパフォーマンスと容量のチャートを表示するには、[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、"[Workload Analyzerで表示されるデータ](#)"。

ワークロードにポリシーを割り当てる

[すべてのワークロード]ページから、さまざまなナビゲーション 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にポリシーを割り当てる

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。

割り当てられたパフォーマンス サービス レベル および ストレージ効率化ポリシー フィールドが有効になっています。

3. 必要なPSL、SEP、またはその両方を選択します。

4. チェック マーク アイコンをクリックして変更を適用します。



ワークロードを選択し、「その他のアクション」をクリックしてポリシーを割り当てることもできます。

複数のストレージワークロードにポリシーを割り当てる

複数のストレージ ワークロードにまとめてPSLまたはSEPを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 ボックスをオンにするか、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」を選択します。SEP を割り当てるには、「ストレージ効率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た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なかったワークロードも、その原因とともに表示されます。



選択したワークロードの数によっては、複数のワークロードに一括でポリシーを適用する処理にしばらく時間がかかることがあります。バックグラウンドで実行 ボタンをクリックすると、操作がバックグラウンドで実行されている間に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、処理が完了するまでは別の要求を開始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る

システム推奨PSLは、データセンター内のPSLが割り当てられていないストレージ ワークロード、または割り当てられたPSLがシステムの推奨事項と一致しないストレージ ワークロードに割り当てることができます。この機能を使用するには、[システム推奨 **PSL** の割り当て] 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。

推奨事項はシステム分析によって内部的に決定され、IOPSなどのパラメータが使用可能なPSLの定義と一致しないワークロードについてはスキップされます。ストレージワークロード `Waiting for I/O` 学習ステータスも除外されます。



Unified Managerは、名前に特別なキーワードを含むワークロードを検索してシステム分析を上書きし、そのワークロードに別のPSLを推奨します。ワークロードの名前に「ora」という文字が含まれている場合は、**Extreme Performance PSL** が推奨されます。また、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、パフォーマンスPSL が推奨されます。

ナレッジベース (KB) の記事も参照してください "[ActiveIQ Unified Managerの「システム推奨パフォーマンスサービスレベルの割り当て」](#) は、変動の激しいワークロードには適応できません。"

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]ページでは、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フ

ファイル共有ボリュームを作成できます。

開始する前に

- 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。
- SMBサービスとNFSサービスのどちらかまたは両方がStorage VMで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ためには、ワークロードを作成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. *ワークロードのプロビジョニング*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** フィールドでは、そのクラスターで使用可能なストレージ VM がフィルターされます。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、さらにオプションでSEPをワークロードに割り当てます。

SEPの仕様がLUNに割り当てられ、ワークロードの作成時にPSLの定義がワークロードに割り当てられます。

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オンにします。

ワークロードにPSLを割り当てると、ワークロードが作成されるアグリゲートがポリシーに定義されているパフォーマンスと容量の目標を満たすことが保証されます。たとえば、ワークロードに「最高レベルのパフォーマンス」PSLが割り当てられている場合、そのワークロードをプロビジョニングするアグリゲートは、「最高レベルのパフォーマンス」ポリシーに設定されたパフォーマンスと容量をサポートできる (SSDストレージ) が必要となります。



このチェック ボックスをオンにしないと、PSLはワークロードに適用されず、ダッシュボードにはワークロードのステータスが「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。

有効な **NAS** オプションが表示されない場合は、選択したストレージ VM が SMB または NFS、あるい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。



ストレージ VM で SMB サービスと NFS サービスの両方が有効になっている場合は、[NFS で共有] および [SMB で共有] チェック ボックスをオンにして、NFS プロトコルと SMB プロトコルの両方をサポートするファイル共有を作成できます。SMB共有とCIFS共有のどちらかを作成する場合は、該当するチェック ボックスのみをオンにします。

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と一致しているかがチェックされ、指定したホストのエクスポート ポリシーが作成されるか、または既存のポリシーがある場合はそのポリシー

ーが使用されます。同じホストに対して複数のNFS共有を作成した場合は、そのホストで使用可能な一致するルールを含むエクスポート ポリシーがすべてのファイル共有で使用されます。APIを使用してNFS共有をプロビジョニングする場合は、個々のポリシーのルールを指定したり、特定のポリシー キーを指定してポリシーを再利用したりすることができます。

7. SMB共有の場合は、アクセスを許可するユーザまたはユーザ グループを指定し、必要な権限を割り当てます。ユーザ グループごとに、新しいアクセス制御リスト (ACL) がファイル共有の作成時に生成されます。
8. *保存*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]ページでは、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。

開始する前に

- 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ためには、ワークロードを作成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. *ワークロードのプロビジョニング*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。

選択したクラスターに基づいて、**STORAGE VM** フィールドでは、そのクラスターで使用可能なストレージ VM がフィルターされます。

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。

選択内容に基づいて、[ホスト情報]セクションの[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、およびオプションでワークロードの SEP を割り当てます。

SEPの仕様がLUNに割り当てられ、ワークロードの作成時にPSLの定義がワークロードに割り当てられます。

4. 割り当てられた 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オンにします。

ワークロードにPSLを割り当てると、ワークロードが作成されるアグリゲートがポリシーに定義されているパフォーマンスと容量の目標を満たすことが保証されます。たとえば、ワークロードに「最高レベルのパフォーマンス」PSLが割り当てられている場合、そのワークロードをプロビジョニングするアグリゲートは、「最高レベルのパフォーマンス」ポリシーに設定されたパフォーマンスと容量をサポートできる (SSDストレージ) が必要となります。



このチェックボックスを選択しないと、PSLはワークロードに適用されず、ダッシュボード上のワークロードのステータスは次のように表示されます。 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、選択したストレージ VM が iSCSI と FCP をサポートしているかどうかを確認してください。
6. ホストOSを選択します。
7. LUNへのイニシエータのアクセスを制御するホスト マッピングを指定します。既存のイニシエータ グループ (igroup) を割り当てるか、新しいigroupを定義してマッピングできます。



LUNのプロビジョニング時に新しいigroupを作成した場合は、次の検出サイクル（最大15分）でそのigroupが検出されるまでLUNの使用を待つ必要があります。したがって、使用可能なigroupのリストから既存のigroupを使用することを推奨します。

新しい igroup を作成する場合は、[新しいイニシエータ グループの作成] ボタンを選択し、igroup の情報を入力します。

8. *保存*をクリックします。

LUNがストレージ ワークロードのリストに追加されます。

パフォーマンスサービスレベル

パフォーマンス サービス レベル (PSL) を使用すると、ワークロードに対してパフォーマンスとストレージの目標を定義することができます。ワークロードの作成時または編集時にPSLをワークロードに割り当てることができます。

ストレージ リソースは、サービス レベル目標 (SLO) に基づいて管理および監視されます。SLOは、必要なパフォーマンスと容量に基づくサービス レベル アグリーメントによって定義されます。Unified Managerでは、SLO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の定義を意味します。ストレージ サービスの内容は、基盤となるリソースのパフォーマンスと利用率に基づいて決定されます。PSLは、ストレージ サービス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に対してパフォーマンスと容量の目標を指定できます。ワークロードにPSLを割り当てると、ONTAP上の対応するワークロードがパフォーマンスと容量の目標で管理されます。各PSLは、ピークIOPS、想定IOPS、絶対最小IOPS、および想定レイテンシで規定されます。

Unified Managerには次のタイプのPSLがあります。

- システム定義: Unified Manager には、変更できないいくつかの既定ポリシーが用意されています。事前定義されたPSLは次のとおりです。
 - 最高レベルのパフォーマンス
 - パフォーマンス
 - Value

「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に当てはまります。

Unified Managerには、データベース アプリケーション用に3種類のパフォーマンス 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厳しいデータベース 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）
- ユーザー定義: 事前定義されたパフォーマンス サービス レベルが要件を満たさない場合は、ニーズを満たす新しい PSL を作成できます。詳細については、"[パフォーマンス サービス レベルの作成と編集](#)"。
- **Beyond Extreme:** Beyond Extreme PSL は、Extreme よりも高い IOPS を要求するワークロードに推奨されるシステム推奨 PSL です。ワークロードは、IOPS、容量、レイテンシに基づいて内部的に分析され、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ごとに Beyond Extreme PSL が推奨されます。PSLをワークロードに適用すると、最適なパフォーマンスを確保することができます。

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 の名前に次の形式で追加されます。Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>。例えば、システムがワークロードのピークIOPと予想IOPを次のように決定した場合、106345`そして `37929`それぞれ、ワークロード用に生成されるBeyond Extreme PSLは次のように命名されます。`Beyond Extreme 106345 37929。これらのPSLはシステムによって推奨されていますが、ワークロードに割り当てると、これらのPSLは次のようにラベル付けされます。`User-defined` タイプで。

PSL を割り当ててワークロードを管理する

PSL には、ポリシー > パフォーマンス サービス レベル ページから、またはストレージ プロバイダー 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れば、ストレージ ワークロードを個別に管理する手間を省くことができます。変更についても、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ができます。Unified Managerは、内部の評価と推奨事項に基づいて、ワークロードにどのPSLを割り当てておくべきかを提案します。

システム推奨PSLをワークロードに割り当てて方法については、以下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る](#)"

[パフォーマンス サービス レベル]ページには使用可能なPSLポリシーが表示され、追加、編集、削除することができます。



システム定義のPSL、またはワークロードに現在割り当てられているPSLは変更できません。ワークロードに割り当てられているPSL、または他に使用可能なPSLがない場合、そのPSLは削除できません。

このページに表示される情報は次のとおりです。

フィールド	説明
Name	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。

フィールド	説明
予想IOPS/TB	LUNまたはファイル共有でアプリケーションが実行すると想定される最小IOPS。想定IOPSは、ストレージオブジェクトの割り当てサイズに基づいて、割り当てられる最小想定IOPSを指定します。
ピークIOPS/TB	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。 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、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。デフォルトの割り当てポリシーはused-spaceです。
絶対最小IOPS	絶対最小IOPSは、想定IOPSがこの値より低い場合に使用されます。システム定義のPSLのデフォルト値は次のとおりです。 • 最高レベルのパフォーマンス：想定IOPS $\geq$ 6144/TBの場合、絶対最小IOPS=1000 • パフォーマンス：6144/TB > 想定IOPS $\geq$ 2048/TBの場合、絶対最小IOPS=500 • バリュース：2048/TB > 想定IOPS $\geq$ 128/TBの場合、絶対最小IOPS=75 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。 • データベースログの極限: 予想される IOPS $>=$ 22528 の場合、絶対最小 IOPS = 4000 • データベース共有データのエクストリーム：予想されるIOPSが16384以上の場合、絶対最小IOPSは2000 • データベースデータの極限: 予想されるIOPSが12288以上の場合、絶対最小IOPSは2000 カスタムPSLの場合、絶対最小IOPSの最大値は75000です。最小値は次の式で計算されます。 1000/想定レイテンシ

フィールド	説明
想定レイテンシ	処理あたりのミリ秒（ms/op）で表したストレージIOPSの想定レイテンシ。
容量	クラスタ内の使用可能容量と使用済み容量の合計。
ワークロード	PSLが割り当てられているストレージ ワークロードの数。

ピーク IOPS と予想 IOPS がONTAPクラスタで一貫した差別化されたパフォーマンスの実現にどのように役立つかについては、次の KB 記事を参照してください

い。 https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F["パフォーマンス予算とは何ですか?"]

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るイベント

ワークロードが過去1時間のうち30%で想定レイテンシの値を超過すると、Unified Managerは次のいずれかのイベントを生成し、潜在的なパフォーマンスの問題として通知します。

- 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、何が高レイテンシを引き起こしているかを確認することができます。

詳細については、次のリンクを参照してください。

- ["ボリューム イベント"](#)
- ["パフォーマンスしきい値ポリシーを超えた場合の動作"](#)
- ["Unified Manager がワークロードの遅延を使用してパフォーマンスの問題を特定する方法"](#)
- ["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	説明と使用例	予想されるレイ テンシ（ミリ秒/ オペレーション ）	ピーク IOPS	想定 IOPS	絶対最小IOPS
最高レベルのパ フォーマンス	最高のスループ 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	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 / 仮想アプリケー ションに最適	2	4096	2048	500
Value	高いストレージ 容量を適度なレ イテンシで実現 大容量アプリケ ーション（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）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。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	説明と使用例	予想されるレイ テンシ（ミリ秒/ オペレーション ）	ピーク 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 ていて、データ ベース間で共有 されているデー タベース アプリ ケーション デー タに最適	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	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に合わない場合は、ワークロードに合わせて独自のパフォーマンス サービス レベルを作成できます。

開始する前に

- 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、次の予約済みキーワードは使用できません。

Prime、Extreme、Performance、Value、Unassigned、Learning、Idle、Default、そして 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 レベルを作成または編集するには、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。



ワークロードに現在割り当てられているパフォーマンス サービス レベルは変更できません。

手順

1. 左側のナビゲーション ペインの [設定] の下で、[ポリシー] > [パフォーマンス サービス レベル] 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適切なボタンをクリックします。

目的	次の手順に従ってください...
新しいパフォーマンス サービス レベルを作成する	*[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ためのページが表示されます。

3. パフォーマンス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、[送信] をクリックしてパフォーマンス サービス レベルを保存します。

新しく作成または変更したパフォーマンス 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をプロビジョニングするときに、ワークロード（LUN、NFSファイル共有、CIFS共有）に適用できます。

ストレージ効率ポリシーの管理

ストレージ効率化ポリシー（SEP）を使用して、ワークロードのストレージ効率化を定義することができます。ワークロードの作成時または編集時にSEPをワークロードに割り当てることができます。

ストレージ効率化では、ストレージ利用率を高めてストレージ コストを削減するシンプロビジョニング、重複排除、データ圧縮などのテクノロジーも使用されます。SEPを作成する一方で、このような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により、ストレージ効率を最大限に高めることができます。ポリシーをストレージ ワークロードに関連付けると、指定されたポリシー設定がストレージ ワークロードに割り当てられます。Unified Managerでは、システム定義とユーザ定義のSEPを割り当てて、データセンターのストレージ リソースを最適化できます。

Unified Manager には、高と低の 2 つのシステム定義の SEP が用意されています。これらのSEPはデータセンターのほとんどのストレージ ワークロードに当てはまりますが、システム定義のSEPが要件に合わない場合は独自のポリシーを作成できます。

システム定義のSEP、またはワークロードに現在割り当てられているSEPは変更できません。ワークロードに割り当てられているSEP、または他に使用可能なSEPがない場合、そのSEPは削除できません。

[ストレージ効率化ポリシー] 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、削除することができます。このページに表示される情報は次のとおりです。

フィールド	説明
Name	SEPの名前。

フィールド	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： ・ インライン: ワークロードに書き込まれている間に重複排除が行われます ・ 背景: 重複排除はワークロード内で行われる ・ 無効: ワークロードで重複排除が無効になっています
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： ・ インライン: ワークロードに書き込まれている間にデータ圧縮が行われます ・ 背景: データ圧縮はワークロード内で行われる ・ 無効: ワークロードでデータ圧縮が無効になっています
ワークロード	SEPが割り当てられているストレージ ワークロードの数

カスタムのストレージ効率化ポリシー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さない場合、カスタムのSEPを作成できます。ただし、なるべくシステム定義のSEPを使用し、必要な場合にのみカスタムの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]ページおよび[ボリューム / 健全性の詳細]ページで確認できます。これらのストレージ効率に基づいたクラスター レベルのデータ削減率 (スナップショット コピーなし) は、ダッシュボードの [容量] パネルと [容量: すべてのクラスター] ビューで確認できます。

ストレージ効率ポリシーの作成と編集

システム定義のストレージ効率化ポリシーがワークロードの要件に合わない場合は、ワークロードに合わせて独自のストレージ効率化ポリシーを作成できます。

開始する前に

- ・ 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名は一意である必要があり、次の予約済みキーワードは使用できません。

High、Low、Unassigned、Learning、Idle、Default、そして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または編集するには、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 [設定] の下で、[ポリシー] > [ストレージ効率] を選択します。
2. ストレージ効率ポリシー ページで、新しいストレージ効率ポリシーを作成するか、既存のストレージ効率ポリシーを編集するかに応じて適切なボタンをクリックします。

目的	次の手順に従ってください...
新しいストレージ効率化ポリシーを作成する	*追加*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. ストレージ効率特性を指定してストレージ効率ポリシーをカスタマイズし、「送信」をクリックしてストレージ効率ポリシーを保存します。

新しく作成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をプロビジョニングするときに、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構成の管理と監視

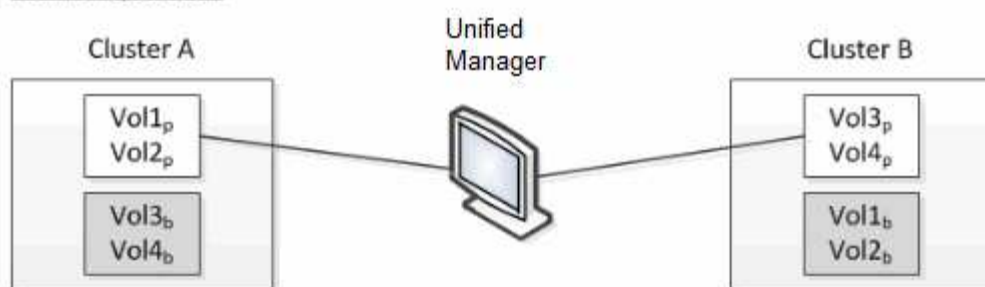
Unified Manager Web UIでは、MetroCluster構成を監視して、MetroCluster over FC構成とMetroCluster over IP構成に接続の問題が生じていないかを確認できます。接続の問題を早期に検出することで、MetroCluster構成を効果的に管理できます。

スイッチオーバーおよびスイッチバックの発生時のボリュームの動作

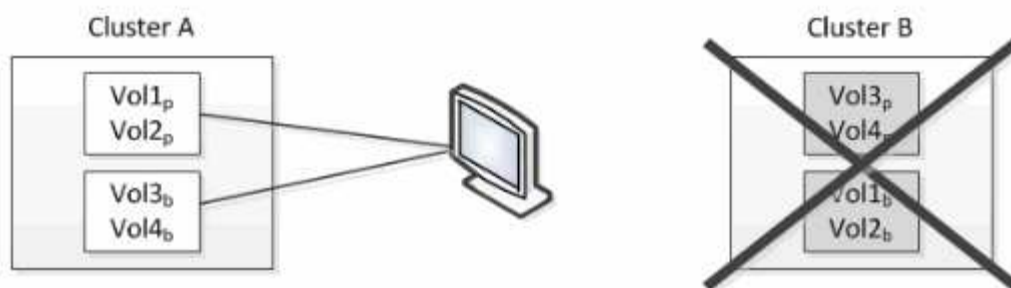
スイッチオーバーまたはスイッチバックをトリガーするイベントが発生すると、ディザスタ リカバリ グループの一方のクラスタからもう一方のクラスタにアクティブなボリュームが切り替わります。クライアントにデータを提供していたアクティブなクラスタのボリュームは停止され、代わりにアクティブになったもう一方のクラスタのボリュームからデータの提供が開始されます。Unified Managerでは、実行中のアクティブなボリュームのみが監視されます。

ボリュームが一方のクラスタからもう一方のクラスタに切り替わるため、両方のクラスタを監視することを推奨します。Unified Managerでは単一のインスタンスでMetroCluster構成の両方のクラスタを監視できますが、監視する2つのクラスタ間の距離によっては、両方のクラスタを監視するためにUnified Managerインスタンスが2つ必要になる場合もあります。次の図は、Unified Managerの単一のインスタンスを示しています。

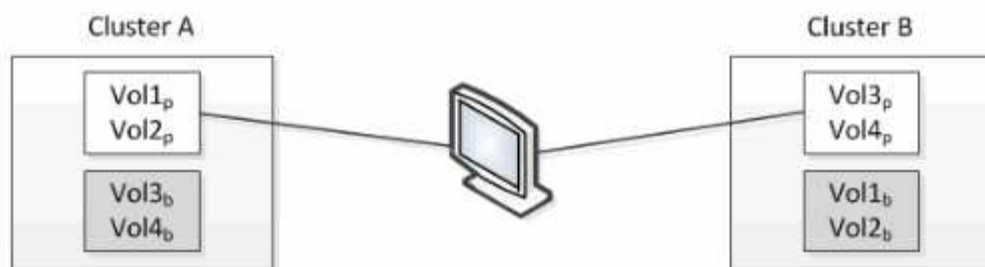
Normal operation



Cluster B fails --- switchover to Cluster A



Cluster B is repaired --- switchback to Cluster B



□ = active and monitored

■ = inactive and not monitored

名前に「p」が付いているボリュームはプライマリ ボリュームで、「b」が付いているボリュームはSnapMirrorで作成されたバックアップ用のミラー ボリュームです。

通常運用時の状態は次のとおりです。

- クラスタ A には、Vol1p と Vol2p という 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 には、Vol3b と Vol4b という 2 つの非アクティブなボリュームがあります。
- クラスタ B には、Vol1b と Vol2b という 2 つの非アクティブなボリュームがあります。

Unified Managerにより、アクティブなボリュームのそれぞれに関する情報（統計やイベントなど）が収集されます。Vol1pとVol2pの統計がクラスタAから収集され、Vol3pとVol4pの統計がクラスタBから収集されます。

重大な障害が発生してアクティブなボリュームがクラスタBからクラスタAにスイッチオーバーされると次のようになります。

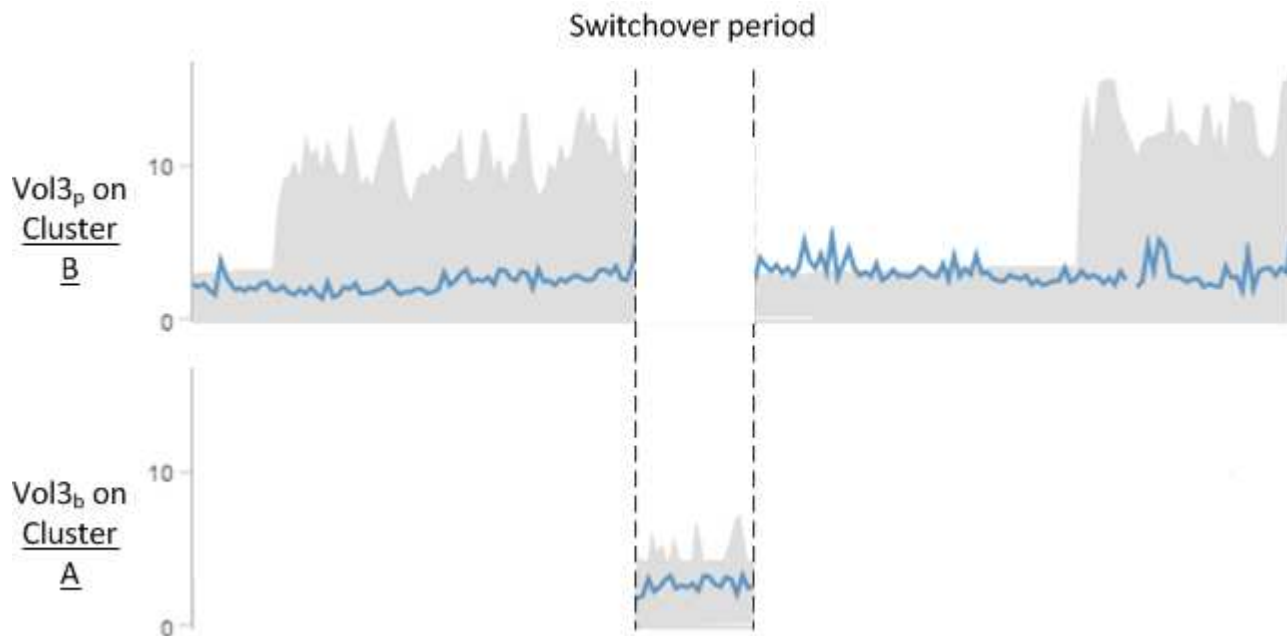
- クラスター A には、Vol1p、Vol2p、Vol3b、Vol4b の 4 つのアクティブ ボリュームがあります。
- クラスター B には、Vol3p、Vol4p、Vol1b、Vol2b の 4 つの非アクティブなボリュームがあります。

通常運用時と同様に、Unified Managerでアクティブなボリュームのそれぞれに関する情報が収集されます。ただし、この場合は、Vol1pとVol2pの統計がクラスターAから収集され、Vol3pとVol4pの統計もクラスターAから収集されます。

Vol3pとVol3bは異なるクラスターにあり、同じボリュームではないことに注意してください。Unified Managerに表示されるVol3pの情報は、Vol3bと同じにはなりません。

- クラスターAにスイッチオーバーしている間は、Vol3pの統計とイベントは表示されません。
- スwitchオーバーの発生直後は、履歴情報がないため、Vol3bは新規のボリュームのように見えます。

クラスターBが復旧してスイッチバックが実行されると、クラスターBのVol3pが再びアクティブになり、スイッチオーバーしていた期間を除いた状態で過去の統計が表示されます。クラスターAのVol3bの情報は、次にスイッチオーバーが発生するまでは表示されません。



- スwitchバック後のクラスター A の Vol3b など、非アクティブなMetroClusterボリュームは、「このボリュームは削除されました」というメッセージで識別されます。このボリュームは、実際には削除されていませんが、アクティブなボリュームでないためUnified Managerで現在監視されていません。
- 単一のUnified ManagerでMetroCluster構成の両方のクラスターを監視している場合にボリュームを検索すると、その時点でアクティブなボリュームの情報が返されます。たとえば、スイッチオーバーが発生してクラスターAでVol3がアクティブになっている場合、「Vol3」を検索するとクラスターAのVol3bの統計とイベントが返されます。

MetroCluster over FC構成のクラスター接続ステータスの定義

FC 経由のMetroCluster構成内のクラスター間の接続は、最適、影響あり、またはダウンのいずれかのステータスになります。接続ステータスを理解しておく、MetroCluster構

成を効果的に管理できるようになります。

接続ステータス	説明	アイコンが表示されました
最適	MetroCluster構成のクラスタ間の接続は正常な状態です。	
影響を受けた	1つ以上のエラーによってフェイルオーバー可用性のステータスが損なわれていますが、MetroCluster構成の両方のクラスタは稼働しています。たとえば、ISLリンクが停止している、クラスタ間IPリンクが停止している、パートナー クラスタにアクセスできないなどの場合です。	
下	一方または両方のクラスタが停止しているか、クラスタがフェイルオーバー モードになっているため、MetroCluster構成のクラスタ間の接続が停止しています。たとえば、災害によってパートナー クラスタが停止している、テスト目的で計画的スイッチオーバーを実行中などの状況が考えられます。	スイッチオーバーでエラー：  スイッチオーバー成功： 

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、データのミラーリングが可能で、サイト全体が利用できない状態になった場合にフェイルオーバーを開始する機能もあります。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、「正常」または「ミラーリング利用不可」のいずれかになります。これらのステータスを理解しておくと、MetroCluster構成を効率的に管理できます。

データミラーリングステータス	説明	アイコンが表示されました
平常時	MetroCluster構成のクラスタ間のデータ ミラーリングが正常な状態です。	

データミラーリングステータス	説明	アイコンが表示されました
ミラーリングは利用できません	スイッチオーバーが原因で、MetroCluster構成のクラスタ間のデータ ミラーリングが利用できない状態になっています。たとえば、災害によってパートナー クラスタが停止している、テスト目的で計画的スイッチオーバーを実行中などの状況が考えられます。	スイッチオーバーでエラー：  スイッチオーバー成功： 

MetroCluster構成の監視

MetroCluster構成の接続の問題を監視することができます。クラスタ内のコンポーネントおよび接続のステータス、MetroCluster構成のクラスタ間の接続ステータスなどの詳細情報を確認できます。ここでは、MetroCluster over FC構成とMetroCluster over IP構成で保護されているクラスタの接続の問題を監視する方法について説明します。

MetroCluster構成は、Active IQ Unified Managerの左側のナビゲーション ペインから表示する次のビューで監視できます。

- ストレージ > クラスタ > 保護: **MetroCluster** ビュー
- 保護 > 関係 > 関係: **MetroCluster** ビュー

Unified Managerでは、システム健全性アラートを使用して、MetroCluster構成のコンポーネントおよび接続のステータスを示します。

開始する前に

- 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構成では、Mediatorがサポートされる場合は、対応するAPIでMediatorを設定してクラスタに追加する必要があります。
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

MetroCluster over FC構成の接続の問題の監視

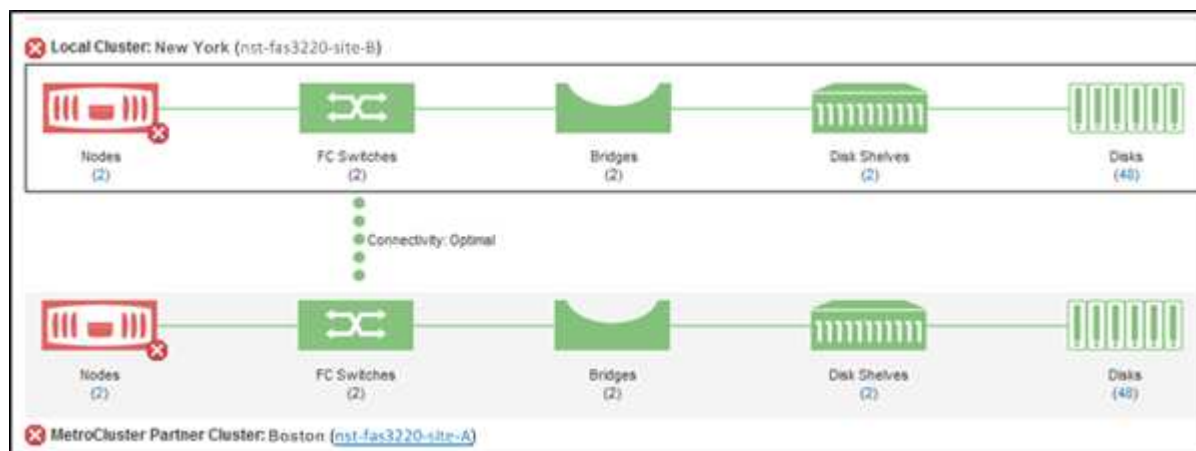
MetroCluster over FC 構成内のクラスターの場合、接続チャートは クラスター / ヘルス 詳細ページに表示されます。次の手順を実行します。

手順

1. 左側のナビゲーション ペインで、ストレージ > クラスター 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. 保護: **MetroCluster** ビューから、MetroCluster over FC 構成の詳細を表示するクラスタの名前をクリックします。または、MetroCluster構成のクラスタでフィルタすることもできます。
3. クラスタ/ヘルス*詳細ページで、MetroCluster接続*タブをクリックします。* MetroCluster接続* タブは、MetroCluster over FC 構成でのみ使用できます。



対応するクラスタ オブジェクト領域にMetroCluster構成のトポロジが表示されます。[クラスタ / 健全性の詳細]ページに表示される情報を基に、接続の問題を修正できます。たとえば、クラスタ内のノードとスイッチの間の接続がダウンしている場合は、次のアイコンが表示されます。



アイコンにカーソルを合わせると、生成されたイベントに関する詳細情報が表示されます。

MetroCluster構成で接続の問題が見つかった場合は、System ManagerにログインするかONTAP CLIにアクセスして問題を解決する必要があります。

クラスタの健全性の判定の詳細については、以下を参照してください。"[MetroCluster over FC構成でクラスタの健全性を確認する](#)"。

MetroCluster over IP構成の接続の問題の監視

MetroCluster over IP 構成内のクラスターの場合、接続チャートは クラスター 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、ストレージ > クラスター 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. 保護: **MetroClusters** ビューから、MetroCluster over IP 構成の詳細を表示するクラスタの名前をクリックします。または、MetroCluster構成のクラスタでフィルタすることもできます。
3. カーソルをクリックして行を展開します。`v`アイコン。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ればMediatorを表示できます。表示できる情報は次のとおりです。

- サイト間の接続
- 両方のサイトの健全性と可用性の問題（ある場合）
- Mediator関連の問題
- レプリケーション関連の問題



以下のステータスが報告されます: クリティカル (❌)、エラー (⚠️)、または通常 (✅)。同じトポロジ内のプライマリ データとミラー データ間のアグリゲート データのレプリケーション ステータスも表示できます。

次の図では、ソース クラスタとデスティネーション クラスタ間にサイト間接続がなく、クラスタ間にMediatorが設定されていないことがわかります。



- ステータス アイコンをクリックします。エラー定義を含むメッセージが表示されます。MetroCluster over IP 構成の問題に関する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、イベントの詳細を表示できます。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通常の状態 (✅)。
- さらに詳しい構成の詳細は、クラスタ/ヘルス*詳細ページの*構成*タブにある MetroClusterの概要*および*保護*セクションで確認できます。



MetroCluster over IP 構成の場合のみ、クラスター ページでクラスター トポロジを表示できます。MetroCluster over FC 構成のクラスターの場合、トポロジは クラスター/ヘルス 詳細ページの * MetroCluster接続* タブに表示されます。

関連情報

- ["\[クラスタ / 健全性の詳細ページ\]"](#)
- *Relationship: MetroCluster*ビューの詳細については、["MetroCluster構成の監視"](#)。
- *関係:過去1か月間の転送ステータス*ビューの詳細については、["関係: 過去1か月間の転送ステータスビュー"](#)。
- *関係:過去1か月間の転送率*ビューの詳細については、["関係: 過去1か月間の転送率ビュー"](#)。

- *関係: すべての関係*ビューの詳細については、"[関係: すべての関係ビュー](#)"。

MetroClusterレプリケーションを監視する

データのミラーリング中に論理接続の全体的な健全性を監視し、診断することができます。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では、システム ヘルス アラートを使用して、MetroCluster構成のコンポーネントおよび接続のステータスを監視します。

開始する前に

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を表示する

MetroCluster over IP構成では、Unified Managerの左側のナビゲーション ペインから次のビューを表示すると、MetroCluster over IPで保護されているクラスタのトポロジ ビューにデータのレプリケーション ステータスが表示されます。

- ストレージ > クラスタ > 保護: **MetroCluster** ビュー
- 保護 > 関係 > 関係: **MetroCluster** ビュー

詳細については、"[MetroCluster over IP の接続の問題を監視する](#)"。

FC構成上のMetroClusterのレプリケーションを表示する

次の手順に従って、MetroCluster over FC構成のデータ レプリケーションの問題を特定します。

手順

1. 左側のナビゲーション ペインで、ストレージ > クラスタ 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. **[ヘルス: すべてのクラスター]** 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ー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構成のトポロジが、データのミラー先であるリモート サイトの情報とともに表示されます。アイコンにカーソルを合わせると、生成されたイベントに関する詳細情報が表示されます。

[クラスタ / 健全性の詳細]ページに表示される情報を基に、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

"[\[クラスタ / 健全性の詳細ページ\]](#)"

割り当てを管理する

ユーザ クォータとグループ クォータを使用して、ユーザまたはユーザ グループが使用できるディスク スペースの量やファイルの数を制限できます。ディスクやファイルの使用量、ディスクに設定されている各種の制限など、ユーザ クォータとユーザ グループ クォータの情報を確認することができます。

クォータ制限とは

ユーザ クォータ制限とは、ユーザのスペース使用量がそのユーザのクォータで設定されている制限値に近づいているかどうか、または到達したかどうかを評価するために Unified Manager サーバで使用される値です。ソフト制限を超えた場合、またはハード制限に達した場合、Unified Manager サーバはユーザー クォータ イベントを生成します。

デフォルトでは、Unified Manager サーバは、クォータ ソフト制限を超えたか、クォータ ハード制限に達し、ユーザー クォータ イベントが設定されているユーザーに通知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。

ユーザーとユーザー グループの割り当てを表示する

[Storage VM / 健全性の詳細] ページには、SVM に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た制限、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 アドレスを表示できます。

開始する前に

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、ストレージ > ストレージ **VM** をクリックします。
2. 「正常性: すべてのストレージ **VM**」 ビューで、ストレージ VM を選択し、「ユーザーとグループのクォータ」 タブをクリックします。

関連情報

["ユーザの追加"](#)

メールアドレスを生成するルールを作成する

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。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- [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]ページのガイドラインを確認しておく必要があります。

クォータのEメール アドレスのルールを定義して、実行順にそれらを入力する必要があります。たとえば、abcで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、それ以外のグループについてはEメール アドレス「`dl-$GROUP@$DOMAIN`」を使用する場合は、次の順序でルールを指定する必要があります。

- `if ( $USER == 'abc' ) then abc@xyz.com`
- `if ( $GROUP == * ) then dl-$GROUP@$DOMAIN`

指定したどのルールの条件も満たされなかった場合は、デフォルトのルールが使用されます。

```
if ( $USER_OR_GROUP == * ) then $USER_OR_GROUP@$DOMAIN
```

手順

1. 左側のナビゲーション ペインで、全般 > クォータ電子メール ルール 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. ルールの構文を検証するには、[検証] をクリックします。

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*をクリックします。
5. 作成した電子メール アドレスが、ストレージ **VM**/ヘルス 詳細ページの ユーザーおよびグループ クォータ タブに表示されていることを確認します。

ユーザーおよびユーザー グループのクォータに関する電子メール通知形式を作成する

クォータ関連の問題が発生したとき（ソフト リミットを超えたとき、またはハード リミットに達したとき）にユーザまたはユーザ グループに送信するEメール通知の形式を作成できます。

開始する前に

アプリケーショ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、全般 > クォータ メール形式 をクリックします。
2. 送信元、件名、*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. 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. プレビュー ウィンドウを閉じるには、[閉じる] をクリックします。
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*をクリックします。

ユーザーとグループのクォータのメールアドレスを編集する

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 アドレスの変更は、[ユーザ クォータおよびグループ クォータの E メール アドレスを生成するルール]ダイアログ ボックスで指定したルールに従って生成されたEメール アドレスを上書きする場合に行います。

開始する前に

- 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。
- あなたは、["ルール作成のガイドライン"](#)。

Eメール アドレスを編集すると、ユーザ クォータおよびグループ クォータのEメール アドレスを生成するルールがクォータに適用されなくなります。指定したルールに従って生成されたEメール アドレスに通知を送信するには、Eメール アドレスを削除して変更内容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、ストレージ > **SVM** をクリックします。
2. 「健全性: すべてのストレージ **VM**」 ビューで、SVM を選択し、「ユーザーとグループのクォータ」 タブをクリックします。
3. タブの行の下にある*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	操作
指定したルールに従って生成されたEメール アドレスに通知を送信する	a. メールアドレス フィールドのメールアドレスを削除します。 b. *保存*をクリックします。 c. F5キーを押してブラウザをリフレッシュし、[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ます。指定されたルールによって生成された電子メール アドレスが 電子メール アドレス フィールドに表示されます。
指定したEメール アドレスに通知を送信する	a. メールアドレス フィールドのメールアドレスを変更します。 b. *保存*をクリックします。ユーザ クォータおよびグループ クォータのEメール アドレスを生成するルールがクォータに適用されなくなります。

クォータについてさらに詳しく

クォータに関する概念を理解しておく、ユーザ クォータとユーザ グループ クォータを効率的に管理できるようになります。

クォータ プロセスの概要

クォータには、ソフト クォータとハード クォータがあります。ソフト クォータでは、指定された制限を超過すると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過すると書き込み処理が失敗します。

ONTAPでユーザまたはユーザ グループからFlexVolへの書き込み要求が受信されると、そのボリュームでこ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チェックされ、次の点を確認されます。

- ハード リミットに到達するか

到達する場合は、ハード リミットに到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

超える場合は、ソフト リミットを超えても書き込み処理が成功し、ソフト クォータ通知が送信されます。

- 書き込み処理でソフト リミットを超えないか

超えない場合は、書き込み処理が成功し、通知は送信されません。

クォータについて

クォータを使用すると、ユーザ、グループ、またはqtreeによって使用されるディスク スペースやファイル数を制限したり、追跡したりできます。クォータを指定するには、`/etc/quotas` ファイル。クォータは、特定のボリュームまたはqtreeに適用されます。

クォータの使用目的

クォータは、FlexVol内のリソース使用量を制限したり、リソース使用量が特定のレベルに達したときに通知したり、リソース使用量を追跡したりするために使用できます。

次のような場合にクォータを指定します。

- ユーザやグループが使用できる、またはqtreeに格納できる、ディスク スペースの容量やファイル数を制限する場合
- 制限を適用せずに、ユーザ、グループ、またはqtreeによって使用されるディスク スペースの容量やファイル数を追跡する場合
- ユーザが使用するディスク容量やファイル数が多いときにユーザに警告する場合

クォータのダイアログ ボックスの説明

[ヘルス: すべてのストレージ VM] ビューの [ユーザーおよびグループ クォータ] 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電子メール通知の形式を構成したり、ユーザー クォータに基づいて電子メール アドレスを指定す

るルールを構成したりすることができます。

電子メール通知の形式ページ

[Eメール通知の形式]ページには、クォータに関する問題が発生（ソフト リミットを超過するかハード リミットに到達）したとき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。

電子メール通知は、次のユーザーまたはユーザー 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: ユーザーまたはグループ クォータのディスク領域のソフト制限に達しました、ユーザーまたはグループ クォータのファイル数のソフト制限に達しました、ユーザーまたはグループ クォータのディスク領域のハード制限に達しました、またはユーザーまたはグループ クォータのファイル数のハード制限に達しました。

- 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も可能です。デフォルトは、[通知]ページで指定されたEメール アドレスです。

- 主題

通知メールの件名が表示されます。

- メールの詳細

通知メールのテキストが表示されます。テキストは必要に応じて変更が可能です。たとえば、クォータ属性に関する情報を使用してキーワードの数を減らすことができます。ただし、キーワードは変更しないでください。

有効なキーワードは次のとおりです。

- \$EVENT_NAME

Eメール通知の原因となったイベントの名前を示します。

- \$QUOTA_TARGET

クォータが適用されるqtreeまたはボリュームを示します。

- \$QUOTA_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 リミットについて、ユーザまたはユーザ グループが使用している割合を示します。

- \$QUOTA_LIMIT

ユーザまたはユーザ グループがリミットに達して次のいずれかのイベントが生成されたディスクのハード リミットまたはファイルのハード リミットを示します。

- ユーザ / グループ クォータのディスク スペースがハード リミットに到達
 - User or Group Quota Disk Space Soft Limit Reached
 - ユーザ クォータまたはグループ クォータのファイル数がハード リミットに到達

- User or Group Quota File Count Soft Limit Reached

- \$QUOTA_USED

ユーザまたはユーザ グループが使用しているディスク スペースと作成したファイルの数を示します。

- \$QUOTA_USER

ユーザまたはユーザ グループの名前を示します。

コマンド ボタン

各コマンド ボタンを使用して、Eメール通知の形式に対する変更内容をプレビュー、保存、キャンセルできます。

- プレビュー

通知メールのプレビューが表示されます。

- 工場出荷時のデフォルトに戻す

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。

ユーザーおよびグループクォータの電子メールアドレスを生成するルールページ

[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]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。

ルールエリア

クォータのEメール アドレスに関するルールを定義する必要があります。ルールを説明するコメントを追加することもできます。

ルールを定義する方法

ルールは実行する順序で入力する必要があります。最初のルールの条件が満たされると、そのルールに基づいてEメール アドレスが生成されます。この条件が満たされなかった場合は、その次のルールへと順番に条件が評価されます。各ルールは個別の行にリストされます。デフォルトのルールはリストの一番下に表示されます。ルールの優先順位は変更可能です。ただし、デフォルトのルールの順序は変更できません。

たとえば、qtree1でのクォータ違反に関する通知をEメール アドレス「qtree1@xyz.com」で受信し、それ以外のqtreeについてはEメール アドレス「admin@xyz.com」を使用する場合は、次の順序でルールを指定する必要があります。

- if (\$QTREE == 'qtree1') then qtree1@xyz.com

- if (\$QTREE == *) then admin@xyz.com

指定したどのルール of の条件も満たされなかった場合は、デフォルト of のルールが使用されます。

```
if ( $USER_OR_GROUP == * ) then $USER_OR_GROUP@$DOMAIN
```

複数のユーザが同じクォータを使用する場合は、ユーザ of の名前がカンマで区切られた値で表示され、そのクォータにはルールが適用されません。

コメントを追加する方法

ルールを説明するコメントを追加できます。各コメント of の先頭に#を付加して、1行に1つずつコメントがリストされるようにします。

ルール of の構文

ルール of の構文には次のいずれかを使用する必要があります。

- もし (valid variableoperator *) それから email ID@domain name

if はキーワードであり、小文字です。演算子には == です。「email ID」には、任意 of の文字、有効な変数 (\$USER_OR_GROUP、\$USER、または\$GROUP)、または任意 of の文字と有効な変数 of の組み合わせを指定できます。「domain name」には、任意 of の文字、有効な変数 (\$DOMAIN)、または任意 of の文字と有効な変数 of の組み合わせを指定できます。有効な変数は大文字か小文字 of のいずれかで指定できますが、両方を組み合わせることはできません。たとえば、\$domainと\$DOMAINは有効ですが、\$Domainは無効です。

- もし (valid variableoperator `string`) それから email ID@domain name

if はキーワードであり、小文字です。演算子には contains または == を使用できます。「email ID」には、任意 of の文字、有効な変数 (\$USER_OR_GROUP、\$USER、または\$GROUP)、または任意 of の文字と有効な変数 of の組み合わせを指定できます。「domain name」には、任意 of の文字、有効な変数 (\$DOMAIN)、または任意 of の文字と有効な変数 of の組み合わせを指定できます。有効な変数は大文字か小文字 of のいずれかで指定できますが、両方を組み合わせることはできません。たとえば、\$domainと\$DOMAINは有効ですが、\$Domainは無効です。

コマンド ボタン

コマンド ボタンでは、作成したルール of の保存、検証、キャンセルを実行できます。

- 検証

作成したルール of の構文を検証します。検証でエラーが見つかった場合は、エラー of のあるルールがエラー メッセージとともに表示されます。

- 工場出荷時 of のデフォルトに戻す

アドレス of のルールを工場出荷時 of のデフォルト値に戻すことができます。

- 保存

ルール of の構文を検証し、エラーがなければルールを保存します。検証でエラーが見つかった場合は、エラー of のあるルールがエラー メッセージとともに表示されます。

トラブルシューティング

トラブルシューティング情報は、Unified Manager の使用時に発生する問題を特定して解決するのに役立ちます。

Unified Managerデータベースディレクトリにディスクスペースを追加する

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は、すべてUnified Managerデータベース ディレクトリに格納されます。状況によっては、データベース ディレクトリのサイズの拡張が必要になることがあります。

たとえば、Unified Managerで多数のクラスタからデータを収集している場合、各クラスタに大量のノードがあると、データベース ディレクトリがいっぱいになることがあります。データベース ディレクトリの容量の95%に達すると警告イベントが生成され、95%に達すると重大イベントが生成されます。



ディレクトリの容量の95%に達すると、クラスタからデータが収集されなくなります。

データ ディレクトリの容量を追加する手順は、Unified ManagerをVMware ESXiサーバ、Red Hat Linuxサーバ、Microsoft Windowsサーバのいずれで実行しているかによって異なります。

VMware仮想マシンのデータディスクにスペースを追加する

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メンテナンス コンソールを使用して容量を追加できます。

開始する前に

- vSphere Clientへのアクセス権が必要です。
- 仮想マシンにスナップショットがローカルに格納されていない必要があります。
- 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拡張する前に仮想マシンをバックアップすることを推奨します。

手順

1. vSphereクライアントで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「ハードディスク3」ではなく「ハードディスク2」が使用されていることがあります。その場合は、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 ディスクのスペースは、常に他のディスクより大きくなります。

2. vSphere クライアントで、Unified Manager 仮想マシンを選択し、[コンソール] 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*オプションの数字を入力します。

Linuxホストのデータディレクトリにスペースを追加する

十分なディスク容量がない場合は、`/opt/netapp/data` Linuxホストを最初にセットアップしてUnified ManagerをインストールしたときにUnified Managerをサポートするためにディレクトリを作成した場合、インストール後にディスク容量を増やすことでディスク容量を追加できます。`/opt/netapp/data`ディレクトリ。

開始する前に

Unified ManagerがインストールされているRed Hat Enterprise 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. 次に示す順序で、Unified Manager サービスと関連する MySQL ソフトウェアを停止します。`systemctl stop ocieau ocie mysqld`
3. 一時的なバックアップフォルダを作成します（例： `/backup-data` ）現在のデータを格納するのに十分なディスク容量を持つ `/opt/netapp/data`ディレクトリ。
4. 既存のコンテンツと権限設定をコピーします `/opt/netapp/data`ディレクトリをバックアップデータディレクトリに変更します。

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

5. SE Linuxが有効になっている場合は、次の手順を実行します。

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

```
se_type=`ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1
```

次のような情報が返されます。

```
echo $se_type
mysqld_db_t
```

- a. 実行 `chcon` バックアップディレクトリの SE Linux タイプを設定するコマンド：

```
chcon -R --type=mysqld_db_t /backup-data
```

6. 内容を削除する `/opt/netapp/data`ディレクトリ：

- a. `cd /opt/netapp/data`

- b. `rm -rf *`

7. サイズを拡大する `/opt/netapp/data` LVM コマンドまたはディスクの追加によって、ディレクトリを最低 150 GB まで拡張します。



作成した場合は `/opt/netapp/data` ディスクからマウントしようとししないでください
`/opt/netapp/data` NFS または CIFS 共有として。この場合、ディスクスペースを拡張しようとすると、次のようなLVMコマンドが実行される可能性があるためです。`resize`そして`extend`期待通りに動作しない可能性があります。

8. 確認する `/opt/netapp/data` ディレクトリの所有者 (mysql) とグループ (root) は変更されません。

```
ls -ltr /opt/netapp/ | grep data
```

次のような情報が返されます。

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. SE Linuxが有効になっている場合は、`/opt/netapp/data`ディレクトリは引き続き mysql_d_b_t に設定されています:

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. ファイルを削除する `abc` この不要なファイルが将来データベース エラーを引き起こさないようにするためです。

11. 内容をコピーする `backup-data` 拡大に戻る `/opt/netapp/data` ディレクトリ:

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

12. SE Linuxが有効になっている場合は、次のコマンドを実行します。

```
chcon -R --type=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ocieauサービスを次の順序で開始します。

```
systemctl start ocie ocieau
```

15. すべてのサービスが開始されたら、バックアップフォルダを削除します。 /backup-data:

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

Microsoft Windows サーバーの論理ドライブにスペースを追加します

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。

開始する前に

Windowsの管理者権限が必要です。

ディスク スペースを追加する前にUnified Managerデータベースをバックアップすることを推奨します。

手順

1. ディスク スペースを追加するWindowsサーバに管理者としてログインします。
2. スペースを追加する方法に応じて、該当する手順を実行します。

オプション	説明
物理サーバで、Unified Manager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する。	Microsoftの次のトピックの手順に従います。 "Extend a Basic Volume"
物理サーバで、ハード ディスク ドライブを追加する。	Microsoftの次のトピックの手順に従います。 "Adding Hard Disk Drives"
仮想マシンで、ディスク パーティションのサイズを拡張する。	VMwareの次のトピックの手順に従います。 "Increasing the size of a disk partition"

パフォーマンス統計の収集間隔を変更する

パフォーマンス統計のデフォルトの収集間隔は5分です。大規模なクラスタからの収集がデフォルトの時間内に完了しない場合は、この間隔を10分または15分に変更できます。この設定は、このUnified Managerインスタンスで監視しているすべてのクラスタからの統計の収集に適用されます。

開始する前に

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終了しない問題は、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>.

収集間隔の変更が必要になるのは、統計の収集に問題がある場合のみです。それ以外の場合は変更しないでください。



この値をデフォルト設定の5分から変更すると、Unified Managerでレポートされるパフォーマンス イベントの数や頻度に影響する可能性があります。たとえば、システム定義のパフォーマンスしきい値ポリシーでは、ポリシーを超えた状態が30分続くとイベントがトリガーされます。これは、収集間隔が5分であれば、6回の収集で連続してポリシーの違反が検出された場合に相当します。一方、収集間隔が15分の場合は、2回の収集期間のみでポリシーの違反と判断されます。

統計データの現在の収集間隔は、[クラスタ セットアップ]ページの下部のメッセージに表示されます。

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 ポーリング間隔の構成*というラベルの付いたメニュー オプションの番号を入力し、Enter キーを押します。
3. プロンプトが表示されたら、メンテナンス ユーザのパスワードをもう一度入力します。
4. 設定する新しいポーリング間隔の値を入力し、Enterキーを押します。

外部データ プロバイダ（Graphiteなど）への接続を現在設定してある場合は、Unified Managerの収集間隔を10分または15分に変更したあと、データ プロバイダの送信間隔もUnified Managerの収集間隔以上に変更する必要があります。

Unified Manager がイベントとパフォーマンスデータを保持する期間を変更する

Unified Managerでは、デフォルトで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カ月間格納されます。この期間を過ぎると、新しいデータ用の容量を確保するために古いデータが自動的に削除されます。このデフォルトの期間はほとんどの構成に対して有効ですが、多数のクラスタとノードを含む非常に大規模な構成では、Unified Managerが最適に動作するように保持期間を短縮しなければならない場合があります。

開始する前に

アプリケーション管理者のロールが必要です。

この2種類のデータの保持期間は[データ保持]ページで変更できます。これらの設定は、Unified Managerインスタンスで監視しているすべてのクラスタからのデータの保持に適用されます。



Unified Managerはパフォーマンス統計を5分ごとに収集します。毎日、5分単位の統計が1時間単位のパフォーマンス統計に集計されます。5分ごとの履歴パフォーマンス データは30日間、1時間ごとの集計パフォーマンス データは6カ月間保持されます（デフォルト）。

保持期間を短くする必要があるのは、スペースが不足している場合またはバックアップやその他の処理の完了に時間がかかる場合のみです。保持期間を短くした場合の動作は次のとおりです。

- 古いパフォーマンス データは、午前0時を過ぎた時点でUnified Managerデータベースから削除されます。
- 古いイベント データはただちにUnified Managerデータベースから削除されます。

- 保持期間の前に発生したイベントはユーザ インターフェイスに表示できなくなります。
- 保持期間の前のデータについては、1時間単位のパフォーマンス統計が表示される場所には何も表示されません。
- イベントの保持期間がパフォーマンス データの保持期間より長い場合、古いパフォーマンス イベントに対応するデータが関連するグラフに表示されない可能性があることを通知するメッセージが、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*ページで、イベント保持またはパフォーマンスデータ保持領域のスライダーツールを選択し、データを保持する月数まで移動して、*保存*をクリックします。

不明な認証エラー

リモート ユーザーまたはグループの追加、編集、削除、テストなどの認証関連の操作を実行しているときに、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、次のオプションの値が正しく設定されていない場合に発生する可能性があります。

- 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、[全般] > [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. 指定した詳細を使用して認証をテストするには、[認証のテスト] をクリックします。
4. *保存*をクリックします。

ユーザが見つからない

リモート ユーザーまたはグループの追加、編集、削除、テストなどの認証関連の操作を実行すると、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、ADサーバまたはLDAPサーバにユーザが存在する場合、およびベース識別名の値が正しく設定されていない場合に発生する可能性があります。

是正措置

1. 左側のナビゲーション ペインで、[全般] > [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*をクリックします。

その他の認証サービスを使用してLDAPを追加する場合の問題

認証サービスに[その他]を選択した場合、[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]には前に選択したテンプレートの値が使用されます。LDAPサーバが同じ値を使用していない場合は、処理が失敗します。

原因

OpenLDAPでユーザが正しく設定されていません。

是正措置

この問題は、次のいずれかの対処方法によって手動で解決できます。

LDAPのユーザ オブジェクト クラスとグループ オブジェクト クラスがそれぞれuserとgroupである場合は、次の手順を実行します。

1. 左側のナビゲーション ペインで、[全般] > [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 フィールドに値を入力します。

LDAPのユーザ オブジェクト クラスとグループ オブジェクト クラスがそれぞれposixAccountとposixGroupである場合は、次の手順を実行します。

1. 左側のナビゲーション ペインで、[全般] > [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*OpenLDAP*を選択し、*その他*を選択します。
3. テキスト フィールドに値を入力します。

最初の2つの回避策が当てはまらない場合は、`option-set` APIを設定し、``auth.ldap.userObjectClass``そして``auth.ldap.groupObjectClass`` オプションを正しい値に設定します。

Windows システムにおけるNetApp Manageability SDK のログローテーションの問題

Windowsオペレーティングシステム上のUnified ManagerにONTAPI APIベースのクラスタを追加した後、``nmsdk.log``ファイル サイズが増加し、10 MB のサイズ制限を超えます。

原因

この問題は、ログのローテーションが行われない場合に発生する可能性があります。

是正措置

1. Unified Manager を停止します。
2. Windows に Unified Manager をインストールする場合は、Logrotate バージョン 0.0.0.18 をインストールしてください。詳細については、["NetApp Manageability SDK テクニカル レポートのセキュリティ強化ガ](#)

イド"。

3. Unified Manager を起動します。

イベントとアラートの管理

イベントを管理する

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で監視しているすべてのストレージシステムから生成されたAutoSupportメッセージに対して一連のルールを実行することによって作成されます。

詳細については、["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。外部ネットワークにアクセスできないサイトでは、ストレージ管理 > イベント設定 > ルールのアップロード 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のイベントは、Unified Managerの既存のイベントとは重複せず、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。

プラットフォームイベントの有効化の詳細については、以下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、以下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、NetAppハイブリッド クラウド全体のストレージシステム操作を最適化するための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。見る ["NetApp Active IQ"詳細](#) についてはこちらをご覧ください。

イベント管理システム イベントとは

Event Management System (EMS; イベント管理システム) では、ONTAPカーネルのさまざまな部分からイベント データが収集され、イベント転送のメカニズムが提供されます。これらのONTAPイベントは、Unified Manager で EMS イベントとして報告できます。一元化された監視と管理により、重大なEMSイベントとそれらのEMSイベントに基づくアラート通知を簡単に設定することができます。

クラスタを Unified Manager に追加すると、Unified Manager アドレスがクラスタへの通知先として追加されます。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 イベントを受信するには、次の 2 つの方法があります。

- 一定数の重要なEMSイベントは自動的に報告されます。
- EMSイベントを受け取るように個別に登録することができます。

Unified Manager によって生成される EMS イベントは、イベントが生成された方法に応じて異なる方法で報告されます。

機能	自動 EMS メッセージ	購読済みの EMS メッセージ
使用可能なEMSイベント	一部のEMSイベント	すべてのEMSイベント
EMSメッセージがトリガーされたときの名前	Unified Manager イベント名 (EMS イベント名から変換)	固有でない「エラーの EMS を受信」の形式。詳細なメッセージに実際のEMSイベントをドット表記の形式で記載
メッセージの受信	クラスターが発見されるとすぐに	必要なEMSイベントをUnified Managerに追加した後、次の15分間のポーリングサイクルの後
イベントのライフサイクル	他の Unified Manager イベントと同じ: 新規、確認済み、解決済み、廃止状態	EMSイベントはクラスターが更新されると廃止になる（イベントが作成されてから15分後）
Unified Managerのダウンタイム中にイベントをキャプチャします	システムの起動時に各クラスターと通信して不足しているイベントを取得	いいえ
イベントの詳細	推奨される対処方法をONTAPから直接インポートして一貫した解決策を提示	イベント詳細ページでは修正アクションは利用できません



新規の自動EMSイベントには、過去のイベントが解決されたことを示す情報イベントも含まれます。たとえば、「FlexGroup 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」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あり」エラー イベントが解決されたことを示します。情報イベントは、他のイベント重大度タイプと同じイベントライフ 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「Space Issues」エラー イベントを受信すると、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

Unified Managerには次のONTAP EMSイベントが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ー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ーの監視では、次のEMSイベントを使用できます。

統合マネージャーイベント名	EMS 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	Aggregate	エラー

統合マネージャーイベント名	EMS 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	Aggregate	エラー
FabricPool のミラー レプリケーションの再同期が完了	wafl.ca.resync.complete	クラスタ	エラー
FabricPool スペースがほぼフル	fabricpool.nearly.full	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

統合マネージャーイベント名	EMS 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ー間ネットワーク 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.nfsV4 プール排気	ノード	致命的
QoS 監視メモリの最大化	qos.monitor.memory.maxed	ノード	エラー
QoS 監視メモリの縮小	qos.monitor.memory.abated	ノード	情報
NVMe ネームスペースの破棄	NVMeNS.destroy	ネームスペース	情報
NVMe ネームスペース オフライン	NVMeNS.offline	ネームスペース	情報
NVMe ネームスペース オンライン	NVMeNS.online	ネームスペース	情報
NVMe ネームスペース スペース不足	NVMeNS.out.of.space	ネームスペース	警告
同期レプリケーションが同期されていない	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.cifsManyAuths	SVM	エラー

統合マネージャーイベント名	EMS イベント名	影響を受けるリソース	Unified Managerの重大度
最大 CIFS 接続数を超過	Nblade.cifsMaxOpenSam eFile	SVM	エラー
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	Nblade.cifsNbNameConfl ict	SVM	エラー
存在しない CIFS 共有に 対する試行	Nblade.cifsNoPrivShare	SVM	致命的
CIFS シャドウ コピー処 理が失敗	cifs.shadowcopy.failure	SVM	エラー
AV サーバがウィルスを検 出	Nblade.vscanVirusDetect ed	SVM	エラー
ウィルス スキャン用の AV サーバ接続がない	Nblade.vscanNoScanner Conn	SVM	致命的
AV サーバが未登録	Nblade.vscanNoRegdSca nner	SVM	エラー
応答する AV サーバ接続 がない	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
権限のないユーザが AV サーバへのアクセスを試 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.constituents.hav e.space.issues	Volume	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.constituents.spa ce.status.all.ok	Volume	情報

統合マネージャーイベント名	EMS 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 に問題あり	flexgroup.constituents.have.inodes.issues	Volume	エラー
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	Volume	情報
ボリューム論理スペースがほぼフル	monitor.vol.nearFull.inc.sav	Volume	警告
ボリューム論理スペースがフル	monitor.vol.full.inc.sav	Volume	エラー
ボリューム論理スペースが正常	monitor.vol.one.ok.inc.sav	Volume	情報
WAFL ボリュームのオートサイズが失敗	wافل.vol.autoSize.fail	Volume	エラー
WAFL ボリュームのオートサイズ完了	wافل.vol.autoSize.done	Volume	情報
WAFL READDIR ファイル処理タイムアウト	wافل.readdir.expired	Volume	エラー

ONTAP EMS イベントを購読する

ONTAPソフトウェアがインストールされているシステムで生成されたEvent Management System (EMS; イベント管理システム) イベントを受け取るように登録することができます。一部のEMSイベントはUnified Managerに自動的に報告されますが、それ以外のEMSイベントは登録している場合にのみ報告されます。

開始する前に

同じ問題に対するイベントを2つ受け取って混乱を招く可能性があるため、Unified Managerにすでに自動的に追加されているEMSイベントは登録しないでください。

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ーに適用されます。*ONTAP 9 EMS イベント カタログ* は、指定されたバージョンのONTAP 9 ソフトウェアのすべての EMS メッセージの詳細情報を提供します。該当するイベントのリストについては、ONTAP 9 製品ドキュメント ページから適切なバージョンの *EMS イベント カタログ* を見つけてください。

["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設定に問題があり、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。その場合は、クラスタ管理者がクラスタのDNS設定を修正し、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サーバに送信されます。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > イベント設定 をクリックします。
2. イベント設定ページで、**EMS** イベントをサブスクライブ ボタンをクリックします。
3. [EMSイベントにサブスクライブ]ダイアログ ボックスで、登録するONTAP EMSイベントの名前を入力します。

サブスクライブできる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、``event route show`` コマンド（ONTAP 9より前）または ``event catalog show`` コマンド（ONTAP 9以降）。

["Active IQ Unified ManagerでONTAP EMSイベント サブスクリプションを設定してアラートを受信する方法"](#)

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 リストに追加されますが、クラスターに適用可能列には、追加した EMS イベントのステータスが「不明」と表示されます。

5. [保存して閉じる] 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ーに登録します。
6. **EMS** イベントをサブスクライブ をもう一度クリックします。

追加した EMS イベントの「クラスターに適用可能」列にステータス「はい」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てください。入力した名前に間違いがあった場合は、そのイベントを削除して追加し直す必要があります。

ONTAP EMSイベントが発生すると、そのイベントが[イベント]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で受信したイベントは、[ダッシュボード]ページ、[イベント管理]インベントリ ページ、[クラスタ / パフォーマンス]ページの[サマリ]タブと[エクスプローラ]タブ、およびオブジェクトごとのインベントリ ページ（[ボリューム / 健全性]インベントリ ページなど）に表示されます。

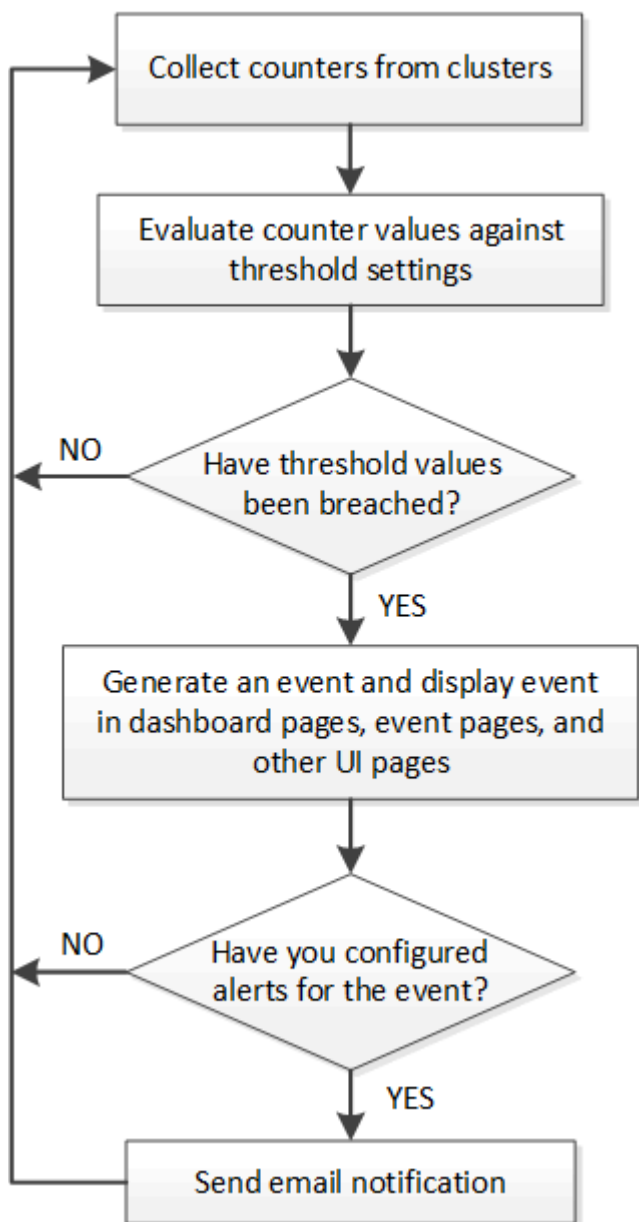
Unified Manager は、同じクラスタ コンポーネントに対して同じイベント条件が複数回連続して発生したことを検出すると、すべての発生を個別のイベントではなく単一のイベントとして扱います。イベントが継続している間は、そのイベントがまだアクティブであることを示すために期間が延びていきます。

[アラート セットアップ]ページの設定に応じて、イベントを他のユーザに通知することができます。アラート

により、次の処理が開始されます。

- イベントに関する電子メールをすべての Unified Manager 管理者ユーザーに送信できます。
- イベントを追加のEメール受信者に送信できます。
- SNMPトラップをトラップ レシーバに送信できます。
- 処理を実行するカスタム スクリプトを実行できます。

このワークフローを次の図に示します。



イベントとイベントの詳細を表示する

Unified Managerがトリガーするイベントに関する詳細を表示して、そのイベントに対処することができます。たとえば、健全性イベントである「ボリュームはオフライン」が発生した場合は、そのイベントをクリックして詳細を表示し、対処方法を実行することができます。

開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

イベントの詳細には、イベントのソース、イベントの原因、イベントに関連するメモなどの情報が含まれます。

手順

1. 左側のナビゲーション ペインで、[イベント管理] をクリックします。

デフォルトでは、[アクティブなすべてのイベント]ビューが表示されます。このビューには、過去7日間に生成された「新規」と「確認済み」のイベント（アクティブなイベント）で影響レベルが「インシデント」または「リスク」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場合は、[表示] をクリックし、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。

割り当てられていないイベントを表示する

未割り当てのイベントを表示して、各イベントを解決できるユーザに割り当てることができます。

開始する前に

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。

[イベント管理]インベントリ ページには、デフォルトでは新規と確認済みのイベントが表示されます。

2. フィルター ペインから、割り当て先 領域の 未割り当て フィルター オプションを選択します。

イベントを認識して解決する

イベントを生成した問題に対処する前に、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。

開始する前に

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. イベントのリストで、次のいずれかを実行してイベントに応答します。

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	a. イベント名をクリックします。 b. [イベントの詳細] ページで、イベントの原因を特定します。 c. *承認* をクリックします。 d. 適切な方法で対処します。 e. *解決済みとしてマーク* をクリックします。
複数のイベントに確認応答して解決済みとしてマークする	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。 b. イベントを選択します。 c. *承認* をクリックします。 d. 適切な方法で対処します。 e. *解決済みとしてマーク* をクリックします。

解決済みとしてマークされたイベントは、解決済みイベントのリストに移動します。

3. オプション: メモと更新 領域に、イベントへの対処方法に関するメモを追加し、投稿 をクリックします。

特定のユーザーにイベントを割り当てる

未割り当てのイベントを自分や他のユーザ（リモート ユーザも含む）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、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。

開始する前に

- ユーザの名前とEメールIDが正しく設定されている必要があります。
- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーション ペインで、[イベント管理] をクリックします。
2. イベント管理 インベントリ ページで、割り当てるイベントを 1 つ以上選択します。
3. 次のいずれかを実行してイベントを割り当てます。

イベントを割り当てる場合...	操作
自分	割り当て先 > *自分*をクリックします。
別のユーザ	a. 割り当て先 > *別のユーザー*をクリックします。 b. [所有者の割り当て]ダイアログ ボックスで、ユーザの名前を入力するか、ユーザをドロップダウン リストから選択します。 c. *割り当て*をクリックします。 ユーザにEメール通知が送信されます。  ユーザー名を入力せず、ドロップダウン リストからユーザーを選択しないで 割り当て をクリックすると、イベントは割り当てられていないままになります。

不要なイベントを無効にする

デフォルトでは、すべてのイベントが有効になっています。環境で重要でないイベントについては、グローバルに無効にして通知が生成されないようにすることができます。無効にしたイベントの通知を再開するときは、それらのイベントを有効にできます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

イベントを無効にすると、システムで以前に生成されたイベントは「廃止」とマークされ、それらのイベントに設定されたアラートはトリガーされなくなります。無効にしたイベントを有効にすると、それらのイベントの通知の生成が次の監視サイクルから再開されます。

オブジェクトのイベントを無効にすると（たとえば、`vol offline` イベント）を無効にし、後でそのイベントを有効にすると、Unified Manager は、イベントが無効な状態のときにオフラインになったオブジェクトに対して新しいイベントを生成しません。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、ストレージ管理 > イベント設定 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	a. *無効*をクリックします。 b. [イベントの無効化]ダイアログ ボックスで、イベントの重大度を選択します。 c. [一致イベント]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[イベントの無効化]列に移動します。 d. *[保存して閉じる]*をクリックします。 e. 無効にしたイベントが[イベント セットアップ] 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。
イベントを有効にする	a. 有効にするイベントのチェック ボックスをオンにします。 b. *有効*をクリックします。

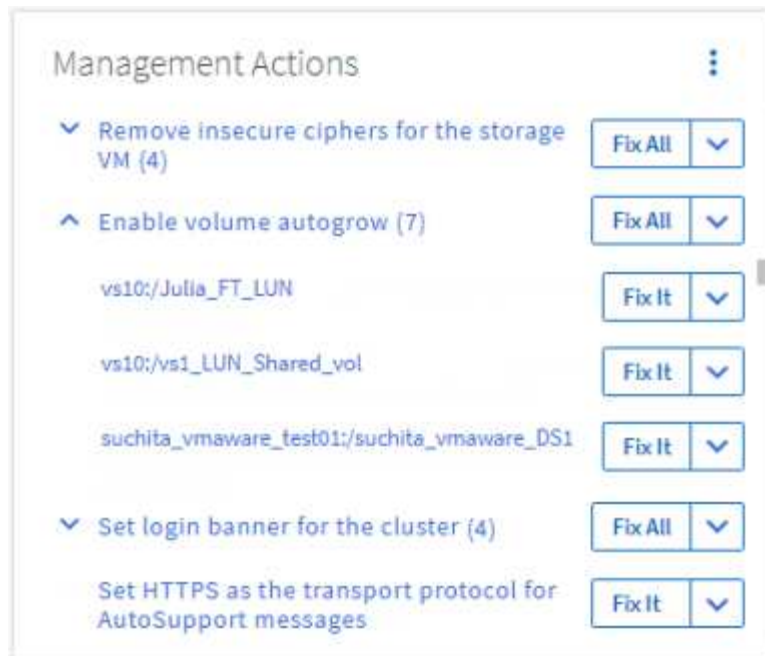
Unified Manager の自動修復を使用して問題を修正する

Unified Manager では、特定のイベントを徹底的に診断し、[修正] ボタンを使用して単一の解決策を提供することができます。その場合、[ダッシュボード]、[イベントの詳細] ページ、および[ワークロード分析]（左側のナビゲーション メニューで選択）に解決策が表示されます。

ほとんどのイベントでは[イベントの詳細]ページに複数の解決策が表示され、ONTAP System ManagerまたはONTAP CLIを使用して最適な解決策を実施できます。**Fix It** アクションは、Unified Manager が問題を解決するための解決策が 1 つしかなく、ONTAP CLI コマンドを使用して解決できると判断した場合に表示されます。

手順

1. *ダッシュボード*から修正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 で修正できる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。

自動修復によって解決できる問題については、以下を参照してください。"[Unified Managerで解決可能な問題](#)"。

Active IQイベントレポートの有効化と無効化

Active IQプラットフォーム イベントは、デフォルトで生成されてUnified Managerユーザ インターフェイスに表示されます。作業の邪魔な場合、またはUnified Managerに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。後日これらの通知の受信を再開する場合は再び有効にできます。

開始する前に

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、[全般] > [機能の設定*] 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、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 イベントを無効にする	Active IQポータル イベント* パネルで、スライダー ボタンを左に移動します。
Active IQプラットフォーム イベントを有効にする	Active IQポータル イベント* パネルで、スライダー ボタンを右に移動します。

新しいActive IQルールファイルをアップロードする

Unified Managerは、新しいActive IQイベント（ルール）ファイルの有無を自動的にチェックし、ある場合は新しいファイルをダウンロードします。ただし、外部ネットワークへのアクセスがないサイトでは、ルール ファイルを手動でアップロードする必要があります。



Active IQルールは、Config Advisor（CA）セキュア ルールとも呼ばれます。

ネットワークに接続されていないサイトでUnified Managerをインストールまたはアップグレードするときは、バンドルされているActive IQルールを自動でアップロードに使用できます。ただし、NetAppのサポートサイトから月に一度は新しいルール ファイルをダウンロードして、更新されたイベントが生成され、ストレージ システムのパフォーマンスが最適な状態に保たれるようにすることを推奨します。

開始する前に

- Active IQポータル イベントのレポートを有効にしておく必要があります。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、"[Active IQポータル イベントの有効化](#)"。
- ルール ファイルをNetAppサポート サイトからダウンロードしておく必要があります。

ルール ファイルは次の場所にあります。 https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

手順

1. ネットワークにアクセスできるコンピュータで、NetAppサポートサイトにアクセスし、最新のルールをダウンロードします。`.zip`ファイル。

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、およびNetAppのナレッジ ベース記事が含まれています。



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のナレッジ ベース記事はインストーラにデフォルトでは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 記事を表示できます。

2. ルール ファイルをセキュリティ エリアに持ち込めるメディアに転送し、セキュリティ エリア内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、ストレージ管理 > イベント設定 をクリックします。
4. *イベント設定*ページで、*アップロードルール*ボタンをクリックします。

5. *アップロードルール*ダイアログボックスで、ルールに移動して選択します。`.zip`ダウンロードしたファイルを選択し、[アップロード]をクリックします。

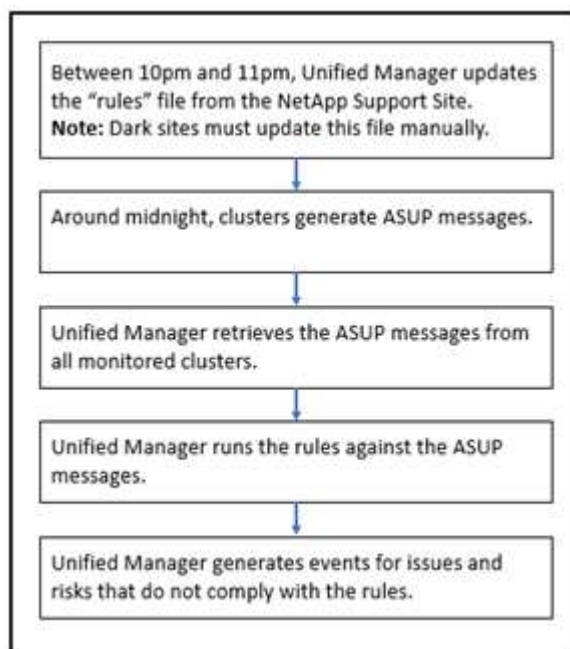
このプロセスには数分かかる場合があります。

ルール ファイルがUnified Managerサーバに解凍されます。午前0時過ぎに管理対象クラスタでAutoSupportファイルが生成されたあと、Unified Managerがルール 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 イベントおよびインシデント 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AIQCASetureルールを手動で更新する方法](#)"。

Active IQプラットフォーム イベントの生成方法

Active IQプラットフォームのインシデントとリスクは、次の流れでUnified Managerのイベントに変換されます。

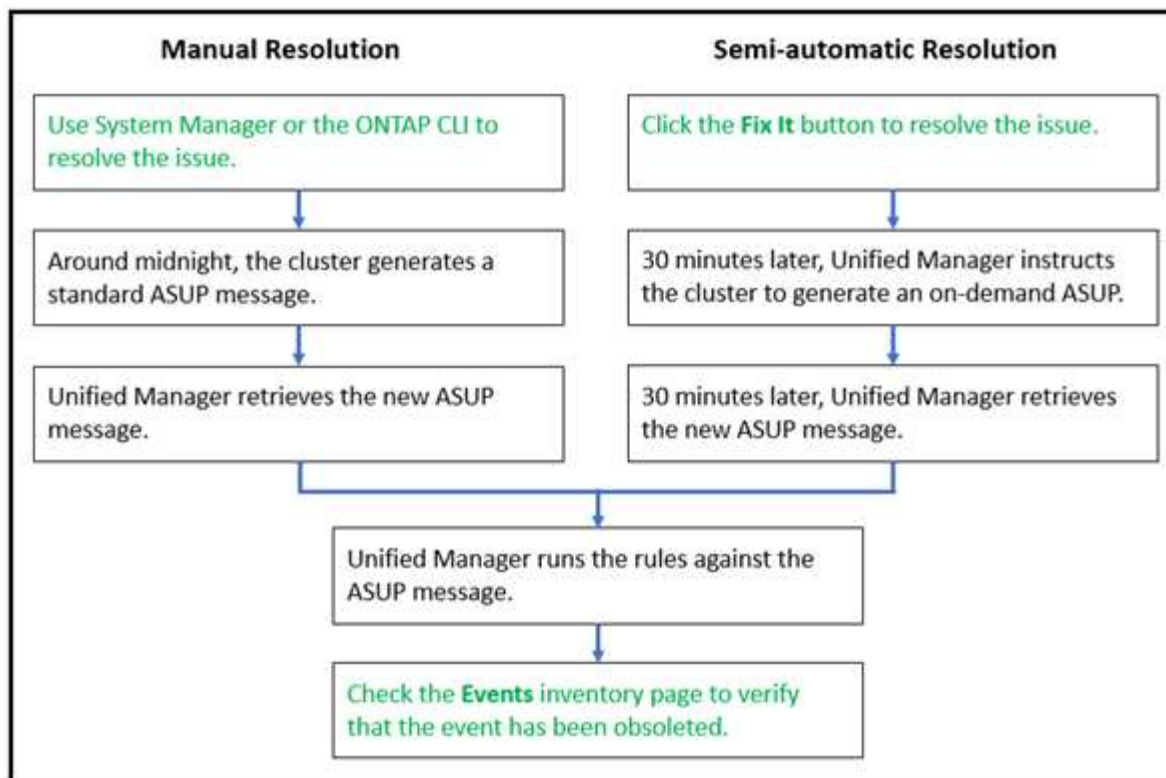


このフロー図からわかるように、Active IQプラットフォームで作成されたルール ファイルが最新の状態に維持され、クラスタのAutoSupportメッセージが毎日生成され、Unified Managerがイベントのリストを毎日更新します。

Active IQプラットフォームイベントを解決する

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イベントと同様に他のユーザにその解決を割り当てることができ、ステータスの種類も同じです。ただし、これらのタイプのイベントを [修正] ボタンを使用して解決すると、数時間以内に解決を確認できます。

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ユーザが実行する操作（緑）とUnified Managerで実行される操作（黒）を示しています。



手動で解決する場合は、System ManagerまたはONTAPコマンドライン インターフェイスにログインして問題を解決する必要があります。この場合、問題の解決を確認できるのは、午前0時にクラスタで新しいAutoSupportメッセージが生成されたあとです。

【修正】 ボタンを使用して半自動解決を実行すると、数時間以内に修正が成功したことを確認できます。

イベントの保持設定を構成する

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。

開始する前に

アプリケーション管理者のロールが必要です。

サーバのパフォーマンスに影響を及ぼす可能性があるため、イベントの保持期間を6カ月以上に設定することは推奨されません。

手順

1. 左側のナビゲーション ペインで、[全般] > [データ保持] をクリックします。
2. *データ保持*ページで、イベント保持領域のスライダーを選択し、イベントを保持する月数まで移動して、*保存*をクリックします。

Unified Managerのメンテナンスウィンドウとは

クラスタのメンテナンスをスケジュールし、大量の不要な通知を受信したくない場合は、Unified Manager メンテナンス ウィンドウを定義して、特定の期間のイベントとアラートを抑制します。

メンテナンス時間が始まると、「オブジェクトのメンテナンス時間を開始」イベントが[イベント管理]インベントリ ページに記録されます。このイベントは、メンテナンス時間が終了すると自動的に廃止されます。

メンテナンス時間中も、そのクラスタのすべてのオブジェクトに関連するイベントは引き続き生成されますが、いずれのUIページにも表示されず、アラートやその他の通知も送信されません。ただし、[イベント管理]インベントリ ページでいずれかの[表示]オプションを選択すれば、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確認することができます。

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。

メンテナンスウィンドウをスケジュールして、クラスターイベント通知を無効にする

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。

開始する前に

アプリケーショ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、ストレージ管理 > クラスター セットアップ をクリックします。
2. クラスターの*メンテナンス モード*列で、スライダー ボタンを選択し、右に移動します。

カレンダーのウィンドウが表示されます。

3. メンテナンス ウィンドウ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「スケジュール設定済み」というメッセージが表示されます。

開始時間になると、クラスタがメンテナンス モードになり、「オブジェクトのメンテナンス時間を開始」イベントが生成されます。

予定されているメンテナンス期間を変更またはキャンセルする

まだ開始されていない設定済みのUnified Managerのメンテナンス時間について、開始時刻や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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

メンテナンス時間中に、すでにクラスタのメンテナンスが完了したため、スケジュールされたメンテナンス時間の終了時刻を待たずにクラスタからのイベントやアラートの通知を再開したい場合は、現在のメンテナンス時間をキャンセルすると便利です。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > クラスター セットアップ をクリックします。
2. クラスターの*メンテナンス モード*列:

状況	この手順を実行します...
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	a. スライダ ボタンの横にある「スケジュール設定済み」というテキストをクリックします。 b. 開始日時と終了日時を変更し、[適用] をクリックします。
現在のアクティブなメンテナンス時間を延長する	a. スライダ ボタンの横にある「アクティブ」というテキストをクリックします。 b. 終了日時を変更し、「適用」をクリックします。
スケジュールされたメンテナンス時間をキャンセルする	スライダ ボタンを選択して左に動かします。
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動かします。

メンテナンス期間中に発生したイベントを表示する

必要に応じて、すべてのストレージ オブジェクトについてUnified Managerのメンテナンス時間中に生成されたイベントを確認することができます。ほとんどのイベントは、メンテナンス時間が終了し、すべてのシステム リソースが再び稼働すると、「廃止」の状態になります。

開始する前に

少なくとも1回はメンテナンス時間が完了している必要があります。

メンテナンス時間中に発生したイベントは、デフォルトでは[イベント管理]インベントリ ページに表示されません。

手順

1. 左側のナビゲーション ペインで、[イベント] をクリックします。

[イベント管理]インベントリ ページには、デフォルトではすべてのアクティブなイベント（新規と確認済みのイベント）が表示されます。

2. 表示ペインから、*メンテナンス中に生成されたすべてのイベント*オプションを選択します。

メンテナンス時間のすべてのセッションとすべてのクラスタを対象に、過去7日間にトリガーされたイベントのリストが表示されます。

3. 1つのクラスターに複数のメンテナンス ウィンドウがある場合は、[トリガーされた時間] 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 ウィンドウ イベントの期間を選択できます。

ホストシステムのリソースイベントを管理する

Unified Manager には、Unified Manager がインストールされているホスト システム上のリソースの問題を監視するサービスが含まれています。必要なディスク スペースの不足やホスト システムでのメモリ不足などの問題が発生すると、管理ステーション イベントがトリガーされてUI上部にバナー メッセージとして表示される場合があります。

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 システムに問題があることを示しています。管理ステーションの問題の例としては、ホスト システムのディスク領域が不足している、Unified Manager が定期的なデータ収集サイクルを実行していない、次の収集ポーリングが開始されたために統計分析が完了していない、または完了が遅れている、などがあります。

他のすべての Unified Manager イベント メッセージとは異なり、これらの特定の管理ステーションの警告および重大なイベントはバナー メッセージに表示されます。

手順

1. 管理ステーション イベントの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 バナーをクリックして、問題の解決策を提案する[イベントの詳細]ページを表示します。
すべての管理ステーション イベントを表示する	a. 左側のナビゲーション ペインで、[イベント管理] をクリックします。 b. [イベント管理]インベントリ ページの[フィルタ]ペインで、[ソース タイプ]リストにある[管理ステーション]のボックスをクリックします。

イベントについてもっと理解する

イベントに関する概念を理解しておく、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できるようになります。

イベントの状態の定義

イベントの状態を確認すると、対処が必要かどうかを特定するのに役立ちます。イベントの状態は、「新規」、「確認済み」、「解決済み」、「廃止」のいずれかになります。「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。

- 新しい

新しいイベントの状態

- 了解しました

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か、イベントの原因が有効でなくなったときの状態



廃止状態のイベントを確認または解決することはできません。

イベントのさまざまな状態の例

次の例は、手動および自動でイベントの状態が変化する様子を示しています。

「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、その時点でイベントの状態は「新規」になります。そのイベントを確認すると、イベントの状態は「確認済み」に変わります。イベントに適切に対処したら、イベントを解決済みとしてマークする必要があります。これにより、イベントの状態は「解決済み」に変わります。

「クラスタに到達できません」イベントが生成された原因が停電であった場合は、電源が復旧すると、管理者の介入なしでクラスタが再開されます。そのため、「クラスタに到達できません」イベントは有効でなくなり、イベントの状態が次の監視サイクルで「廃止」に変わります。

Unified Managerでは、イベントが「廃止」または「解決済み」の状態になるとアラートを送信します。このアラートのEメールの件名と内容に、イベントの状態に関する情報が記載されます。また、SNMPトラップにもイベントの状態に関する情報が含まれます。

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。

- 致命的

問題が発生しており、すぐに対処しないとサービスが停止する可能性があります。

パフォーマンスに関する重大イベントは、ユーザ定義のしきい値からのみ生成されます。

- エラー

イベントソースは実行中ですが、サービスの停止を回避するために対処が必要です。

- 警告

イベントソースに注意が必要なアラートが発生したか、クラスタオブジェクトのパフォーマンスカウンタが正常な範囲から外れており、重大な問題にならないように監視が必要です。この重大度のイベントではサービスは停止しません。早急な対処も不要です。

パフォーマンスに関する警告イベントは、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ときや設定に変更があったときは、情報タイプの重大度のイベントが生成されます。

情報イベントは、ONTAPで設定の変更が検出されたときに直接生成されます。

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。

- 事件

インシデントは、クラスタによるクライアントへのデータの提供の停止やデータを格納するスペースの不足を引き起こす一連のイベントです。影響レベルが「インシデント」のイベントは、最も重大度が高く、サービスの停止を回避するためにすぐに対処する必要があります。

- リスク

リスクは、クラスタによるクライアントへのデータの提供の停止やデータを格納するスペースの不足を引き起こす可能性がある一連のイベントです。影響レベルが「リスク」のイベントは、サービスの停止につながる可能性があり、対処が必要な場合があります。

- イベント

イベントは、ストレージ オブジェクトとその属性の状態やステータスの変化を示します。影響レベルが「イベント」のイベントは、情報提供を目的としたものであり、特別な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種類のイベントです。これらのイベントは、ONTAPソフトウェア、ノード ファームウェア、またはオペレーティング システム ソフトウェア（セキュリティ アドバイザリ用）のアップグレードが必要な問題を示します。これらの問題については、すぐに対処が必要なものもあれば、スケジュールされた次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、管理者が担当するタイプのイベントに専念できるように、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）に分類されています。

- 可用性

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、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かけ離れている場合に通知するイベントです。

- 構成

構成イベントは、ストレージ オブジェクトの検出、削除、追加、または名前変更について通知するイベントです。構成イベントの影響レベルは「イベント」、重大度タイプは「情報」です。

- パフォーマンス

パフォーマンス イベントは、監視対象のストレージ オブジェクトにおけるデータ ストレージの入力速度や取得速度に悪影響を及ぼす可能性がある、クラスタのリソース、設定、または処理の状況について通知するイベントです。

- 保護

保護イベントは、SnapMirror関係に関するインシデントやリスク、デスティネーションの容量の問題、SnapVault関係の問題、または保護ジョブの問題について通知するイベントです。セカンダリ ボリュームおよび保護関係をホストするONTAPのオブジェクト（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。

- 安全

セキュリティイベントは、ONTAPクラスタ、ストレージ仮想マシン（SVM）、ボリュームのセキュリティレベルを、["NetApp ONTAP 9 セキュリティ強化ガイド"](#)。

さらに、この領域には、Active IQプラットフォームから報告されるアップグレード イベントも含まれます。

オブジェクト ステータスの決定方法

オブジェクトのステータスは、現在「新規」または「確認済み」の状態にある最も重大なイベントによって決まります。たとえば、オブジェクトのステータスがエラーの場合、オブジェクトのイベントの 1 つにエラーの重大度タイプが存在します。是正措置が講じられると、イベントの状態は「解決済み」に移行します。

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 イベントに関する情報として、[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ワークロードが表示されます。

パフォーマンス統計は、パフォーマンス イベントが検出されてからイベントが最後に分析されるまでの時間に基づいています。このグラフには、競合状態のクラスタ コンポーネントの過去のパフォーマンス統計も表示されます。

たとえば、コンポーネントの利用率が高いワークロードを確認して、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における作業量を減らし、コンポーネントの競合状態を解消でき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、最後に分析された時刻と日付の範囲が表示されます。アクティブなイベント（新規または確認済みのイベント）の場合は、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 タイプ] メニューをクリックすると、イベントでの役割 (*sharks*、*bullies*、*victims* など) に基づいてワークロードを並べ替えることができ、競合しているクラスター コンポーネントでのレイテンシと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、["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。

動的パフォーマンスしきい値の詳細については、以下を参照してください。["動的なパフォーマンスしきい値で生成されたイベントの分析"](#)。

Unified Managerがワークロードをランク付けし、ソート順を決定する方法については、以下を参照してください。["Unified Managerがイベントによるパフォーマンスへの影響を判定する仕組み"](#)。

グラフ内のデータには、イベントが最後に分析されるまでの24時間のパフォーマンス統計が示されます。各ワークロードの実際の値と想定値は、ワークロードがイベントに関連した時間に基づいています。たとえば、イベントの検出後にワークロードがそのイベントに関連した可能性があるため、パフォーマンス統計がイベント検出時の値に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 は最大 30 日間の 5 分間の履歴パフォーマンスおよびイベント データを保持するため、イベントが 30 日以上経過している場合はパフォーマンス データは表示されません。

• ワークロードソート列

◦ レイテンシーチャート

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列

競合状態のクラスター 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。赤のバーは、イベント期間（検出時間から最後の分析時間まで）を示します。詳細については、["ワークロードパフォーマンス測定値"](#)。



ネットワーク コンポーネントの場合は、クラスター以外のアクティビティに基づいてネットワーク パフォーマンス統計が作成されるため、この列は表示されません。

◦ コンポーネントの使用法

ネットワーク処理、データ処理、およびアグリゲート コンポーネントの利用率（割合）の履歴またはQoSポリシー グループ コンポーネントのアクティビティ（割合）の履歴が表示されます。ネットワーク コンポーネントまたはインターコネクト コンポーネントについてはこのグラフは表示されません。統計にカーソルを合わせると、特定の時点における使用状況を表示できます。

- 合計書き込み**MB/秒**履歴

MetroClusterのリソース コンポーネントの場合にのみ、MetroCluster構成のパートナー クラスタにミラーリングされるすべてのボリューム ワークロードについて、書き込みスループットの合計が1秒あたりのメガバイト数 (MBps) で表示されます。

- イベント履歴

競合状態のコンポーネントの過去のイベントを示す赤い影付きの線が表示されます。廃止状態のイベントの場合は、選択したイベントが検出される前に発生したイベントおよびそのイベントが解決されたあとに発生したイベントがチャートに表示されます。

Unified Managerで検出される構成の変更

Unified Manager は、クラスタの構成変更を監視して、変更がパフォーマンス イベントの原因となったか、または一因となったかどうかを判断できるようにします。パフォーマンスエクスプローラーのページには、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 エクスプローラー]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 イベントと同時にその前後に変更が検出されていれば、その変更が原因でイベントのアラートがトリガーされた可能性があります。

Unified Manager は、情報イベントとして分類される次の変更イベントを検出できます。

- ボリュームがアグリゲート間で移動されたとき。

Unified Manager は、移動が進行中か、完了したか、失敗したかを検出できます。ボリュームの移動中に Unified Manager がダウンした場合、Unified Manager が復旧するとボリュームの移動が検出され、その変更イベントが表示されます。

- 1つ以上の監視対象ワークロードを含むQoSポリシー グループのスループット (MBpsまたはIOPS) の制限が変更されたとき。

ポリシー グループ制限を変更するとレイテンシ (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 ペア内のノードは、パートナー ノードのストレージを引き継ぐか、または返します。

Unified Manager は、テイクオーバー、部分テイクオーバー、またはギブバック操作が完了したことを検出できます。パニック状態のノードによってテイクオーバーが発生した場合、Unified Manager はイベントを検出しません。

- ONTAPのアップグレードやリバートの処理が正常に完了したとき。

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

イベント リストを使用すると、Unified Manager に表示される各イベントのイベント カテゴリ、イベント名、重大度タイプについてさらに詳しく知ることができます。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でリストされています。

アグリゲート イベント

アグリゲート イベントは、アグリゲートのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

アスタリスク (*) は、Unified Manager イベントに変換された EMS イベントを示します。

イベント名 (トラップ名)	影響レベル	ソース タイプ	重大度
アグリゲートはオフライン (ocumEvtAggregateStateOffline)	インシデント	Aggregate	致命的
アグリゲートで障害 (ocumEvtAggregateStateFailed)	インシデント	Aggregate	致命的
アグリゲートは制限状態 (ocumEvtAggregateStateRestricted)	リスク	Aggregate	警告
アグリゲートは再構築中 (ocumEvtAggregateRaidStateReconstructing)	リスク	Aggregate	警告
アグリゲートはデグレード状態 (ocumEvtAggregateRaidStateDegraded)	リスク	Aggregate	警告
クラウド階層に一部到達可能 (ocumEventCloudTierPartiallyReachable)	リスク	Aggregate	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	Aggregate	エラー
集約の再配置のためにクラウド層アクセスが拒否されました *(arlNetraCaCheckFailed)	リスク	Aggregate	エラー
ストレージフェイルオーバー中にアグリゲートの再配置でクラウド層アクセスが拒否されました *(gbNetraCaCheckFailed)	リスク	Aggregate	エラー
MetroCluster で残ったアグリゲートあり (ocumEvtMetroClusterAggregateLeftBehind)	リスク	Aggregate	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	Aggregate	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	Aggregate	警告
アグリゲート スペースがフル (ocumEvtAggregateFull)	リスク	Aggregate	エラー
アグリゲートのフルまでの日数 (ocumEvtAggregateDaysUntilFullSoon)	リスク	Aggregate	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	Aggregate	エラー
アグリゲートがほぼオーバーコミット (ocumEvtAggregateAlmostOvercommitted)	リスク	Aggregate	警告
アグリゲートの Snapshot リザーブがフル (ocumEvtAggregateSnapshotReserveFull)	リスク	Aggregate	警告
アグリゲートの増加率 - 異常 (ocumEvtAggregateGrowthRateAbnormal)	リスク	Aggregate	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	Aggregate	情報
アグリゲートの名前を変更（該当なし）	イベント	Aggregate	情報
アグリゲートを削除（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 の重大しき値を超過 (ocumAggregateIopsIncident)	インシデント	Aggregate	致命的

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	Aggregate	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	Aggregate	致命的
アグリゲート MBps の警告しきい値を超過 (ocumAggregateMbpsWarning)	リスク	Aggregate	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	Aggregate	致命的
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	Aggregate	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	Aggregate	致命的
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	Aggregate	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	Aggregate	致命的
アグリゲート利用率の警告しきい値を超過 (ocumAggregateUtilizationWarning)	リスク	Aggregate	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	Aggregate	警告
アグリゲート動的イベントのしきい値を超過 (ocumAggregateDynamicEventWarning)	リスク	Aggregate	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まとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

アスタリスク（*）は、Unified Manager イベントに変換された EMS イベントを示します。

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
クラスタにスペア ディスクなし (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
クラスタ監視失敗 (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
NVMe-oF 猶予期間が開始されました *(nvmfGracePeriodStart)	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-oF 猶予期間アクティブ *(nvmfGracePeriodActive)	リスク	クラスタ	警告
NVMe-oF 猶予期間が終了しました *(nvmfGracePeriodExpired)	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 (objectMaintenanceWindowStarted)	イベント	クラスタ	致命的
オブジェクトのメンテナンス時間を終了 (objectMaintenanceWindowEnded)	イベント	クラスタ	情報
MetroCluster で残ったスペア ディスクあり (ocumEvtSpareDiskLeftBehind)	リスク	クラスタ	エラー
MetroCluster の自動計画外スイッチオーバーが無効 (ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	リスク	クラスタ	警告
クラスターユーザーの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

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しました *(wafCaResyncComplete)	イベント	クラスタ	警告
FabricPool のスペースがほぼいっぱいです *(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
ノードの追加（該当なし）	イベント	クラスタ	情報
ノードを削除（該当なし）	イベント	クラスタ	情報
クラスタを削除（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
クラスタの名前を変更（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	致命的
重大な EMS を受信（該当なし）	イベント	クラスタ	致命的
アラートの EMS を受信（該当なし）	イベント	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
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
致命的	緊急 致命的
エラー	アラート
警告	エラー 警告 デバッグ 知らせ 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

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 IOPS の重大しき値を超過 (ocumClusterIopsIncident)	インシデント	クラスタ	致命的
クラスタ IOPS の警告しき値を超過 (ocumClusterIopsWarning)	リスク	クラスタ	警告
クラスタ MBps の重大しき値を超過 (ocumClusterMbpsIncident)	インシデント	クラスタ	致命的
クラスタ MBps の警告しき値を超過 (ocumClusterMbpsWarning)	リスク	クラスタ	警告
クラスタ動的イベントの警告しき値を超過 (ocumClusterDynamicEventWarning)	リスク	クラスタ	警告

影響領域：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
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

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
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 バナーを変更 (ocumClusterLoginBannerChanged)	リスク	クラスタ	警告
ログ転送先を変更 (ocumLogForwardDestinationsChanged)	リスク	クラスタ	警告
NTP サーバ名を変更 (ocumNtpServerNamesChanged)	リスク	クラスタ	警告
NTP サーバ数が不足 (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ない (ocumClusterPeerEncryptionDisabled)	リスク	クラスタ	警告
SSH でセキュアでない暗号を使用 (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
一部の ONTAP ユーザ アカウントで安全性が低い MD5 ハッシュ関数を使用 (ocumClusterMD5PasswordHashUsed)	リスク	クラスタ	警告

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
クラスタで自己署名証明書を使用 (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間がまもなく終了 (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 (ocumEvtClusterCertificateExpired)	リスク	クラスタ	エラー

ディスク イベント

ディスクのイベントは、ディスクのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
フラッシュ ディスク - スペア ブロックをほぼ使用 (ocumEvtClusterFlashDiskFewerSpareBlockError)	リスク	クラスタ	エラー
フラッシュ ディスク - スペア ブロックなし (ocumEvtClusterFlashDiskNoSpareBlockCritical)	インシデント	クラスタ	致命的
未割り当てディスクあり (ocumEvtClusterUnassignedDisksSome)	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
障害ディスクあり (ocumEvtDisksSomeFailed)	インシデント	クラスタ	致命的

エンクロージャ イベント

エンクロージャのイベントは、データセンター内のディスク シェルフ エンクロージャのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
ディスク シェルフのファンに障害 (ocumEvtShelfFanFailed)	インシデント	ストレージ シェルフ	致命的
ディスク シェルフの電源装置に障害 (ocumEvtShelfPowerSupplyFailed)	インシデント	ストレージ シェルフ	致命的
ディスク シェルフ マルチパス未設定 (ocumDiskShelfConnectivityNotInMultiPath)	リスク	ノード	警告
このイベントは以下のものには適用されません: • MetroCluster構成のクラスタ • 次のプラットフォーム: FAS2554、FAS2552、FAS2520、および FAS2240			
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
ディスク シェルフを検出（該当なし）	イベント	ノード	情報
ディスク シェルフを削除（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上のファンの状態に関する情報を提供するため、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
1 つ以上のファンに障害（ocumEvtFansOneOrMoreFailed）	インシデント	ノード	致命的

フラッシュ カード イベント

フラッシュ カードのイベントは、データセンター内のノードに取り付けられているフラッシュ カードのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
フラッシュ カードはオフライン（ocumEvtFlashCardOffline）	インシデント	ノード	致命的

inode イベント

inode イベントは、inode がフルまたはほぼフルになったことを通知します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
inode がほぼフル (ocumEvtInodesAlmostFull)	リスク	Volume	警告
inode がフル (ocumEvtInodesFull)	リスク	Volume	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（LIF）イベントは、LIFのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
ネットワーク インターフェイスのステータス - 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実行不可 (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未設定（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	致命的
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	致命的
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	致命的
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まとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

アスタリスク (*) は、Unified Manager イベントに変換された EMS イベントを示します。

イベント名 (トラップ名)	影響レベル	ソース タイプ	重大度
LUN はオフライン (ocumEvtLunOffline)	インシデント	LUN	致命的
LUN が破棄されました *(lunDestroy)	イベント	LUN	情報
igroup でサポートされないオペレーティング システムに LUN をマッピング (igroupUnsupportedOsType)	インシデント	LUN	警告
LUN にアクセスするためのアクティブなパスが 1 つのみ (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	致命的
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ない (ocumEvtLunHaPathInactive)	リスク	LUN	警告

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
HA ペアの一方向のノードから 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なし (ocumEvtLunSnapshotNotPossible)	リスク	Volume	警告

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
igroup でサポートされないオペレーティング システムに LUN をマッピング (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	致命的
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	致命的

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
LUN MBps の警告しきい値を超過 (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	致命的
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	致命的
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	致命的
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

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
LUNレイテンシ / アグリゲート使用済みパフォーマンス容量の重大しきい値を超過 (ocumLunLatencyAggregatePerfCapacityUsedIncident)	インシデント	LUN	致命的
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
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	致命的
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	致命的
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

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
LUNレイテンシ / ノードの使用済みパフォーマンス容量 - テイクオーバーの重大しきい値を超過 (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	インシデント	LUN	致命的
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	致命的
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 (ocumConformanceLatencyWarning)	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に関する情報を提供するため、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：構成

イベント名 (トラップ名)	影響レベル	ソース タイプ	重大度
管理サーバのディスク スペースがほぼフル (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	致命的
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なし (ocumEvtUnifiedManagerMemoryAlmostOut)	インシデント	管理ステーション	致命的
MySQL ログ ファイルのサイズを拡張 (再起動が必要) (ocumEvtMysqlLogFileSizeWarning)	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が まもなく最大割り当てに到達	リスク	管理ステーション	警告
syslog サーバ証明書の有効期間がまもなく終了	リスク	管理ステーション	警告
syslog サーバ証明書の有効期間が終了	リスク	管理ステーション	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
監査ログ ファイルが改ざん	リスク	管理ステーション	警告
監査ログ ファイルが削除	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 サーバ構成が変更	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	致命的



最後の2つのパフォーマンス イベントは、Unified Manager 7.2でのみ使用されていたものです。これらのいずれかのイベントが新規の状態で存在している場合、Unified Managerソフトウェアを新しいバージョンにアップグレードしたときにイベントは自動的にページされません。これらのイベントについては、手動で解決済みの状態にする必要があります。

MetroClusterブリッジ イベント

MetroClusterブリッジ イベントは、ブリッジのステータス情報を提供します。これにより、MetroCluster over FC構成の潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
ブリッジに到達不能 (ocumEvtBridgeUnreachable)	インシデント	MetroClusterブリッジ	致命的

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
ブリッジの温度が異常 (ocumEvtBridgeTemperatureAbnormal)	インシデント	MetroClusterブリッジ	致命的

MetroCluster接続イベント

接続イベントは、クラスタ内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構成内のクラスタ間の接続に関する情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

両方の構成に共通のイベント

次の接続イベントは、MetroCluster over FC構成とMetroCluster over IP構成に共通です。

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	致命的
MetroCluster パートナーにピアリング ネットワーク経由で到達不能 (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	インシデント	MetroCluster関係	致命的
MetroCluster ディザスタリカバリ機能への影響 (ocumEvtMetroClusterDRStatusImpacted)	リスク	MetroCluster関係	致命的
MetroCluster 構成をスイッチオーバー (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 (ocumEvtMetroClusterAllSLBetweenSwitchesDown)	インシデント	MetroClusterスイッチ間の接続	致命的
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ブリッジのスタック接続	致命的
MetroCluster 構成を一部スイッチオーバー (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	致命的
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	致命的

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	致命的
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	致命的
ノード間の一部の 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	致命的
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	致命的
ノードからストレージ スタックへの一部の 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

次のイベントは、MetroCluster over IP構成に関係します。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
MetroCluster IP サイト間 接続ステータスが停止 (mccIntersiteconnectivity StatusDown)	リスク	MetroCluster関係	致命的
MetroCluster IP ノードから スイッチへの接続がオフライン (mcclpPortStatusOffline)	リスク	ノード	エラー

MetroClusterスイッチ イベント

MetroCluster over FC構成についてのMetroClusterスイッチ イベントは、MetroClusterスイッチのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
スイッチの温度が異常 (ocumEvtSwitchTemperatureAbnormal)	インシデント	MetroClusterスイッチ	致命的
スイッチに到達不能 (ocumEvtSwitchUnreachable)	インシデント	MetroClusterスイッチ	致命的
スイッチのファンに障害 (ocumEvtSwitchFansOneOrMoreFailed)	インシデント	MetroClusterスイッチ	致命的
スイッチの電源装置に障害 (ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	インシデント	MetroClusterスイッチ	致命的

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
スイッチの温度センサーに障害 (ocumEvtSwitchTemperatureSensorFailed)  このイベントはCiscoスイッチにのみ関係します。	インシデント	MetroClusterスイッチ	致命的

NVMeネームスペース イベント

NVMeネームスペース イベントは、ネームスペースのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

アスタリスク（*）は、Unified Manager イベントに変換された EMS イベントを示します。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
NVMeNS オフライン *(nvmeNamespaceStatusOffline)	イベント	ネームスペース	情報
NVMeNS オンライン *(nvmeNamespaceStatusOnline)	イベント	ネームスペース	情報
NVMeNS スペース不足 *(nvmeNamespaceSpaceOutOfSpace)	リスク	ネームスペース	警告
NVMeNS 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	致命的
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	致命的
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
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	致命的
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	致命的
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

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 / MBps の重大しき値を超過 (ocumNvmeNamespaceLatencyMbpsIncident)	インシデント	ネームスペース	致命的
NVMe ネームスペース レイテンシ / MBps の警告しき値を超過 (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まとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

アスタリスク (*) は、Unified Manager イベントに変換された EMS イベントを示します。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
ノードのルート ボリュームのスペースがほぼフル (ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	リスク	ノード	警告
クラウド AWS メタデータ接続失敗 *(ocumCloudAwsMetadataConnFail)	リスク	ノード	エラー
クラウド AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	リスク	ノード	エラー
クラウド AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	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
クラウド AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	リスク	ノード	エラー
クラウド AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	イベント	ノード	情報
クラウド AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	リスク	ノード	エラー
クラウド AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	リスク	ノード	エラー
クラウド層ホストが解決できません *(ocumObjstoreHostUnresolvable)	リスク	ノード	エラー
クラウド層クラスタ間ネットワークインターフェースがダウンしています *(ocumObjstoreInterClusterLifDown)	リスク	ノード	エラー
NFSv4 プールの 1 つが使い果たされました *(nbladeNfsv4PoolExhaust)	インシデント	ノード	致命的
リクエストの不一致クラウド層署名 *(oscSignatureMismatch)	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 モニター メモリ最大 *(ocumQosMonitorMemoryMaxed)	リスク	ノード	エラー
QoS モニター メモリ削減 *(ocumQosMonitorMemoryAbated)	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 (ocumNodeIopsIncident)	インシデント	ノード	致命的
ノード IOPS の警告しき い値を超過 (ocumNodeIopsWarning)	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	致命的
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	致命的

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 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	致命的
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	致命的
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	致命的
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 ペアの情報しきい値を超過 (ocumNodeHaPairOverUtilizedInformation)	イベント	ノード	情報

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
ノード ディスク断片化の警告しきい値を超過 (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
ノード動的イベントの警告しきい値を超過 (ocumNodeDynamicEventWarning)	リスク	ノード	警告

影響領域：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-<アドバイザリID>(ocumx)	リスク	ノード	致命的

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まとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
NVRAM バッテリー低下 (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	致命的

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て、ポートでの変更や問題（ポートがダウンしているかどうかなど）を監視できるようにします。

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
ポート ステータス - 停止 (ocumEvtPortStatusDown)	インシデント	ノード	致命的

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	致命的
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	致命的
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	致命的

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	致命的
FCP ポート利用率の警告しきい値を超過 (ocumFcpPortUtilizationWarning)	リスク	ポート	警告

電源装置イベント

電源装置イベントは、ハードウェアのステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
1 つ以上の電源装置に障害 (ocumEvtPowerSupplyOneOrMoreFailed)	インシデント	ノード	致命的

保護イベント

保護イベントは、ジョブの失敗や中止を通知して、問題を監視できるようにします。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：保護

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
保護ジョブ失敗 (ocumEvtProtectionJobTaskFailed)	インシデント	ボリュームまたはストレージ サービス	致命的

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
保護ジョブ中止 (ocumEvtProtectionJobAborted)	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 の容量やファイルとディスクの制限に関する情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
qtree スペースがほぼフル (ocumEvtQtreeSpaceNearlyFull)	リスク	qtree	警告
qtree スペースがフル (ocumEvtQtreeSpaceFull)	リスク	qtree	エラー
qtree のスペースが正常 (ocumEvtQtreeSpaceThresholdOk)	イベント	qtree	情報
qtree のファイル数がハード リミットに到達 (ocumEvtQtreeFilesHardLimitReached)	インシデント	qtree	致命的
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 リミットに到達 (ocumEvtQtreeSpaceHardLimitReached)	インシデント	qtree	致命的

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 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まとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
サービス プロセッサが未設定 (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SnapMirror関係と同期SnapMirror関係のステータス情報を提供します。これにより、潜在的な問題を監視できます。非同期SnapMirror関係イベントはStorage VMとボリュームの両方について生成されますが、同期SnapMirror関係イベントはボリューム関係についてのみ生成されます。Storage VMディザスタ リカバリ関係を構成す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まとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：保護

アスタリスク (*) は、Unified Manager イベントに変換された EMS イベントを示します。



SnapMirror関係イベントは、Storage VMディザスタ リカバリで保護されているStorage VMについて生成されますが、コンスティチュエント オブジェクトの関係については生成されません。

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
ミラー レプリケーション は正常でない (ocumEvtSnapmirrorRel ationshipUnhealthy)	リスク	SnapMirror関係	警告
ミラー レプリケーション を切断 (ocumEvtSnapmirrorRel ationshipStateBrokenoff)	リスク	SnapMirror関係	エラー
ミラー レプリケーション の初期化失敗 (ocumEvtSnapmirrorRel ationshipInitializeFailed)	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 (ocumEvtSnapmirrorRel ationshipUpdateFailed)	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 (ocumEvtSnapMirrorRel ationshipLagError)	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 (ocumEvtSnapMirrorRel ationshipLagWarning)	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 (ocumEvtSnapmirrorRel ationshipResyncFailed)	リスク	SnapMirror関係	エラー
同期レプリケーションが 同期していません *(syncSnapmirrorRela tionshipOutofsync)	リスク	SnapMirror関係	警告
同期レプリケーションが 復元されました *(syncSnapmirrorRela tionshipInSync)	イベント	SnapMirror関係	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
同期レプリケーションの自動再同期に失敗しました *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	リスク	SnapMirror関係	エラー
ONTAP Mediator をクラスタに追加 (snapmirrorMediatorAdded)	イベント	クラスタ	情報
ONTAP Mediator をクラスタから削除 (snapmirrorMediatorRemoved)	イベント	クラスタ	情報
ONTAP Mediator にクラスタから到達不能 (snapmirrorMediatorUnreachable)	リスク	メディエーター	警告
ONTAP Mediator にクラスタからアクセス不能 (snapmirrorMediatorMisconfigured)	リスク	メディエーター	エラー
ONTAP Mediator接続を再確立して再同期、SnapMirrorアクティブ同期の準備完了 (snapmirrorMediatorInQuorum)	イベント	メディエーター	情報

非同期ミラー バックアップ関係イベント

非同期ミラー バックアップ関係イベントは、非同期SnapMirror関係とバックアップ関係のステータス情報を提供します。これにより、潜在的な問題を監視できます。非同期ミラー バックアップ関係イベントは、ボリュームとStorage VMの両方の保護関係についてサポートされます。ただし、Storage VMディザスタ リカバリのバックアップ関係はサポートされません。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：保護



SnapMirror関係とバックアップ関係のイベントは、Storage VMディザスタ リカバリで保護されているStorage VMについても生成されますが、コンスティチュエント オブジェクトの関係については生成されません。

イベント名 (トラップ名)	影響レベル	ソース タイプ	重大度
非同期ミラー バックアップは正常でない (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 更新失敗」 イベントは、Active IQポータル (Config Advisor) から生成されません。

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まとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
Snapshot の自動削除が無効（該当なし）	イベント	Volume	情報
Snapshot の自動削除が有効（該当なし）	イベント	Volume	情報
Snapshot の自動削除の設定を変更（該当なし）	イベント	Volume	情報

SnapVault関係イベント

SnapVault関係イベントは、SnapVault関係のステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：保護

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
非同期バックアップは正常でない (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）の設定のイベントは、ストレージ フェイルオーバーが無効な状態または設定されていない状態に関する情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
ストレージ フェイルオーバー インターコネクトの1つ以上のリンクが停止 (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未設定 (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 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実行不可 (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まとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：構成

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
ストレージ サービスを作成（該当なし）	イベント	ストレージ サービス	情報
ストレージ サービスをサブスクライブ（該当なし）	イベント	ストレージ サービス	情報
ストレージ サービスをアンサブスクライブ（該当なし）	イベント	ストレージ サービス	情報

影響範囲：保護

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
管理対象 SnapMirror 関係の予期しない削除 (ocumEvtStorageServiceUnsupportedRelationshipDeletion)	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	致命的

ストレージ シェルフ イベント

ストレージ シェルフ イベントは、ストレージ シェルフが異常な状態である場合に通知します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
異常な電圧範囲 (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、SVM）イベントは、Storage VM（SVM）のステータス情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

アスタリスク（*）は、Unified Manager イベントに変換された EMS イベントを示します。

影響範囲：可用性

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
Storage VM CIFSサービス停止 (ocumEvtVserverCifsServiceStatusDown)	インシデント	SVM	致命的
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	致命的
CIFS NetBIOS 名の競合 *(nbladeCifsNbNameConflict)	リスク	SVM	エラー
CIFS シャドウ コピー操作に失敗しました *(cifsShadowCopyFailure)	リスク	SVM	エラー
多数の CIFS 接続 *(nbladeCifsManyAuths)	リスク	SVM	エラー
最大 CIFS 接続数を超過しました *(nbladeCifsMaxOpenSameFile)	リスク	SVM	エラー
ユーザーあたりの CIFS 接続の最大数を超過しました *(nbladeCifsMaxSessPerUsrConn)	リスク	SVM	エラー
SVM FC / FCoE サービス停止 (ocumEvtVserverFcServiceStatusDown)	インシデント	SVM	致命的
SVM iSCSI サービス停止 (ocumEvtVserverIscsiServiceStatusDown)	インシデント	SVM	致命的

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 NFSサービス停止 (ocumEvtVserverNfsServiceStatusDown)	インシデント	SVM	致命的
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 サーバーがビジー状態のため、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
ウイルススキャン用の AV サーバー接続がありません *(nbladeVscanNoScannerConn)	インシデント	SVM	致命的
AV サーバーが登録されていません *(nbladeVscanNoRegdScanner)	リスク	SVM	エラー
応答する AV サーバー接続がありません *(nbladeVscanConnInactive)	イベント	SVM	情報
AVサーバーへの不正ユーザーによるアクセス試行*(nbladeVscanBadUserPrivAccess)	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
AV サーバーによってウイルスが検出されました *(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 を削除（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 (ocumSvmIopsIncident)	インシデント	SVM	致命的
SVM IOPS の警告しきい値を超過 (ocumSvmIopsWarning)	リスク	SVM	警告
SVM MBps の重大しきい値を超過 (ocumSvmMbpsIncident)	インシデント	SVM	致命的
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	致命的

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 レイテンシの警告しきい値を超過 (ocumSvmLatencyWarning)	リスク	SVM	警告

影響領域：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を使用 (ocumVserverSSHInsecure)	リスク	SVM	警告
ログイン バナーを変更 (ocumVserverLoginBannerChanged)	リスク	SVM	警告
ストレージ VM のランサムウェア対策監視が無効になっています (antiRansomwareSvmStateDisabled)	リスク	SVM	警告
ストレージ VM のランサムウェア対策監視が有効 (学習モード) (antiRansomwareSvmStateDryrun)	イベント	SVM	情報
Storage VM がランサムウェア対策監視に適合 (学習モード) (ocumEvtSvmArwCandidate)	イベント	SVM	情報

ユーザおよびグループ 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まとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：容量

イベント名 (トラップ名)	影響レベル	ソース タイプ	重大度
ユーザ / 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	ユーザまたはグループ クォータ	警告
ユーザ / グループ クォータのディスク スペースがハード リミットに到達 (ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	インシデント	ユーザまたはグループ クォータ	致命的
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	ユーザまたはグループ クォータ	警告
ユーザ クォータまたはグループ クォータのファイル数がハード リミットに到達 (ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	インシデント	ユーザまたはグループ クォータ	致命的

ボリューム イベント

ボリューム イベントは、ボリュームのステータスに関する情報を提供します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

アスタリスク (*) は、Unified Manager イベントに変換された EMS イベントを示します。

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	Volume	警告
ボリュームはオフライン (ocumEvtVolumeOffline)	インシデント	Volume	致命的
ボリュームは一部使用可能 (ocumEvtVolumePartiallyAvailable)	リスク	Volume	エラー
ボリュームをアンマウント（該当なし）	イベント	Volume	情報
ボリュームをマウント（該当なし）	イベント	Volume	情報
ボリュームを再マウント（該当なし）	イベント	Volume	情報
ボリューム ジャンクションパスは非アクティブ (ocumEvtVolumeJunctionPathInactive)	リスク	Volume	警告
ボリュームのオートサイズを有効化（該当なし）	イベント	Volume	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	Volume	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	Volume	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	Volume	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
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 (ocumThinProvisionVolumeSpaceAtRisk)	リスク	Volume	警告
ボリューム効率化処理エラー (ocumEvtVolumeEfficiencyOperationError)	リスク	Volume	エラー
ボリューム スペースがフル (ocumEvtVolumeFull)	リスク	Volume	エラー
ボリューム スペースがほぼフル (ocumEvtVolumeNearlyFull)	リスク	Volume	警告
ボリューム論理スペースフル *(volumeLogicalSpaceFull)	リスク	Volume	エラー
ボリュームの論理スペースがほぼいっぱいです *(volumeLogicalSpaceNearlyFull)	リスク	Volume	警告
ボリューム論理スペース正常 *(volumeLogicalSpaceAllOK)	イベント	Volume	情報
ボリュームの Snapshot リザーブ スペースがフル (ocumEvtSnapshotFull)	リスク	Volume	警告
Snapshot コピー数の上限を超過 (ocumEvtSnapshotTooMany)	リスク	Volume	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
ボリュームの qtree クォータがオーバーコミット (ocumEvtVolumeQtreeQuotaOvercommitted)	リスク	Volume	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	Volume	警告
ボリュームの増加率 - 異常 (ocumEvtVolumeGrowthRateAbnormal)	リスク	Volume	警告
ボリュームのフルまでの日数 (ocumEvtVolumeDaysUntilFullSoon)	リスク	Volume	エラー
ボリュームのスペース ガランティを無効化（該当なし）	イベント	Volume	情報
ボリュームのスペース ガランティを有効化（該当なし）	イベント	Volume	情報
ボリュームのスペース ガランティを変更（該当なし）	イベント	Volume	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	Volume	エラー
FlexGroup構成員にスペースの問題があります *(flexGroupConstituentsHaveSpaceIssues)	リスク	Volume	エラー

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
FlexGroup構成要素スペースステータスすべて OK *(flexGroupConstituentsSpaceStatusAllOK)	イベント	Volume	情報
FlexGroup構成要素に Inode の問題があります *(flexGroupConstituentsHaveInodesIssues)	リスク	Volume	エラー
FlexGroup構成要素の Inode ステータスすべて 正常 *(flexGroupConstituentsInodesStatusAllOK)	イベント	Volume	情報
WAFLボリュームの自動サイズ設定失敗 *(wafVolAutoSizeFail)	リスク	Volume	エラー
WAFLボリュームの自動サイズ調整が完了しました *(wafVolAutoSizeDone)	イベント	Volume	情報
FlexGroupボリュームの使用率は80%を超えています*	インシデント	Volume	エラー
FlexGroupボリュームの使用率は 90% 以上です*	インシデント	Volume	致命的
ボリューム ストレージ効率の異常 (ocumVolumeAbnormalStorageEfficiencyWarning)	リスク	Volume	警告
ボリューム Snapshot リザーブの使用率が低い (volumeSnapshotReserveUnderutilizedWarning)	イベント	Volume	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 Snapshot リザーブの使用率が低い (volumeSnapshotReserveUnderutilizedCleared)	イベント	Volume	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	Volume	情報
ボリュームを検出（該当なし）	イベント	Volume	情報
ボリュームを削除（該当なし）	イベント	Volume	情報

影響範囲：パフォーマンス

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
QoS ボリューム最大 IOPS の警告しきい値を超過 (ocumQosVolumeMaxIopsWarning)	リスク	Volume	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	Volume	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	Volume	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
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 (ocumConformanceLatencyWarning)	リスク	Volume	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	Volume	致命的
ボリューム IOPS の警告しきい値を超過 (ocumVolumeIopsWarning)	リスク	Volume	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	Volume	致命的
ボリューム MBps の警告しきい値を超過 (ocumVolumeMbpsWarning)	リスク	Volume	警告
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	Volume	致命的
ボリューム レイテンシの警告しきい値を超過 (ocumVolumeLatencyWarning)	リスク	Volume	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	Volume	致命的

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 キャッシュ ミス率の警告しきい値を超過 (ocumVolumeCacheMissRatioWarning)	リスク	Volume	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	Volume	致命的
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	Volume	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	Volume	致命的
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	Volume	警告
ボリューム レイテンシ / アグリゲートの使用済みパフォーマンス容量の重大しきい値を超過 (ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	インシデント	Volume	致命的
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 (ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	リスク	Volume	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	Volume	致命的
ボリリューム 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	Volume	警告
ボリリューム 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 (ocumVolumeLatencyNodePerfCapacityUsedIncident)	インシデント	Volume	致命的
ボリリューム 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 (ocumVolumeLatencyNodePerfCapacityUsedWarning)	リスク	Volume	警告
ボリリューム 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	Volume	致命的
ボリリューム 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	Volume	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 / ノード利用率の重大しき値を超過 (ocumVolumeLatencyNodeUtilizationIncident)	インシデント	Volume	致命的
ボリューム レイテンシ / ノード利用率の警告しき値を超過 (ocumVolumeLatencyNodeUtilizationWarning)	リスク	Volume	警告

影響領域：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	Volume	情報
ボリュームのランサムウェア対策監視が無効になっています (antiRansomwareVolumeStateDisabled)	リスク	Volume	警告
ボリュームランサムウェア対策監視が有効（学習モード） (antiRansomwareVolumeStateDryrun)	イベント	Volume	情報
ボリュームランサムウェア対策監視が一時停止中（学習モード） (antiRansomwareVolumeStateDryrunPaused)	リスク	Volume	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	Volume	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無効になっています (antiRansomwareVolumeStateDisableInProgress)	リスク	Volume	警告
ランサムウェアアクティビティ検出 (callHomeRansomwareActivitySeen)	インシデント	Volume	致命的
ボリュームがランサムウェア対策監視に適合（学習モード） (ocumEvtVolumeArwCandidate)	イベント	Volume	情報
ボリュームがランサムウェア対策監視に適合（アクティブ モード） (ocumVolumeSuitedForActiveAntiRansomwareDetection)	リスク	Volume	警告
ボリュームにランサムウェア対策のアラートあり (antiRansomwareFeatureNoisyVolume)	リスク	Volume	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
ボリュームでローカル Snapshot の保護が十分でない (volumeLacksLocalProtectionWarning)	リスク	Volume	警告
ボリュームでローカル Snapshot の保護が十分でない (volumeLacksLocalProtectionCleared)	リスク	Volume	警告

ボリューム移動ステータス イベント

ボリューム移動のステータスのイベントは、ボリューム移動のステータスについて通知します。これにより、潜在的な問題を監視できます。影響範囲別にイベントがまとめられ、イベント名とトラップ名、影響レベル、ソース タイプ、および重大度が表示されます。

影響範囲：容量

イベント名（トラップ名）	影響レベル	ソース タイプ	重大度
ボリューム移動ステータス: 進行中(該当なし)	イベント	Volume	情報
ボリューム移動ステータス - 失敗 (ocumEvtVolumeMoveFailed)	リスク	Volume	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	Volume	情報
ボリューム移動ステータス - カットオーバー保留 (ocumEvtVolumeMoveCutoverDeferred)	リスク	Volume	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 ページおよび[イベントの詳細]ページを使用してすべてのイベントを監視できます。[通知セットアップ オプション]ダイアログ ボックスでは、通知を設定できます。[イベント セットアップ]ページでは、イベントを無効または有効にすることができます。

[通知]ページ

Unified Managerサーバでは、イベントが生成されたときやユーザに割り当てられたときに通知を送信するように設定することができます。また、通知メカニズムを設定することもできます。たとえば、通知をEメールやSNMPトラップとして送信できます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

Eメール

この領域では、アラート通知に対して次の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サーバ設定を行うことができます。

- ホスト名またはIPアドレス

SMTPホスト サーバのホスト名を指定します。このホスト名は、指定した受信者へのアラート通知の送信に使用されます。

- ユーザー名

SMTPユーザ名を指定します。SMTPユーザ名は、SMTPサーバでSMTPAUTHが有効になっている場合にのみ必要です。

- パスワード

SMTPパスワードを指定します。SMTPユーザ名は、SMTPサーバでSMTPAUTHが有効になっている場合にのみ必要です。

- ポート

アラート通知を送信するSMTPホスト サーバで使用されるポートを指定します。

デフォルト値は25です。

- **START/TLS** を使用する

このチェック ボックスをオンにすると、TLS/SSLプロトコル（start_tlsおよびStartTLSとも表記）を使用してSMTPサーバと管理サーバの間のセキュアな通信が確立されます。

- **SSL**を使用する

このチェック ボックスをオンにすると、SSLプロトコルを使用してSMTPサーバと管理サーバの間のセキュアな通信が確立されます。

SNMP

この領域では、次のSNMPトラップ設定を行うことができます。

- バージョン

必要なセキュリティのタイプに応じて、使用するSNMPバージョンを指定します。[バージョン 1]、[バージョン 3]、[バージョン 3、認証を使用]、[バージョン 3、認証と暗号化を使用]の各オプションがあります。デフォルト値は[バージョン 1]です。

- トラップ先ホスト

管理サーバによって送信されるSNMPトラップを受信するホスト名またはIPアドレス（IPv4またはIPv6）を指定します。トラップの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。



他のすべてのSNMP設定（バージョンやアウトバウンド 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。

- 送信トラップポート

管理サーバによって送信されるトラップをSNMPサーバが受信する際に使用するポートを指定します。

デフォルト値は162です。

- コミュニティ

ホストにアクセスするためのコミュニティ スtringです。

- エンジンID

SNMPエージェントの一意的識別子を指定します。この識別子は、管理サーバによって自動的に生成されます。[エンジン ID]は、[SNMP バージョン 3]、[SNMP バージョン 3、認証を使用]、および[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。

- ユーザー名

SNMPユーザ名を指定します。[ユーザ名]は、[SNMP バージョン 3]、[SNMP バージョン 3、認証を使用]、および[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。

- 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。プロトコルのオプションには[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 バージョン 3、認証を使用]および[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。

- 認証パスワード

ユーザの認証時に使用するパスワードを指定します。[認証パスワード]は、[SNMP バージョン 3、認証を使用]および[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。

- プライバシープロトコル

SNMPメッセージの暗号化に使用するプライバシー プロトコルを指定します。プロトコルのオプションには[AES 128]と[DES]があります。デフォルト値は[AES 128]です。[プライバシー プロトコル]は、[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。

- プライバシーパスワード

プライバシー プロトコルの使用時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オブジェクトとトラップの詳細については、"[Active IQ Unified ManagerMIB](#)" NetAppサポート サイトから。

[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確認できます。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。

- 定義済みのフィルター選択リストから選択するための表示メニュー。

たとえば、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あります。

- 完全な用語または部分的な用語を入力してイベントのリストを絞り込むための検索ペイン。
- [フィルタ]ボタン。[フィルタ]ペインを起動し、使用可能なすべてのフィールドとフィールド属性から条件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。

- 割り当て先

イベントを割り当てるユーザを選択できます。イベントをユーザに割り当てると、イベント リストの選択したイベントの該当するフィールドに、そのユーザの名前とイベントを割り当てた時刻が追加されます。

- 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、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。

- 認める

選択したイベントを確認します。

イベントを確認すると、イベント リストの選択したイベントの該当するフィールドに、自分のユーザ名とイベントを確認した時刻が追加されます。確認したイベントについては、自分で対処する必要があります。



情報イベントに確認応答することはできません。

- 解決済みとしてマーク

イベントの状態を解決済みに変更できます。

イベントを解決すると、イベント リストの選択したイベントの該当するフィールドに、自分のユーザ名とイベントを解決した時刻が追加されます。イベントに対処したら、そのイベントを解決済みとしてマークする必要があります。

- アラートを追加

[アラートの追加]ダイアログ ボックスが表示され、選択したイベントにアラートを追加できます。

- レポート

現在のイベント ビューの詳細をカンマ区切り値 (.csv) ファイルまたはPDFドキュメントとしてエクスポートできます。

- 列セレクトターの表示/非表示

ページに表示する列とその表示順序を選択できます。

【イベント】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 イベント」ビューが表示され、過去 7 日間の、インシデントまたはリスクの影響レベルを持つ新規および確認済みのイベントが表示されます。

- トリガー時間

イベントが生成された時刻。

- 重大度

イベントの重大度: 重大 (❌)、エラー (🔴)、警告 (⚠️)、および情報 (ℹ️)。

- 州

イベントの状態: 新規、確認済み、解決済み、または廃止。

- 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、またはアップグレード。

- 影響エリア

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、またはセキュリティ。

- 名前

イベント名。名前を選択して、そのイベントの[イベントの詳細]ページを表示できます。

- ソース

イベントが発生したオブジェクトの名前。名前を選択して、そのオブジェクトの健全性またはパフォーマンスの詳細ページを表示できます。

共有QoSポリシーの違反の場合、このフィールドには、IOPSまたはMBpsが高い上位のワークロード オブジェクトのみが表示されます。このポリシーを使用する他のワークロードは[イベントの詳細]ページに表示されます。

- ソースタイプ

イベントが関連付けられているオブジェクトのタイプ（Storage VM、ボリューム、qtreeなど）。

- 担当者

イベントが割り当てられているユーザの名前。

- イベントの起源

「Active IQポータル」のイベントか、「Active IQ Unified Manager」から直接のイベントか。

- 注釈名

ストレージ オブジェクトに割り当てられたアノテーションの名前。

- 注記

イベントに追加されているメモの数。

- 未払い日数

イベントが最初に生成されてからの経過日数。

- 指定時間

イベントがユーザに割り当てられてからの経過時間。1週間を過ぎたイベントには、割り当て時のタイムスタンプが表示されます。

- 謝辞

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。

- 承認された時間

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。

- 時代遅れの時間

イベントの状態が「廃止」になった時刻。

[イベントの詳細]ページ

[イベントの詳細]ページでは、選択したイベントの重大度、影響レベル、影響領域、イベントソースなどの詳細を確認できます。問題を解決するための考えられる対処方法に関する追加情報も確認できます。

- イベント名

イベントの名前と最終確認時刻。

パフォーマンス イベント以外のイベントの場合は、状態が「新規」または「確認済み」のときは最終確認時刻が不明なため、この情報は表示されません。

- イベントの説明

イベントの簡単な説明。

イベントの説明には、イベントがトリガーされた理由が含まれる場合があります。

- 競合中のコンポーネント

動的なパフォーマンス イベントについて、クラスターの論理コンポーネントと物理コンポーネントを表すアイコンが表示されます。コンポーネントが競合状態にある場合は、アイコンが赤い丸で強調表示されます。

ここで表示されるコンポーネントの説明については、「クラスター コンポーネントとそれらが競合する理由」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

- 私に割り当てる

イベントを自分に割り当てます。

- 他の人に割り当てる

[所有者の割り当て]ダイアログ ボックスが開き、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。

イベントをユーザに割り当てると、イベント リストの選択したイベントの該当するフィールドに、そのユーザの名前とイベント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。

- 認める

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応答した時刻が追加されます。確認応答したイベントについては、自分で対処する必要があります。

- 解決済みとしてマーク

イベントの状態を「解決済み」に変更できます。

イベントを解決すると、イベント リスト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。

- アラートを追加

[アラートの追加]ダイアログ ボックスが表示され、選択したイベントにアラートを追加できます。

[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 タイプに関係のないフィールドは表示されません。イベントに関する次の詳細を確認できます。

- イベントトリガー時間

イベントが生成された時刻。

- 州

イベントの状態: 新規、確認済み、解決済み、または廃止。

- 廃止された原因

イベントが廃止になった理由（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たときまでの時間です。廃止状態のイベントの場合は、イベントが検出されてから解決されるまでの時間です。

このフィールドは、すべてのパフォーマンス イベントに対して表示されます。その他のタイプのイベントについては、解決されるか廃止になったあとにのみ表示されます。

- 最終閲覧

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、イベントがアクティブである限り、このフィールドはパフォーマンス データが新たに収集されるたびに更新されるため、この値はイベント トリガー時間よりも新しいものになることがあります。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: 重大 (❌)、エラー (🔴)、警告 (⚠️)、および情報 (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、またはアップグレード。

- 影響エリア

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、またはセキュリティ。

- ソース

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。

- ソース注釈

イベントが関連付けられているオブジェクトのアノテーションの名前と値が表示されます。

このフィールドは、クラスタ、SVM、およびボリュームの健全性イベントに対してのみ表示されます。

- ソースグループ

該当するオブジェクトがメンバーとして属しているすべてのグループの名前が表示されます。

このフィールドは、クラスタ、SVM、およびボリュームの健全性イベントに対してのみ表示されます。

- ソースタイプ

イベントが関連付けられているオブジェクト タイプ (SVM、ボリューム、Qtrees など)。

- クラスター上

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の数

イベントの影響を受けるオブジェクトの数。

オブジェクトのリンクをクリックすると、インベントリ ページが表示され、現在このイベントの影響を受けているオブジェクトを確認できます。

このフィールドは、パフォーマンス イベントに対してのみ表示されます。

- 影響を受けるボリューム

このイベントの影響を受けるボリュームの数。

このフィールドは、ノードまたはアグリゲートのパフォーマンス イベントに対してのみ表示されます。

- トリガーされたポリシー

イベントを発行したしきい値ポリシーの名前。

ポリシー名にカーソルを合わせると、しきい値ポリシーの詳細を確認できます。アダプティブQoSポリシーの場合は、定義されているポリシー、ブロック サイズ、および割り当てのタイプ（割り当てスペースまたは使用スペース）も表示されます。

このフィールドは、パフォーマンス イベントに対してのみ表示されます。

- ルールID

Active IQプラットフォーム イベントの場合、これはイベントを生成するためにトリガーされたルールの数です。

- 謝辞

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。

- 担当者

イベントへの対応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たアラートがない場合、「アラートを追加」リンクが表示されます。

リンクをクリックすると、[アラートの追加]ダイアログ ボックスが開きます。

- 選択したイベントにアラートが1つ関連付けられている場合は、そのアラートの名前が表示されます。

リンクをクリックすると、[アラートの編集]ダイアログ ボックスが開きます。

- 選択したイベントにアラートが複数関連付けられている場合は、アラートの数が表示されます。

リンクをクリックすると、[アラート セットアップ]ページが開き、それらのアラートに関する詳細が表示されます。

無効になっているアラートは表示されません。

- 最終通知送信

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。推奨される操作は、イベントのタイプまたは超過したしきい値のタイプに基づいてカスタマイズされます。

この領域は、一部のタイプのイベントに対してのみ表示されます。

場合によっては、特定のアクションを実行するための手順など、多くの推奨アクションに関する追加情報を参照する ヘルプ リンクがページ上に提供されます。一部の対処方法では、Unified Manager、ONTAP System Manager、OnCommand Workflow Automation、ONTAP CLIコマンド、またはこれらのツールの組み合わせを使用する場合があります。

ここで提案されているアクションは、このイベントを解決するためのガイドとしてのみ考慮する必要があります。このイベントを解決するために実行するアクションは、環境のコンテキストに基づいて決定する必要があります。

オブジェクトとイベントをさらに詳細に分析する場合は、[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の詳細な診断の結果、単一の解決策が提示されることがあります。利用可能な場合、それらの解決策は「修正する」ボタンとともに表示されます。このボタンをクリックすると、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、このセクションには、問題と考えられる解決策を説明するNetAppナレッジベースの記事へのリンク (利用可能な場合) が含まれることがあります。外部ネットワークにアクセスできないサイトでは、ナレッジベースの記事の PDF がローカルで開かれます。この PDF は、Unified Manager インスタンスに手動でダウンロードするルール ファイルの一部です。

[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 イベントについては、トリガーされたイベントに関連するグラフが表示されます。通常は、過去10日間のIOPSまたはMBpsのグラフとレイテンシのグラフです。これらのグラフを確認することで、イベントがアクティブなときにレイテンシに影響している、または影響を受けているストレージ コンポーネントを特定することができます。

動的なパフォーマンス イベントについては、次のグラフが表示されます。

- ワークロード レイテンシ - 競合状態のコンポーネントのVictim、Bully、Sharkの上位のワークロードについて、レイテンシの履歴が表示されます。
- ワークロード アクティビティ - 競合状態のクラスタ コンポーネントのワークロードの使用量に関する詳細が表示されます。
- リソース アクティビティ - 競合状態のクラスタ コンポーネントの過去のパフォーマンス統計が表示されます。

一部のクラスタ コンポーネントが競合状態にある場合は、これ以外のグラフが表示されます。

その他のイベントについては、ストレージ オブジェクトに対して実行されている分析タイプの簡単な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 ポリシーの場合は、複数の行 (分析されたコンポーネントごとに1行) が表示されることがあります。この場合、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。

イベント設定ページ

[イベント セットアップ]ページには、無効なイベントのリストが表示されます。また、関連付けられているオブジェクト タイプやイベントの重大度などの情報が提供されます。イベントのグローバルな無効化 / 有効化などのタスクを実行することもできます。

このページにアクセスできるのは、アプリケーション管理者ロールまたはストレージ管理者ロールが割り当てられている場合のみです。

コマンド ボタン

選択したイベントについて、各コマンド ボタンを使用して次のタスクを実行できます。

- 無効

[イベントの無効化]ダイアログ ボックスを起動します。イベントを無効にする場合に使用できます。

- 有効にする

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。

- アップロードルール

[ルールをアップロード]ダイアログ ボックスを起動します。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する場合に使用できます。ルールはクラスターの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、ケーブル接続、ベスト プラクティス、および可用性に関するイベントを生成します。

- **EMS**イベントに登録する

[EMS イベントにサブスクライブ]ダイアログ ボックスを起動します。監視しているクラスタから特定の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できます。EMSでは、クラスタで発生したイベントに関する情報を収集します。サブスクライブされた EMS イベントの通知を受信すると、適切な重大度で 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

生成されるイベントのソース タイプが表示されます。

[イベントの無効化]ダイアログ ボックス

[イベントの無効化]ダイアログ ボックスには、イベントを無効にできるイベント タイプのリストが表示されます。イベント タイプの特定の重大度のイベントを無効にするか、一連のイベントを指定して無効にできます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

[イベント プロパティ]領域

[イベント プロパティ]領域で、イベントについて次の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 (重大、エラー、警告、情報) に基づいてイベントを選択できます。

- イベント名に含まれるもの

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。

- マッチングイベント

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。

アラートを管理する

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

イベントは継続的に発生しますが、Unified Manager は、イベントが指定されたフィルタ条件を満たした場合にのみ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ときや、オブジェクトがオフラインになったときなど）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、UIでイベントの詳細ページを確認できるように、各イベントのハイパーリンクもEメール メッセージ内に記載されています。

アラートEメールは、アラートを受信するように登録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 カウンタや容量の値が収集期間内に大きく変わった場合、同じしきい値ポリシーに対して重大イベントと警告イベントの両方が同時にトリガーされることがあります。この場合、警告イベントのEメールと重大イベントのEメールを1通ずつ受信する可能性があります。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信するように個別に登録できるためです。

アラートEメールの例を次に示します。

```
From: 10.11.12.13@company.com|
Sent: Tuesday, May 1, 2018 7:45 PM
To: 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
```

アラートを追加する

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。

開始する前に

- イベントが生成されたときに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。

アラートは、ここで説明する手順に従って[アラート セットアップ]ページで作成できるほか、イベントを受け取ったあとに[イベントの詳細]ページで直接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、ストレージ管理 > アラート設定 をクリックします。
2. *アラート設定*ページで、*追加*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、アラートの名前と説明を入力します。
4. *リソース*をクリックし、アラートに含めるまたはアラートから除外するリソースを選択します。

*名前に含まれる*フィールドにテキスト文字列を指定してフィルターを設定し、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利用可能なリソースのリストに表示されます。テキスト文字列の指定では、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. *イベント*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. アクション をクリックし、通知するユーザーを選択し、通知頻度を選択し、トラップ受信者に SNMP トラップを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。



該当するユーザのEメール アドレスを変更し、その後アラートを編集するために開くと、[名前]フィールドは空欄になります。これは、Eメールが変更されたことでユーザとのマッピングが無効になったためです。また、選択したユーザのEメール アドレスを[ユーザ]ページで変更した場合、変更後のEメール アドレスは反映されません。

SNMPトラップを使用してユーザに通知することもできます。

7. *保存*をクリックします。

アラートの追加例

ここでは、次の要件を満たすアラートを作成する例を示します。

- 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含め、名前に「xyz」を含むすべてのボリュームを対象から除外する
- イベント：健全性に関するすべての重大なイベントを対象に含める
- 処理：「Test」スクリプトを割り当て、「sample@domain.com」のユーザに15分ごとに通知する

[Add Alert]ダイアログ ボックスで、次の手順を実行します。

1. 名前*をクリックして入力してくださいHealthTest*アラート名*フィールドに*を入力します。
2. *リソース*をクリックし、含めるタブでドロップダウンリストから*ボリューム*を選択します。

- a. 入力*abc*「名前を含む」フィールドに*と入力すると、名前に「abc」が含まれるボリュームが表示されます。
 - b. を選択<<All Volumes whose name contains 'abc'>> を [使用可能なリソース] 領域から選択し、[選択したリソース] 領域に移動します。
 - c. 除外*をクリックして入力してくださいxyz*「名前に含まれる」フィールドに入力し、「追加」をクリックします。
3. *イベント*をクリックし、イベントの重大度フィールドから*重大*を選択します。
 4. [一致するイベント] 領域から すべての重要なイベント を選択し、[選択したイベント] 領域に移動します。
 5. アクション*をクリックして入力しますsample@domain.com* [これらのユーザーに警告] フィールドに入力します。
 6. ユーザーに 15 分ごとに通知するには、[15 分ごとに通知] 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*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、ノード、アグリゲート、ボリュームなど）とイベントの重大度に基づいて追加することができます。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

アラートを効率的に追跡できるように、わかりやすい説明を入力します。

- 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。リソースは必要に応じて追加したり除外したりできます。たとえば、アラートを設定してアグリゲートを詳細に監視する場合は、リソースのリストから必要なアグリゲートを選択する必要があります。

たとえば、リソースのカテゴリを選択した場合、+[All User or Group Quotas] + の場合、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を受信します。



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を対象とするアラートを作成した場合、受信するアラートの対象はクラスタの重大イベントのみです。ノードやアグリゲートなどの重大イベントに対するアラートは受信しません。

- イベントの重大度

イベントの重大度（重大、エラー、警告）ごとにアラートをトリガーするかどうかを決めて、アラートをトリガーする重大度を指定する必要があります。

- 選択したイベント

生成されるイベントのタイプに基づいてアラートを追加する場合は、アラートが必要なイベントを決める必要があります。

イベントの重大度を選択し、かつ個々のイベントを選択しなかった場合（[選択したイベント]列を空白にした場合）は、カテゴリのすべてのイベントに関するアラートが表示されます。

- アクション

通知を受信するユーザのユーザ名とEメール アドレスを指定する必要があります。通知のモードとしてSNMPトラップを指定することもできます。アラートが生成されたときに実行されるように、アラートにスクリプトを関連付けることができます。

- 通知の頻度

指定した期間、受信者に繰り返し通知を送信するようにアラートを設定できます。アラートに対してイベント通知をアクティブにする時間を決める必要があります。イベントが確認されるまでイベント通知を再送する場合は、通知を再送する頻度を決める必要があります。

- スクリプトを実行

アラートにスクリプトを関連付けることができます。スクリプトはアラートが生成されると実行されます。

パフォーマンスイベントのアラートを追加する

パフォーマンス イベントのアラートは、Unified Managerで受信する他のイベントと同様に、イベントごとに個別に設定することができます。また、すべてのパフォーマンス イベントを同じように扱い、同じユーザにEメールを送信する場合は、重大または警告のパフォーマンス イベントがトリガーされたときに通知する共通のアラートを作成することもできます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

ここでは、レイテンシ、IOPS、およびMBpsのすべての重大イベントに対するアラートを作成する例を示します。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て、すべての警告イベントに対する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、ストレージ管理 > アラート設定 をクリックします。
2. *アラート設定*ページで、*追加*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、アラートの名前と説明を入力します。
4. リソース ページでリソースを選択しないでください。

リソースを選択していないため、クラスタ、アグリゲート、ボリュームなど、何に対するイベントを受信したかに関係なく、すべてのリソースにアラートが適用されるようになります。

5. *イベント*をクリックし、次のアクションを実行します。
 - a. イベントの重大度リストで、「重大」を選択します。
 - b. イベント名に含まれるフィールドに、*latency* 次に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. イベント名に含まれるフィールドに、*iops* 次に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. イベント名に含まれるフィールドに、*mbps* 次に矢印をクリックして、一致するすべてのイベントを選択します。
6. *アクション*をクリックし、*これらのユーザーに警告*フィールドで警告メールを受信するユーザーの名前を選択します。
7. SNMPトラップの発行やスクリプトの実行など、このページの他のオプションを設定します。
8. *保存*をクリックします。

アラートのテスト

アラートをテストして、アラートが正しく設定されていることを確認できます。イベントがトリガーされるとアラートが生成され、設定した受信者にアラートEメールが送信されます。テスト アラートを使用して、通知が送信されるかどうか、およびスクリプトが実行されるかどうかを確認できます。

開始する前に

- 通知の設定（受信者のEメール アドレス、SMTPサーバ、SNMPトラップなど）を実行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、ストレージ管理 > アラート設定 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。

解決済みおよび廃止されたイベントのアラートを有効または無効にする

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（新規、確認済み、解決済み、廃止）が変わるたびにアラート メッセージが送信されます。イベントが解決済み / 廃止状態に移行したときにアラートを受信したくない場合は、ア

ラートを抑制するようグローバルに設定できます。

開始する前に

アプリケーショ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、ストレージ管理 > アラート設定 をクリックします。
2. *アラート設定*ページで、*解決済みおよび廃止されたイベントのアラート*項目の横にあるスライダー コントロールを使用して、次のいずれかのアクションを実行します。

目的	操作
イベントが解決済みまたは廃止状態に移行したときのアラートの送信を停止する	スライダを左に移動する
イベントが解決済みまたは廃止状態に移行したときのアラートの送信を開始する	スライダを右に移動する

災害復旧の宛先ボリュームをアラート生成から除外する

ボリュームのアラートを設定するときは、[アラート]ダイアログ ボックスで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。

開始する前に

アプリケーショ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_name>:/<volume_name>" の形式で SVM 名とボリューム名の両方が含まれているために可能になります。

ここでは、プライマリSVM「vs1」にあるボリューム「vol1」に対するアラートを作成し、SVM「vs1-dr」にある同じ名前のボリュームはアラート生成の対象から除外する例を示します。

[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、アラートの名前と説明を入力します。
2. *リソース*をクリックし、*含める*タブを選択します。
 - a. ドロップダウンリストから*ボリューム*を選択し、入力します*vol1*「名前を含む」フィールドに * と入力すると、名前に「vol1」が含まれるボリュームが表示されます。

- b. を選択<<All Volumes whose name contains 'vol1'>> [利用可能なリソース] 領域から [選択したリソース] 領域に移動します。
3. 除外*タブを選択し、*ボリューム*を選択して入力しますvs1-dr*「名前に含まれる」フィールドに入力し、「追加」をクリックします。

これにより、SVM「vs1-dr」にあるボリューム「vol1」がアラートの生成対象から除外されます。
4. イベント をクリックし、ボリュームに適用するイベントを 1 つまたは複数選択します。
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. このページで、SNMP トラップの発行とスクリプトの実行に関するその他のオプションを設定し、[保存] をクリックします。

アラートを表示

さまざまなイベントに対して作成されるアラートのリストを[アラート セットアップ]ページから表示できます。また、アラートのプロパティを表示することもできます。このプロパティには、アラートの説明、通知方式と通知頻度、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（例：クラスタ、アグリゲート、ボリューム）などがあります。

開始する前に

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、ストレージ管理 > アラート設定 をクリックします。

[アラート セットアップ]ページにアラートのリストが表示されます。

アラートを編集する

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。

開始する前に

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、ストレージ管理 > アラート設定 をクリックします。
2. *アラート設定*ページで、編集するアラートを選択し、*編集*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、必要に応じて名前、リソース、イベント、アクションのセクションを編集します。

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*をクリックします。

アラートを削除する

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、そのリソースについて作成されたアラートを削除できます。

開始する前に

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、ストレージ管理 > アラート設定 をクリックします。
2. *アラート設定*ページで、削除するアラートを選択し、*削除*をクリックします。
3. 削除要求を確認するには、[はい] をクリックします。

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ようにアラートを設定します。アラートのリストは、[アラート セットアップ]ページで確認できます。

アラート設定ページ

[アラート セットアップ]ページには、アラートのリストおよびアラート名、ステータス、通知方式、通知頻度に関する情報が表示されます。また、このページでアラートを追加、編集、削除、有効化、無効化することもできます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

コマンド ボタン

- 追加

[アラートの追加]ダイアログ ボックスが表示され、新しいアラートを追加できます。

- 編集

[アラートの編集]ダイアログ ボックスが表示され、選択したアラートを編集できます。

- 消去

選択したアラートを削除します。

- 有効にする

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。

- 解決済みおよび廃止されたイベントに関するアラート

イベントが解決済みまたは廃止状態に移行した場合のアラートの送信を有効または無効にすることができます。これにより、ユーザは不要な通知を受信せずに済みます。

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しい情報を詳細領域に表示することもできます。

- 状態

アラートが有効かどうかを指定します () または無効 ()。

- 警告

アラートの名前が表示されます。

- 説明

アラートの説明が表示されます。

- 通知方法

アラート用に選択した通知方式が表示されます。EメールまたはSNMPトラップを使用してユーザに通知できます。

- 通知頻度

イベントが確認または解決されるか、廃止状態に設定されるまでの間、管理サーバが通知を送信する頻度（分）を示します。

詳細領域

詳細領域には、選択したアラートに関する詳細情報が表示されます。

- アラート名

アラートの名前が表示されます。

- アラートの説明

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。

- 含まれるもの

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際に実行されます。

- 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。

[アラートの追加]ダイアログ ボックス

アラートを作成すると、特定のイベントが生成されたときに通知されるため、問題に迅速に対処し、環境に対する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。

Name

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。

- アラートの説明

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対象のリソースを選択できます。リソースは個別に選択できるほか、動的ルールに基づいてグループ化することも可能です。動的ルールは、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。

- 含む

アラートをトリガーする対象に含めるリソースを指定できます。テキスト文字列を指定すると、その文字列に一致するリソースをグループ化し、そのグループをアラートの対象として選択することができます。たとえば、「abc」という文字列が名前に含まれるすべてのボリュームをグループ化できます。

- 除外

アラートをトリガーする対象から除外するリソースを指定できます。たとえば、「xyz」と指定して、この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を選択した場合にのみ表示されます。例: <<All Volumes>>または<<All Volumes whose name contains 'xyz'>>。

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

イベント

この領域では、アラートを作成するイベントを選択できます。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」、または「警告」のいずれかになります。

- イベント名に含まれるもの

指定した文字が名前に含まれる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場合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。

該当するユーザのEメール アドレスを変更し、その後アラートを編集するために開くと、[名前]フィールド

ドは空欄になります。これは、Eメールが変更されたことでユーザとのマッピングが無効になったためです。また、選択したユーザのEメール アドレスを[ユーザ]ページで変更している場合、変更後のEメール アドレスは反映されません。

- 通知頻度

イベントが確認または解決されるか、廃止状態に設定されるまでの間、管理サーバが通知を送信する頻度を指定できます。

次のいずれかの通知方式を選択できます。

- 1回だけ通知する。
- 指定の頻度で通知する。
- 指定の期間に指定の頻度で通知する。

- **SNMP**トラップを発行

このチェック ボックスをオンにすると、グローバルに設定されたSNMPホストにSNMPトラップを送信するかどうかを指定できます。

- スクリプトを実行

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際に実行されます。



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。必要に応じて、ストレージ管理 > 機能設定 からこの機能を有効にできます。

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。

[アラートの編集]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。

Name

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。

- アラートの説明

アラートの説明を指定できます。

- 警戒状態

アラートを有効または無効にできます。

リソース

この領域では、アラートをトリガーする対象のリソースを選択できます。リソースは個別に選択できるほか、動的ルールに基づいてグループ化することも可能です。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。

- 含む

アラートをトリガーする対象に含めるリソースを指定できます。テキスト文字列を指定すると、その文字列に一致するリソースをグループ化し、そのグループをアラートの対象として選択することができます。たとえば、名前に「vol10」という文字列が含まれるすべてのボリュームをグループ化できます。

- 除外

アラートをトリガーする対象から除外するリソースを指定できます。たとえば、名前に「xyz」という文字列が含まれる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を選択した場合にのみ表示されます（例：+[\[All Volumes\]](#) + または +[\[All Volumes whose name contains 'xyz'\]](#) +）。

イベント

この領域では、アラートをトリガーするイベントを選択できます。アラートは特定の重大度のイベントに対してトリガーするか、一連のイベントを指定してトリガーできます。

- イベントの重大度

重大度タイプに基づいてイベントを選択できます。タイプは、「重大」、「エラー」、または「警告」のいずれかになります。

- イベント名に含まれるもの

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

通知の受信者のEメール アドレスまたはユーザ名を編集できます。新しいEメール アドレスまたはユーザ名を指定することもできます。

- 通知頻度

管理サーバからの通知の送信頻度を編集できます。イベントが確認されるか、解決されるか、廃止状態になるまで、この頻度で通知が送信されます。

次のいずれかの通知方式を選択できます。

- 1回だけ通知する。
- 指定の頻度で通知する。
- 指定の期間に指定の頻度で通知する。

- **SNMP**トラップを発行

グローバル設定の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。

- スクリプトを実行

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際に実行されます。

コマンド ボタン

- 保存

変更内容を保存してダイアログ ボックスを閉じます。

- キャンセル

変更内容を破棄してダイアログ ボックスを閉じます。

スクリプトを管理する

スクリプトを使用して、Unified Manager 内の複数のストレージ 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。イベントでアラートがトリガーされるとスクリプトが実行されます。カスタム スクリプトをアップロードし、アラートが生成されたときの動作をテストできます。

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により組織がこの機能を許可したくない場合は、ストレージ管理 > 機能設定 からこの機能を無効にすることができます。

関連情報

["スクリプト アップロード機能の有効化 / 無効化"](#)

スクリプトとアラートの連携方法

Unified Managerでイベントに対するアラートが発生したときにスクリプトが実行されるように、アラートにスクリプトを関連付けることができます。スクリプトを使用して、

ストレージ オブジェクトの問題を解決したり、イベントの生成元のストレージ オブジェクトを特定したりできます。

Unified Manager でイベントのアラートが生成されると、指定された受信者にアラート メールが送信されます。アラートをスクリプトに関連付けた場合は、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のEメールで確認できます。



カスタム スクリプトを作成し、それを特定のイベント 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アクションが実行され、修正 アクションは [管理アクション] ページまたは Unified Manager ダッシュボードでデフォルトでは使用できなくなります。

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、関連するイベントの情報を収集したり、ストレージ オブジェクトを変更したりできます。

スクリプトから引数を取得する例

```
`print "$ARGV[0] : $ARGV[1]\n"`  
`print "$ARGV[7] : $ARGV[8]\n"`
```

アラートが生成されると、このスクリプトが実行されて次のような出力が表示されます。

```
-`eventID : 290`  
-`eventSourceID : 4138`
```

スクリプトを追加する

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。

開始する前に

- 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ているファイル形式は、Perl、Shell、PowerShell、Python、および`.bat`ファイル。

Unified Managerがインストールされているプラットフォーム	サポートされる言語
VMware	Perl / シェル スクリプト
Linux	Perl / Python / シェル スクリプト
Windows	PowerShell / Perl / Python / .batスクリプト

- Perl スクリプトの場合、Unified Manager サーバーに Perl がインストールされている必要があります。VMware環境にはPerl 5がデフォルトでインストールされ、Perl 5のサポート対象のみがスクリプトでサポートされます。Unified ManagerのあとにPerlをインストールした場合は、Unified Managerサーバを再起動する必要があります。
- PowerShellスクリプトを使用するには、スクリプトを実行するための適切なPowerShell実行ポリシーがWindowsサーバで設定されている必要があります。



スクリプトでログ ファイルを作成してアラート スクリプトの進捗を追跡する場合は、ログ ファイルがUnified Managerのインストール フォルダ内に作成されないようにする必要があります。

- アプリケーション管理者またはストレージ管理者のロールが必要です。

カスタム スクリプトをアップロードし、アラートに関するイベントの詳細を収集できます。



この機能がユーザ インターフェイスに表示されない場合は、管理者によって無効にされています。必要に応じて、ストレージ管理 > 機能設定 からこの機能を有効にできます。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > スクリプト 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 / 無効化"](#)

スクリプトを削除する

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。

開始する前に

- アプリケーショ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、ストレージ管理 > スクリプト 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。

テストスクリプトの実行

ストレージ オブジェクトに対してアラートが生成されたときにスクリプトが正しく実行されるかどうかを確認することができます。

開始する前に

- アプリケーショ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、ストレージ管理 > スクリプト をクリックします。
2. *スクリプト*ページで、テスト スクリプトを追加します。
3. 左側のナビゲーション ペインで、ストレージ管理 > アラート設定 をクリックします。
4. *アラート設定*ページで、次のいずれかのアクションを実行します。

目的	操作
アラートを追加する	a. *[追加]*をクリックします。 b. [操作]セクションで、テスト スクリプトにアラートを関連付けます。
アラートを編集する	a. アラートを選択し、[編集] をクリックします。 b. [操作]セクションで、テスト スクリプトにアラートを関連付けます。

5. *保存*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

ム、qtree、LUNなどのストレージ オブジェクトに対するクエリを実行することができます。CLI コマンドを使用して、Unified Manager 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、処理の開始時や終了時に実行されるスクリプト、アラートがトリガーされたときに実行されるスクリプトでも使用できます。

すべてのコマンドはコマンドの前に置かなければなりません `um cli login` 認証には有効なユーザー名とパスワードが必要です。



um run コマンドを実行するには、アカウントに *console* アプリケーション アクセス権があることを確認してください。

CLIコマンド	説明	出力
<code>um cli login -u <username> [-p <password>]</code>	CLIにログインします。セキュリティ上の理由から、「-u」オプションのあとにはユーザ名のみを入力してください。こうすることでパスワードの入力を求めるプロンプトが表示され、パスワードが履歴またはプロセス テーブルに記録されることはありません。セッションの有効期限はログインしてから3時間で、3時間を過ぎると再ログインが必要になります。	対応するメッセージが表示されます。
<code>um cli logout</code>	CLIからログアウトします。	対応するメッセージが表示されます。
<code>um help</code>	第1レベルのすべてのサブコマンドを表示します。	第1レベルのすべてのサブコマンドを表示します。
<code>um run cmd [-t <timeout>] <cluster> <command></code>	1つまたは複数のホストでコマンドを実行する最も簡単な方法です。主にアラートのスクリプティングでONTAPの処理を取得または実行するために使用します。オプションのtimeout引数で、コマンドがクライアントで完了するのを待機する最大時間（秒）を設定できます。デフォルトは0（無期限に待機）です。	ONTAPから受け取った情報がそのまま表示されます。
<code>um run query <sql command></code>	SQLクエリを実行します。実行できるクエリはデータベースからの読み取りだけです。更新、挿入、削除の各操作はサポートされません。	結果は表形式で表示されます。返される結果が空になる場合、構文エラーがある場合、または要求が無効な場合は、該当するエラー メッセージが表示されます。

CLIコマンド	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際は、-u（ユーザ名）オプションと-P（パスワード）オプションを必ず指定する必要があります。オプションの-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。オプションの-p（ポート）では、クラスタとの通信に使用するポートを指定します。ポートが指定されていない場合は、該当するプロトコルのデフォルト値が試行されます。このコマンドは、ストレージ管理者のみが実行できます。	ユーザに証明書の承認を求め、対応するメッセージを表示します。
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。	次の値を表形式で表示します。 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つまたは複数のデータソース 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が表示されます。
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が表示されます。
um option list [<option> ..]	setコマンドを使用して設定できるすべてのオプションのリストを表示します。	次の値を表形式で表示します。 Name, Value, Default Value, and Requires Restart.

CLIコマンド	説明	出力
<code>um option set <option-name>=<option-value> [<option-name>=<option-value> ...]</code>	1つまたは複数のオプションを設定します。このコマンドは、ストレージ管理者のみが実行できます。	対応するメッセージが表示されます。
<code>um version</code>	Unified Managerソフトウェアのバージョンを表示します。	Version ("9.6")
<code>um lun list [-q] [-ObjectType <object-id>]</code>	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はヘッダーを非表示にするオプションで、すべてのコマンドで使用できます。ObjectTypeには、lun、qtree、cluster、volume、quota、svmのいずれかを指定できます。 例えば： um lun list -cluster 1 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。	次の値を表形式で表示します。ID and LUN path.
<code>um svm list [-q] [-ObjectType <object-id>]</code>	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。 例えば： um svm list -cluster 1 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。	次の値を表形式で表示します。Name and Cluster ID.

CLIコマンド	説明	出力
um qtree list [-q] [-ObjectType <object-id>]	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はヘッダーを非表示にするオプションで、すべてのコマンドで使用できます。ObjectTypeには、lun、qtree、cluster、volume、quota、svmのいずれかを指定できます。 例えば： um qtree list -cluster 1 この例では、objectTypeが「-cluster」で、objectIdが「1」です。このコマンドを実行すると、IDが1のクラスタに含まれるすべてのqtreeのリストが表示されます。	次の値を表形式で表示します。 Qtree ID and Qtree Name.
um disk list [-q] [-ObjectType <object-id>]	指定したオブジェクトでフィルタリングしたディスクのリストを表示します。ObjectTypeには、disk、aggr、node、clusterのいずれかを指定できます。 例えば： um disk list -cluster 1 この例では、objectTypeが「-cluster」で、objectIdが「1」です。このコマンドを実行すると、IDが1のクラスタに含まれるすべてのディスクのリストが表示されます。	次の値を表形式で表示します ObjectType and object-id.

CLIコマンド	説明	出力
um cluster list [-q] [-ObjectType <object-id>]	指定したオブジェクトでフィルタリングしたクラスタのリストを表示します。ObjectTypeには、disk、aggr、node、cluster、lun、qtree、volume、quota、svmのいずれかを指定できます。 例えば： um cluster list -aggr 1 この例では、objectTypeが「-aggr」で、objectIdが「1」です。このコマンドを実行すると、IDが1のアグリゲートが属しているクラスタが表示されます。	次の値を表形式で表示します。Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key。
um cluster node list [-q] [-ObjectType <object-id>]	指定したオブジェクトでフィルタリングしたクラスタ ノードのリストを表示します。ObjectTypeには、disk、aggr、node、clusterのいずれかを指定できます。 例えば： um cluster node list -cluster 1 この例では、objectTypeが「-cluster」で、objectIdが「1」です。このコマンドを実行すると、IDが1のクラスタに含まれるすべてのノードのリストが表示されます。	次の値を表形式で表示します Name and Cluster ID。

CLIコマンド	説明	出力
um volume list [-q] [-ObjectType <object-id>]	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。 例えば： <pre>um volume list -cluster 1</pre> 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。	次の値を表形式で表示します Volume ID and Volume Name。
um quota user list [-q] [-ObjectType <object-id>]	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。 例えば： <pre>um quota user list -cluster 1</pre> 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。	次の値を表形式で表示します ID, Name, SID and Email。

CLIコマンド	説明	出力
<code>um aggr list [-q] [-ObjectType <object-id>]</code>	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。 例えば： um aggr list -cluster 1 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。	次の値を表形式で表示します Aggr ID, and Aggr Name。
<code>um event ack <event-ids></code>	1つまたは複数のイベントに応答します。	対応するメッセージが表示されます。
<code>um event resolve <event-ids></code>	1つまたは複数のイベントを解決します。	対応するメッセージが表示されます。
<code>um event assign -u <username> <event-id></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が表示されます。
<code>um event list [-s <source>] [-S <event-state-filter-list>..] [<event-id> ..]</code>	システムまたはユーザによって生成されたイベントのリストを表示します。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できます。	次の値を表形式で表示します Source, Source type, Name, Severity, State, User and Timestamp。
<code>um backup restore -f <backup_file_path_and_name></code>		対応するメッセージが表示されます。

スクリプトのウィンドウとダイアログ ボックスの説明

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

スクリプトページ

[スクリプト]ページでは、Unified Managerにカスタム スクリプトを追加できます。追加したスクリプトをアラートに関連付けると、ストレージ オブジェクトが自動的に再設定されます。

[スクリプト]ページでは、Unified Managerに対してスクリプトを追加または削除できます。

コマンド ボタン

- 追加

[スクリプトの追加]ダイアログ ボックスが開き、スクリプトを追加できます。

- 消去

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。

- 説明

スクリプトの説明が表示されます。

[スクリプトの追加]ダイアログ ボックス

[スクリプトの追加]ダイアログ ボックスで、Unified Managerにスクリプトを追加できます。スクリプトを使用して、ストレージ オブジェクトに対して生成されたイベントを自動的に解決するようにアラートを設定することができます。

アプリケーション管理者またはストレージ管理者のロールが必要です。

- スクリプトファイルを選択

アラートに使用するスクリプトを選択できます。

- 説明

スクリプトの説明を指定できます。

クラスタ パフォーマンスの監視と管理

Active IQ Unified Managerによるパフォーマンス監視の概要

Active IQ Unified Manager（旧OnCommand Unified Manager）は、NetApp ONTAPソフトウェアを実行するシステムを対象に、パフォーマンス監視機能とパフォーマンス イベントの根本原因分析機能を提供します。

Unified Manager は、クラスタ コンポーネントを過剰に使用し、クラスタ上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するのに役立ちます。パフォーマンスしきい値ポリシーを定義して特定のパフォーマンス カウンタの最大値を指定し、しきい値を超えた場合にイベントが生成されるようにすることも可能です。Unified Manager は、これらのパフォーマンス イベントについて警告を発し、修正アクションを実行してパフォーマンスを通常の操作レベルに戻すことができるようにします。Unified Manager UI でイベントを表示および分析できます。

Unified Manager は、次の 2 種類のワークロードのパフォーマンスを監視します。

- ユーザ定義のワークロード

このワークロードは、クラスタに作成したFlexVolとFlexGroupボリュームで構成されます。

- システム定義のワークロード

このワークロードは、内部のシステム アクティビティで構成されます。

Unified Managerのパフォーマンス監視機能

Unified Manager は、ONTAPソフトウェアを実行しているシステムからパフォーマンス統計を収集して分析します。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。

長い応答時間（レイテンシ）は、ストレージ オブジェクト（ボリュームなど）の実行速度が通常よりも遅いことを示しています。また、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ます。Unified Manager は、パフォーマンスの問題が発生するストレージ コンポーネントを識別し、パフォーマンスの問題に対処するために実行できる推奨アクションのリストを提供します。

Unified Manager には次の機能が含まれています。

- ONTAPソフトウェアを実行しているシステムからワークロードのパフォーマンス統計を監視して分析します。
- クラスタ、ノード、アグリゲート、ポート、SVM、ボリューム、LUN、NVMe 名前空間、およびネットワーク インターフェイス (LIF) のパフォーマンス カウンターを追跡します。
- IOPS（処理数）、MBps（スループット）、レイテンシ（応答時間）、利用率、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を時系列で示す詳細なグラフを表示します。
- しきい値を超えた場合にイベントをトリガーしてEメール アラートを送信する、ユーザ定義のパフォーマンスのしきい値ポリシーを作成できます。

- システム定義のしきい値とワークロードのアクティビティを学習する動的なパフォーマンスしきい値を使用して、パフォーマンスの問題を特定してアラートを送信します。
- ボリュームおよびLUNに適用されるサービス品質（QoS）ポリシーとパフォーマンス サービス レベル ポリシー（PSL）を特定します。
- 競合状態のクラスタ コンポーネントを特定します。
- クラスタ コンポーネントを過剰に使用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るワークロードを識別します。

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**のインターフェイス

ここでは、Active IQ Unified Managerでデータ ストレージの容量、可用性、保護に関する問題をトラブルシューティングするための2種類のユーザ インターフェイスについて説明します。2 つの UI 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）を併せてインストールし、設定する必要があります。

Unified Manager Web UI

Unified Manager Web UI を使用すると、管理者はデータ ストレージの容量、可用性、および保護に関連するクラスタの問題を監視およびトラブルシューティングできます。

以降のセクションで、管理者がUnified Manager Web UIに表示されるストレージ容量、データの可用性、または保護に関する問題をトラブルシューティングする際に従う共通のワークフローについて説明します。

メンテナンス コンソール

Unified Manager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 が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形式となります。

この情報は、メンテナンス コンソールにアクセスしてUnified Managerサーバの機能に関連する問題を解決するのに役立ちます。

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

クラスタ構成データの収集間隔は 15 分です。たとえば、クラスタを追加した後、Unified Manager UI にクラスタの詳細が表示されるまでに 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すると、次のポーリング間隔（最大 15 分）後にそれらの新しいオブジェクトが UI に表示されます。

Unified Manager は、監視対象のすべてのクラスタから 5 分ごとに現在のパフォーマンス統計を収集します。そのデータを分析することでパフォーマンス イベントや潜在的な問題を特定します。5 分間の履歴パフォーマンス データが 30 日間、1 時間のパフォーマンス データが 180 日間保持されます。これにより、過去1カ月間の非常にきめ細かなパフォーマンスの詳細と最大1年間のパフォーマンスの傾向を確認することができ

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。

次の表は、Unified Manager が実行する収集アクティビティを示しています。

アクティビティ	時間間隔	説明
パフォーマンス統計のポーリング	5分ごと	各クラスタからリアルタイムのパフォーマンス データを収集します。
統計分析	5分ごと	すべての統計ポーリングの後に、Unified Manager は収集されたデータをユーザー定義、システム定義、および動的しきい値と比較します。 パフォーマンスしきい値を超えた場合、Unified Manager はイベントを生成し、設定されている場合は指定されたユーザーに電子メールを送信します。
構成のポーリング	15分ごと	各クラスターから詳細なインベントリ情報を収集し、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) を識別します。
集計	1時間ごと	5分ごとに収集した最新の12回分のパフォーマンス データを集計して1時間の平均を求めます。 1 時間ごとの平均値は一部の UI 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時から	クラスタのデータを分析し、次の24時間のボリュームのレイテンシとIOPSの動的なしきい値を設定します。 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。
データの削除	毎日午前2時から	180 日以上経過したイベントと180 日以上経過した動的しきい値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	説明
データの削除	毎日午前3時30分以降	180 日より古い 1 時間のパフォーマンス 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。データ継続性収集により、Unified Manager はリアルタイム データを収集できなかった場合に発生する統計データのギャップを埋めることができます。

Unified Manager は、次のイベントが発生すると、履歴パフォーマンス データのデータ継続性収集ポーリングを実行します。

- 最初にクラスタが Unified Manager に追加されます。

Unified Manager は、過去 15 日間の履歴パフォーマンス データを収集します。これにより、クラスタが追加されてから数時間で2週間分の履歴パフォーマンス情報を表示できます。

さらに、該当する期間にシステム定義のしきい値のイベントが発生していた場合はそれらのイベントも報告されます。

- 現在のパフォーマンス データ収集サイクルが所定の時間に完了しなかったとき。

リアルタイムのパフォーマンスのポーリングが5分間の収集期間内に完了しなかった場合、データの継続性収集サイクルが開始され、収集されなかった期間の情報が収集されます。データの継続性収集が実行されなかった場合、次の収集期間がスキップされます。

- Unified Manager は、次の状況のように、一定期間アクセス不能になった後、オンラインに戻ります。
 - Unified Managerが再起動された。
 - ソフトウェアのアップグレードやバックアップ ファイルの作成のためにUnified Managerがシャットダウンされた。
 - ネットワーク停止から復旧した。
- 次の状況により、クラスタに一時的にアクセスできなくなり、そのあとオンラインに戻ったとき。
 - ネットワーク停止から復旧した。
 - 低速なワイド エリア ネットワーク接続により、通常のパフォーマンス データの収集に遅延が生じた。

データの継続性収集サイクルは、最大24時間の履歴データを収集できます。Unified Manager が 24 時間以上ダウンすると、UI ページにパフォーマンス データのギャップが表示されます。

データの継続性収集サイクルとリアルタイムのデータ収集サイクルを同時に実行することはできません。データの継続性収集サイクルが完了してからでないと、リアルタイムのパフォーマンス データ収集は開始されません。1 時間を超える履歴データを収集するためにデータ継続性収集が必要な場合は、[通知] ペインの上部にそのクラスターのバナー 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

収集された健全性やパフォーマンスのデータに表示されるタイムスタンプ（イベントの検出時刻のタイムスタンプ）は、ONTAPクラスタの時刻に基づいており、Webブラウザで設定されているタイムゾーンに応じて調整されます。

Unified Manager サーバ、ONTAPクラスタ、および Web ブラウザの時刻を同期するには、Network Time Protocol (NTP) サーバを使用することを強くお勧めします。



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 GUIでパフォーマンスワークフローをナビゲートする

Unified Manager インターフェイスには、パフォーマンス情報の収集と表示のためのページが多数用意されています。左側のナビゲーション パネルを使用して各ページに移動し、ページ上のタブやリンクを使用して情報を表示、設定します。

クラスタのパフォーマンス情報を監視し、トラブルシューティングを行うには、以下のすべてのページを使います。

- ダッシュボード ページ
- ストレージおよびネットワーク オブジェクトのインベントリ ページ
- ストレージ オブジェクトの詳細ページ（パフォーマンス エクスプローラを含む）
- 構成および設定ページ
- イベント ページ

UIにログインする

Unified ManagerのUIには、サポートされているWebブラウザからログインできます。

開始する前に

- Webブラウザが最小要件を満たしている必要があります。

相互運用性マトリックスについては、"mysupport.netapp.com/matrix"サポートされているブラウザバージョンの完全なリストについては、こちらをご覧ください。

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

1時間何も操作を行わないと、セッションから自動的にログアウトされます。この期間は、「一般」>「機能設定」で設定できます。

手順

1. Webブラウザに、下記の形式でURLを入力します。URLは、Unified ManagerサーバのIPアドレスまたは完全修飾ドメイン名（FQDN）です。

- IPv4の場合: `https://URL/`
- IPv6の場合: `https://[URL]/`

自己署名のデジタル証明書がサーバで使用されている場合、信頼されていない証明書であることを伝える警告がブラウザ画面に表示されることがあります。その場合は、危険を承諾してアクセスを続行するか、認証局（CA）の署名のあるデジタル証明書をインストールしてサーバを認証します。。ログイン画面で、ユーザ名とパスワードを入力します。

Unified Managerのユーザ インターフェイスへのログインがSAML認証で保護されている場合は、Unified Managerのログイン ページではなくアイデンティティ プロバイダ（IdP）のログイン ページでクレデンシャルを入力します。

[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。これら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 は非常に柔軟性が高く、さまざまな方法で複数のタスクを実行できます。Unified Manager で作業すると、さまざまなナビゲーション パスが見つかります。使用できる操作手順をすべて紹介することは不可能なので、ここでは代表的な操作手順をいくつか紹介します。

クラスタ オブジェクト監視時の操作

Unified Managerで管理しているクラスタ内のすべてのオブジェクトのパフォーマンスを監視できます。ストレージ オブジェクトの監視では、クラスタとオブジェクトのパフォーマンスの概要を確認し、パフォーマンス イベントを監視します。パフォーマンスとイベントの総合的な情報を表示することも、オブジェクトのパフォーマンスとパフォーマンス イベントの詳しいデータを表示して調査することもできます。

次に、クラスタ オブジェクトを監視する際の操作例を紹介します。

1. [ダッシュボード]ページで、[パフォーマンス容量]パネルの詳細を確認して使用済みパフォーマンス容量が最も多いクラスタを特定し、棒グラフをクリックしてそのクラスタのノードのリストに移動します。
2. 使用済みパフォーマンス容量の値が最も高いノードを特定し、そのノードをクリックします。
3. ノード / パフォーマンス エクスプローラー ページで、[表示と比較] メニューから このノードの集計 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 エクスプローラー」 ページで、「表示と比較」メニューから このアグリゲートのボリューム をクリックします。
6. IOPSが最も高いボリュームを特定します。

特定したボリュームを調べて、QoSポリシーまたはパフォーマンス サービス レベル ポリシーを適用するかどうかを判断するか、またはポリシーの設定を変更し、これらのボリュームが使用するIOPSの割合が少なくなるようにします。

Dashboard All Clusters

Management Actions

- Enable takeover on panic (2)
- Disable telnet (2)
- Enable volume autogrow (9)

Capacity

31 events (No new in past 24 hours)

CLUSTER	USED	DAYS TO FULL	REDUCTION
opm-sl...	40.5 TB	< 1 month	13.0:1
umeng...	83.6 TB	51 days	8.0:1
sysmgr...	33 TB	142 days	6.3:1

Performance Capacity

No new events

CLUSTER	USED	DAYS TO FULL
umeng-aff220-01-02	83%	< 1 month
sysmgr-fas8060-1-8	49%	< 1 month
fas8040-206-21	46%	77 days

Nodes

Last updated: Nov 15, 2019, 10:48 AM

VIEW Nodes on umeng-aff220-01-02 Search Nodes Filter Hardware Inventory Report

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports Show/Hide

Status	Node	Latency	IOPS	MB/s	Performance Capacity Used	Utilization	Fr
✖	umeng-aff220-01	21.7 ms/op	27,333 IOPS	221 MB/s	73%	50%	3.1
✖	umeng-aff220-02	8.33 ms/op	83.4 IOPS	102 MB/s	53%	43%	6.1

Node / Performance : umeng-aff220-01

Summary Explorer Failover Planning Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Aggregates on this Node Filter

Aggregate	Latency	IOPS	MB/s	Perf...
NSLM12_002	12.4 ...	47.51 ...	5.8 M...	8%
NSLM12_001	11.4 ...	216 L...	4.33 ...	5%

Aggregate / Performance : NSLM12_002

Summary Explorer Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Volumes on this Aggregate Filter

Volume	Latency	IOPS	MB/s
suchita_vmware_d...	6.38 ms...	76.8 IOPS	2.55 MB/s
suchita_vmware_d...	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画面操作

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 イベントを監視します。パフォーマンスとイベントの総合的な情報を表示することも、クラスタとオブジェクトのパフォーマンス、パフォーマンス イベントの詳しい

データを表示して調査することもできます。

次に、クラスタ パフォーマンスを監視する際の操作例を紹介します。

1. 左側のナビゲーション ペインで、ストレージ > アグリゲート をクリックします。
2. これらの集計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: すべての集計」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、[表示と比較] メニューでこの集計と比較する他のオブジェクトを選択し、オブジェクトの1つを比較ペインに追加します。

両方のオブジェクトの統計データが、比較できるようにカウンタ グラフに表示されます。

5. エクスプローラー ページの右側にある比較ペインで、いずれかのカウンター チャートの **ズーム表示** をクリックすると、その集計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%
☐	!	mes_aggr2	HDD	10.4 ms/op	52.9 IOPS	7.28 MB/s	3%	2%

Aggregate / Performance : aggr4

Switch to Health View Last updated: Nov 15, 2019, 1:20 PM ?

Summary Explorer Information

Compare the performance of associated objects and display detailed charts ?

TIME RANGE Last 72 Hours

VIEW AND COMPARE Aggregates on same Node Filter

Aggregate	Latency	IOPS	MB/s	Perf...
aggr3	5.06 ...	3.06 ...	< 1 M...	6%
aggr_evt	0.29 ...	3.79 ...	< 1 M...	< 1%
aggr_automation	0.27...	6.35 ...	< 1 M...	< 1%

Comparing
1 Additional Object
aggr4
aggr3

CHOOSE CHARTS 7 Charts Selected ?

Events for Aggregate: aggr4
No data to display

Latency VIEW Total Zoom View
Latency - Total view (ms/op)
aggr4
aggr3
Nov 14, 2019, 6:39 AM

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

Comparing Objects
aggr4
aggr3

Latency - Total view (ms/op)
aggr4
aggr3
Nov 14, 2019, 1:24 AM

Unified Managerのイベント詳細ページには、パフォーマンス イベントに関する詳しい情報が表示されます。トラブルシューティングやシステムのパフォーマンスの微調整を行う際に、このページでパフォーマンス イベントを調査できます。

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

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

以下は、イベントを調査する際の手順の一例です。

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] メニューから、[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]や[推奨される操作]（利用可能な場合）で、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。ワークロードの分析 ボタンをクリックすると、詳細なパフォーマンス チャートが表示され、問題をさらに分析するのに役立ちます。

Event Management

Last updated: Nov 15, 2019, 11:23 AM

VIEW **Active performance events** Search Events Filter +

Assign To Acknowledge Mark as Resolved Add Alert

Show / Hide

Triggered Time	Severity	State	Impact Lev	Impact Area	Name	Source	Source Ty
Nov 14, 2019, 11:39 AM	Warning	New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs7:/julia_feb12_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_vmwvar...nt_delete_01	Volume
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency...Service Level Policy	iscsi_boot/ia.../ocum-c220-01	LUN
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency...Service Level Policy	iscsi_boot/ia.../ocum-c220-07	LUN

Event: QoS Volume Peak IOPS/TB Warning Threshold Breached

(Last Seen: Nov 15, 2019, 11:19 AM)

IOPS value of 570 IOPS on policy group NSLM_vs7_Performance_2_0 has triggered a WARNING event to identify performance problems for the workloads in this policy group.



Actions

Suggested Actions to Fix The Issue

Troubleshoot

Analyze Workload

Take Action

This is an Adaptive QoS Policy that might be used by other workloads in the system.

If it is acceptable that changes you make to the QoS setting will be applied to other workloads that are using this policy,

- Increase the threshold to 4950 IOPS/TB for this Adaptive QoS Policy.

If you are satisfied with the current limitation on workload throughput

- Leave the QoS configuration setting as it is.

Event Information

EVENT TRIGGER TIME	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	ION 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

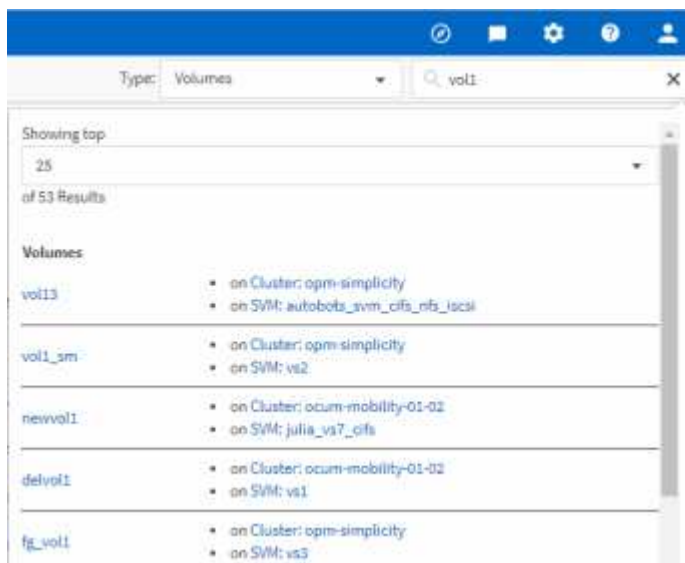
保管オブジェクトの検索

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を検索] フィールドを使用できます。すべてのオブジェクトをグローバルに検索できるので、特定のタイプのオブジェクトが簡単に見つかります。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、[タイプ]ドロップダウンメニューを使用してさらに絞り込むことができます。検索キーワードは3文字以上入力する必要があります。

グローバル検索では結果の合計数が表示されますが、アクセスできるのは上位 25 件の検索結果のみです。そのため、グローバル検索機能は、探している項目が具体的にわかっているときにすばやくアクセスするためのショートカット ツールと考えることができます。検索結果をすべて表示したいときは、オブジェクトのインベントリ ページの検索機能とフィルタリング機能を使用してください。

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[タイプ]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 オブジェクトを検索 フィールドにオブジェクト名またはイベント名の 3 文字以上を入力し、**Enter** を押すと、次のような検索結果が表示されます。

- 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
- SVM: 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。

次の例では、[タイプ]ドロップダウン ボックスで[ボリューム]オブジェクト タイプが選択されています。すべてのストレージ オブジェクトを検索 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。オブジェクト検索の場合、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 エクスプローラー ページに移動できます。イベント検索の場合、検索結果の項目をクリックすると、イベントの詳細ページに移動します。

在庫ページのコンテンツをフィルタリングする

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、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。

*フィルタリング*を使用して、好みに応じてグリッド ビューをカスタマイズします。使用可能なフィルタ オプションは、グリッドで表示しているオブジェクト タイプによって異なります。現在フィルタが適用されている場合は、適用されているフィルタの数が[フィルタ]ボタンの右側に表示されます。

次の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、含む、で始まる、で終わる、*含まない*です。
数値	演算子は、より大きい、より小さい、最後、および*間*です。
列挙（テキスト）	演算子は is と is not です。

それぞれのフィルタに、[列]、[演算子]、[値]の各フィールドが必要です。使用可能なフィルタは、現在のページのフィルタ可能な列に基づいて決まります。適用できるフィルタは4つまでです。フィルタ パラメータの組み合わせに基づいてフィルタされた結果が表示されます。フィルタされた結果は、現在表示しているページだけでなく、フィルタで検索するすべてのページに適用されます。

フィルタは[フィルタ]パネルで追加できます。

1. ページの上部にある*フィルター*ボタンをクリックします。[フィルタ]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、オブジェクト (たとえば、*Cluster* またはパフォーマンス カウンター) を選択します。
3. 中央のドロップダウン リストをクリックし、使用する演算子を選択します。
4. 最後のリストで、値を選択または入力してそのオブジェクトのフィルタを完成させます。
5. 別のフィルターを追加するには、[フィルターを追加] 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。上記と同じ手順で追加のフィルタを設定します。 4 番目のフィルターを追加すると、[フィルターを追加] ボタンが表示されなくなることに注意してください。
6. *フィルターを適用*をクリックします。フィルタ オプションがグリッドに適用されて、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、[フィルタ]パネルで、削除するフィルタの右にあるごみ箱の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、フィルタリング 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

この図では、[フィルタ]パネルで3つのフィルタを設定しています。フィルターの数が最大 4 個より少ない場合、「+ フィルターを追加」 ボタンが表示されます。

MBps	greater than	5	MBps	
Node	name starts with	test		
Type	is	FCP Port		
+ Add Filter				
				Cancel Apply Filter

*フィルターを適用*をクリックすると、フィルタリングパネルが閉じ、フィルターが適用され、適用されたフィルターの数が表示されます（ 3 ）。

ダッシュボードからクラスターのパフォーマンスを監視する

Unified Manager ダッシュボードには、Unified Manager のこのインスタンスによって監視されているすべてのクラスターの高レベルのパフォーマンス ステータスを表示するパネルがいくつか用意されています。管理対象クラスター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を理解する

Unified Manager ダッシュボードには、環境内で監視されているすべてのクラスターの高レベルのパフォーマンス ステータスを表示するパネルがいくつか用意されています。すべてのクラスターまたは個々のクラスターのステータスを表示できます。

ほとんどのパネルには、パフォーマンス情報に加えて、そのカテゴリのアクティブ イベントの数および過去24時間に追加された新しいイベントの数が表示されます。この情報から、報告されたイベントを解決するために詳細な分析が必要なクラスターを決定できます。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[イベント管理]インベントリ ページへのリンクが表示されます。

次のパネルにはパフォーマンス ステータスが表示されます。

- パフォーマンス容量パネル

すべてのクラスターを表示している場合、このパネルには、各クラスター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、そのクラスターの[ノード]インベントリ ページが表示されます。ノード インベントリ ページには過去 72 時間の平均パフォーマンス容量が表示されるため、この値はダッシュボードの値と一致しない可能性があることに注意してください。

単一のクラスターを表示している場合、このパネルには、そのクラスターのパフォーマンス容量、合計 IOPS、合計スループットが表示されます。

- ワークロード IOPS パネル

ワークロードのアクティブ管理が有効になっていて、単一のクラスターを表示している場合、このパネルに

は、特定の範囲のIOPSで現在実行されているワークロードの総数が表示されます。

- ワークロードパフォーマンスパネル

ワークロードのアクティブ管理が有効になっている場合、このパネルには、定義された各パフォーマンス サービス レベルに割り当てられている準拠ワークロードと非準拠ワークロードの総数が表示されます。棒グラフをクリックすると、そのポリシーに割り当てられているワークロードが[ワークロード]ページに表示されます。

- 使用状況概要パネル

すべてのクラスタを表示している場合、IOPSまたはスループット（MBps）が高い順にクラスタを表示できます。

単一のクラスタを表示している場合は、そのクラスタのワークロードをIOPSまたはスループット（MBps）が高い順に表示できます。

パフォーマンスのバナー メッセージと説明

Unified Managerの[通知]ページ（通知ベルからアクセス）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	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 収集サービスが停止しており、どのクラスターからもパフォーマンス データは収集されていません。	この問題を解決するには、Unified Managerを再起動します。それでも問題が解決しない場合は、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に、データの継続性収集サイクルによるパフォーマンス データの収集が実行中です。	対処は不要です。現在のパフォーマンス データは、データの継続性収集サイクルの完了後に収集されます。 データ継続性収集サイクルは、新しいクラスタが追加されたとき、または何らかの理由で Unified Manager が現在のパフォーマンス データを収集できなかったときに実行されます。

パフォーマンス統計の収集間隔を変更する

パフォーマンス統計のデフォルトの収集間隔は5分です。大規模なクラスタからの収集がデフォルトの時間内に完了しない場合は、この間隔を10分または15分に変更できます。この設定は、このUnified Managerインスタンスで監視しているすべてのクラスタからの統計の収集に適用されます。

開始する前に

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終了しない問題は、バナーメッセージで示されます。Unable to consistently collect from cluster <cluster_name>`または`Data collection is taking too long on cluster <cluster_name>。

収集間隔の変更が必要になるのは、統計の収集に問題がある場合のみです。それ以外の場合は変更しないでください。



この値をデフォルト設定の5分から変更すると、Unified Managerでレポートされるパフォーマンス イベントの数や頻度に影響する可能性があります。たとえば、システム定義のパフォーマンスしきい値ポリシーでは、ポリシーを超えた状態が30分続くとイベントがトリガーされます。これは、収集間隔が5分であれば、6回の収集で連続してポリシーの違反が検出された場合に相当します。一方、収集間隔が15分の場合は、2回の収集期間のみでポリシーの違反と判断されます。

統計データの現在の収集間隔は、[クラスタ セットアップ]ページの下部のメッセージに表示されます。

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 ポーリング間隔の構成*というラベルの付いたメニュー オプションの番号を入力し、Enter キーを押します。
3. プロンプトが表示されたら、メンテナンス ユーザのパスワードをもう一度入力します。
4. 設定する新しいポーリング間隔の値を入力し、Enterキーを押します。

外部データ プロバイダ（Graphiteなど）への接続を現在設定してある場合は、Unified Managerの収集間隔を10分または15分に変更したあと、データ プロバイダの送信間隔もUnified Managerの収集間隔以上に変更する必要があります。

ワークロード アナライザーを使用してワークロードをトラブルシューティングする

Workload Analyzerは、1つのワークロードに関する健全性とパフォーマンスの重要な条件を1つのページに表示して、トラブルシューティングを支援します。あるワークロードの現在と過去のイベントをすべて確認できるため、ワークロードに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判断できます。

また、アプリケーションのパフォーマンスの問題がストレージに起因しているか、あるいはネットワークやその他の関連する問題に起因している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 メニューで[ワークロード分析]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て
- 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、またはSMB/CIFS共有）から、詳細アイコン  次、*ワークロードを分析*します。
- 仮想マシンページで、任意のデータストアオブジェクトの*ワークロードの分析*ボタンをクリックします。

左側のナビゲーションメニューからツールを起動した場合、分析するワークロードの名前を入力し、トラブルシューティングを行う期間を選択できます。任意のワークロードまたは仮想マシンのインベントリページからツールを起動した場合、ワークロードの名前は自動的に入力され、デフォルトである2時間分のワークロードデータが表示されます。[イベントの詳細]ページからツールを起動した場合、ワークロードの名前は自動的に入力され、10日分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解決するための推奨事項、およびパフォーマンスと容量の履歴を分析するためのグラフが表示されます。

ページの上部では、分析するワークロード（ボリュームまたはLUN）の名前と、統計情報を表示する期間を指定します。表示する期間はいつでも短縮または延長することができます。

ページの他の領域には、分析結果およびパフォーマンスと容量のグラフが表示されます。



LUNのワークロードグラフに表示される統計情報レベルは、ボリュームのワークロードグラフと同じではないため、これら2種類のワークロードで異なる値が表示されることもあります。

• イベント概要エリア

一定期間内に発生したイベントの数と種類の簡単な概要を表示します。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。

期間中に発生したイベントが1つだけの場合は、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に移動した場合、選択したイベントのアイコンが大きく表示され、イベントを識別できるようになります。

• パフォーマンスチャートエリア

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。さらに詳細な分析を実行したい場合は、[パフォーマンスの詳細を表示]リンクをクリックして、ワークロードの[パフォーマンスエクスプローラー]ページを表示できます。

- レイテンシには、選択した期間におけるワークロードのレイテンシが表示されます。このグラフに

は、次の3つのビューがあります。

- *合計*レイテンシ
- 内訳 レイテンシ (読み取り、書き込み、その他のプロセス別)
- クラスタ コンポーネント のレイテンシ (クラスタ コンポーネント別の内訳)

見る"**クラスタ コンポーネントとその競合要因**"ここで表示されるクラスター コンポーネントの説明。 スループット は、選択した期間のワークロードの **IOPS** と **MB/秒**のスループットの両方を表示します。グラフには次の 4 つのビューがあり、次の情報を確認できます。* 合計 スループット * 内訳 スループット (読み取り、書き込み、およびその他のプロセス別) * 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ている MB/秒。クラウドに容量を階層化しているワークロードの場合) * 予測付き **IOPS** (期間全体で予想される **IOPS** スループットの上限と下限の予測) このグラフには、構成されている場合、サービス品質 (**QoS**) の最大および最小スループットしきい値設定も表示されるため、システムが **QoS** ポリシーを使用して意図的にスループットを制限している可能性がある場所を確認できます。 使用率は、選択した期間にわたって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使用率を表示します。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。

• 容量チャートエリア

過去1カ月のワークロードに対するデータ容量とSnapshot容量のグラフが表示されます。

ボリュームの場合、さらに分析を実行したい場合には、「容量の詳細を表示」リンクをクリックしてワークロードの「ヘルスの詳細」ページを表示できます。LUN にはヘルス詳細ページがないため、このリンクは提供されません。

- 容量ビュー には、ワークロードに割り当てられた使用可能な合計スペースと、論理的に使用されているスペース (すべてのNetApp最適化後) が表示されます。
- スナップショット ビュー には、スナップショット コピー用に予約されている合計スペースと、現在使用されているスペースの量が表示されます。LUNにはSnapshotビューが表示されません。
- *クラウド層ビュー*には、ローカル パフォーマンス層で使用されている容量とクラウド層で使用されている容量が表示されます。これらのグラフには、このワークロードの容量がフルになるまでの推定残り時間が表示されます。この情報は過去の使用状況に基づいており、最低10日間のデータが必要です。残りの容量が 30 日未満になると、Unified Manager はストレージを「ほぼいっぱい」と認識します。

Workload Analyzerを使用するタイミング

Workload Analyzerは、ユーザから報告されたレイテンシの問題をトラブルシューティングする場合、報告されたイベントやアラートを詳しく分析する場合、動作に異常があるワークロードについて調べる場合に使用します。

アプリケーションの実行速度が非常に遅いという連絡をユーザから受けた場合は、アプリケーションが実行されているワークロードのレイテンシ、スループット、利用率の各グラフを調べて、パフォーマンスの問題がストレージに起因しているかどうかを確認できます。ONTAPシステムで容量の使用率が85%を超えるとパフォーマンスの問題が生じる可能性があるため、容量グラフを使用して使用率が上昇していないかも確認できます。これらのグラフから、問題の原因がストレージであるか、ネットワークであるか、あるいはその他の関連する問題であるかを判別できます。

Unified Manager によってパフォーマンス イベントが生成され、問題の原因をより徹底的に確認したい場合

は、[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てワークロード アナライザーを起動し、ワークロードのレイテンシ、スループット、容量の傾向を調査できます。

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、またはSMB/CIFS共有）を表示しているときに、ワークロードが異常に動作していると思われる場合は、詳細アイコンをクリックします。 ⓘ をクリックし、ワークロードの分析 をクリックしてワークロード分析ページを開き、ワークロードをさらに詳しく調べます。

ワークロードアナライザーを使用する

Workload Analyzerは、ユーザ インターフェイスからさまざまな方法で起動できます。ここでは、左側のナビゲーション ペインからツールを起動する方法について説明します。

手順

1. 左側のナビゲーション ペインで、[ワークロード分析] をクリックします。

[ワークロード分析]ページが表示されます。

2. ワークロード名がわかっている場合は入力します。完全な名前がわからない場合は、3文字以上入力すると、その文字列に一致するワークロードのリストが表示されます。
3. デフォルトの 2 時間よりも長い期間の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、設定した期間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。

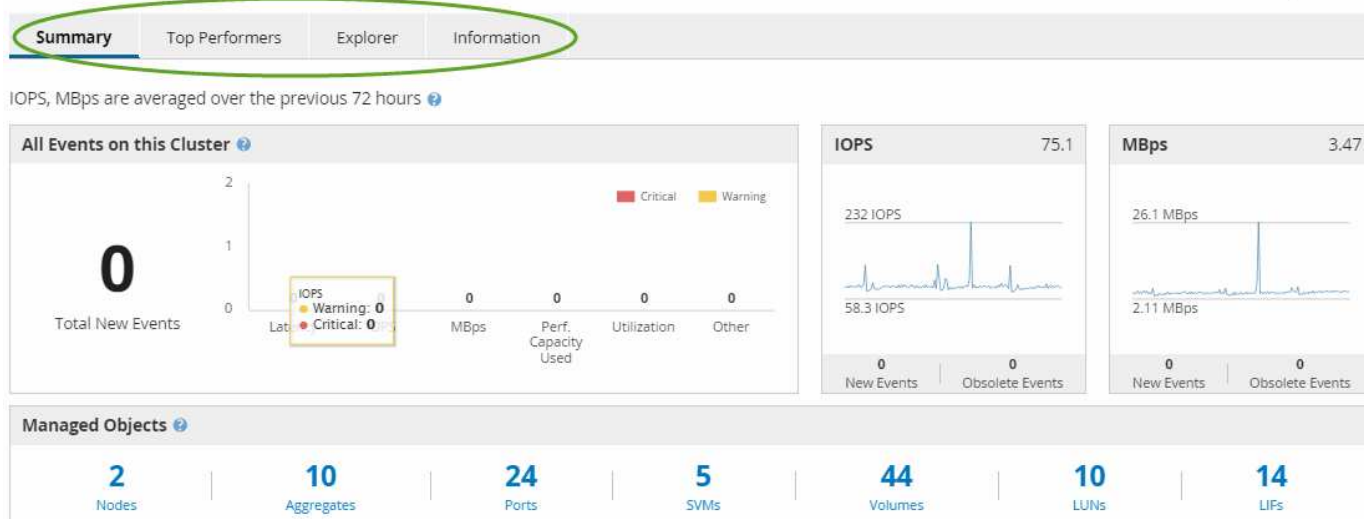
パフォーマンス クラスター ランディング ページからクラスターのパフォーマンスを監視します。

[パフォーマンス クラスター ランディング]ページには、Unified Managerのインスタンスで監視し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。このページを使用すると、特定のクラスタの全体的なパフォーマンスを評価し、クラスター固有のイベントをすばやく把握して特定し、解決策を適用することができます。

パフォーマンス クラスターのランディング ページを理解する

[パフォーマンス クラスター 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[このクラスタのすべてのイベント]パネルに表示されます。

[パフォーマンス クラスター ランディング]ページには、Unified Managerのインスタンスで管理され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[パフォーマンス クラスター ランディング]ページの例を示しています。



[クラスタ サマリ]ページのイベント件数は、[パフォーマンス イベント インベントリ]ページのイベント件数と一致しない場合があります。これは、組み合わせしきい値ポリシーに違反した場合、[クラスタ サマリ]ページでは[レイテンシ]バーと[利用率]バーにそれぞれ1つのイベントを表示できるのに対して、[パフォーマンス イベント インベントリ]ページでは1つのイベントしか表示されないためです。



クラスタが Unified Manager による管理から削除された場合、ページ上部のクラスタ名の右側にステータス「削除済み」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 ランディング ページには、選択したクラスタの高レベルのパフォーマンス ステータスが表示されます。このページを使用して、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 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る 4 つのタブがあります。

- [サマリ]ページ
 - クラスタイベントペイン
 - MB/s 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
- エクスプローラーページ
- 情報ページ

[パフォーマンス クラスタ サマリ]ページ

パフォーマンス クラスタ サマリー ページには、クラスタのアクティブ イベント、IOPS パフォーマンス、MB/s 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。

[クラスター パフォーマンス イベント] ペイン

クラスター パフォーマンス イベント ペインには、クラスターのパフォーマンス統計とすべてのアクティブなイベントが表示されます。これは、クラスターやクラスター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特に役立ちます。

このクラスターペインのすべてのイベント

「このクラスターのすべてのイベント」 ペインには、過去 72 時間のすべてのアクティブなクラスター パフォーマンス イベントが表示されます。アクティブ イベントの合計数は左端に表示されます。この数値は、このクラスター内のすべてのストレージ オブジェクトのすべての新規イベントと確認済みイベントの合計を表します。[アクティブ イベントの合計] リンクをクリックすると、これらのイベントを表示するようにフィルターされた [イベント インベントリ] ページに移動できます。

クラスターの「アクティブ イベントの合計」棒グラフには、アクティブな重大イベントと警告イベントの合計数が表示されます。

- 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（クラスター、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（クラスター、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 イベントが含まれます。

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。*更新*をクリックすると、カウンター パネルのデータを更新できます。

凡例の 重大 および 警告 アイコンをクリックすると、合計アクティブ イベントのパフォーマンス グラフで重大イベントと警告イベントを表示または非表示にすることができます。特定のイベント タイプを非表示にした場合、凡例の該当する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時間のクラスター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カウンターパネル

IOPSは、クラスターの動作速度（1秒あたりのI/O処理数）を示します。このカウンタ パネルでは、過去72時間のクラスターの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。

- **MB/sカウンターパネル**

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の値が表示されます。

グラフ右上のグレーのバーに表示される数字は、過去72時間の平均値です。トレンド グラフの上下に表示される数字は、過去72時間の最大値と最小値です。グラフ下のグレーのバーには、過去72時間のアクティブなイベント（新規および確認済みのイベント）と廃止イベントの件数が表示されます。

カウンタ パネルには、2種類のイベントが表示されます。

- **アクティブ**

現在アクティブなパフォーマンス イベント（新規または確認済みのイベント）を示します。自己修復または解決されていないイベントで、ストレージ オブジェクトのパフォーマンス カウンタがパフォーマンス しきい値を超えたままになっているものです。

- **廃止**

アクティブではなくなったイベントを示します。自己修復または解決されたイベントで、ストレージ オブジェクトのパフォーマンス カウンタがパフォーマンス しきい値を上回らなくなったものです。

アクティブ イベント*の場合、イベントが 1 つあるときは、イベント アイコンの上にカーソルを置き、イベント番号をクリックすると、適切なイベントの詳細ページにリンクします。イベントが複数ある場合は、[*すべてのイベントを表示] をクリックして、選択したオブジェクト カウンター タイプのすべてのイベントを表示するようにフィルターされた [イベント インベントリ] ページを表示できます。

[管理対象オブジェクト]ペイン

[パフォーマンス サマリー] タブの [管理対象オブジェクト] ペインには、クラスターのストレージ オブジェクトの種類と数のトップレベルの概要が表示されます。このペインを使用すると、各クラスタのオブジェクトのステータスを追跡できます。

管理対象オブジェクトの数は、前回の収集期間以降のある時点におけるデータです。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[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です。

- **集計**

保護およびプロビジョニングの際に1つのユニットとして管理可能な、複数のRedundant Array of Independent Disks（RAID）グループの集まりです。

- ポート

ネットワーク上の他のデバイスへの接続に使用される、ノード上の物理接続ポイントです。

- ストレージVM

一意のネットワーク アドレスでネットワーク アクセスを提供する仮想マシンです。SVM は別個の名前空間からデータを提供する可能性があり、クラスターの残りの部分とは個別に管理できます。

- 卷

サポートされているプロトコルを使用してアクセス可能なユーザ データを格納する論理エンティティです。数にはFlexVolとFlexGroupボリュームはどちらも含まれますが、FlexGroupコンスティチュエントは含まれません。

- LUN

Fibre Channel (FC) 論理ユニットまたはiSCSI論理ユニットの識別子です。一般的にストレージ ボリュームに対応する論理ユニットで、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ース

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 インターフェイスです。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のイベント）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。[ボリューム]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。使用可能な期間は次のとおりです。

- 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

- メトリック

別のカウンターを選択するには、[メトリック] メニューをクリックします。選択できるカウンタはオブジェクト タイプに固有です。たとえば、ボリューム オブジェクトで利用できるカウンターは、レイテンシ、**IOPS**、および **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。

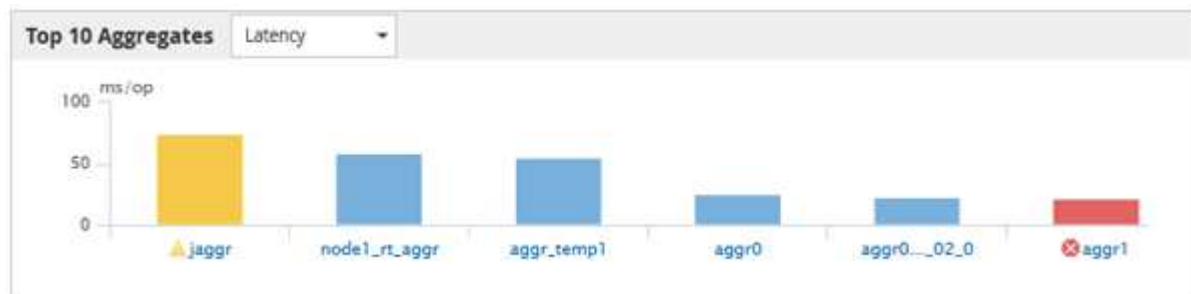
使用可能なカウンタは次のとおりです。

- レイテンシー
 - IOPS
 - MB/秒
 - パフォーマンス使用容量（ノードおよびアグリゲート用）
 - 利用率（ノードとアグリゲートの場合）
- 選別

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ー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、「最高から最低」と「最低から最高」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。しきい値違反がアクティブの場合（新規または確認済みのイベント）、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（）、重要なイベントは赤色で表示されます（）。さらに、イベントの重大度アイコン（警告イベントと重大イベント）も表示されます。



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対応する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]ページに移動します。

- 重大度イベントインジケーター

*重大度イベント*インジケーターアイコンは、アクティブなクリティカル（）または警告（）イベントをトップ パフォーマーのグラフに表示します。*重大度イベント*インジケーターアイコンをクリックすると、次の内容が表示されます。

- 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

作成します`.csv`カウンターバーに表示されるデータが含まれるファイル。表示している単一のクラスタについてのファイルのほか、データセンターのすべてのクラスタについてのファイルを作成することもできます。

パフォーマンスインベントリページを使用してパフォーマンスを監視する

[オブジェクト インベントリ パフォーマンス]ページには、そのオブジェクト 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、および健全性が表示されます。これにより、クラスタ内の各オブジェクト（すべてのノードまたはすべてのボリュームなど）のパフォーマンス ステータスの概要をひと目で確認できます。

[オブジェクト インベントリ パフォーマンス]ページには、オブジェクト ステータスの概要が表示されるため、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。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

Search Nodes

Assign Performance Threshold Policy

Clear Performance Threshold Policy

Schedule Report

	Status ▾	Node	Latency	IOPS	MBps	Flash Cache Reads	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster
		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
		opm-simplicity-01	2.01 ms/op	39,358 IOPS	153 MBps	< 1%	119%	88%	4.88 TB	18.3 TB	opm-simplicity
		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
		opm-simplicity-02	17 ms/op	14,627 IOPS	124 MBps	< 1%	29%	20%	212 GB	5.88 TB	opm-simplicity

パフォーマンス インベントリ ページのオブジェクトは、デフォルトでは、オブジェクトのパフォーマンスの重大度に基づいてソートされます。新しい重大なパフォーマンス イベントが報告されたオブジェクトが最初に表示され、そのあとに警告イベントが報告されたオブジェクトが表示されます。これにより、対処が必要な問題を簡単に特定できます。パフォーマンス データはいずれも72時間の平均値です。

オブジェクト名の列で名前をクリックすると、[オブジェクト インベントリ パフォーマンス]ページからその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、「パフォーマンス/すべてのノード」インベントリ ページで、「ノード」列のノード オブジェクトをクリックします。オブジェクトの詳細ページには、アクティブなイベントを並べた比較など、選択したオブジェクトの詳細情報が表示されます。

すべてのストレージ オブジェクトのパフォーマンス インベントリ ページを表示します。

パフォーマンス インベントリ ページでは、クラスタ、アグリゲート、ボリュームなど、

使用可能な各ストレージ オブジェクトに関するパフォーマンス情報の概要を確認できます。パフォーマンス オブジェクト詳細ページへのリンクを使用して、特定のオブジェクトの詳しい情報も確認できます。

ビュー ページ内のオブジェクトは、デフォルトでは、イベントの重大度に基づいてソートされます。重大なイベントが報告されたオブジェクトが最初に表示され、そのあとに警告イベントが報告されたオブジェクトが表示されます。これにより、対処が必要な問題を簡単に特定できます。

これらのページからデータをカンマ区切りの値でエクスポートできます(.csv) ファイル、Microsoft Excel ファイル(.xlsx) 、 または(.pdf) ドキュメントを レポート ボタンを使用してエクスポートし、エクスポートしたデータを使用してレポートを作成します。さらに、ページをカスタマイズし、[スケジュールされたレポート] ボタンを使用して、定期的にレポートを作成して電子メールで送信するようにスケジュールすることもできます。

これらのページのフィールドは、すべてカスタム ビューとレポートで使用できます。一部のフィールドは関連ページにリンクされており、より詳細な表示が可能です。

パフォーマンス: すべてのクラスタービュー

「パフォーマンス: すべてのクラスター」ビューには、Unified Manager のインスタンスによって監視される各クラスタのパフォーマンス イベント、データ、および構成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、オブジェクト インベントリ ページ上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を割り当てたり、任意のオブジェクトからしきい値ポリシーをクリアしたりできます。

以下は、「パフォーマンス: すべてのクラスター」ビューの重要なフィールドです。

- クラスター FQDN: クラスターの完全修飾ドメイン名 (FQDN)。
- IOPS: クラスター上の 1 秒あたりの入出力操作数。
- MB/秒: クラスターのスループット (MiB/秒単位で測定)。
- 容量フィールド: 空き容量と合計容量 (GiB 単位)。
- ホスト名または IP アドレス: クラスター管理 LIF のホスト名または IP アドレス (IPv4 または IPv6)。
- OS バージョン: クラスター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。



クラスター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、[パフォーマンス: すべてのノード] ビューから確認できます。

- 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 (複数可)。ポリシー名に省略記号 (...) が含まれている場合、ポリシー名にカーソルを合わせると完全なポリシー名または割り当てられているポリシー名のリストが表示されます。左端のチェック ボックスをクリックして1つ以上のオブジェクトを選択すると、[Assign Performance Threshold Policy] ボタンと[Clear Performance Threshold Policy]ボタンを使用できるようになります。

パフォーマンス: すべてのボリュームビュー

「パフォーマンス: すべてのボリューム」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 volume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したい場合は、その他のオプションボタンをクリックします。次に*ワークロードを分析*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表示できます。System Managerの有効なクレデンシャルがあれば、System Managerで詳細を確認することができます。



データ保護 (DP) ボリュームについては、ユーザが生成したトラフィックのカウンタ値のみが表示されます。ルート ボリュームはこのページに表示されません。

以下は、「パフォーマンス: すべてのボリューム」ビューの重要なフィールドです。

- スタイル: FlexVolまたはFlexGroup のいずれか。
- レイテンシ: FlexVolボリュームの場合、これはすべての I/O 要求に対するボリュームの平均応答時間であり、操作ごとにミリ秒単位で表されます。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: ワークロードによって消費されている合計スペースに基づいて、1 秒あたりに処理される入出力操作の数 (テラバイト単位)。このグラフは、一定のストレージ容量で提供可能なパフォーマンスを表します。
- IOPS: FlexVolボリュームの場合、これはボリュームの 1 秒あたりの入出力操作の数です。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IOPS。
- MB/秒: FlexVolボリュームの場合、これはボリューム上のスループットであり、1 秒あたりのメガバイト単位で測定されます。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。
- 容量フィールド: 空き容量と合計容量 (GiB 単位)。

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に適用された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の階層化の推奨について"](#)
- ["パフォーマンス グラフを使用した同じ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: すべての集計ビュー

「パフォーマンス: すべてのアグリゲート」ビューには、Unified Manager のインスタンスによって監視される各アグリゲートのパフォーマンス イベント、データ、および構成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。

以下は、「パフォーマンス: すべての集計」ビューの重要なフィールドです。

- タイプ: 集計のタイプ:
 - 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です。
 - 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)
- 非アクティブ データのレポート: このアグリゲートで非アクティブ データのレポート機能が有効になっているか無効になっているかを示します。有効にすると、このアグリゲート上のボリュームの「パフォーマンス: すべてのボリューム」ビューにコールド データの量が表示されます。Inactive Data ReportingをサポートしていないONTAPのバージョンでは、このフィールドの値は「N/A」になります。
- 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 (複数可)。ポリシー名に省略記号 (...) が含まれている場合、ポリシー名にカーソルを合わせると完全なポリシー名または割り当てられているポリシー名のリストが表示されます。左端のチェック ボックスをクリックして1つ以上のオブジェクトを選択すると、[Assign Performance Threshold Policy]ボタンと[Clear Performance Threshold Policy]ボタンを使用できるようになります。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: すべてのノードビュー

「パフォーマンス: すべてのノード」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、および構成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]には、ノードでの読み取り処理のうち、ディスクではなくキャッシュで処理された割合が表示されます。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ノードについてのみ表示されます。

Unified Manager とそれが管理するクラスタが外部ネットワーク接続のないサイトにインストールされている場合、[レポート] メニューに [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、オブジェクト インベントリ ページ上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を割り当てたり、任意のオブジェクトからしきい値ポリシーをクリアしたりできます。

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"](#)
- ["契約更新用ハードウェア インベントリ レポートの生成"](#)

パフォーマンス: すべてのストレージVMビュー

「パフォーマンス: すべてのストレージ 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ストレージ仮想マシン (SVM) のパフォーマンス イベント、データ、および構成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[レイテンシ]フィールドには、すべてのI/O要求の平均応答時間 (ms/op) が報告されます。



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"](#)

パフォーマンス: すべてのLUNビュー

「パフォーマンス: すべての LUN」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、および構成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したい場合は、詳細アイコンをクリックします。⋮をクリックし、*ワークロードの分析*を選択すると、*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表示できます。

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での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"](#)
- ["特定のボリュームまたはLUNに適用された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 名前空間ビュー

「パフォーマンス: すべての NVMe 名前空間」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 名前空間のパフォーマンス イベント、データ、および構成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: 名前空間の現在の状態。* オフライン - 名前空間への読み取りまたは書き込みアクセスは許可されません。* オンライン - 名前空間への読み取りおよび書き込みアクセスが許可されます。* NVFail - NVRAM障害のため、名前空間が自動的にオフラインになりました。* スペース エラー - 名前空間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

「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」ビューには、Unified Manager のこのインスタンスによって監視され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、および構成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。以下は、「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」ビューの重要なフィールドです。

- IOPS: 1 秒あたりの入出力操作数。NFS LIFとCIFS LIFには[IOPS]が該当しないため、「N/A」と表示されます。
- レイテンシ: すべての I/O 要求の平均応答時間。操作ごとにミリ秒単位で表されます。NFS LIFとCIFS LIFには[レイテンシ]が該当しないため、「N/A」と表示されます。
- ホーム ロケーション: インターフェイスのホーム ロケーション。ノード名とポート名として表示され、コロン (:) で区切られます。場所が省略記号 (...) とともに表示される場合は、場所の名前にカーソルを合わせることで場所全体が表示されます。
- 現在の場所: インターフェイスの現在の場所。ノード名とポート名として表示され、コロン (:) で区切られます。場所が省略記号 (...) とともに表示される場合は、場所の名前にカーソルを合わせることで場所全体が表示されます。
- ロール: インターフェイス ロール: データ、クラスタ、ノード管理、またはクラスタ間。



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。

パフォーマンス: すべてのポートビュー

「パフォーマンス: すべてのポート」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、および構成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。ポートのロールについては、ネットワーク ポートの役割（「データ」または「クラスタ」）が表示されます。FCP ポートにはロールを設定できず、ロールは N/A と表示されます。



パフォーマンス カウンタの値が表示されるのは物理ポートについてのみです。VLANまたはインターフェイス グループについて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"](#)

パフォーマンス: QoS ポリシー グループ ビュー

[パフォーマンス: QoS ポリシー グループ]ビューには、Unified Managerによって監視され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るQoSポリシーが含まれます。

以下は、「パフォーマンス: QoS ポリシー グループ」ビューの重要なフィールドです。

- **QoS ポリシー グループ:** QoS ポリシー グループの名前。Unified Manager 9.7以上にインポートされたNetApp Service Level Manager (NSLM) 1.3ポリシーの場合、ここに表示される名前には、SVM名、およびパフォーマンス サービス レベルがNSLMで定義された時点では名前に含まれていないその他の情報が含まれます。たとえば「NSLM_vs6_Performance_2_0」という名前は、SVM「vs6」に対して作成された、想定レイテンシ「2ミリ秒/処理」の、NSLMシステム定義の「パフォーマンス」PSLポリシーであることを意味します。
- **SVM:** QoS ポリシー グループが属するストレージ VM (SVM)。Storage VM名をクリックすると、そのStorage VMの詳細ページが表示されます。管理Storage VMはクラスタを表すため、管理Storage VMでQoSポリシーが作成されている場合、このフィールドは空白になります。
- **最小スループット:** ポリシー グループが提供することが保証される最小スループット (IOPS 単位)。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。
- **最大スループット:** ポリシー グループが超えてはならないスループット (IOPS および/または MB/秒)。このフィールドが空白の場合、ONTAPには無制限の最大スループット定義されています。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:** 適応型ポリシーの場合、これは予想される IOPS がこの値より小さい場合にオーバーライドとして使用される絶対最小 IOPS 値です。
- **ブロック サイズ:** QoS アダプティブ ポリシーに指定されたブロック 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「割り当て済みスペース」を使用するか「使用済みスペース」を使用するか。
- **予想されるレイテンシ:** ストレージの入出力操作の予想される平均レイテンシ。
- **共有:** 従来の QoS ポリシーの場合、ポリシー グループで定義されたスループット値が複数のオブジェクト間で共有されるかどうか。
- **関連オブジェクト:** 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。展開ボタン (▼) QoS ポリシー グループ名の横にあるアイコン をクリックすると、ポリシー グループの詳細が表示されます。
- **割り当てられた容量:** 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。
- **関連オブジェクト:** ボリュームと LUN に分けて、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。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、以下のトピックをご覧ください。["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 データの内容を調整して特定のデータをすばやく簡単に見つけられるようにするツール

が含まれています。

パフォーマンス オブジェクト インベントリ ページに含まれる情報は広範囲にわたる場合があります、複数のページにまたがることもあります。この種の包括的なデータは、パフォーマンスの監視、追跡、改善には非常に役立ちますが、特定のデータにたどり着くには探しているデータをすばやく特定するためのツールが必要です。したがって、パフォーマンス オブジェクト インベントリ ページには、検索、並べ替え、フィルタリングの機能が含まれています。検索とフィルタリングを一緒に使用して、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検索

[オブジェクト インベントリ パフォーマンス]ページで文字列を検索できます。ページの右上にある 検索 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見つけることができます。オブジェクトとその関連データを特定したり、ポリシーを特定して関連するポリシーのオブジェクト データを表示したりできます。

手順

1. 検索対象に応じて次のどちらかのオプションを実行します。

これを探すには...	これを入力してください...
特定のオブジェクト	*検索*フィールドにオブジェクト名を入力し、*検索*をクリックします。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	*検索*フィールドにポリシー名の全部または一部を入力し、*検索*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並べ替える

[オブジェクト インベントリ パフォーマンス]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。オブジェクト インベントリ データをすばやく特定できるため、パフォーマンスの調査時やトラブルシューティングの開始時に役立ちます。

ソート用に選択した列は列見出しが強調表示され、ソート方向を示す矢印アイコンが見出し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。デフォルトの並べ替え順序は、ステータス (イベントの重要度) の降順で、最も重要なパフォーマンス イベントが最初にリストされます。

手順

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。

[オブジェクト インベントリ パフォーマンス]ページの内容は、選択した列を基準に昇順または降順でソートされます。

オブジェクトインベントリパフォーマンスページでデータをフィルタリングする

[オブジェクト インベントリ パフォーマンス]ページでデータをフィルタリングし、特定の条件に基づいてデータをすばやく特定できます。フィルタリングを使用すると、[オブジェクト インベントリ パフォーマンス]ページの内容を絞り込んで、指定した結果だけを表示できます。そのため、関心のあるパフォーマンス データだけを効率的に表示できます。

[フィルタ]パネルを使用して、グリッド ビューをカスタマイズできます。使用可能なフィルタ オプションは、グリッドで表示しているオブジェクト タイプによって異なります。現在フィルタが適用されている場合は、適用されているフィルタの数が[フィルタ]ボタンの右側に表示されます。

次の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、含む、で始まる、で終わる、*含まない*です。
数値	演算子は、より大きい、より小さい、最後、および*間*です。
列挙（テキスト）	演算子は is と is not です。

それぞれのフィルタに、[列]、[演算子]、[値]の各フィールドが必要です。使用可能なフィルタは、現在のページのフィルタ可能な列に基づいて決まります。適用できるフィルタは4つまでです。フィルタ パラメータの組み合わせに基づいてフィルタされた結果が表示されます。フィルタされた結果は、現在表示しているページだけでなく、フィルタで検索するすべてのページに適用されます。

フィルタは[フィルタ]パネルで追加できます。

1. ページの上部にある*フィルター*ボタンをクリックします。[フィルタ]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、オブジェクト (たとえば、*Cluster* またはパフォーマンス カウンター) を選択します。
3. 中央のドロップダウン リストをクリックし、使用する演算子を選択します。
4. 最後のリストで、値を選択または入力してそのオブジェクトのフィルタを完成させます。
5. 別のフィルターを追加するには、[フィルターを追加] 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。上記と同じ手順で追加のフィルタを設定します。4 番目のフィルターを追加すると、[フィルターを追加] ボタンが表示されなくなることに注意してください。
6. *フィルターを適用*をクリックします。フィルタ オプションがグリッドに適用されて、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、[フィルタ]パネルで、削除するフィルタの右にあるごみ箱の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、フィルタリング パネルの下部にある [リセット] をクリックします。

この図では、[フィルタ]パネルで3つのフィルタを設定しています。フィルタの数が最大 4 個より少ない場合、「+ フィルターを追加」ボタンが表示されます。

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

*フィルターを適用*をクリックすると、フィルタリングパネルが閉じ、フィルターが適用され、適用されたフィルタの数が表示されます (3)。

クラウドにデータを階層化するための **Unified Manager** の推奨事項を理解する

「パフォーマンス: すべてのボリューム」ビューには、非アクティブ (コールド) のボリュームに保存されているユーザー データのサイズに関連する情報が表示されます。場合によっては、Unified Manager は、非アクティブなデータをFabricPool対応アグリゲートのクラウド層 (クラウド プロバイダまたはStorageGRID) に階層化することでメリットが得られるボリュームを特定します。



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は、Unified Manager によるデータの階層化の推奨事項に従って、ONTAPソフトウェアをアップグレードする必要があります。さらに、`auto`階層化ポリシーはONTAP 9.4で導入され、`all`階層化ポリシーはONTAP 9.6 で導入されたため、自動階層化ポリシーの使用が推奨されている場合は、ONTAP 9.4 以降にアップグレードする必要があります。

「パフォーマンス: すべてのボリューム」ビューの次の 3 つのフィールドには、非アクティブなデータをクラウド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を向上させ、パフォーマンス層のスペースを節約できるかどうかに関する情報が提供されます。

• 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。

このフィールドには、ボリュームに対して設定されている階層化ポリシーが、ボリュームが現在FabricPoolアグリゲートにない場合も含めて表示されます。階層化ポリシーが適用されるのは、ボリュームが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。

ONTAP 9.4以降のソフトウェアを使用している場合にのみ、ここに値が表示されます。これは、ボリュームが展開されているアグリゲートに **inactive data reporting parameter** に設定 **enabled**、および最低冷却日数のしきい値が満たされていることを確認します (**snapshot-only** または **auto** 階層化ポリシー)。それ以外の場合、値は「N/A」として表示されます。

- クラウド推奨

ボリューム上のデータ アクティビティに関する十分な情報が取得された後、Unified Manager は、必要なアクションがないと判断するか、非アクティブなデータをクラウド層に階層化することでパフォーマンス層のスペースを節約できると判断する場合があります。



[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、[クラウドに関する推奨事項]フィールドは7日ごと（ボリューム上でコールド データ分析が実行されるとき）に更新されます。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。[クラウドに関する推奨事項]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、[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。非アクティブ データのレポート機能がない場合、Unified Manager はパフォーマンス統計を使用して、ボリューム上のデータが非アクティブかどうかを判断します。この場合、非アクティブデータの量は [コールド データ] フィールドには表示されませんが、**Tier** という単語の上にカーソルを置いてクラウドの推奨事項を表示すると表示されます。

クラウドに関する推奨事項には、次のいずれかが表示されます。

- 学ぶ。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。
- ティア。分析の結果、アクセス頻度の低いコールド データがボリュームにあり、そのデータをクラウド階層に移動するようにボリュームを設定することが推奨されます。一部のケースでは、ボリュームをまずFabricPool対応アグリゲートに移動する必要があります。ボリュームがすでにFabricPoolアグリゲートにあれば、階層化ポリシーの変更だけで済みます。
- アクションなし。ボリュームに非アクティブな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「自動」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、ボリューム階層化ポリシーや集約非アクティブ データ レポート設定を変更したりするには、ONTAP System Manager、ONTAP CLI コマンド、またはこれらのツールの組み合わせを使用します。

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、**Tier** という単語の上にカーソルを移動すると、クラウド推奨事項で ボリュームの構成 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 のボリューム ページが開き、推奨される変更を行うことができます。

パフォーマンス エクスプローラー ページを使用してパフォーマンスを監視する

パフォーマンス エクスプローラー ページには、クラスター内の各オブジェクトのパフォーマンスに関する詳細情報が表示されます。すべてのクラスター オブジェクトのパフォーマンスの詳細を表示でき、さまざまな期間にわたる特定のオブジェクトのパフォーマンス データを選択して比較できます。

すべてのオブジェクトの全体的なパフォーマンスを評価したり、オブジェクトのパフォーマンス データを並べて表示して比較したりできます。

ルートオブジェクトを理解する

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。これにより、他のオブジェクトのデータとルート オブジェクトのデータを表示および比較できるようになり、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と改善に役立つパフォーマンス データ分析が提供されます。

ルート オブジェクト名は、比較ペインの上部に表示されます。その他のオブジェクトはルート オブジェクトの下に表示されます。比較ペインに追加できるオブジェクトの数に制限はありませんが、ルート オブジェクトは1つだけ許可されます。ルート オブジェクトのデータは、[カウンター チャート] ペインのグラフに自動的に表示されます。

ルート オブジェクトを変更することはできず、表示中のオブジェクト ページに常に表示されます。たとえばVolume1の[ボリューム パフォーマンス エクスプローラ]ページを開くと、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、グリッドにボリュームが25個ある場合、フィルタを使用することで、それらのボリュームの中からスループットが90MBps未満のボリュームのみを表示したり、レイテンシが1ミリ秒/処理を超えるボリュームだけを表示したりできます。

関連オブジェクトの時間範囲を指定する

[パフォーマンス エクスプローラ]ページの[期間]セレクトアを使用して、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、[パフォーマンス エクスプローラ]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 データだけが表示されます。

期間を絞り込むと、関心のあるパフォーマンス データだけを効率的に表示できます。事前定義の期間を選択するか、または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。

定義済みの時間範囲を選択する

事前定義の期間を選択すると、クラスタ オブジェクトのパフォーマンス データを表示する際に、すばやく効率的にデータ出力をカスタマイズして絞り込むことができます。事前定義された期間を選択する場合、最大で13カ月分のデータを利用できます。

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*パネルの右側から、定義済みの時間範囲を選択します。
3. *範囲を適用*をクリックします。

カスタム時間範囲を指定する

[パフォーマンス エクスプローラ]ページを使用して、パフォーマンス データの期間を指定できます。カスタムの期間を指定すると、クラスタ オブジェクトのデータを絞り込む際に、事前定義の期間を使用するよりも柔軟に設定できます。

1 時間から 390 日までの時間範囲を選択できます。1 か月は30日としてカウントされるため、390日は13か月に相当します。日時の範囲を指定することで、特定のパフォーマンス イベントや一連のイベントにフォーカスして詳細を確認することができます。また、日時の範囲を指定すると、パフォーマンス イベントに関連するデータがより詳しく表示されるため、潜在的なパフォーマンスの問題のトラブルシューティングにも役立ちます。時間範囲 コントロールを使用して、定義済みの日付と時刻の範囲を選択するか、最大 390 日間の独自のカスタム日付と時刻の範囲を指定します。事前定義された時間範囲のボタンは、「過去 1 時間」から「過去 13 か月」までさまざまです。

過去 13 か月 オプションを選択するか、30 日を超えるカスタム日付範囲を指定すると、30 日を超える期間のパフォーマンス データは 5 分ごとのデータ ポーリングではなく 1 時間ごとの平均を使用してグラフ化されることを警告するダイアログ 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 [今後表示しない] オプションをクリックすると、[過去 13 か月] オプションを選択したり、30 日を超えるカスタム日付範囲を指定したりしても、メッセージは表示されません。時間範囲に今日から 30 日を超える時間/日付が含まれる場合、要約データはより短い時間範囲にも適用されます。

時間範囲 (カスタムまたは定義済み) を選択する場合、30 日以下の時間範囲は 5 分間隔のデータ サンプルに基づきます。30日を超える場合は、1時間ごとのデータ サンプルに基づいてデータが表示されます。

1. *時間範囲*ドロップダウン ボックスをクリックすると、時間範囲パネルが表示されます。
2. 定義済みの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場合、最大で13か月分のデータを利用できます。選択した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刻フィールドに表示されます。
3. カスタムの日付範囲を選択するには、左側の「開始」カレンダーで開始日をクリックします。カレンダー内を前方または後方に移動するには、< または > をクリックします。終了日を指定するには、右側の「終了」カレンダーで日付をクリックします。終了日は、別の日付を指定しないかぎり、デフォルトでは現在の日付になります。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、カスタム日付範

囲を選択したことが示されます。

4. カスタムの時間範囲を選択するには、[開始] カレンダーの下の [時間] コントロールをクリックし、開始時刻を選択します。終了時刻を指定するには、右側の 終了 カレンダーの下の 時間 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、カスタム時間範囲を選択したことが示されます。
5. 事前定義された日付範囲を選択し、開始時間と終了時間を指定することもできます。前述の説明に従って事前定義された日付範囲を選択したあと、上記と同じ方法で開始時間と終了時間を選択します。選択した日付は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は 時間 コントロールに表示され、カスタム範囲 ボタンが強調表示されます。
6. 日付と時刻の範囲を選択した後、「範囲を適用」をクリックします。グラフと[イベント]タイムラインに、その期間のパフォーマンス統計が表示されます。

比較グラフ化のための関連オブジェクトのリストを定義する

[カウンタ グラフ]ペインでは、データおよびパフォーマンスを比較する関連オブジェクトのリストを定義できます。たとえば、Storage Virtual Machine (SVM) でパフォーマンス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、問題の原因となったボリュームを特定できます。

関連オブジェクト グリッド内の任意のオブジェクトを[比較]ペインと[カウンタ グラフ]ペインに追加できます。これにより、複数のオブジェクト同士、およびルート オブジェクトとの間でデータを表示して比較できます。関連オブジェクト グリッドにオブジェクトを追加したり、グリッドからオブジェクトを削除したりできますが、比較ペインのルート オブジェクトは削除できません。



比較ペインに多数のオブジェクトを追加すると、パフォーマンスに悪影響を与える可能性があります。パフォーマンスを維持するには、データ比較用チャートを何個も選択しないでください。

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見つけて、[追加] ボタンをクリックします。

追加 ボタンが灰色に変わり、オブジェクトが比較ペインの追加オブジェクト リストに追加されます。オブジェクトのデータは、カウンター チャート 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非表示または表示します。

作業	対処方法
選択したオブジェクトを非表示にする	選択したオブジェクトの目のアイコン () を比較ペインで選択します。オブジェクトのデータが非表示になり、そのオブジェクトの目のアイコンがグレーに変わります。

作業	対処方法
非表示のオブジェクトを表示する	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。 目のアイコンは元の色に戻り、オブジェクト データが [カウンター チャート] ペインのグラフに再度追加されます。

3. オプション: 選択したオブジェクトを 比較 ペインから削除します。

作業	対処方法
選択したオブジェクトを1つ削除する	比較ペインで選択したオブジェクトの名前にマウスを移動してオブジェクトの削除ボタン (X) を表示し、ボタンをクリックします。オブジェクトは比較ペインから削除され、そのデータはカウンター チャートからクリアされます。
選択したオブジェクトをすべて削除する	比較ペインの上部にあるすべてのオブジェクトの削除ボタン (X) をクリックします。選択したすべてのオブジェクトとそのデータが削除され、ルート オブジェクトだけが残ります。

カウンターチャートを理解する

カウンター チャート ペインのチャートを使用すると、ルート オブジェクトと相関オブジェクト 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。パフォーマンスの傾向を把握して、パフォーマンスの問題を特定および解決するのに便利です。

デフォルトで表示されるカウンター チャートは、イベント、レイテンシ、IOPS、MBps です。表示を選択できるオプションのチャートは、使用率、パフォーマンス使用容量、使用可能な IOPS、IOPS/TB、キャッシュミス率です。さらに、レイテンシ、IOPS、MBps、使用済みパフォーマンス容量のグラフの合計値または内訳値を表示するように選択できます。

パフォーマンス エクスプローラーには、ストレージ オブジェクトがすべてのカウンター チャートをサポートしているかどうかに関係なく、デフォルトで特定のカウンター チャートが表示されます。カウンターがサポートされていない場合、カウンターチャートは空になり、メッセージが表示されます。`Not applicable for <object>` が表示されます。

グラフには、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傾向が表示されます。各グラフには次のようにデータが表示されます。

- **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。

トレンド ラインの色は、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。ラインの特定のポイントにカーソルを合わせると、そのポイントの時間と値の詳細を表示できます。

チャート内の特定の期間について調査するには、次のいずれかを実行します。

- ・ < ボタンを使用して、カウンター チャート ペインをページの幅全体に拡張します。
- ・ カーソルを使用して（虫眼鏡に変わる）チャート内の一部の期間を選択し、拡大する。[グラフのズームをリセット]をクリックすると、グラフをデフォルトの期間に戻すことができます。
- ・ ズーム表示 ボタンを使用すると、拡大された詳細としきい値インジケーターを含む大きな単一カウンターチャートが表示されます。



ラインが連続しておらず、切れ目が表示されることがあります。ギャップは、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 がダウンしている可能性があることを意味します。

パフォーマンス カウンタ グラフのタイプ

標準のパフォーマンス グラフには、選択したストレージ オブジェクトのカウンタの値が表示されます。内訳カウンタ グラフには、合計値が読み取り、書き込み、およびその他のカテゴリに分けて表示されます。さらに、一部の内訳カウンタ グラフには、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）。

次の表は、使用可能なパフォーマンス カウンタ グラフを示しています。

利用可能なチャート	チャートの説明
イベント	ルート オブジェクトの統計グラフに関連し、重大、エラー、警告、情報のイベントが表示されます。パフォーマンス イベントに加えて健全性イベントも表示されるため、パフォーマンスに影響する可能性がある原因を総合的に確認できます。
レイテンシ - 合計	アプリケーションの要求に応答するまでのミリ秒数。平均レイテンシの値は、I/Oの重み付きの値です。
レイテンシ - 内訳	[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。このチャート オプションは、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、または名前空間である場合にのみ適用されます。

利用可能なチャート	チャートの説明
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 コンポーネントごと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、「合計」を選択すると、ローカル ノードまたはリモート ノードに存在する可能性のある、このノードを通過するデータの IOPS が表示され、「合計 (ローカル)」を選択すると、現在のノードにのみ存在するデータの IOPS が表示されます。
IOPS - 内訳	[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。このチャート オプションは、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、または名前空間である場合にのみ適用されます。 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)。 ノードに対して表示される場合、「Breakdown」を選択すると、ローカル ノードまたはリモート ノードに存在する可能性のある、このノードを通過するデータの IOPS の内訳が表示され、「Breakdown (Local)」を選択すると、現在のノードにのみ存在するデータの IOPS の内訳が表示されます。
IOPS - プロトコル	[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。このチャート オプションは、選択したオブジェクトが SVM の場合にのみ適用されます。
IOPS/TB - 合計	ワークロードで消費される合計スペース (TB) に基づく、1秒間に処理される入出力処理数。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可能なパフォーマンスを示します。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 / ピーク 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)。 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。

利用可能なチャート	チャートの説明
MBps - 合計	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)
MBps - 内訳	[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)。 このチャート オプションは、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、または名前空間である場合にのみ適用されます。  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ノードについてのみ表示されます。
使用済みパフォーマンス容量 - 合計	ノードまたはアグリゲートによるパフォーマンス容量の消費率。
使用済みパフォーマンス容量 - 内訳	使用済みパフォーマンス容量。ユーザ プロトコルおよびシステムのバックグラウンド プロセスに分けて表示されます。また、空きパフォーマンス容量が表示されます。
使用可能な IOPS - 合計	このオブジェクトで現在使用可能な (空き) 1秒あたりの入出力処理数。この数値は、Unified Manager がオブジェクトが実行できると計算した合計 IOPS から現在使用されている IOPS を差し引いた結果です。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。
使用状況 - 合計	オブジェクトの使用可能なリソースの利用率。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)、および帯域幅の利用率 (ポートの場合) を示します。このグラフは、選択したオブジェクトがノード、アグリゲート、またはポートの場合にのみ表示されます。
キャッシュ ミス率 - 合計	クライアント アプリケーションからの読み取り要求に対してキャッシュからではなくディスクからデータが返される割合。このグラフは、選択したオブジェクトがボリュームの場合にのみ表示されます。

表示するパフォーマンスチャートを選択

[グラフを選択]ドロップダウン リストを使用して、[カウンタ グラフ]ペインに表示するパフォーマンス カウンタ グラフのタイプを選択できます。パフォーマンス要件に基づいて、特定のデータやカウンタを表示できます。

手順

1. カウンター チャート ペインで、チャートの選択 ドロップダウン リストをクリックします。
2. チャートを追加または削除します。

目的	操作
チャートを個別に追加または削除する	表示または非表示にするチャートの横のチェックボックスをオンにします。
すべてのチャートを追加する	*すべて選択*をクリックします
すべてのチャートを削除する	*すべて選択解除*をクリック

選択したチャートは、「カウンター チャート」ペインに表示されます。グラフを追加すると、追加したグラフが[グラフを選択]ドロップダウン リストと同じ順番で[カウンタ グラフ]ペインに挿入されます。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。

カウンターチャートペインを展開する

カウンター チャート ペインを展開すると、チャートが大きくなって読みやすくなります。

比較オブジェクトとカウンターの時間範囲を定義したら、より大きなカウンター チャート ペインを表示できます。ペインを展開するには、パフォーマンス エクスプローラー ウィンドウの中央にある < ボタンを使用します。

手順

1. カウンター チャート ペインを拡大または縮小します。

目的	操作
カウンターチャートペインをページの幅に合わせて拡大します	< ボタンをクリックしてください
カウンターチャートペインをページの右半分に縮小します	> ボタンをクリックしてください

カウンターチャートの焦点をより短い期間に変更します

[カウンタ グラフ]ペインや[カウンタ グラフ ズーム ビュー]ウィンドウでは、マウスを使

用して期間を短くすることで、特定の期間に絞って情報を表示できます。これにより、タイムラインの任意の部分について、パフォーマンス データ、イベント、およびしきい値をより細かく確認することができます。

開始する前に

この機能がアクティブになっているときは、カーソルが虫眼鏡に変わります。



この機能を使用すると、タイムラインがより詳細な表示に対応する値を表示するようになりますが、*時間範囲*セクターの時間と日付の範囲は、グラフの元の値から変更されません。

手順

1. 特定の期間を拡大して表示するには、虫眼鏡を使用してクリックしてドラッグし、詳細を表示する部分を囲みます。

選択した期間のカウンタの値が、カウンタ チャートに拡大して表示されます。

2. *時間範囲*セクターで設定された元の期間に戻すには、*チャートのズームをリセット*ボタンをクリックします。

カウンタ チャートの表示が元の状態に戻ります。

イベントタイムラインでイベントの詳細を表示する

[パフォーマンス エクスプローラ]の[イベント タイムライン]ペインでは、すべてのイベントと関連する詳細を表示できます。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しきい値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、選択した時間範囲内にルート オブジェクトで発生した重大なイベント、エラー イベント、警告イベント、および情報イベントが表示されます。イベントの重大度ごとに独自のタイムラインがあり、単一または複数イベントがタイムライン上に点で表されます。イベントを示す点にカーソルを合わせると、イベントの詳細を確認できます。複数イベントについてより詳細に表示するには、期間を縮小します。複数イベントが複数の単一のイベントとして表示されるため、各イベントを個々に表示して確認することができます。

イベント タイムライン上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ー チャートのトレンド ラインの対応するスパイクと垂直に並びます。イベントと全体的なパフォーマンスの間に直接的な相関関係があることを確認できます。健全性イベントもタイムラインに表示されますが、これらのタイプのイベントはいずれかのパフォーマンス グラフのイベントが急増しているポイントと揃うとはかぎりません。

手順

1. イベント タイムライン ペインで、タイムライン上のイベント ドットの上にカーソルを置くと、そのイベント ポイントにおけるイベントの概要が表示されます。

イベント タイプ、イベントが発生した日時、状態、イベントの期間に関する情報がポップアップ ダイアログに表示されます。

2. 1つまたは複数のイベントの詳細を表示します。

作業	これをクリックしてください...
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します。
複数イベントの詳細を表示する	 複数のイベント ダイアログで 1 つのイベントをクリックすると、適切なイベントの詳細ページが表示されます。

カウンタ グラフ ズーム ビュー

カウンター チャートには、指定した期間のパフォーマンスの詳細を拡大表示できるズーム ビューが用意されています。これによりパフォーマンスの詳細やイベントをより細かく確認できるため、パフォーマンスの問題のトラブルシューティングを行うときに便利です。

ズーム ビューで表示した場合、一部の内訳グラフでは、ズーム ビュー以外では表示されない追加の情報が表示されます。たとえば、IOPS、IOPS/TB、およびMBpsの内訳グラフのズーム ビュー ページには、ONTAPで設定されている場合、ボリュームおよびLUNのQoSポリシーの値が表示されます。



システム定義のパフォーマンスしきい値ポリシーの場合、ポリシー リストからは「ノード リソース過剰使用」および「QoS スループット制限違反」ポリシーのみを使用できます。システム定義の他のしきい値ポリシーは、現時点では利用できません。

カウンターチャートのズームビューを表示する

カウンタ グラフ ズーム ビューには、選択したカウンタ グラフのより詳細な情報と関連するタイムラインが表示されます。カウンタ グラフのデータが拡大して表示され、パフォーマンス イベントやその原因を詳しく調べることができます。

カウンタ グラフ ズーム ビューは、どのカウンタ グラフについても表示できます。

手順

1. *ズーム表示*をクリックすると、選択したグラフが新しいブラウザ ウィンドウで開きます。
2. 内訳チャートを表示しているときに「ズーム表示」をクリックすると、内訳チャートがズーム表示で表示されます。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。

ズームビューで時間範囲を指定する

カウンター チャートのズーム 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、選択したチャートの日付と時刻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 日までの時間範囲を選択できます。1カ月は30日としてカウントされるため、390日は13カ月に相当します。日時の範囲を指定することで、特定のパフォーマンス イベントや一連のイベントにフォーカスして詳細を確認することができます。また、日時の範囲を指定すると、パフォーマンス イベントに関連するデータがより詳しく表示されるため、潜在的なパフォーマンスの問題のトラブルシューティングにも役立ちます。時間範囲 コントロールを使用して、定義済みの日付と時刻の範囲を選択するか、最大 390 日間の独自のカスタム日付と時刻の範囲を指定します。事前定義された時間範囲のボタンは、「過去 1 時間」から「過去 13 か月」までさまざまです。

過去 13 か月 オプションを選択するか、30 日を超えるカスタム日付範囲を指定すると、30 日を超える期間のパフォーマンス データは 5 分ごとのデータ ポーリングではなく 1 時間ごとの平均を使用してグラフ化されることを警告するダイアログ 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 [今後表示しない] オプションをクリックすると、[過去 13 か月] オプションを選択したり、30 日を超えるカスタム日付範囲を指定したりしても、メッセージは表示されません。時間範囲に今日から 30 日を超える時間/日付が含まれる場合、要約データはより短い時間範囲にも適用されます。

時間範囲 (カスタムまたは定義済み) を選択する場合、30 日以下の時間範囲は 5 分間隔のデータ サンプルに基づきます。30日を超える場合は、1時間ごとのデータ サンプルに基づいてデータが表示されます。

The screenshot displays the time range selection interface. It consists of two calendar panels, 'From' and 'To', both for April 2015. The 'From' calendar has the 12th selected, and the 'To' calendar has the 15th selected. Below the calendars are time dropdown menus set to 6:00 am. To the right is a list of predefined time ranges: Last Hour, Last 24 Hours, Last 72 Hours, Last 7 Days, Last 30 Days, Last 13 Months, and Custom Range. The 'Custom Range' button is highlighted. At the bottom right are 'Cancel' and 'Apply Range' buttons.

1. *時間範囲*ドロップダウン ボックスをクリックすると、時間範囲パネルが表示されます。
2. 定義済みの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場合、最大で13カ月分のデータを利用できます。選択した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刻フィールドに表示されます。
3. カスタムの日付範囲を選択するには、左側の「開始」カレンダーで開始日をクリックします。カレンダー内を前方または後方に移動するには、< または > をクリックします。終了日を指定するには、右側の「終了」カレンダーで日付をクリックします。終了日は、別の日付を指定しないかぎり、デフォルトでは現在の日付になります。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、カスタム日付範囲を選択したことが示されます。
4. カスタムの時間範囲を選択するには、[開始] カレンダーの下の [時間] コントロールをクリックし、開始時刻を選択します。終了時刻を指定するには、右側の 終了 カレンダーの下の 時間 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、カスタム時間範囲を選択したことが示されます。
5. 事前定義された日付範囲を選択し、開始時間と終了時間を指定することもできます。前述の説明に従って事前定義された日付範囲を選択したあと、上記と同じ方法で開始時間と終了時間を選択します。選択した日付は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は 時間 コントロールに表示され、カスタム範囲 ボタンが強調表示されます。

6. 日付と時刻の範囲を選択した後、「範囲を適用」をクリックします。グラフと[イベント]タイムラインに、その期間のパフォーマンス統計が表示されます。

カウンターチャートのズームビューでパフォーマンスしきい値を選択する

カウンタ グラフ ズーム ビューでしきい値を適用すると、該当するパフォーマンスしきい値イベントに関する詳細が表示されます。しきい値を適用または削除してすぐに結果を表示でき、トラブルシューティングが必要かどうかを判断する際に役立ちます。

カウンタ グラフ ズーム ビューでしきい値を選択すると、パフォーマンスしきい値イベントに関する正確なデータを確認できます。カウンター チャートのズーム ビューの ポリシー 領域の下に表示される任意のしきい値を適用できます。

カウンタ グラフ ズーム ビューでは、オブジェクトに一度に1つずつポリシーを適用できます。

手順

1. 選択または選択解除  ポリシーに関連付けられているもの。

選択したしきい値がカウンタ グラフ ズーム ビューに適用されます。重大なしきい値は赤い線が表示され、警告しきい値は黄色の線が表示されます。

クラスターコンポーネント別にボリュームのレイテンシを表示する

[ボリューム パフォーマンス エクスプローラ]ページで、ボリュームのレイテンシについて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。このグラフは、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場合に便利です。

さらに、[レイテンシ - クラスター コンポーネント]グラフには、クラスター コンポーネントごとのレイテンシの詳細な比較が表示されます。これは、ボリュームでの合計レイテンシに各クラスターがどのように影響しているかを特定するのに役立ちます。以下のクラスター 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
- クラスター インターコネクト
- データ処理
- アグリゲートの処理
- ボリュームのアクティブ化
- MetroCluster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 エクスプローラー」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「クラスター コンポーネント」を選択します。

[レイテンシ - クラスター コンポーネント]グラフが表示されます。

2. グラフを拡大表示するには、[ズーム表示] を選択します。

クラスター コンポーネント別のグラフが表示されます。選択解除または選択することで比較を制限できます。 各クラスター コンポーネントに関連付けられています。

3. 特定の値を表示するには、グラフ内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。

プロトコル別に**SVM IOPS**トラフィックを表示する

[パフォーマンス / SVM エクスプローラ]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。

さらに、[IOPS - プロトコル]グラフには、SVMで使用されているプロトコルごとの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** エクスプローラー 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. グラフを拡大表示するには、[ズーム表示] を選択します。

IOPSのプロトコル別の詳細グラフが表示されます。選択解除または選択することで比較を制限できます。 プロトコルに関連付けられています。

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内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**のレイテンシチャートを表示してパフォーマンス保証を確認します

「パフォーマンス保証」プログラムに加入しているボリュームと 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。

レイテンシのパフォーマンス保証は、1処理あたりの時間（ミリ秒）で定義され、レイテンシがその値を超えないように保証するものです。値は、デフォルトの5分間のパフォーマンス収集期間ではなく、1時間あたり

の平均値です。

手順

1. パフォーマンス: すべてのボリューム ビューまたは パフォーマンス: すべての **LUN** ビューで、関心のあるボリュームまたは LUN を選択します。
2. 選択したボリュームまたは LUN の パフォーマンス エクスプローラー ページで、統計情報の表示場所 セクターから 時間平均 を選択します。

レイテンシ グラフの表示が5分間隔の収集データから1時間あたりの平均値に変わり、グラフの振れ幅が少なくなります。

3. 同じアグリゲートにパフォーマンス保証の対象となるボリュームがほかにもある場合は、それらのボリュームを追加して同じグラフでレイテンシの値を確認できます。

すべての**SAN**アレイクラスタのパフォーマンスを表示する

「パフォーマンス: すべてのクラスター」ビューを使用して、すべての SAN アレイ クラスターのパフォーマンス ステータスを表示できます。

開始する前に

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 クラスターの概要情報は [パフォーマンス: すべてのクラスター] ビューで表示でき、詳細は [クラスター/パフォーマンス エクスプローラー] ページに表示されます。

手順

1. 左側のナビゲーション ペインで、ストレージ > クラスター をクリックします。
2. *「ヘルス: すべてのクラスター」ビューに「パーソナリティ」列が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 クラスターに対して「All SAN Array」が表示されます。

3. これらのクラスター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: すべてのクラスター] 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確認します。

4. これらのクラスタのパフォーマンスに関する詳細情報を表示するには、オールSANアレイ クラスタの名前をクリックします。
5. *エクスプローラー*タブをクリックします。
6. クラスター / パフォーマンス エクスプローラー ページで、表示と比較 メニューから このクラスター上の ノード を選択します。

このクラスタの両方のノードのパフォーマンス統計を比較して、両方のノードの負荷がほぼ同じであることを確認できます。2つのノードの間に大きな差がある場合は、2つ目のノードをグラフに追加し、もっと長い期間の値を比較することで、構成の問題を特定することができます。

ローカルノードにのみ存在するワークロードに基づいてノード**IOPS**を表示する

ノードのIOPSカウンタ グラフでは、リモート ノード上のボリュームに対する読み取り / 書き込み処理を実行するために、処理がネットワークLIFを使用してローカル ノードのみを経由する箇所を特定できます。IOPS - 「合計 (ローカル)」および「内訳 (ローカル)」チャートには、現在のノード上のローカル ボリュームに存在するデータの IOPS のみが表示されます。

これらのカウンター チャートの「ローカル」バージョンは、ローカル ボリューム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。

これらのカウンター チャートの「ローカル」バージョンをこれらのカウンター チャートの通常の合計バージョンと比較すると、リモート ノード上のボリュームにアクセスするためにローカル ノードを通過するトラフィックが大量にあるかどうかを確認できます。ローカル ノードを経由してリモート ノード上のボリュームにアクセスしている処理が多すぎるとパフォーマンスの問題を引き起こすことがあり、ノードにおける高利用率として報告される可能性があります。このような場合は、ボリュームをローカル ノードに移動したり、ホストからそのボリュームにアクセスしているトラフィックを接続可能なリモート ノードにLIFを作成したりすることができます。

手順

1. 選択したノードの パフォーマンス/ノード エクスプローラー ページの IOPS チャートで、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. *ズーム表示*をクリックすると、新しいブラウザタブにグラフの拡大版が表示されます。
3. パフォーマンス/ノード エクスプローラー ページに戻り、IOPS チャートのドロップダウン 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. *ズーム表示*をクリックすると、新しいブラウザタブにグラフの拡大版が表示されます。
5. グラフを並べて表示し、IOPS値が大きく異なっている領域を特定します。
6. これらの領域にカーソルを合わせて、特定の時点におけるローカルと合計のIOPSを比較します。

[オブジェクト ランディング]ページの構成要素

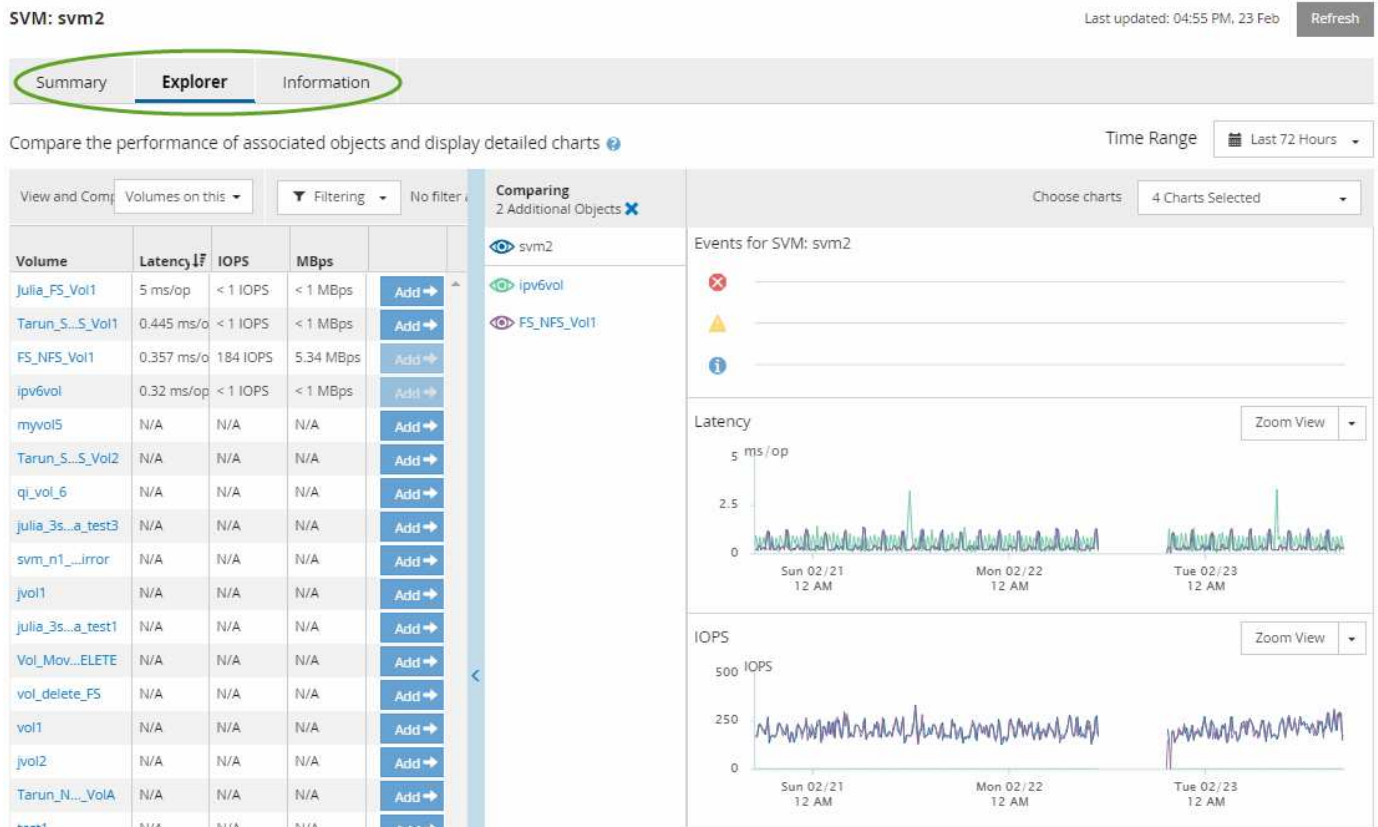
[オブジェクト ランディング]ページには、重大、警告、および情報のすべてのイベントについての詳細が表示されます。すべてのクラスタ オブジェクトのパフォーマンスの詳細が表示され、個々のオブジェクトを選択してさまざまな期間のデータを比較することができます。

[オブジェクト ランディング]ページでは、すべてのオブジェクトの全体的なパフォーマンスを確認したり、オブジェクトのパフォーマンス データを並べて表示して比較したりできます。これはパフォーマンスの評価やイベントのトラブルシューティングを行うときに便利です。



カウンタの概要パネルおよび[カウンタ グラフ]には、5分間のサンプリング間隔に基づくデータが表示されます。ページの左側にあるオブジェクトのインベントリ グリッドには、1時間のサンプリング間隔に基づくデータが表示されます。

次の図は、[エクスプローラ]の情報が表示された[オブジェクト ランディング]ページの例を示しています。



[オブジェクト ランディング]ページでは、表示するストレージ 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 データが次のタブに表示されます。

- まとめ

各オブジェクトの過去72時間のイベントやパフォーマンスを示すカウンタ グラフが3つか4つ表示されます。グラフには、その期間の高い値と低い値の傾向を示す線も表示されます。

- エクスプローラ

現在のオブジェクトに関連するストレージ オブジェクトがグリッド形式で表示され、現在のオブジェクトと関連オブジェクトのパフォーマンスの値を比較することができます。このタブには最大11個のカウンタ グラフと期間セレクトが表示され、さまざまな比較が可能です。

- 情報

ストレージ オブジェクトに関するパフォーマンス以外の構成の属性が表示されます。インストールされているONTAPソフトウェアのバージョン、HAパートナーの名前、ポートやLIFの数などが含まれます。

- パフォーマンス上位

クラスタの場合：選択したパフォーマンス カウンタに基づいて、パフォーマンスが上位または下位のスト

レージ オブジェクトが表示されます。

- フェイルオーバー計画

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に対する影響の推定値が表示されます。

- 詳細

ボリュームの場合：選択したボリュームのワークロードに対するすべてのI/Oアクティビティと処理について、詳細なパフォーマンス統計が表示されます。このタブは、FlexVol、FlexGroupボリューム、およびFlexGroupのコンスティチュエントに対して表示されます。

[サマリ]ページ

[サマリ]ページには、過去72時間を対象に、オブジェクト別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。概要ページのグラフは、「さらに詳しく調べる必要があるか?」という質問に答えます。

グラフとカウンタの統計

サマリ グラフには、過去72時間の概要が表示され、さらに調査が必要な潜在的な問題の特定に役立ちます。

[サマリ]ページのカウンタ値はグラフに表示されます。

グラフ上のラインにカーソルを合わせると、特定の時点のカウンタ値を表示できます。サマリ グラフには、以下のカウンタについて、過去72時間のアクティブな重大イベントと警告イベントの合計数も表示されます。

- レイテンシー

すべてのI/O要求の平均応答時間。処理あたりのミリ秒で表されます。

すべてのオブジェクト タイプについて表示されます。

- IOPS

平均処理速度。1秒あたりの入出力処理数で表されます。

すべてのオブジェクト タイプについて表示されます。

- MB/秒

平均スループット。1秒あたりのメガバイト数で表されます。

すべてのオブジェクト タイプについて表示されます。

- 使用される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平均消費率。

ノードとアグリゲートについてのみ表示されます。

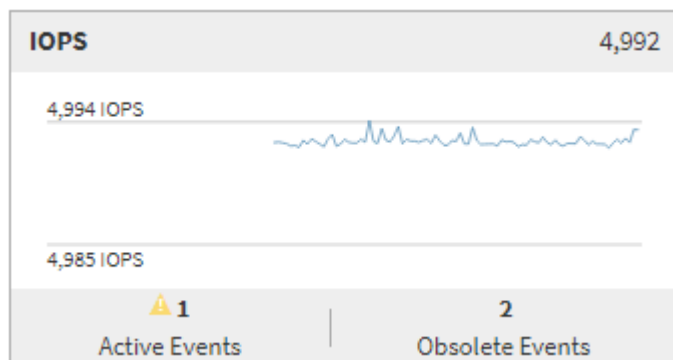
- 利用

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件数にカーソルを合わせると、各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。

グラフ右上のグレーのバーに表示される数字は、過去72時間の平均値です。トレンド グラフの上下に表示される数字は、過去72時間の最大値と最小値です。グラフ下のグレーのバーには、過去72時間のアクティブなイベント（新規および確認済みのイベント）と廃止イベントの件数が表示されます。



- レイテンシーカウンターチャート

[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。レイテンシは、すべてのI/O要求の平均応答時間（処理あたりのミリ秒）を表し、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処理時間、待機時間、またはその両方が考慮されます。

上部 (カウンター値): ヘッダーの数字は、過去 72 時間の平均を表示します。

中央 (パフォーマンス グラフ): グラフの下部の数字は最低のレイテンシを示し、グラフの上部の数字は過去 72 時間の最高レイテンシを示します。グラフ上のラインにカーソルを合わせると、その時点のレイテンシの値が表示されます。

下部 (イベント): マウスをホバーすると、ポップアップにイベントの詳細が表示されます。グラフの下の「アクティブ イベント」リンクをクリックすると、「イベント インベントリ」ページに移動し、完全なイベントの詳細が表示されます。

- IOPSカウンターチャート

[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 システムの処理速度（1秒あたりのI/O処理数）を示します。

上部 (カウンター値): ヘッダーの数字は、過去 72 時間の平均を表示します。

中央 (パフォーマンス グラフ): グラフの下部の数字は最低 IOPS を示し、グラフの上部の数字は過去 72 時間の最高 IOPS を示します。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。

下部 (イベント): マウスをホバーすると、ポップアップにイベントの詳細が表示されます。グラフの下の「アクティブ イベント」リンクをクリックすると、「イベント インベントリ」ページに移動し、完全なイベントの詳細が表示されます。

- **MB/sカウンターチャート**

[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。これは、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。

上部 (カウンター値): ヘッダーの数字は、過去 72 時間の平均 MB/秒数を表示します。

中央 (パフォーマンス グラフ): グラフの下部の値は最低 MB/秒数を示し、グラフの上部の値は過去 72 時間の最高 MB/秒数を示します。グラフ上のラインにカーソルを合わせると、その時点のMBpsの値が表示されます。

下部 (イベント): マウスをホバーすると、ポップアップにイベントの詳細が表示されます。グラフの下の「アクティブ イベント」リンクをクリックすると、「イベント インベントリ」ページに移動し、完全なイベントの詳細が表示されます。

- **パフォーマンス使用容量カウンターチャート**

[使用済みパフォーマンス容量]カウンタのグラフには、オブジェクトが消費しているパフォーマンス容量の割合が表示されます。

上部 (カウンター値): ヘッダーの数字は、過去 72 時間の平均使用パフォーマンス容量を示します。

中央 (パフォーマンス グラフ): グラフの下部の値は、過去 72 時間の期間における最低の使用済みパフォーマンス容量のパーセンテージを示し、グラフの上部の値は、最高の使用済みパフォーマンス容量のパーセンテージを示します。グラフ上のラインにカーソルを合わせると、その時点のパフォーマンス容量使用率の値が表示されます。

下部 (イベント): マウスをホバーすると、ポップアップにイベントの詳細が表示されます。グラフの下の「アクティブ イベント」リンクをクリックすると、「イベント インベントリ」ページに移動し、完全なイベントの詳細が表示されます。

- **利用率カウンターチャート**

[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。

上位 (カウンター値): ヘッダーの数字は、過去 72 時間の平均使用率を示します。

中央 (パフォーマンス グラフ): グラフの下部の値は最低使用率を示し、グラフの上部の値は過去 72 時間の最高使用率を示します。グラフ上のラインにカーソルを合わせると、その時点の利用率の値が表示されます。

下部 (イベント): マウスをホバーすると、ポップアップにイベントの詳細が表示されます。グラフの下の「アクティブ イベント」リンクをクリックすると、「イベント インベントリ」ページに移動し、完全なイベントの詳細が表示されます。

イベント

該当する場合、イベント履歴テーブルに、そのオブジェクトで発生した最近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]ページの構成要素

[パフォーマンス エクスプローラ]ページを使用すると、クラスタに含まれる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することができます。これは、パフォーマンス イベントのトラブルシューティングやオブジェクトのパフォーマンスの微調整を行う際に便利です。各オブジェクトを他のオブジェクトとの比較でベースラインとなるルート オブジェクトと比較することもできます。

ヘルス ビューに切り替える ボタンをクリックすると、このオブジェクトのヘルス詳細ページが表示されます。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 エクスプローラー ページには、クラスター 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。このページでは、同じタイプのすべてのクラスター オブジェクト（ボリュームとそのオブジェクト固有のパフォーマンス統計など）が表形式で表示されます。このビューで、クラスター オブジェクトのパフォーマンスの概要を効率的に確認することができます。



表のいずれかのセルに「N/A」が表示される場合、現時点でそのオブジェクトに I/O がないため、そのカウンター値は利用できないことを意味します。

パフォーマンス エクスプローラー ページには、次のコンポーネントが含まれています。

- 時間範囲

オブジェクト データの期間を選択できます。

事前定義の範囲を選択できるほか、カスタムの期間を独自に指定することもできます。

- 表示して比較

グリッドに表示する関連オブジェクトのタイプを選択できます。

使用可能なオプションは、ルート オブジェクトのタイプと利用可能なデータによって異なります。「表示と比較」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のタイプがリストに表示されます。

- フィルタリング

受け取るデータの量を設定に基づいて絞り込むことができます。

IOPSが4を超えるオブジェクトに限定するなど、オブジェクト データに適用するフィルタを作成することができます。フィルタは最大で4つまで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対象として選択したオブジェクトのリストが表示されます。

比較ペイン内のオブジェクトのデータは、カウンター チャートに表示されます。

- 統計情報を表示

ボリュームおよびLUNの統計を各収集サイクル（デフォルトは5分）後に表示するか、または1時間あたりの平均として表示するかを選択できます。この機能を使用して、NetApp「パフォーマンス保証プログラム」の状況を確認するためにレイテンシ グラフを表示することができます。

- カウンターチャート

オブジェクトのパフォーマンスのカテゴリ別にグラフ形式のデータが表示されます。

通常、デフォルトではグラフが3つか4つのみ表示されます。グラフの選択コンポーネントを使用すると、追加のグラフを表示したり、特定のグラフを非表示にしたりできます。イベント タイムラインを表示するか非表示にするかを選択することもできます。

- イベントタイムライン

時間範囲コンポーネントで選択したタイムライン全体で発生するパフォーマンス イベントとヘルス イベントを表示します。

QoSポリシーグループ情報を使用してパフォーマンスを管理する

Unified Manager を使用すると、監視対象のすべてのクラスタで使用可能なサービス品質 (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) を使用して、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たものです。Unified Manager では、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、以下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）、あるいは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す。

「従来の」 QoS ポリシー グループは、単一のボリュームまたは LUN などの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、そのワークロードがスループットを上限まで使用できます。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。その場合、スループット制限はワークロード間で「共有」されます。たとえば、3つのワークロードに9,000 IOPSのQoS制限を割り当てた場合、IOPSの合計が9,000 IOPSを超えないように制限されます。

「Adaptive」 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 サイズを指定できます。これにより、ワークロードが非常に大きなブロック サイズを使用していて、その結果スループットの大半を使用しているケースでは、ポリシーのしきい値がIOPS/TBからMBpsに変換されます。

グループでQoSポリシーを共有している場合、ポリシー グループ内のすべてのワークロードのIOPSまたはMBpsが設定された上限を超えると、ワークロードが調整されてそのアクティビティが制限されます。その結果、ポリシー グループ内の全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係するポリシー 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] ビューでは、影響を受けたボリュームを IOPS と MB/秒で並べ替えて、イベントの原因となった可能性のある使用率が最も高いワークロードを確認できます。[パフォーマンス/ボリューム エクスプローラー] ページで、他のボリュームまたはボリューム上の LUN を選択して、影響を受けるワークロードの IOPS または MBps スループット使用量と比較できます。

ノード リソースを過剰に消費しているワークロードは、より制限の厳しいポリシー グループに割り当てます。これにより、ポリシー グループによる調整でワークロードのアクティビティが制限されて、そのノードでのリソースの使用が削減されます。一方、ワークロードで使用できるノードのリソースを増やす場合は、ポリシー グループの値を大きくすることができます。

System Manager、ONTAPコマンド、またはUnified Managerのパフォーマンス サービス レベルを使用してポリシー グループを管理できます。これには次のタスクが含まれます。

- ポリシー グループの作成
- 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利用可能なすべての **QoS** ポリシー グループを表示します

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、ストレージ > **QoS** ポリシー グループ をクリックします。

デフォルトでは、「パフォーマンス: 従来の QoS ポリシー グループ」ビューが表示されます。

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。

- 展開ボタン (▼ QoS ポリシー グループ名の横にあるアイコン ()) をクリックすると、ポリシー グループの詳細が表示されます。
- [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を表示する

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およびLUNのリストを表示できます。

複数のボリューム間で「共有」されている従来の QoS ポリシー グループの場合、これは、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を過剰に使用しているかどうかを確認するのに役立ちます。また、他のボリュームに悪影響を及ぼすことなくポリシー グループにボリュームを追加できるかどうかを判断することもできます。

アダプティブQoSポリシーとUnified Managerのパフォーマンス サービス レベル ポリシーでは、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

- 左側のナビゲーション ペインで、ストレージ > **QoS** ポリシー グループ をクリックします。

デフォルトでは、「パフォーマンス: 従来の QoS ポリシー グループ」ビューが表示されます。

- 従来のポリシー グループを対象とする場合は、このページを表示したままにします。それ以外の場合は、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。
- 関心のあるQoSポリシーで、展開ボタン (▼ QoS ポリシー グループ名の横にあるアイコン ()) をクリックすると、詳細が表示されます。

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 ⚙️

Schedule Report ⬇️ ⚙️								
QoS Policy Group	Cluster	SVM	Min Through...	Max Through...	Absolute Min...	Block Size	Asso	
▼ julia_vs2_cifs_Performance	opm-simplicity	julia_vs2_cifs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		1	▲
▲ julia_vs1_nfs_Performance	opm-simplicity	julia_vs1_nfs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		2	
Details Allocated Capacity 0.99 TB 1.15 TB Associated Objects 2 Volumes 0 LUNs Events None								
▼ julia_nfs_extreme_Extreme_Performance	ocum-mobility-01-02	julia_nfs_extreme	6144.0 IOPS/TB	12288.0 IOPS/TB	1000IOPS	any	1	
▼ julia_extreme_jan16_aqos	ocum-mobility-01-02	julia_nfs_extreme	10000.0 IOPS/TB	12000.0 IOPS/TB	1000IOPS	any	1	

- [ボリューム]リンクまたは[LUN]リンクをクリックして、このQoSポリシーを使用しているオブジェクトを表示します。

ボリュームまたはLUNの[パフォーマンス]インベントリ ページに、QoSポリシーを使用しているオブジェクトのリストが表示されます。

特定のボリュームまたはLUNに適用されたQoSポリシーグループ設定を表示する

ボリュームおよび LUN に適用されている QoS ポリシー グループを表示できます。また、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 ポリシーの詳細な構成設定を表示できます。

ボリュームに適用された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、ストレージ > ボリューム をクリックします。

デフォルトでは、「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て、**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. 展開ボタン (▼ QoS ポリシー グループ名の横にあるアイコン ()) をクリックすると、ポリシー グループの詳細が表示されます。

パフォーマンス チャートを表示して、同じ **QoS** ポリシー グループ内のボリュームまたは **LUN** を比較します。

同じQoSポリシー グループ内のボリュームとLUNを表示し、1つの[IOPS]、[MBps]、または[IOPS/TB]グラフ上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、ストレージ > ボリューム をクリックします。

デフォルトでは、「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. [表示と比較] メニューで、[同じ QoS ポリシー グループ内のボリューム] を選択します。

同じQoSポリシーを共有する他のボリュームが下のテーブルに表示されます。

5. 追加 ボタンをクリックしてこれらのボリュームをチャートに追加し、チャートで選択したすべてのボリュームの IOPS、MB/秒、IOPS/TB、およびその他のパフォーマンス カウンター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]と[ワークロード分析]のIOPS、IOPS/TB、およびMBpsの各グラフで、ボリュームやLUNに適用されているONTAP定義のサービス品質（QoS）ポリシーの設定を確認することができます。グラフに表示される情報は、ワークロードに適用されているQoSポリシーのタイプによって異なります。

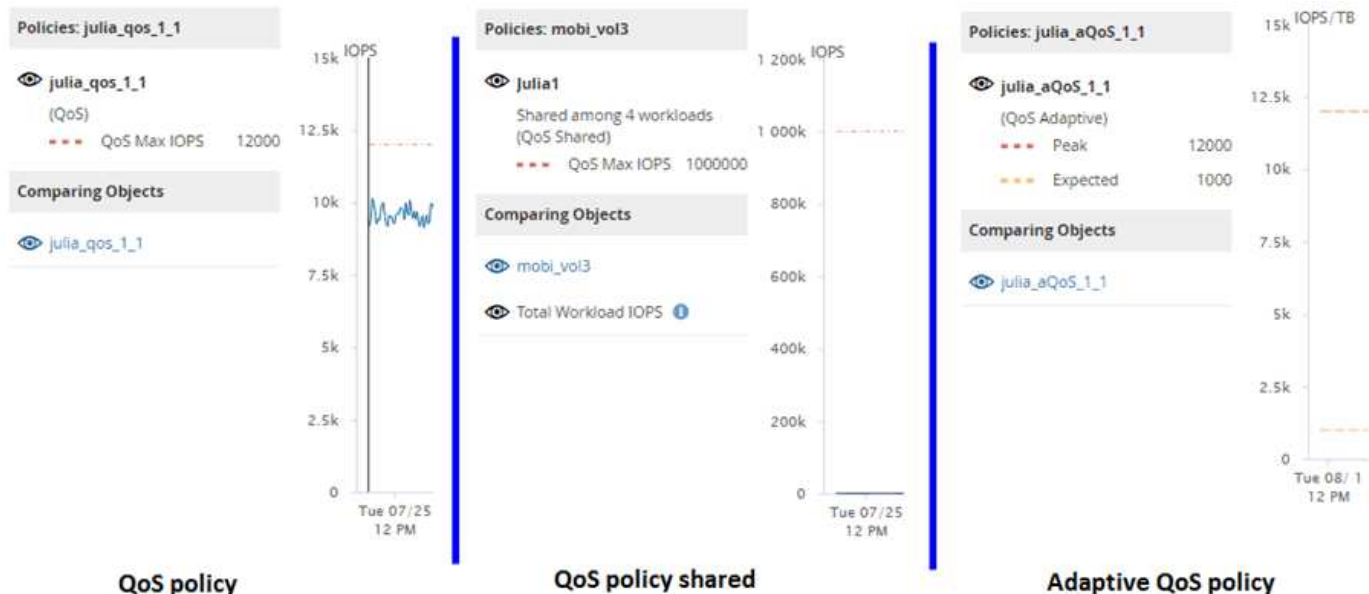
スループットの最大値（または「ピーク」）設定は、ワークロードが消費できる最大スループットを定義し、それによってシステム リソースをめぐる競合するワークロードへの影響を制限します。スループットの最小値（または「期待値」）設定は、競合するワークロードの需要に関係なく、重要なワークロードが最小スループット目標を満たすように、ワークロードで使用可能である必要がある最小スループットを定義します。

IOPS および MB/秒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下限と上限を定義します。ONTAP 9.3 で導入された IOPS/TB の適応型 QoS ポリシーでは、「予想」と「ピーク」という用語を使用して下限と上限を定義します。

ONTAPではこの2つのタイプの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通りの方法でQoSポリシーが表示されます。

ポリシーの種類	機能	Unified Managerインターフェースのインジケーター
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が共有	「(QoS 共有)」と表示されます
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 Adaptive)」と表示されます

次の図は、カウンタ グラフでの3通りの表示方法の例を示したものです。



IOPS で定義された通常の 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、IOPS で定義されています」というテキストとともに表示します。

IOPS/TB で定義されたアダプティブ QoS ポリシーがワークロードの IOPS チャートに表示されると、ONTAP は IOPS/TB 値を IOPS 値に変換し、Unified Manager は、ピーク IOPS 割り当て設定の構成に応じて、そのポリシーを「QoS アダプティブ - 使用済み、IOPS/TB で定義」または「QoS アダプティブ - 割り当て済み、IOPS/TB で定義」というテキストとともに IOPS チャートに表示します。割り当て設定が「allocated-space」に設定されている場合、ピーク IOPS はボリュームのサイズに基づいて計算されます。割り当て設定が「used-space」に設定されている場合、ピーク IOPS は、ストレージ効率を考慮して、ボリュームに保存されているデータの量に基づいて計算されます。



[[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以上のときだけです。選択した期間に使用済み容量が128GBを下回る期間がある場合、その間のデータはグラフに表示されません。

パフォーマンス エクスプローラーでワークロード **QoS** の最小および最大設定を表示します。

パフォーマンス エクスプローラー チャートで、ボリュームまたは LUN 上の ONTAP 定義のサービス品質 (QoS) ポリシー設定を表示できます。最大スループット設定は、競合するワークロードによるシステム リソースへの影響を抑制するために使用されます。最小スループット設定は、競合するワークロードによる要求に関係なく、重要なワークロードに最小限のスループットを確保するために使用されます。

QoS スループットの「最小」および「最大」IOPS と MB/s 設定は、ONTAP で設定されている場合にのみカウンター チャートに表示されます。最小スループット設定は、ONTAP 9.2以降のソフトウェアを実行しているシステムでのみ使用できます。対象は AFF システムのみで、現時点では IOPS についてのみ設定できます。

アダプティブ QoS ポリシーは ONTAP 9.3以降で使用できる機能で、IOPS の代わりに IOPS/TB が使用されます。アダプティブ ポリシーは、QoS ポリシーの値をワークロードごとにボリューム サイズに基づいて自動的に調整し、ボリューム サイズが変わっても容量に対する IOPS の比率を維持します。アダプティブ QoS ポリシーグループはボリュームにのみ適用できます。適応型 QoS ポリシーでは、最小値と最大値の代わりに、QoS

用語の「期待値」と「ピーク」が使用されます。

Unified Manager は、過去 1 時間の各パフォーマンス収集期間中にワークロード スループットが定義された QoS 最大ポリシー設定を超えた場合に、QoS ポリシー違反の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は、各収集期間中に短時間のみ QoS しきい値を超えることがあります。Unified Manager は収集期間中の「平均」スループットをグラフに表示します。そのため、QoS のイベントが表示された場合でも、グラフではワークロードのスループットがポリシーのしきい値を超えていないように見ることがあります。

手順

1. 選択したボリュームまたは LUN の パフォーマンス エクスプローラー 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 合計または内訳チャートで、[ズーム表示] をクリックします。
MBpsの上限（QoS最大）を表示する	MB/s 合計または内訳チャートで、[ズーム表示] をクリックします。
IOPSの下限（QoS最小）を表示する	IOPS 合計または内訳チャートで、[ズーム表示] 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、IOPS/TB チャートで [ズーム表示] をクリックします。
IOPS/TBの下限（QoS想定）を表示する	ボリュームの場合、IOPS/TB チャートで [ズーム表示] をクリックします。

ONTAPで設定されている最大スループットと最小スループットの値が横方向の点線で示されます。QoS値に対する変更がいつ実装されたかも確認できます。

2. IOPSおよびMBpsの具体的な値をQoS設定と比較して確認するには、グラフ領域にカーソルを合わせてポップアップ ウィンドウを参照します。

特定のボリュームまたは LUN の IOPS または MB/秒が非常に高く、システム リソースに負荷がかかっていることに気付いた場合は、System Manager またはONTAP CLI を使用して QoS 設定を調整し、こ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を与えないようにすることができます。

QoS設定の調整の詳細については、以下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利用可能なIOPS情報を使用してパフォーマンスを管理する

パフォーマンス容量 は、リソースの有用なパフォーマンスを超えることなく、リソースからどれだけのスループットを得ることができるかを示します。既存のパフォーマンスカウンタを使用した場合、レイテンシの問題が発生することなく、ノードまたはアグリゲートを最大限利用可能なポイントがパフォーマンス容量です。

Unified Manager は、各クラスタ内のノードと集約からパフォーマンス容量統計を収集します。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あり、空きパフォーマンス容量 はまだ使用可能な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は、まだ使用可能なリソースの割合を示しますが、使用可能な IOPS は、最大パフォーマンス容量に達する前にリソースに追加できる IOPS の数を示します。この指標を使用すると、あらかじめ決めた数のIOPSのワークロードを安心してリソースに追加できます。

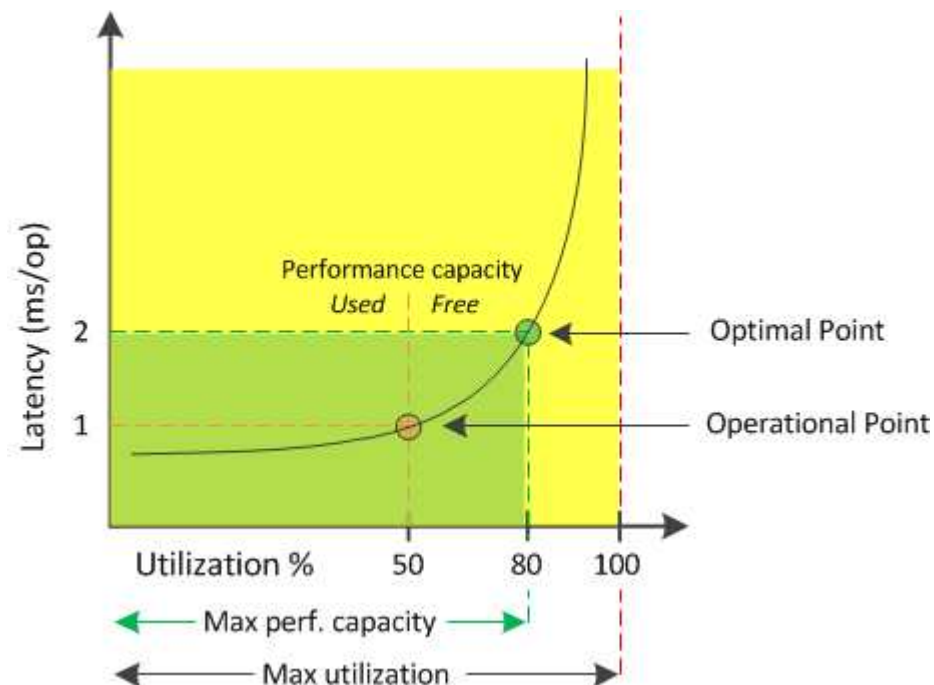
パフォーマンス容量情報を監視すると、次のような利点があります。

- ワークフローのプロビジョニングとバランシングに役立つ。
- ノードの過負荷や、ノードのリソースが最適ポイントを超えるのを回避して、トラブルシューティングの必要性を減らす。
- ストレージ機器の追加が必要なケースを正確に判断する。

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、それ以上ワークロードが増えるとパフォーマンスが低下する可能性があるポイントにノードまたはアグリゲートのパフォーマンスが達していないかどうかを特定するのに役立ちます。また、特定の期間のノードまたはアグリゲートの使用率が高すぎないかどうかを調べることもできます。使用済みパフォーマンス容量は、利用率と似ていますが、特定のワークロードに使用できる物理リソースのパフォーマンス容量に関するより詳しい情報を提供します。

ノードまたはアグリゲートの利用率とレイテンシ（応答時間）が最適で、効率的に使用されているポイントが、使用済みパフォーマンス容量の最適ポイントとなります。アグリゲートのレイテンシと利用率の関係を示す曲線の例を次の図に示します。



この例では、動作ポイントは、アグリゲートが現在 50% の使用率で動作しており、レイテンシが 1.0 ms/op 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、_最適ポイント_は、集約の使用率が 80% でレイテンシが 2.0 ms/op であるポイントとして識別されます。したがって、このアグリゲートにさらにボリュームやLUNを追加することで、システムをより効率的に使用することができます。

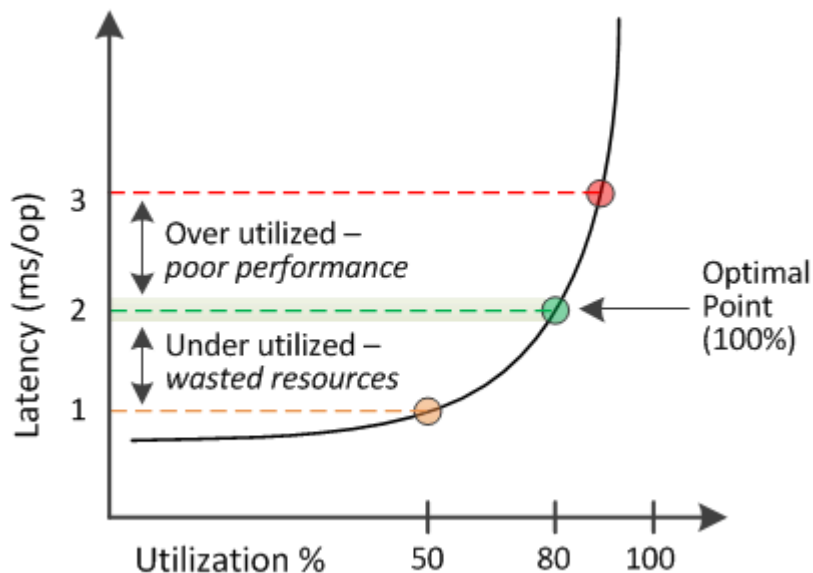
パフォーマンス容量はレイテンシに影響を与えるため、使用されたパフォーマンス容量カウンタは「utilization」カウンタよりも大きな数値になると予想されます。たとえば、ノードまたはアグリゲートの利用率が70%の場合、使用済みパフォーマンス容量の値はレイテンシの値に応じて80~100%になると想定されます。

ただし、[ダッシュボード]ページでは、利用率カウンタの値の方が大きくなる場合があります。これは、このダッシュボードには、Unified Managerのユーザ インターフェイスの他のページのような一定期間の平均値ではなく、各収集期間の最新のカウンタの値が更新されて表示されるためです。使用済みパフォーマンス容量カウンタは一定期間のパフォーマンスの平均を確認するのに適した指標であり、利用率カウンタは特定の時点でのリソースの使用状況を確認するのに適した指標です。

使用済みパフォーマンス容量の値の意味

使用済みパフォーマンス容量の値は、利用率が高い状態や低い状態のノードやアグリゲートを特定するのに役立ちます。この情報に基づいて、ストレージ リソースをより効率的に活用できるようにワークロードを再分配することができます。

次の図は、リソースのレイテンシと利用率の関係を示す曲線を示したものです。現在の運用ポイントを色付きの3つの点で示してあります。



- 使用済みパフォーマンス容量が100%の状態が最適ポイントです。

このポイントであれば、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が100%を超えている場合は、ノードまたはアグリゲートの利用率が高く、ワークロードのパフォーマンスが最適な状態ではないことを示します。

新しいワークロードをリソースに追加することは推奨されず、既存のワークロードの再分配が必要になる可能性があります。

- 使用済みパフォーマンス容量が100%未満の場合は、ノードまたはアグリゲートの利用率が低く、リソー

スが効率的に活用されていないことを示します。

リソースにワークロードをさらに追加することができます。



利用率とは異なり、使用済みパフォーマンス容量は100%を超えることがあります。この値に上限はありませんが、一般に、リソースの利用率が高いときで110~140%ほどになります。この値が大きいほど、リソースの問題が深刻であることを示します。

使用可能なIOPSとは

使用可能なIOPSカウンタは、リソースの上限に達するまでにノードまたはアグリゲートに追加できる残りのIOPSの数を示します。

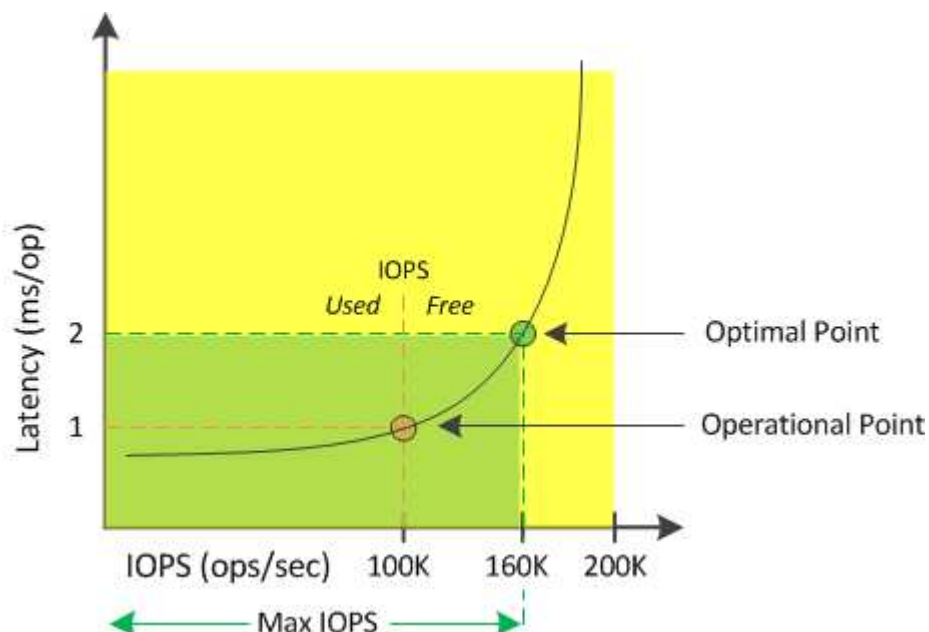
ノードで提供可能な合計IOPSは、CPUの数、CPUの速度、RAMの容量など、ノードの物理仕様に基づきます。アグリゲートで提供可能な合計IOPSは、ディスクがSATA、SAS、またはSSDのいずれであるかなど、ディスクの物理特性に基づきます。

アグリゲート内のすべてのボリュームの合計IOPSがアグリゲートの合計IOPSと一致しない場合があります。これについては、次のナレッジベースの記事で説明されています: [KB"集約内のすべてのボリューム IOP の合計が集約 IOP と一致しないのはなぜですか?"](#)

空きパフォーマンス容量カウンタは使用可能な残りのリソースの割合を示すのに対し、使用可能なIOPSカウンタは最大パフォーマンス容量に達するまでにリソースに追加できるIOPS（ワークロード）の正確な数を示します。

たとえば、FAS2520とFAS8060のストレージシステムを使用している場合、空きパフォーマンス容量の値が30%であれば、空きパフォーマンス容量がいくらか残っていることがわかります。ただし、この値からは、それらのノードに追加で導入できるワークロードの数はわかりません。使用可能なIOPSカウンタの場合は、使用可能なIOPSがFAS8060には500あり、FAS2520には100だけのように、正確な数が示されます。

ノードのレイテンシとIOPSの関係を示す曲線の例を次の図に示します。



リソースで提供可能な最大IOPSは、使用済みパフォーマンス容量カウンタが100%（最適ポイント）の時点

のIOPSの数です。運用ポイントから、このノードの現在のIOPSは100Kで、レイテンシは1.0ミリ秒/処理です。ノードからキャプチャされたUnified Managerの統計によると、このノードの最大IOPSは160Kであり、あと60KのIOPSを利用できます。したがって、このノードにさらにワークロードを追加することで、システムをより効率的に使用することができます。



ユーザ アクティビティが少ないリソースについては、一般的なワークロードを想定し、CPUコアあたりのIOPSを約4,500として使用可能なIOPSの値が計算されます。これは、配分されるワークロードの特性を正確に見積もるためのデータがUnified Managerで得られないためです。

ノードと集計パフォーマンス容量の使用値を表示する

クラスタ内のすべてのノードまたはアグリゲートの使用済みパフォーマンス容量の値、または、1つのノードあるい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 エクスプローラ]ページ、および詳細グラフに表示されます。たとえば、「パフォーマンス: すべての集計」ページには、すべての集計の使用済みパフォーマンス容量の値を表示するための「使用済みパフォーマンス容量」列があります。

Aggregates ⓘ Last updated: 04:11 PM, 08 Feb Refresh

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

Filtering No filter applied Search Aggregates Data X Search

Assign Threshold Policy Clear Threshold Policy

	Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used if	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-io...vity	opm-io...ty-01	aggr_IOPS
☐	⚠	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-io...vity	opm-io...ty-01	aggr_IOPS

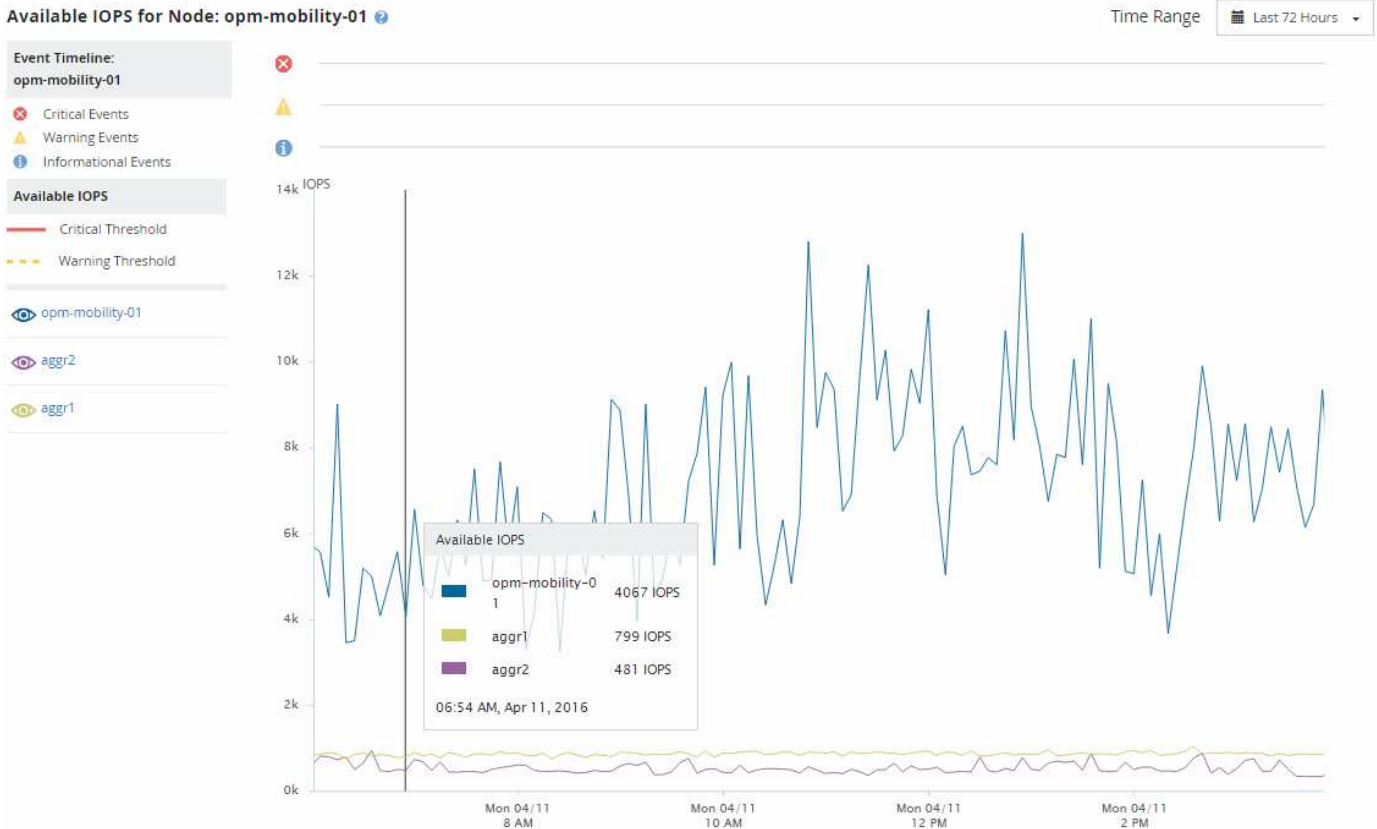
パフォーマンス使用容量カウンタを監視すると、次のことを識別できます。

- ・クラスタ上に使用済みパフォーマンス容量の値が大きいノードまたはアグリゲートがないか
- ・クラスタ上にアクティブな使用済みパフォーマンス容量のイベントが発生しているノードまたはアグリゲートがないか
- ・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における[レイテンシ]カウンタと[利用率]カウンタの値
- ・HAペアのどちらかのノードに障害が発生した場合のノードの使用済みパフォーマンス容量への影響
- ・使用済みパフォーマンス容量の値が大きいアグリゲート上の最も負荷の高いボリュームとLUN

ノードと集計の利用可能な IOPS 値を表示する

クラスタ内のすべてのノードまたはアグリゲートの使用可能なIOPSの値、または、1つのノードあるいはアグリゲートの詳細を表示できます。

使用可能なIOPSの値は、[パフォーマンス インベントリ]ページおよび[パフォーマンス エクスプローラ]ページのノードとアグリゲートのグラフに表示されます。たとえば、ノード/パフォーマンス エクスプローラ ページでノードを表示するときに、リストから「使用可能な IOPS」カウンター チャートを選択すると、ノードと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。



利用可能な IOPS カウンターを監視すると、次のことを識別できます。

- 使用可能なIOPSの値が最も大きいノードまたはアグリゲート。今後ワークロードを導入可能な場所を判断します。
- 使用可能なIOPSの値が最も小さいノードまたはアグリゲート。今後発生する可能性のあるパフォーマンスの問題について監視が必要なリソースを特定します。
- 使用可能なIOPSの値が小さいアグリゲート上の最も負荷の高いボリュームとLUN。

パフォーマンス容量カウンターチャートを表示して問題を特定します

[パフォーマンス エクスプローラ]ページには、ノードと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。

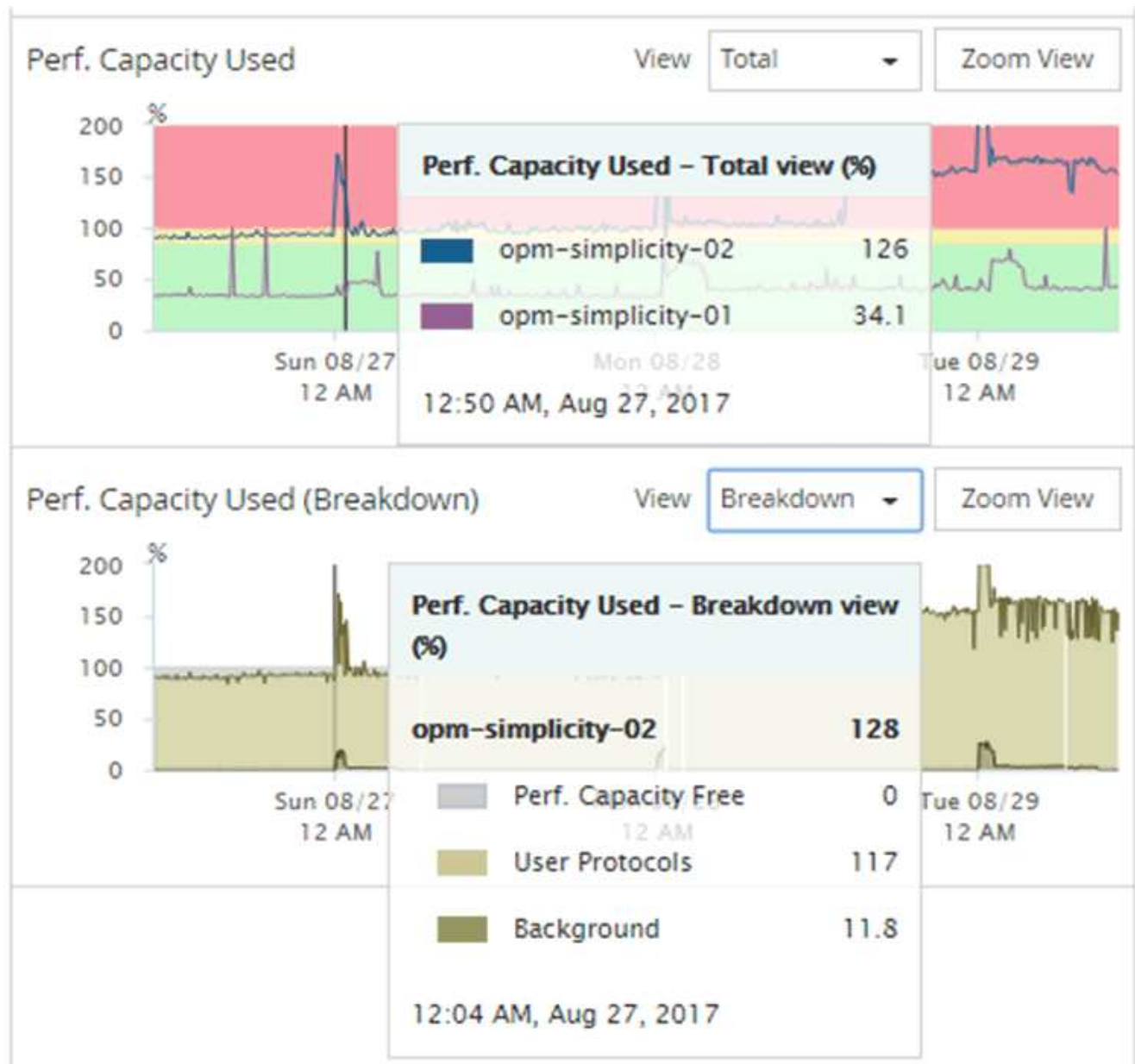


システムとデータの管理に関連する一部のバックグラウンド アクティビティはユーザ ワークロードとみなされ、ユーザ プロトコルに分類されるため、これらのプロセスの実行時にはユーザ プロトコルの割合が一時的に高く見えることがあります。通常、これらのプロセスはクラスタの使用量が少ない午前0時頃に実行されます。ユーザ プロトコルのアクティビティが午前0時頃に急増している場合は、その時間にクラスタのバックアップ ジョブまたはその他のバックグラウンド アクティビティの実行が設定されていないかどうかを確認してください。

手順

1. ノードまたは集約 ランディング ページから エクスプローラー タブを選択します。
2. カウンター チャート ペインで、チャートを選択 をクリックし、パフォーマンスを選択します。使用容量チャート。
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は黄色、利用率が低いオブジェクトは緑、利用率が高いオブジェクトは赤で表示されます。内訳グラフには、ルート オブジェクトについてのみ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形式で表示するには、[ズーム表示] 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くことで、使用済みパフォーマンス容量の値を同じ期間のIOPSまたはMBpsの値と比較できます。

使用済みパフォーマンス容量のパフォーマンスしきい値条件

ユーザ定義のパフォーマンスしきい値ポリシーを作成して、ノードまたはアグリゲートの使用済みパフォーマンス容量の値が定義されている使用済みパフォーマンス容量しきい値の設定を超えたときにイベントがトリガーされるようにすることができます。

さらに、ノードは「パフォーマンス容量使用引き継ぎ」しきい値ポリシーを使用して構成できます。このしきい値ポリシーは、HA ペアの両方のノードのパフォーマンス容量使用統計を合計し、一方のノードに障害が発生した場合に一方のノードで十分な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、同じパフォーマンス容量を使用するテイクオーバー ポリシーを両方のノードに適用できます。



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、一方のノードからそのフェイルオーバー パートナーへのノード間トラフィックが大量にある場合、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ている場合と、もう一方のパートナー ノードですべてのワークロードを実行している場合の使用済みパフォーマンス容量の合計は、どちらのノードで障害が発生したかによっては多少異なる可能性があります。

LUNとボリュームのしきい値を定義する場合は、使用済みパフォーマンス容量の条件を2つ目のパフォーマンスしきい値の設定として使用して、組み合わせしきい値ポリシーを作成することもできます。使用済みパフォーマンス容量の条件は、ボリュームやLUNが格納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ー	警告しきい値	臨界閾値	間隔
Volume	レイテンシー	15ms/op	25ms/op	20分
Aggregate	使用されたパフォーマンス容量	80%	95%	

組み合わせしきい値ポリシーでは、期間全体を通じ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。

パフォーマンス容量使用カウンタを使用してパフォーマンスを管理する

通常、組織は、ピーク期間の需要をサポートするために追加のパフォーマンス容量を予約しながらリソースを効率的に使用できるように、パフォーマンス容量の使用率を 100 未満で運用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。

パフォーマンスの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。このような企業は、使用済みパフォーマンス容量のしきい値を70～80%の範囲に設定する必要があります。小規模な製造業で、ITコストを低減するためにパフォーマンスを犠牲にしてもよいと考えている場合、確保するパフォーマンス容量を少なくするという選択もあります。このような企業では、使用済みパフォーマンス容量のしきい値を85～95%の範囲に設定する必要があります。

使用済みパフォーマンス容量の値がユーザ定義のしきい値ポリシーで設定した割合を超えると、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応できます。これらのイベントを、ノードやアグリゲート内でワークロードを移動および変更するタイミングを図るインジケータとして使用することもできます。

ノードフェイルオーバー計画ページを理解して使用する

[パフォーマンス / ノード フェイルオーバー プラン]ページでは、ある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、そ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 ペアのノードの過去のパフォーマンスに基づいて推定を行います。

フェイルオーバーのパフォーマンスへの影響を見積もることで、次のシナリオに備えて計画することができま

す。

- フェイルオーバーによって、テイクオーバー ノードの推定パフォーマンスが常に許容できないレベルまで低下する場合は、フェイルオーバーによるパフォーマンスへの影響を軽減する対応策を実施することを検討できます。
- ハードウェアのメンテナンス タスクを実行するために手動フェイルオーバーを開始する前に、フェイルオーバーがテイクオーバー ノードのパフォーマンスに及ぼす影響を見積もって、タスクを実行する最適なタイミングを判断できます。

ノードフェイルオーバー計画ページを使用して修正アクションを決定します

[パフォーマンス / ノード フェイルオーバー プラン]ページに表示される情報に基づいて、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することができます。

たとえば、フェイルオーバーによるパフォーマンスへの推定影響を軽減するには、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ー内の他のノードに移動することができます。これにより、プライマリ ノードはフェイルオーバー後も許容されるパフォーマンスを引き続き提供できます。

[ノード フェイルオーバー プラン]ページの構成要素

パフォーマンス/ノード フェイルオーバー プランニング ページのコンポーネントは、グリッドと比較ペインに表示されます。これらのセクションで、ノードのフェイルオーバーによるテイクオーバー ノードのパフォーマンスに対する影響を評価することができます。

パフォーマンス統計グリッド

「パフォーマンス/ノード フェイルオーバー プランニング」ページには、レイテンシ、IOPS、使用率、および使用された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。



ノードのフェイルオーバーを予測するための値の計算には異なるパフォーマンス カウンターが使用されるため、このページと [パフォーマンス/ノード パフォーマンス エクスプローラー] ページに表示されるレイテンシと IOPS の値は一致しない可能性があります。

グリッドでは、各ノードに次のいずれかのロールが割り当てられます。

- プライマリ

HAパートナーで障害が発生した場合にパートナーをテイクオーバーするノードです。ルート オブジェクトは常にプライマリ ノードになります。

- パートナー

フェイルオーバー シナリオで障害が発生したノードです。

- 推定テイクオーバー

プライマリ ノードと同じです。このノードに対して表示されるパフォーマンス統計は、障害が発生したパートナーをテイクオーバーしたあとのテイクオーバー ノードのパフォーマンスを示します。



テイクオーバー ノードのワークロードはフェイルオーバー後の両方のノードのワークロードの合計に相当しますが、推定テイクオーバー ノードの統計はプライマリ ノードとパートナー ノードの統計の合計にはなりません。たとえば、プライマリ ノードのレイテンシが2ミリ秒/処理でパートナー ノードのレイテンシが3ミリ秒/処理の場合に、推定テイクオーバー ノードのレイテンシが4ミリ秒/処理になることがあります。この値は、Unified Manager が実行する計算です。

パートナー ノードをルート オブジェクトにする場合は、そのノードの名前をクリックします。[パフォーマンス/ノード パフォーマンス エクスプローラー] ページが表示されたら、[フェイルオーバー プランニング] タブをクリックして、このノード障害シナリオで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。たとえば、Node1がプライマリ ノードでNode2がパートナー ノードの場合、Node2をクリックしてプライマリ ノードに切り替えることができます。これにより、どちらのノードで障害が発生したかに応じて、予想されるパフォーマンスの変化を確認することが可能です。

比較ペイン

次のリストは、比較ペインにデフォルトで表示されるコンポーネントについて説明しています。

- イベントチャート

これらは、パフォーマンス/ノード パフォーマンス エクスプローラー ページと同じ形式で表示されます。プライマリ ノードのみが対象になります。

- カウンターチャート

グリッドに表示されるパフォーマンス カウンタの過去の統計が表示されます。各チャートの推定テイクオーバー ノードのグラフには、フェイルオーバーが特定の時点で発生した場合の予想される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。これは、その時刻にフェイルオーバーが発生した場合にテイクオーバー ノードの利用率が73%になることを示しています。

過去の統計は、テイクオーバー ノードに過大な負荷をかけずにフェイルオーバーを開始する最適な時刻を特定するのに役立ちます。テイクオーバー ノードの予測パフォーマンスを確認して、許容される時間にフェイルオーバーをスケジュールすることができます。

デフォルトでは、ルート オブジェクトとパートナー ノードの両方の統計が比較ペインに表示されます。パフォーマンス/ノード パフォーマンス エクスプローラー ページとは異なり、このページには、統計の比較のためにオブジェクトを追加するための 追加 ボタンは表示されません。

パフォーマンス/ノード パフォーマンス エクスプローラー ページと同じ方法で、比較ペインをカスタマイズできます。チャートをカスタマイズする例を次に示します。

- ノード名をクリックすると、カウンタ チャートでそのノードの表示と非表示が切り替わります。
- *ズーム表示*をクリックすると、特定のカウンターの詳細なグラフが新しいウィンドウに表示されます。

ノードフェイルオーバー計画ページでしきい値ポリシーを使用する

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まで低下する可能性がある場合に、[パフォー

マンス / ノード フェイルオーバー プラン]ページに通知が表示されます。

「ノード HA ペア過剰使用」というシステム定義のパフォーマンスしきい値ポリシーは、6 つの連続した収集期間 (30 分) にわたっ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 ペア内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みなされます。

このシステム定義のしきい値ポリシーで生成されたイベントは、フェイルオーバーによってテイクオーバーノードのレイテンシが許容できないレベルまで上昇することを警告します。特定のノードについてこのポリシーで生成されたイベントが表示された場合は、そのノードの[パフォーマンス / ノード フェイルオーバー プラン]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を使用するだけでなく、「パフォーマンス使用容量 - テイクオーバー」カウンターを使用してしきい値ポリシーを作成し、選択したノードにポリシーを適用することもできます。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のイベントが生成される前に通知を受け取るには、しきい値を超える最低期間を30分未満に指定することもできます。

たとえば、HA ペア内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 175% を超えた場合に警告イベントを生成するしきい値ポリシーを定義できます。HA ペアの Node1 と Node2 にこのポリシーを適用できます。Node1 または Node2 について警告イベント通知を受信したら、そのノードの[パフォーマンス / ノード フェイルオーバー プラン]ページを確認して、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。実際にフェイルオーバーが発生した場合は、テイクオーバー ノードの過負荷を回避するための対処を実行できます。ノードの使用済みパフォーマンス容量の合計が200%を下回っている間に対処を行うと、この期間にフェイルオーバーが発生してもテイクオーバー ノードのレイテンシが許容できないレベルに到達することはありません。

フェイルオーバー計画にはパフォーマンス使用容量の内訳チャートを使用します

[使用済みパフォーマンス容量 (内訳)]グラフには、プライマリ ノードとパートナー ノードの使用済みパフォーマンス容量が表示されます。また、推定テイクオーバー ノードの空きパフォーマンス容量も表示されます。この情報から、パートナー ノードで障害が発生した場合にパフォーマンスの問題が生じる可能性があるかどうかを判断できます。

内訳グラフでは、ノードの使用済みパフォーマンス容量の合計に加えて、各ノードの値がユーザ プロトコルとバックグラウンド プロセスに分けて表示されます。

- ユーザ プロトコルは、ユーザ アプリケーションとクラスタとの間のI/O処理です。
- バックグラウンド プロセスは、ストレージ効率化、データ レプリケーション、およびシステム健全性に関連する内部システム プロセスです。

これらの詳細情報を確認することにより、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の再構築、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

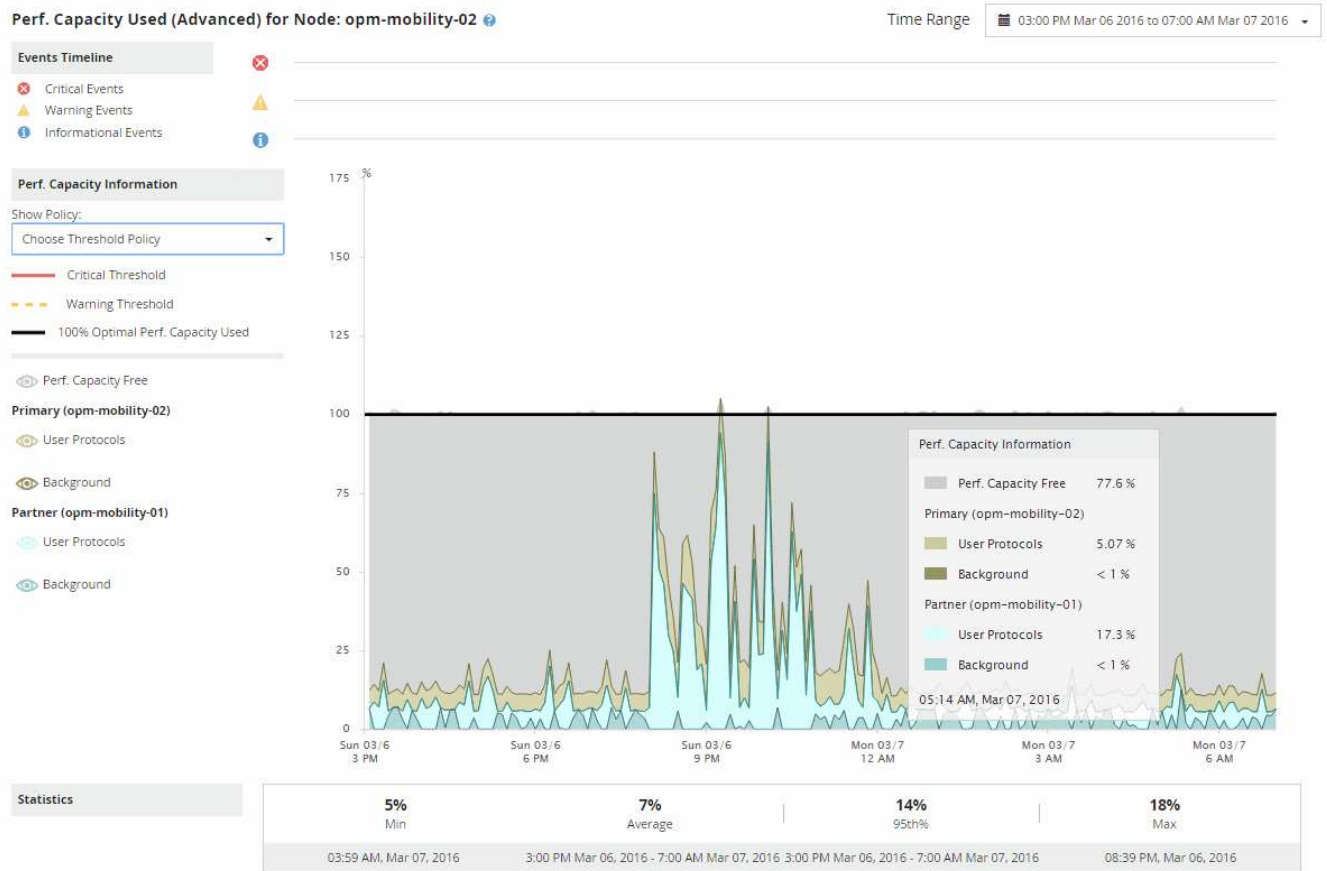
1. 推定引き継ぎノードとして機能するノードの パフォーマンス/ノード フェイルオーバー プランニング ページに移動します。
2. *時間範囲*セレクターから、カウンター グリッドとカウンター チャートに履歴統計を表示する期間を選択します。

カウンタ グラフにプライマリ ノード、パートナー ノード、推定テイクオーバー ノードの統計が表示され

ます。

3. チャートを選択*リストから*Perfを選択します。使用容量。
4. *Perf.で。使用容量*チャートを表示するには、*内訳*を選択し、*ズーム表示*をクリックします。

[使用済みパフォーマンス容量]の詳細グラフが表示されます。



5. 詳細グラフにカーソルを合わせて、ポップアップ ウィンドウに表示される使用済みパフォーマンス容量の情報を確認します。

パフォーマンス。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。これは、フェイルオーバー後にテイクオーバー ノードに残っているパフォーマンス容量を示します。0% の場合は、フェイルオーバーによってテイクオーバー ノードのレイテンシが許容できないレベルまで増加します。

6. その場合、空きパフォーマンス容量の割合の低下を回避するための対処を検討します。

ノードのメンテナンスのためにフェイルオーバーを予定している場合は、空きパフォーマンス容量の割合が0でない時間帯にパートナー ノードを停止するようにします。

データを収集し、ワークロードのパフォーマンスを監視する

Unified Manager は、パフォーマンス イベントを識別するために 5 分ごとにワークロード アクティビティを収集して分析し、15 分ごとに構成の変更を検出します。5分ごとのパフォーマンスとイベントの履歴データが最大30日分保持され、そのデータを使用して

監視対象のすべてのワークロードの想定レイテンシ範囲が予測されます。

Unified Managerでは、少なくとも3日分のワークロード アクティビティを収集して分析してから、[ワークロード分析]ページおよび[イベントの詳細]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します。このアクティビティを収集して表示されるレイテンシ予測には、ワークロード アクティビティにおける変化がすべて反映されるわけではありません。3 日間のアクティビティを収集した後、Unified Manager は 24 時間ごとに午前 12 時にレイテンシ予測を調整し、ワークロード アクティビティの変化を反映して、より正確な動的パフォーマンスしきい値を確立します。

Unified Manager がワークロードを監視している最初の 4 日間に、最後のデータ収集から 24 時間以上経過すると、レイテンシ チャートにそのワークロードのレイテンシ予測は表示されません。前回の収集よりも前に検出されたイベントは引き続き表示されます。



システム時間が夏時間（DST）に切り替わると、監視しているワークロードのパフォーマンス統計で使用するレイテンシ予測も変わります。Unified Managerは、レイテンシ予測の修正を即座に開始しますが、完了までに15日間ほどかかります。その間もUnified Managerの使用は継続できますが、Unified Managerはレイテンシ予測を使用して動的イベントを検出するため、一部のイベントは正確でなくなる可能性があります。時間の変更前に検出されたイベントは影響を受けません。

Unified Managerで監視されるワークロードのタイプ

Unified Manager を使用すると、ユーザー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。

• ユーザー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。これらは読み取り要求と書き込み要求に関するプロセスです。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ー定義のワークロードです。



Unified Managerは、クラスタ内のワークロードだけを監視します。アプリケーションやクライアント、アプリケーションとクラスタ間のパスは監視しません。

ワークロードに次の 1 つ以上の条件が当てはまる場合、Unified Manager で監視することはできません。

- 読み取り専用モードのデータ保護（DP）コピーである（DPボリュームについてはユーザ生成のトラフィックが監視されます）。
- ボリュームがオフライン データ クローンである。
- ボリュームが MetroCluster 構成のミラー ボリュームである。

• システム定義のワークロード

次のストレージ効率化、データ レプリケーション、およびシステム健全性に関する内部プロセスです。

- ストレージ効率化（重複排除など）
- ディスク健全性（RAIDの再構築、ディスク スクラビングなど）
- 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

- ファイルシステム健全性（各種WAFL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ストレージ効率化処理など）
- 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るクラスタ コンポーネントが競合状態の場合にのみ表示されます。たとえば、システム定義のワークロードの名前を検索して、そのパフォーマンス データを表示することはできません。

ワークロードパフォーマンス測定値

Unified Manager は、履歴統計値と予測統計値に基づいてクラスタ上のワークロードのパフォーマンスを測定し、ワークロードのレイテンシ値の予測を作成します。実際のワークロードの統計値とレイテンシ予測を比較して、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される範囲外になった場合、動的なパフォーマンス イベントがトリガーされてユーザに通知されます。

次の図では、期間内に実際に測定されたパフォーマンス統計の実測値を赤色で示してあります。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。



次の表は、ワークロードのパフォーマンス測定値を示しています。

項目	説明
アクティビティ	ポリシー グループのワークロードで使用されているQoS制限の割合です。  Unified Manager が、ボリュームの追加や削除、QoS 制限の変更など、ポリシー グループの変更を検出すると、実際の値と予想値が設定された制限の100% を超える可能性があります。設定された上限の100%を超える場合、値は「>100%」と表示されます。設定された上限の1%に満たない場合は「<1%」と表示されます。
実測値	特定の時点に測定された特定のワークロードのパフォーマンスの値です。
偏差	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。  負の偏差値はワークロードのパフォーマンスが予想よりも低いことを示し、正の偏差値はワークロードのパフォーマンスが予想よりも高いことを示します。
想定	特定のワークロードについての過去のパフォーマンス データの分析に基づく想定値です。Unified Manager はこれらの統計値を分析して、値の予想範囲 (遅延予測) を決定します。
レイテンシ予測 (想定範囲)	レイテンシ予測は、ある時刻にパフォーマンス値の上限と下限がどうなるかを予測するものです。ワークロードのレイテンシの場合、上限値がパフォーマンスしきい値を形成します。実測値がパフォーマンスしきい値を超えると、Unified Managerによって動的なパフォーマンス イベントがトリガーされます。
ピーク	一定の期間に測定された最大値です。
ピーク偏差	一定の期間に測定された偏差の最大値です。
キュー深度	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要求の数です。

項目	説明
利用率	ネットワーク処理、データ処理、およびアグリゲート コンポーネントのワークロード処理を完了するためにビジー状態になる一定期間における時間の割合です。たとえば、ネットワーク処理やデータ処理のコンポーネントでI/O要求を処理するのにかかる時間の割合や、アグリゲートで読み取りや書き込みの要求に対応するのにかかる時間の割合などがあります。
書き込みスループット	MetroCluster構成におけるローカル クラスタのワークロードからパートナー クラスタへの書き込みスループットです。1秒あたりのメガバイト数 (MBps) で示されます。

パフォーマンスの想定範囲とは

レイテンシ予測は、ある時刻にパフォーマンス値の上限と下限がどうなるかを予測するものです。ワークロードのレイテンシの場合、上限値がパフォーマンスしきい値を形成します。実測値がパフォーマンスしきい値を超えると、Unified Managerによって動的なパフォーマンス イベントがトリガーされます。

たとえば、通常の営業時間である午前 9 時から午後 5 時までの間、ほとんどの従業員は午前 9 時から午前 10 時 30 分の間に電子メールをチェックする可能性があります。電子メール サーバーに対する需要の増加は、この時間帯のバックエンド ストレージ上のワークロード アクティビティの増加を意味します。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 時までの昼休みと、午後 5 時以降の勤務終了時には、ほとんどの従業員はコンピューターから離れている可能性があります。この時間帯は、一般にEメール サーバの負荷が減り、バックエンド ストレージの負荷も低下します。あるいは、ストレージ バックアップやウイルス スキャンなどのワークロード操作が午後 5 時以降に開始され、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されている場合もあります。

ワークロード アクティビティの増加と減少を数日間にわたって監視した結果から、アクティビティの想定範囲（レイテンシ予測）が特定され、ワークロードの上限と下限が決まります。オブジェクトの実際のワークロード アクティビティが上限または下限の境界外にあり、一定期間その境界外のままである場合、オブジェクトが過剰に使用されているか、十分に使用されていないことを示している可能性があります。

レイテンシ予測の生成方法

Unified Managerは、少なくとも3日分のワークロード アクティビティを収集して分析してから、GUIに表示するI/O応答時間のレイテンシ予測を決定します。この期間で収集されるデータには、ワークロード アクティビティにおける変化がすべて反映されるわけではありません。最初の 3 日間のアクティビティを収集した後、Unified Manager は、24 時間ごとに午前 12 時にレイテンシ予測を調整して、ワークロード アクティビティの変化を反映し、より正確な動的パフォーマンスしきい値を確立します。



システム時間が夏時間（DST）に切り替わると、監視しているワークロードのパフォーマンス統計で使用するレイテンシ予測も変わります。Unified Managerは、レイテンシ予測の修正を即座に開始しますが、完了までに15日間ほどかかります。その間もUnified Managerの使用は継続できますが、Unified Managerはレイテンシ予測を使用して動的イベントを検出するため、一部のイベントは正確でなくなる可能性があります。時間の変更前に検出されたイベントは影響を受けません。

レイテンシ予測とパフォーマンス分析

Unified Managerは、レイテンシ予測を使用して監視対象のワークロードの一般的なI/Oレイテンシ（応答時間）を表します。ワークロードの実際のレイテンシがレイテンシ予測の上限を上回るとアラートが生成されて動的なパフォーマンス イベントがトリガーされるため、パフォーマンス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 ベースラインです。Unified Manager は、時間の経過とともに過去のパフォーマンス測定から学習し、ワークロードの予想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は、このベースラインを使用して、実際のレイテンシがしきい値を上回る、下回る、あるいは想定範囲外になった時点を判断します。実測値と想定値の比較を基に、ワークロードのパフォーマンス プロファイルが作成されます。

あるワークロードの実際のレイテンシがクラスタ コンポーネントの競合が原因で動的なパフォーマンス しきい値を超えると、レイテンシが上昇し、ワークロードのパフォーマンスは想定を下回ります。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 はしきい値超過イベントを分析し、そのアクティビティがパフォーマンス イベントであ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。このような低アクティビティのボリュームについては、イベントの数を最小限に抑えるために、パフォーマンス イベントの分析中、Unified Managerは処理数およびレイテンシが想定よりもはるかに高いイベントのみをトリガーします。



この例のボリュームのレイテンシ予測（緑で表示）は、3.5～5.5ms/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まで増加した場合、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過します。

ネットワーク トラフィックが減少するか、クラスタ コンポーネントの競合が解消されると、レイテンシはレイテンシ予測の範囲内に戻ります。レイテンシが長期間にわたって10ms/op以上のままの場合、イベントを解決するための対処が必要となることがあります。

Unified Manager がワークロードの遅延を使用してパフォーマンスの問題を特定する方法

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、遅延を使用してパフォーマンス イベントを検出し、警告を発します。

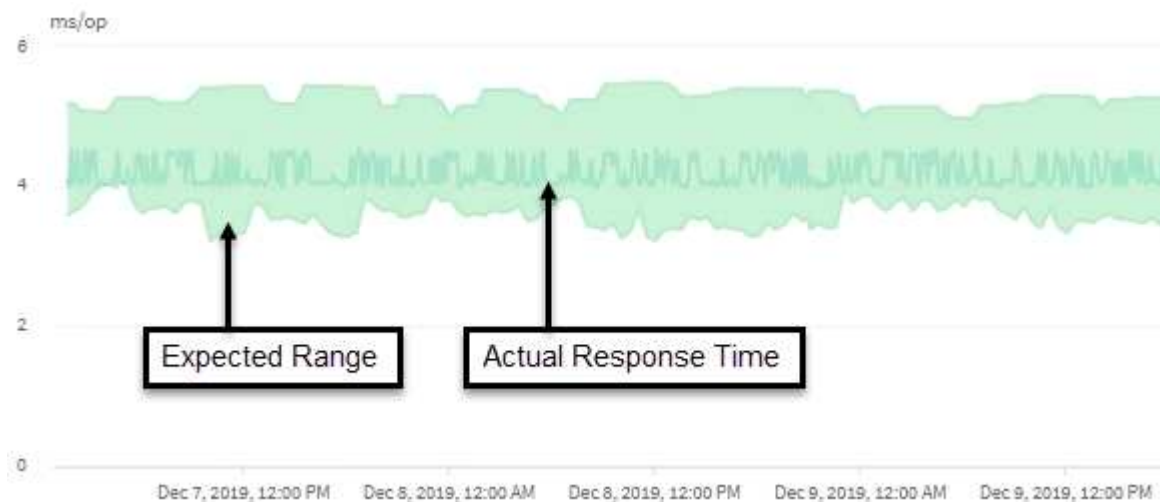
高レイテンシは、アプリケーションからクラスタ上のボリュームへの要求に通常よりも時間がかかっていることを意味します。高レイテンシの原因はクラスタ自体、具体的にはいくつかのクラスタ コンポーネントでの競合にある可能性があります。また、クラスタ外の問題（ネットワークのボトルネックなど）、アプリケーションをホストしているクライアントの問題、またはアプリケーション自体の問題が原因の場合もあります。



Unified Managerは、クラスタ内のワークロードだけを監視します。アプリケーションやクライアント、アプリケーションとクラスタ間のパスは監視しません。

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、高レイテンシの原因になります。実際のレイテンシが想定範囲（レイテンシ予測）の動的パフォーマンスしきい値を超えると、Unified Managerはイベントを分析して、解決が必要なパフォーマンス イベントであるかどうかを判断します。レイテンシは処理あたりのミリ秒（ms/op）単位で測定されます。

[ワークロード分析]ページのレイテンシ合計グラフでは、レイテンシ統計の分析を表示して、個々のプロセス（読み取り / 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に照らして比較できます。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にあたっては、レイテンシの統計値を使用してイベントの原因がクラスタ上の問題にあるかどうかを判断できます。また、イベントに関係しているワークロードのアクティビティまたはクラスタ コンポーネントを特定することもできます。



この例は、レイテンシのグラフを示しています。実際の応答時間（レイテンシ）アクティビティは青い線、レ

イテンシ予測（想定範囲）は緑で表されています。

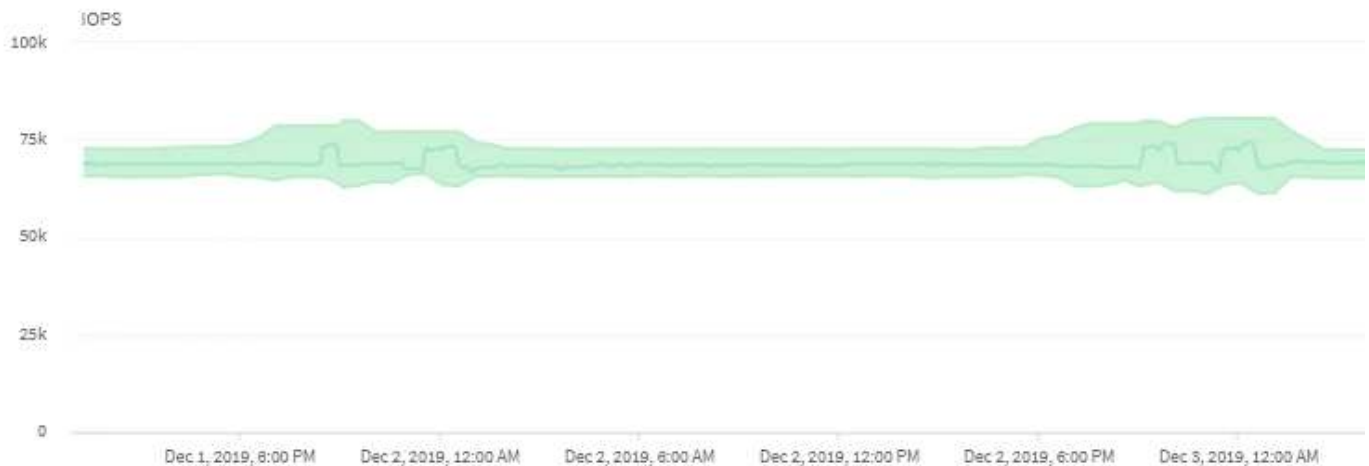


Unified Managerでデータを収集できなかった期間は、青い線が途切れています。これは、クラスタまたはボリュームと通信できなかったか、Unified Managerがその時間にオフになっていたか、データの収集に5分以上かかった場合に起こります。

クラスタでの処理によるワークロードのレイテンシへの影響

処理（IOPS）には、クラスタで実行されるユーザ定義とシステム定義のすべてのワークロードのアクティビティが含まれます。IOPSの統計は、クラスタでの処理（バックアップの作成や重複排除の実行など）がワークロードのレイテンシ（応答時間）に影響を及ぼしていないかどうかやパフォーマンス イベントの原因となっていないかどうかを確認するのに役立ちます。

パフォーマンス イベントを分析するときは、IOPSの統計を使用して、クラスタにおける問題がパフォーマンス イベントの原因となっていないかどうかを確認できます。パフォーマンス イベントの原因となった可能性がある具体的なワークロード アクティビティを特定することができます。IOPSは1秒あたりの処理数（処理数/秒）として測定されます。



この例は、IOPSのグラフを示しています。実際の処理の統計が青い線で、処理のIOPS予測が緑で表示されています。



クラスタが過負荷になっている場合、Unified Managerに次のメッセージが表示されることがあります。Data collection is taking too long on Cluster *cluster_name*。これは、Unified Manager が分析するのに十分な統計が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 を使用すると、MetroCluster構成内のクラスタ間の書き込みスループットを監視して、書き込みスループットの高いワークロードを特定できます。

これらの高パフォーマンスのワークロードによってローカル クラスタ上の他のボリュームの I/O 応答時間が長くなる場合、Unified Manager はパフォーマンス イベントをトリガーして通知します。



Unified Manager は、MetroCluster構成内のクラスタを個別のクラスタとして扱います。クラスタがパートナーかどうかは区別されず、各クラスタからの書き込みスループットが関連付けられることはありません。

MetroCluster構成内のローカル クラスタがデータをパートナー クラスタにミラーリングすると、データはNVRAMに書き込まれ、その後、スイッチ間リンク (ISL) を介してリモート アグリゲートに転送されます。Unified Manager はNVRAMを分析して、書き込みスループットが高くNVRAM を過剰に使用し、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「犠牲者」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も高く競合を引き起こしているワークロードは「いじめっ子」と呼ばれます。書き込み要求のみがパートナー クラスタにミラーリングされるため、Unified Manager は読み取りスループットを分析しません。

MetroCluster構成のいずれかのクラスタのスループットを表示するには、次の各画面で対応するLUNおよびボリュームのワークロードを分析します。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、次のいずれかを選択します。

- ストレージ > クラスタ > パフォーマンス: すべてのクラスタ ビュー。詳細については、
- 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を理解する

パフォーマンス イベントとは、クラスタでのワークロード パフォーマンスに関連するインシデントです。応答時間が長いワークロードを特定するのに役立ちます。同時に発生した健全性イベントと一緒に確認することで、応答時間が長くなった原因と考えられる関連する問題を特定することができます。

Unified Manager は、同じクラスタ コンポーネントに対して同じイベント条件が複数回発生したことを検出すると、すべての発生を個別のイベントではなく単一のイベントとして扱います。

特定の重要度タイプのパフォーマンス イベントが発生したときに自動的にEメール通知を送信するアラートを設定できます。

パフォーマンス イベントのソース

パフォーマンス イベントとは、クラスタでのワークロード パフォーマンスに関連する問題です。応答時間が長い（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、応答時間が長くなった原因と考えられる関連する問題を特定することができます。

Unified Manager は、次のソースからパフォーマンス イベントを受信します。

- ユーザー定義のパフォーマンスしきい値ポリシーイベント

独自に設定したしきい値に基づいたパフォーマンスの問題。アグリゲートやボリュームなどのストレージ オブジェクトに対してパフォーマンスしきい値ポリシーを設定して、パフォーマンス カウンタのしきい値を超えたときにイベントが生成されるようにします。

これらのイベントを受け取るためには、パフォーマンスしきい値ポリシーを定義してストレージ オブジェクトに割り当てる必要があります。

- システム定義のパフォーマンスしきい値ポリシーイベント

システム定義のしきい値に基づいたパフォーマンスの問題。このしきい値ポリシーはUnified Managerにあらかじめ含まれており、一般的なパフォーマンスの問題に対処します。

このしきい値はデフォルトで有効化されており、クラスタの追加後すぐにイベントが生成される場合があります。

- 動的パフォーマンスしきい値イベント

ITインフラストラクチャの障害やエラー、またはクラスタ リソースの使用率が高いワークロードに起因するパフォーマンスの低下。これらのイベントの原因は、時間がたてば修復する、または修理や設定変更によって解決可能な単純な問題である可能性があります。動的しきい値イベントは、共有クラスタ コンポーネントの使用率が高い他のワークロードが原因で、ONTAPシステム上のワークロードが遅くなっていることを示します。

このしきい値はデフォルトで有効になっており、新しいクラスタについてはデータ収集の開始後4日目からイベントが生成されます。

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。

- 致命的

パフォーマンス イベントが発生しており、すぐに対処しないとサービスが停止する可能性があります。

重大イベントは、ユーザ定義のしきい値からのみ生成されます。

- 警告

クラスタ オブジェクトのパフォーマンス カウンタが正常な範囲から外れており、重大な問題にならない

ように監視が必要です。この重大度のイベントではサービスは停止しません。早急な対処も不要です。

警告イベントは、システムまたはユーザ定義のしきい値、あるいは動的なしきい値から生成されます。

- 情報

新しいオブジェクトが検出されたときやユーザ操作が実行されたときに発生します。たとえば、ストレージ オブジェクトが削除されたときや設定に変更があったときは、情報タイプの重大度のイベントが生成されます。

情報イベントは、ONTAPで設定の変更が検出されたときに直接生成されます。

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 は、クラスタの構成変更を監視して、変更がパフォーマンス イベントの原因となったか、または一因となったかどうかを判断できるようにします。パフォーマンス エクスプローラーのページには、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 エクスプローラー]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 イベントと同時にその前後に変更が検出されていれば、その変更が原因でイベントのアラートがトリガーされた可能性があります。

Unified Manager は、情報イベントとして分類される次の変更イベントを検出できます。

- ボリュームがアグリゲート間で移動されたとき。

Unified Manager は、移動が進行中か、完了したか、失敗したかを検出できます。ボリュームの移動中に Unified Manager がダウンした場合、Unified Manager が復旧するとボリュームの移動が検出され、その変更イベントが表示されます。

- 1つ以上の監視対象ワークロードを含むQoSポリシー グループのスループット (MBpsまたはIOPS) の制限が変更されたとき。

ポリシー グループ制限を変更するとレイテンシ (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 ペア内のノードは、パートナー ノードのストレージを引き継ぐか、または返します。

Unified Manager は、テイクオーバー、部分テイクオーバー、またはギブバック操作が完了したことを検出できます。パニック状態のノードによってテイクオーバーが発生した場合、Unified Manager はイベン

トを検出しません。

- ONTAPのアップグレードやリバートの処理が正常に完了したとき。

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、イベントを自動的に生成するいくつかの標準しきい値ポリシーが用意されています。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、またはONTAP Selectシステムでは有効になっていません。

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 によって監視されるすべてのクラスタにデフォルトで割り当てられます。

- クラスター負荷の不均衡

クラスタ内の1つのノードの負荷が他のノードよりもはるかに高く、ワークロードのレイテンシに影響を及ぼす可能性がある状況を特定します。

クラスタ内のすべてのノードの使用済みパフォーマンス容量の値が比較され、30%のしきい値を24時間以上超えているノードがないかチェックされます。これは警告イベントです。

- クラスター容量の不均衡

クラスタ内の1つのアグリゲートの使用済み容量が他のアグリゲートよりもはるかに多く、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、アグリゲート間で70%の差がないかチェックされます。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 によって監視されているクラスタ内のすべてのノードにデフォルトで割り当てられます。

- パフォーマンス容量使用しきい値を超えました

1つのノードが運用効率の上限を超えて稼働していて、ワークロードのレイテンシに影響を及ぼしている可能性がある状況を特定します。

100%以上のパフォーマンス容量を12時間以上使用しているノードがない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 HA ペアが過剰に使用されています

HA ペア内のノードが HA ペアの運用効率の限界を超えて動作している状況を識別します。

これは、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を確認することで行われます。2 つのノードの使用済みパフォーマンス容量の合計が12時間以上にわたって200%を超えている場合は、コントローラ フェイルオーバーがワークロードのレイテンシに影響を及ぼします。これは情報イベントです。

- ノードディスクの断片化

アグリゲート内の1つまたは複数のディスクが断片化されていて、主要なシステム サービスの速度が低下し、ノード上のワークロードのレイテンシに影響を及ぼしている可能性がある状況を特定します。

ノード上のすべてのアグリゲートで特定の読み取り / 書き込み処理の比率が確認されます。このポリシーは、SyncMirrorの再同期中、またはディスク スクラビング処理中にエラーが検出された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アグリゲートは分析されません。

アグリゲートのしきい値ポリシー

システム定義の集約パフォーマンスしきい値ポリシーは、Unified Manager によって監視されているクラスタ内のすべての集約にデフォルトで割り当てられます。

- 集約ディスクが過剰に使用されています

アグリゲートが運用効率の上限を超えて稼働していて、ワークロードのレイテンシに影響を及ぼしている可能性がある状況を特定します。そのために、設定されているディスクの利用率が30分以上にわたって95%を超えているアグリゲートが確認されます。この複数条件ポリシーは、問題の原因を特定するために次の分析を実行します。

- アグリゲート内のディスクがバックグラウンドでメンテナンス作業を実行中かどうか。

ディスクに対してバックグラウンドで実行されるメンテナンス作業には、ディスク再構築、ディスク スクラビング、SyncMirrorの再同期、再パリティ化などがあります。

- ディスク シェルフのFibre Channelインターコネクに通信のボトルネックはあるか。

- アグリゲートの空きスペースが不足しているか。3つの下位ポリシーのうちの1つ（または複数）にも違反しているとみなされた場合にのみ、このポリシーに対して警告イベントが発行されます。アグリゲート内のディスクの利用率が95%以上になっているという条件だけでは、パフォーマンス イベントはトリガーされません。



「アグリゲート ディスク過剰使用」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 およびFabricPoolアグリゲートは分析されません。

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、定義された「予想される遅延」値を持つパフォーマンス サービス レベル ポリシーが構成されたすべての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 レベルで定義されたワークロード ボリューム/**LUN** レイテンシしきい値を超えました

「予想される遅延」制限を超えており、ワークロードのパフォーマンスに影響を与えているボリューム (ファイル共有) と LUN を識別します。これは警告イベントです。

想定レイテンシの値を超えた時間が過去1時間に30%を超えるワークロードがないかどうかを確認されます。

QoSのしきい値ポリシー

システム定義のQoSパフォーマンスしきい値ポリシーは、ONTAPのQoS最大スループット ポリシー (IOPS、IOPS/TB、またはMBps) が設定されているワークロードに割り当てられます。ワークロードのスループットの値が設定されたQoS値の85%に達すると、Unified Managerはイベントをトリガーします。

- **QoS 最大 IOPS または MB/s** しきい値

IOPSまたはMBpsがQoS最大スループット制限を超えていて、ワークロードのレイテンシに影響を及ぼしているボリュームおよびLUNを特定します。これは警告イベントです。

ポリシー グループにワークロードが1つだけ割り当てられている場合は、割り当てられているQoSポリシー グループで定義された最大スループットしきい値を超えているワークロードがないかどうか過去1時間の各収集期間について確認されます。

複数のワークロードで同じQoSポリシーを使用している場合は、ポリシーに割り当てられたすべてのワークロードのIOPSまたはMBpsの合計が求められ、その合計がしきい値を超えていないかどうか確認されます。

- **QoS ピーク IOPS/TB またはブロック サイズしきい値による IOPS/TB**

IOPS/TBがアダプティブQoSピーク スループット制限 (またはブロック サイズ指定のIOPS/TB制限) を超えていて、ワークロードのレイテンシに影響を及ぼしているボリュームを特定します。これは警告イベントです。

このポリシーでは、アダプティブQoSポリシーで定義されたIOPS/TBのピークしきい値を各ボリュームのサイズに基づいてQoS最大IOPSの値に換算し、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確認されます。



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 ポリシーで「ブロック サイズ」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 最大 MB/秒値に変換されます。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確認されます。



このポリシーは、クラスタにONTAP 9.5以降のソフトウェアがインストールされている場合にのみボリュームに適用されます。

パフォーマンス イベントの分析と通知

パフォーマンス イベントは、クラスタ コンポーネントの競合に起因するワークロードのI/Oパフォーマンスの問題を管理者に通知します。Unified Manager はイベントを分析して、関連するすべてのワークロード、競合しているコンポーネント、およびイベントがまだ解決が必要な問題であるかどうかを識別します。

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 (操作) 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となってワークロードの要件を満たす最適なパフォーマンス レベルを提供できません。同じコンポーネントを使用している他のワークロードのパフォーマンスに影響が及び、レイテンシが増加する可能性があります。レイテンシが動的なパフォーマンスしきい値を超えると、Unified Manager はパフォーマンス イベントをトリガーしてユーザに通知します。

イベント分析

Unified Manager は、過去 15 日間のパフォーマンス統計を使用して次の分析を実行し、イベントに関係する被害者ワークロード、攻撃者ワークロード、およびクラスタ 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 ハイブリッド アグリゲート (ローカル層) 上のボリュームの場合、レイテンシが 5 ミリ秒 (ms) を超え、IOPS が 1 秒あたり 10 操作 (ops/sec) を超える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。



クラスタ相互接続における被害ワークロードの遅延が 1 ミリ秒を超える場合、Unified Manager はこれを重大なものとして扱い、クラスタ相互接続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使用し、競合状態を引き起こしているBullyワークロードを特定します。
- クラスタ コンポーネントの利用率またはアクティビティの偏差に基づいて関連するワークロードをランク付けし、クラスタ コンポーネントの使用量の変化が最も大きいBullyワークロードと最も影響を受けたVictimワークロードを特定します。

ごく短時間しか発生せず、コンポーネントの競合状態が解消した時点で自己修復されるイベントもあります。継続的なイベントとは、5分以内に同じクラスタ コンポーネントについて再発し、アクティブな状態のままのイベントのことです。連続イベントの場合、Unified Manager は 2 つの連続する分析間隔中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。

イベントが解決されると、そのイベントはボリュームの過去のパフォーマンスの問題の記録の一部として Unified Manager で引き続き利用できるようになります。各イベントには、イベント タイプとボリューム、クラスタ、および関連するクラスタ コンポーネントを識別する一意のIDが割り当てられます。



1つのボリュームが複数のイベントに同時に関連している場合があります。

イベントの状態

イベントは次のいずれかの状態になります。

- アクティブ

現在アクティブなパフォーマンス イベント（新規または確認済みのイベント）を示します。自己修復または解決されていないイベントで、ストレージ オブジェクトのパフォーマンス カウンタがパフォーマンス しきい値を超えたままになっているものです。

- 廃止

アクティブではなくなったイベントを示します。自己修復または解決されたイベントで、ストレージ オブジェクトのパフォーマンス カウンタがパフォーマンス しきい値を上回らなくなったものです。

イベント通知

イベントは[ダッシュボード]ページをはじめとする多くのユーザ インターフェイス ページに表示され、イベントの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て、推奨される解決方法を確認できます。

イベントの操作

[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が表示されます。

同じ期間にイベントが複数ある場合は、イベント数が表示されます。

- 単一のイベントをクリックすると、イベントの詳細情報（関連するクラスタ コンポーネントなど）がダイアログ ボックスに表示されます。

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。*完全な分析を表示*をクリックすると、イベントの詳細ページで完全な分析を表示できます。同じ期間にイベントが複数ある場合は、最新の3つのイベントの詳細がダイアログ ボックスに表示されます。イベントをクリックすると、[イベントの詳細]ページにイベント分析が表示されます。

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、ワークロードのアクティビティ、使用率、書き込みスループット、クラスタ コンポーネントの使用率、または I/O 遅延 (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断します。この情報によって、各ワークロードのイベントにおける役割と[イベントの詳細]ページでのランク付けが決まります。

Unified Managerは、ワークロードの最新の分析値を値の想定範囲（レイテンシ予測）と比較します。最新の分析値と値の想定範囲の差が最も大きいワークロードが、イベントによってパフォーマンスに最も影響を受けたワークロードです。

たとえば、クラスターにワークロード A とワークロード B という 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操作あたり 5 ～ 10 ミリ秒 (ms/op) で、実際のレイテンシは通常 7 ms/op 程度です。ワークロード B のレイテンシ予測は 10 ～ 20 ミリ秒/操作で、実際のレイテンシは通常 15

ミリ秒/操作程度です。どちらのワークロードも、レイテンシ予測の範囲内に収まっています。クラスタでの競合が原因で両方のワークロードのレイテンシが40ms/opに上昇し、レイテンシ予測の上限である動的なパフォーマンスしきい値を超えた結果イベントがトリガーされたとします。レイテンシの偏差（想定される値とパフォーマンスしきい値を上回った値の差）はワークロードAで約33ms/op、ワークロードBで25ms/opです。どちらのワークロードもレイテンシが40ms/opまで急増しましたが、ワークロードAの方がレイテンシの偏差が大きい（33ms/op）ため、パフォーマンスへの影響も大きかったことが判断できます。

[イベントの詳細]ページの[システム診断]セクションでは、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。並べ替えオプションを選択すると、Unified Manager は、イベントが検出されてからのアクティビティ、使用率、スループット、または遅延の偏差を予想値から分析し、ワークロードの並べ替え順序を決定します。遅延については、赤い点 (●) は、被害ワークロードによるパフォーマンスしきい値の超過と、それに伴うレイテンシへの影響を示します。ドットが多いほどレイテンシの偏差が大きいことを示しており、イベントによってレイテンシが最も影響を受けたVictimワークロードを特定するのに役立ちます。

クラスタ コンポーネントとその競合要因

クラスタ コンポーネントの競合の原因となるクラスタのパフォーマンスの問題を特定することができます。コンポーネントを使用するワークロードのパフォーマンスが低下し、クライアント要求に対する応答時間 (遅延) が長くなり、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、_犠牲者_と呼ばれる他のクラスター コンポーネントとワークロードのパフォーマンスのレイテンシが増加する可能性があります。コンポーネントの競合状態を解消するには、ワークロードを減らすか処理能力を高めることでパフォーマンスを通常のレベルまで戻す必要があります。Unified Managerでは、ワークロード パフォーマンスの収集と分析が5分間隔で行われるため、クラスタ コンポーネントの利用率が高い状態が長時間続いたときにのみ検出されます。利用率が高い状態が5分間のうちの短時間しか続かないような一時的な利用率の急増は検出されません。

ストレージ アグリゲートが競合状態になる原因としては、たとえば、1つ以上のワークロードがそれぞれのI/O要求に対応するために競合する場合などがあります。アグリゲートの他のワークロードに影響し、それらのワークロードのパフォーマンスが低下する可能性があります。アグリゲートのアクティビティを減らす方法はいくつかありますが、たとえば、1つ以上のワークロードを負荷の低いアグリゲートまたはノードに移動し、現在のアグリゲートに対する全体的なワークロードの負荷を低くするなどの方法が効果的です。QoSポリシー グループの場合は、スループット制限を調整したりワークロードを別のポリシー グループに移動したりすることで、ワークロードが抑制されないようにすることができます。

Unified Manager は次のクラスタ コンポーネントを監視し、競合が発生したときに警告を発します。

- ネットワーク

クラスター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。待機時間は、クラスターが I/O 要求に応答する前に、「転送準備完了」トランザクションが完了するのを待機するために費やされる時間です。ネットワーク コンポーネントが競合状態にある場合、ブロック プロトコル レイヤでの長い待機時間は、1つ以上のワークロードのレイテンシに影響していることを意味します。

- ネットワーク処理

プロトコル レイヤとクラスタ間のI/O処理に関与する、クラスタ内のソフトウェア コンポーネントを表します。イベントが検出されてから、ネットワーク処理を実行するノードが変更されている可能性があります。ネットワーク処理コンポーネントが競合状態にある場合、ネットワーク処理ノードでの高利用率は、1つ以上のワークロードのレイテンシに影響していることを意味します。

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、ネットワーク処理のレイテンシの値が両方のノードについて表示され、ノードで負荷を適切に共有していることを確認できます。

- **QoS 制限最大値**

ワークロードに割り当てられたストレージQoSポリシー グループの最大スループット（ピーク）設定を表します。ポリシー グループ コンポーネントが競合状態にある場合、ポリシー グループ内のすべてのワークロードに、スループットの制限によってスロットルが適用され、1つ以上のワークロードのレイテンシに影響していることを意味します。

- **QoS 制限の最小値**

他のワークロードに割り当てられた QoS スループットの最小 (予想) 設定によって発生するワークロードの遅延を表します。特定のワークロードに設定された QoS の最小値が、約束されたスループットを保証するために帯域幅の大部分を使用する場合、他のワークロードは調整され、より多くの遅延が発生します。

- **クラスター相互接続**

クラスタ ノードを物理的に接続するケーブルとアダプタを表します。クラスタ インターコネクト コンポーネントが競合状態にある場合は、クラスタ インターコネクトでのI/O要求の長い待機時間がワークロードのレイテンシに影響していることを意味します。

- **Data Processing**

クラスタとストレージ アグリゲート間でワークロードを含むI/O処理に関与する、クラスタ内のソフトウェア コンポーネントを表します。イベントが検出されてから、データ処理を実行するノードが変更されている可能性があります。データ処理コンポーネントが競合状態にある場合、データ処理ノードでの高利用率は、1つ以上のワークロードのレイテンシに影響していることを意味します。

- **ボリュームアクティベーション**

すべてのアクティブ ボリュームの使用状況を追跡するプロセスです。1,000 を超えるボリュームがアクティブな大規模環境では、このプロセスは、ノードを介してリソースに同時にアクセスする必要の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最大しきい値を超えると、ここで特定されているように、重要でないボリュームの一部で遅延が発生します。

- *** MetroClusterリソース***

NVRAMとインタースイッチ リンク (ISL) を含むMetroClusterリソースを表します。MetroCluster構成のクラスタ間でデータをミラーリングするのに使用します。MetroClusterコンポーネントが競合状態にある場合は、ローカル クラスタのワークロードによる大量の書き込みスループットまたはリンクの不具合が、ローカル クラスタの1つ以上のワークロードのレイテンシに影響していることを意味します。クラスタがMetroCluster構成に含まれていない場合は、このアイコンは表示されません。

- **アグリゲートまたは SSD アグリゲート オペレーション**

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。「SSD アグリゲート」は、すべて SSD (オールフラッシュ アグリゲート) で構成されるか、SSD とクラウド層 (FabricPoolアグリゲート) の組み合わせで構成されます。

- クラウドレイテンシ

クラスタとユーザ データ格納先のクラウド階層の間のI/O処理に関与する、クラスタ内のソフトウェア コンポーネントを表します。クラウド レイテンシ コンポーネントが競合状態にある場合、クラウド階層でホストされたボリュームからの大量の読み取りが1つ以上のワークロードのレイテンシに影響していることを意味します。

- SnapMirrorを同期

SnapMirror同期関係でプライマリ ボリュームからセカンダリ ボリュームにユーザ データを複製する際に関与するクラスター内のソフトウェア 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している場合は、SnapMirror同期操作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を与えていることを意味します。

パフォーマンス イベントに関連したワークロードの役割

Unified Manager は、ルールを使用して、パフォーマンス イベントにおけるワークロードの関与を識別します。役割にはVictim、Bully、Sharkがあります。ユーザ定義のワークロードは同時にVictim、Bully、Sharkとなることがあります。

ルール	説明
Victim	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です。Victimとみなされるのはユーザ定義のワークロードのみです。Unified Manager は、イベント中の実際のレイテンシがレイテンシ予測（予想範囲）から大幅に増加したレイテンシの偏差に基づいて被害ワークロードを識別します。
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）のパフォーマンスを低下させるユーザ定義またはシステム定義のワークロードです。Unified Manager は、イベント中に実際の使用量が予想される使用量の範囲から大幅に増加したクラスタ コンポーネントの使用量の偏差に基づいて、問題のあるワークロードを識別します。
Shark	イベントに関連するすべてのワークロードの中でクラスタ コンポーネントの使用量が最も多いユーザ定義のワークロードです。Unified Manager は、イベント中のクラスタ コンポーネントの使用状況に基づいて、シャーク ワークロードを識別します。

クラスタのワークロードは、クラスタを構成する多数のコンポーネント（アグリゲート、ネットワーク処理やデータ処理を行うCPUなど）を共有します。そのため、あるワークロード（ボリュームなど）が使用するクラスタ コンポーネントの量が、他のワークロードに必要な量を効率的に確保できないところまで増加すると、そのコンポーネントは競合状態になります。この、クラスタ コンポーネントを過剰に消費しているワークロードが「Bully」で、同じコンポーネントを共有しているため、Bullyによってパフォーマンスに影響が出

ているワークロードが「Victim」です。重複排除やスナップショット コピーなどのシステム定義のワークロードからのアクティビティも、「いじめ」にエスカレートする可能性があります。

Unified Manager はイベントを検出すると、イベントの原因となった「bully」ワークロード、競合状態にあるクラスタ 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の増加によりパフォーマンスが低下した「victim」ワークロードなど、関連するすべてのワークロードとクラスタ コンポーネントを識別します。



Unified Manager が攻撃対象のワークロードを識別できない場合は、攻撃対象のワークロードと関連するクラスタ コンポーネントについてのみアラートを発します。

Unified Manager は、Bully ワークロードの被害者であるワークロードを識別できるだけでなく、同じワークロードが Bully ワークロードになるタイミングも識別できます。ワークロードは自身に対してBullyワークロードになることがあります。たとえば、負荷の高いワークロードがポリシー グループの制限によって調整される場合、そのワークロードが含まれるポリシー グループ内のすべてのワークロードが調整されます。継続的なパフォーマンス イベントでは、BullyワークロードまたはVictimワークロードは役割が変わったり、あるいはイベントに関連しなくなる場合があります。

パフォーマンスしきい値を管理する

パフォーマンスしきい値ポリシーを使用すると、Unified Manager がイベントを生成し、ワークロードのパフォーマンスに影響を与え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ポイントを決定できます。これらのしきい値ポリシーは、ユーザー定義 パフォーマンスしきい値と呼ばれます。

このリリースでは、ユーザー定義、システム定義、動的の各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を使用して、Unified Manager はワークロード アクティビティを分析し、適切なしきい値を決定します。ユーザー定義のしきい値の場合、多くのパフォーマンス カウンタおよびストレージ オブジェクトに対してパフォーマンスの上限を定義できます。



システム定義のパフォーマンスしきい値と動的パフォーマンスしきい値は、Unified Manager によって設定され、構成できません。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。

ユーザー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（アグリゲートとボリュームなど）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手順は次のとおりです。

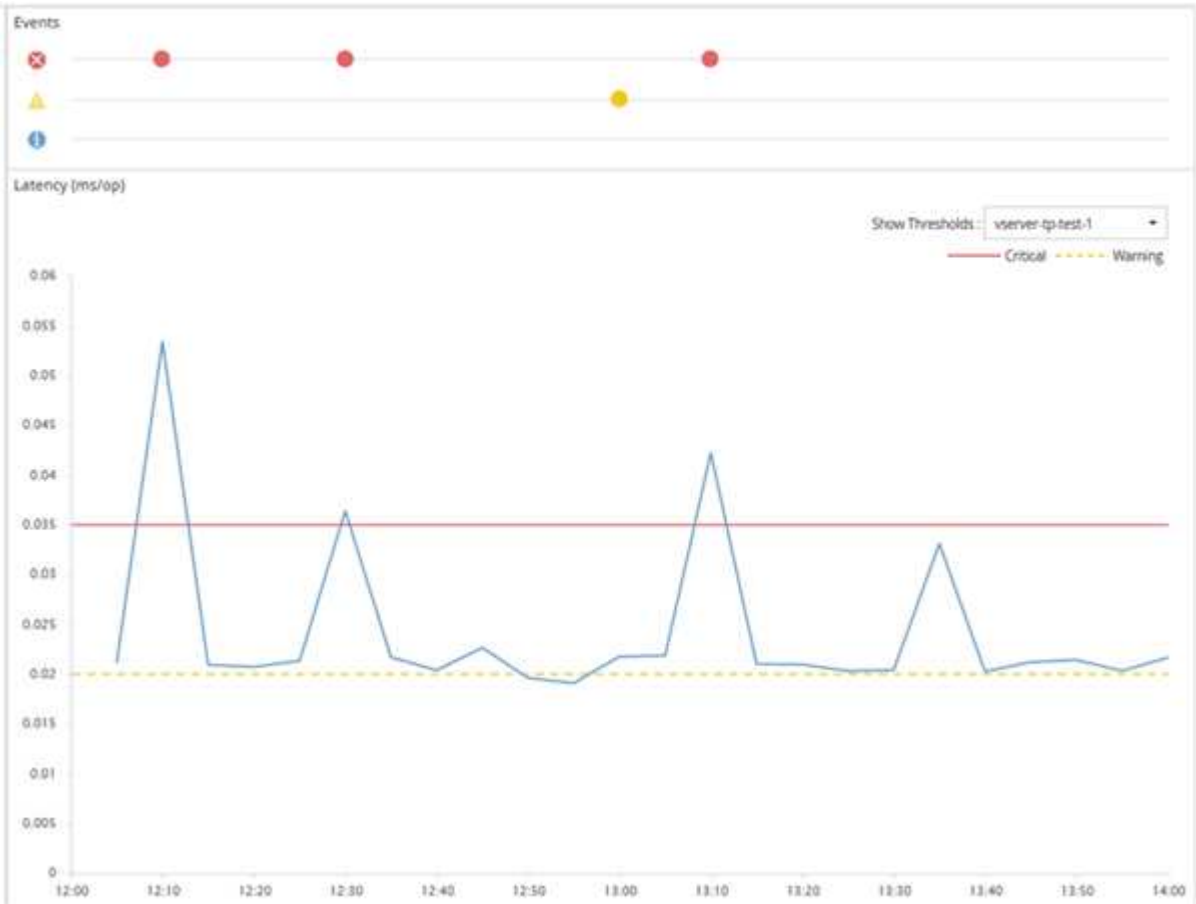
- ストレージ オブジェクトを選択する
- オブジェクトに関連付けられているパフォーマンス カウンタを選択する
- 警告および重大な状況とみなされるパフォーマンス カウンタの上限値を指定する
- カウンタが上限値を超える必要がある期間を指定する

たとえば、ボリュームのIOPSが10分間連続して1秒あたり750件の処理数を超えるたびに重大イベントの通知を受け取るように、ボリュームに対してパフォーマンスしきい値ポリシーを設定できます。同じしきい値ポリシーで、IOPSが10分間継続して1秒あたり500件の処理数を超えたときに警告イベントを送信するように指定することもできます。



現在のリリースでは、カウンタの値が設定値を超えたときにイベントを送信するしきい値を設定できます。カウンタの値が設定値を下回ったときにイベントを送信するしきい値は設定できません。

ここに示すカウンター チャートの例は、1:00 に警告しきい値 (黄色のアイコン) を超え、12:10、12:30、1:10 に重大なしきい値 (赤色のアイコン) を超えたことを示しています。



しきい値の違反は、指定された期間、継続的に発生する必要があります。何らかの理由でしきい値を下回った場合は、その次の違反が新しい期間の開始とみなされます。

一部のクラスターオブジェクトとパフォーマンス カウンタでは、2つのパフォーマンス カウンタが上限を超えた場合にイベントが生成されるしきい値ポリシーを作成できます。たとえば、次の条件を使用してしきい値ポリシーを作成できます。

クラスターオブジェクト	パフォーマンスカウンター	警告しきい値	臨界閾値	間隔
Volume	レイテンシー	10ミリ秒	20ミリ秒	15分
Aggregate	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。上の表に定義されたしきい値ポリシーを使用した場合、次のようになります

ボリュームのレイテンシが平均化している場合...	そして、ディスクの総使用率は...	操作
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 クラスターの概要ページ、イベント ページ、およびオブジェクト固有のパフォーマンス インベントリ ページに表示されます。
- (オプション) イベントに関するEメール アラートを1つ以上の受信先に送信したり、SNMPトラップをトラップ レシーバに送信したりできます。
- (オプション) ストレージ オブジェクトを自動で変更または更新するスクリプトを実行できます。

最初の処理は常に実行されます。オプションの処理を実行するかどうかは、[アラート セットアップ]ページで設定します。警告と重大の各しきい値ポリシーについて、違反した場合の処理をそれぞれ定義することができます。

ストレージ オブジェクトでパフォーマンスしきい値ポリシー違反が発生した場合、カウンタの値がしきい値を下回り、その制限の期間がリセットされるまでは、そのポリシーに対する他のイベントは生成されません。しきい値を超えた状態が続いている間は、イベントが継続していることを示すためにイベントの終了時刻が更新されていきます。

しきい値イベントには重大度やポリシー定義に関するその時点の情報がキャプチャされるため、以降にしきい値ポリシーが変更された場合でもそのイベントに対して表示されるしきい値情報は変化しません。

しきい値を使用して追跡可能なパフォーマンス カウンタ

IOPSやMBpsなど、一部の共通のパフォーマンス カウンタでは、すべてのストレージ オブジェクトを対象にしきい値を設定できます。それ以外のカウンタでは、特定のストレージ オブジェクトに対してのみしきい値を設定できます。

使用可能なパフォーマンス カウンタ

ストレージ オブジェクト	パフォーマンスカウンター	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)	レイテンシー	ノードがアプリケーションの要求に応答するまでの平均時間 (ミリ秒)
利用率	ノードのCPUとRAMの平均使用率	使用済みパフォーマンス容量
ノードによるパフォーマンス容量の平均消費率	使用済みパフォーマンス容量 - テイクオーバー	ノードによるパフォーマンス容量の平均消費率とパートナー ノードのパフォーマンス容量
Aggregate	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)	レイテンシー
アグリゲートがアプリケーションの要求に応答するまでの平均時間 (ミリ秒)	利用率	アグリゲートのディスクの平均使用率
使用済みパフォーマンス容量	アグリゲートによるパフォーマンス容量の平均消費率	Storage VM
IOPS	SVMで処理される1秒あたりの平均入出力処理数	MB/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)	レイテンシー	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)
Volume	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	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)	レイテンシー
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)	レイテンシー
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)
レイテンシー	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
帯域幅利用率	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可能なオブジェクトとカウンタ

組み合わせポリシーと一緒に使用できるパフォーマンス カウンタには種類に制限があります。プライマリとセカンダリのパフォーマンス カウンタが指定されている場合、両方のパフォーマンス カウンタが上限を超えたときにイベントが生成されます。

プライマリストレージオブジェクトとカウンタ	二次記憶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オブジェクトとカウンター	二次記憶オブジェクトとカウンター
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 FlexGroupFlexVol volume 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のは「Volume IOPS」属性と「Volume MB/s」属性のみです。しきい値ポリシーにノードまたはアグリゲートの属性が1つでも含まれていると、そのポリシーは FlexGroup ボリュームには適用されず、エラー メッセージが表示されます。これは、FlexGroup ボリュームは複数のノードまたはアグリゲートにまたがる場合があるためです。

ユーザー定義のパフォーマンスしきい値ポリシーを作成する

ストレージ オブジェクトに対するパフォーマンスしきい値ポリシーを作成して、パフォーマンス カウンタが特定の値を超えたときに通知が送信されるように設定します。イベント通知により、クラスター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。

開始する前に

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] ページでしきい値を入力します。このページですべてのポリシー値を定義して新しいポリシーを作成することも、既存のポリシーのコピーを作成してコピー内の値を変更することもできます (複製 と呼ばれます)。

有効なしきい値は、数値の場合は 0.001 ~ 10,000,000、パーセンテージの場合は 0.001 ~ 100、パフォーマンス使用容量のパーセンテージの場合は 0.001 ~ 200 です。



現在のリリースでは、カウンタの値が設定値を超えたときにイベントを送信するしきい値を設定できます。カウンタの値が設定値を下回ったときにイベントを送信するしきい値は設定できません。

手順

1. 左側のナビゲーション ペインで、イベントしきい値 > パフォーマンス を選択します。

[パフォーマンスしきい値] 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	操作
新しいポリシーを作成する	作成する
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、「複製」をクリックします。

[パフォーマンスしきい値ポリシーの作成]ページまたは[パフォーマンスしきい値ポリシーのクローン]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。

警告または重大のいずれかの制限を少なくとも1つ定義する必要があります。必ずしも両方のタイプの制限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 カウンタを含めた場合は、両方のカウンタが制限値を超えた場合にしきい値違反としてイベントが報告されます。組み合わせポリシーを使用して設定できるオブジェクトとカウンタには制限があります。

- 制限値に違反した状態がどれくらい続いたらイベントを送信するかを定義する期間を選択します。

既存のポリシーのクローンを作成する場合は、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 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。新しいポリシーをストレージ オブジェクトにすぐに適用できるように、該当するオブジェクト タイプのインベントリ ページへのリンクも表示されます。

この時点で新しいしきい値ポリシーをストレージ オブジェクトに適用する場合は、[今すぐオブジェクト タイプに移動] リンクをクリックして [インベントリ] ページに移動します。

ストレージオブジェクトにパフォーマンスしきい値ポリシーを割り当てる

パフォーマンス カウンタの値がポリシーの設定を超えたときにUnified Managerからイベントが報告されるように、ストレージ オブジェクトにユーザ定義のパフォーマンスしきい値ポリシーを割り当てます。

開始する前に

アプリケーション管理者のロールが必要です。

オブジェクトに適用するパフォーマンスしきい値ポリシーを用意しておく必要があります。

パフォーマンス ポリシーは、オブジェクトまたはオブジェクトのグループに一度に1つずつ適用できます。

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、ポリシーがすでに上限まで割り当てられたオブジェクトが含まれていると、Unified Managerでは次のように処理されます。

- 選択したオブジェクトのうち、ポリシーの数が上限に達していないすべてのオブジェクトにポリシーが適用されます。
- ポリシーの数が上限に達しているオブジェクトは無視されます。
- 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. 任意のストレージ 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	操作
単一のオブジェクト	そのオブジェクトの左にあるチェック 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にあるチェック ボックスをオンにします。
ページに表示されたすべてのオブジェクト	その  ドロップダウン ボックスで、[このページのすべてのオブジェクトを選択] を選択します。
同じタイプのすべてのオブジェクト	その  ドロップダウン ボックスで、[すべてのオブジェクトを選択] を選択します。

ソートやフィルタの機能を使用してインベントリ ページに表示されるオブジェクトのリストを絞り込むと、複数のオブジェクトにしきい値ポリシーを簡単に適用できます。

2. 選択を行い、「パフォーマンスしきい値ポリシーの割り当て」をクリックします。

[パフォーマンスしきい値ポリシーの割り当て]ページが表示され、そのタイプのストレージ オブジェクトに対応するしきい値ポリシーのリストが表示されます。

3. 各ポリシーをクリックしてパフォーマンスしきい値設定の詳細を表示し、正しいしきい値ポリシーが選択されていることを確認します。
4. 適切なしきい値ポリシーを選択したら、「ポリシーの割り当て」をクリックします。

しきい値ポリシーがオブジェクトに割り当てられたことを示すメッセージがページの上部に表示されます。このオブジェクトとポリシーに対するアラートを設定できるように、[アラート]ページへのリンクも表示されます。

特定のパフォーマンス イベントが生成されたときにEメールやSNMPトラップでアラートが通知されるようにするには、[アラート セットアップ]ページでアラートを設定する必要があります。

パフォーマンスしきい値ポリシーを表示する

[パフォーマンスしきい値]ページで、現在定義されているパフォーマンスしきい値ポリシーをすべて表示できます。

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ます。このリストには、すべてのタイプのストレージ オブジェクトのポリシーが含まれています。列ヘッダーをクリックすると、その列でポリシーをソートできます。特定のポリシーを検索する場合は、フィルタと検索を使用して、インベントリ リストに表示するしきい値ポリシーを絞り込むことができます。

ポリシー名と条件名にカーソルを合わせると、ポリシーの設定の詳細を確認できます。また、ユーザ定義のしきい値ポリシーを作成、クローニング、編集、および削除するためのボタンもあります。

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 > パフォーマンス を選択します。

[パフォーマンスしきい値]ページが表示されます。

ユーザー定義のパフォーマンスしきい値ポリシーを編集する

既存のパフォーマンスしきい値ポリシーのしきい値の設定を編集することができます。これは、特定のしきい値条件に対するアラートが多すぎたり少なすぎたりする場合に調整するのに役立ちます。

開始する前に

アプリケーション管理者のロールが必要です。

ポリシーの名前や既存のしきい値ポリシーで監視しているストレージ オブジェクトのタイプは変更できません。

手順

1. 左側のナビゲーション ペインで、イベントしきい値 > パフォーマンス を選択します。

[パフォーマンスしきい値]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、「編集」をクリックします。

[パフォーマンスしきい値ポリシーの編集]ページが表示されます。

3. しきい値ポリシーに変更を加え、[保存] 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。

変更を保存すると、そのポリシーを使用するすべてのストレージ オブジェクトにすぐに反映されます。

ポリシーに対して行った変更の種類に応じて、そのポリシーを使用するオブジェクトに対して設定されたアラート設定を[アラート セットアップ]ページで確認できます。

ストレージ オブジェクトからパフォーマンスしきい値ポリシーを削除する

Unified Managerでパフォーマンス カウンタの値を監視する必要がなくなった場合は、ストレージ オブジェクトからユーザ定義のパフォーマンスしきい値ポリシーを削除できます。

開始する前に

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つのみです。

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 オブジェクトから同じしきい値ポリシーを削除できます。

手順

1. 任意のストレージ オブジェクトの インベントリ ページから、少なくとも 1 つのパフォーマンスしきい値ポリシーが適用されている 1 つ以上のオブジェクトを選択します。

しきい値をクリアするには...	操作
単一のオブジェクト	そのオブジェクトの左にあるチェック 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にあるチェック ボックスをオンにします。
ページに表示されたすべてのオブジェクト	クリック ☐ 列ヘッダーに。

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。

選択したストレージ オブジェクトに割り当てられているしきい値ポリシーのリストが[パフォーマンスしきい値ポリシーの解除]ページに表示されます。

3. オブジェクトから削除するしきい値ポリシーを選択し、「ポリシーのクリア」をクリックします。

しきい値ポリシーを選択するとそのポリシーの詳細が表示され、正しいポリシーを選択したかどうかを確認できます。

パフォーマンスしきい値ポリシーが変更された場合の動作

既存のパフォーマンスしきい値ポリシーのカウンタの値や期間を調整した場合、そのポリシーを使用するすべてのストレージ オブジェクトに変更が反映されます。新しい設定は直ちに有効になり、Unified Manager は新しく収集されたすべてのパフォーマンス データのパフォーマンス カウンタ値と新しいしきい値設定の比較を開始します。

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、それらのイベントは「廃止」とマークされ、新たに定義されたしきい値ポリシーとしてカウンタの監視が開始されます。

しきい値が適用されているカウンタを[カウンタ グラフの詳細ビュー]で表示すると、重大と警告しきい値を示す線が現在のしきい値の設定に基づいて表示されます。このページには、古いしきい値の設定が適用されていた期間の履歴データを表示した場合も、元のしきい値の設定は表示されません。



[カウンタ グラフの詳細ビュー]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よりも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、しきい値ポリシーは新しいアグリゲートのボリュームまたはLUNで引き続きアクティブになります。

アグリゲートやノードに追加の条件が割り当てられているなど、セカンダリ カウンタ条件があるしきい値ポリシー（組み合わせポリシー）の場合、ボリュームまたはLUNが移動された新しいアグリゲートやノードにセカンダリ 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「新規」のアクティブなイベントがある場合、それらのイベントは「廃止」とマークされ、新たに定義されたしきい値ポリシーとしてカウンタの監視が開始されます。

ボリューム移動処理が実行されると、ONTAPから情報変更イベントが送信されます。[パフォーマンス エクスプローラ]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表示されます。



オブジェクトを別のクラスタに移動した場合、ユーザ定義のしきい値ポリシーはオブジェクトから削除されます。それらのしきい値ポリシーが必要な場合は、移動処理の完了後に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のテイクオーバー時とギブバック時のしきい値ポリシーの機能

ハイアベイラビリティ（HA）構成でテイクオーバー処理またはギブバック処理が発生した場合、1つのノードから別のノードに移動されたオブジェクトのしきい値ポリシーは手動による移動処理の場合と同じように保持されます。Unified Manager は 15 分ごとにクラスタ構成の変更をチェックするため、新しいノードへの切り替えの影響は、クラスタ構成の次のポーリングまで特定されません。



15分間の構成の変更の収集期間内にテイクオーバーとギブバックの両方の処理が発生した場合、ノード間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

アグリゲートのあるノードから別のノードに移動する場合、`aggregate relocation start` コマンドを実行すると、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に保持され、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の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1つのクラスタから別のクラスタにオブジェクトが移動された場合、ユーザ定義のしきい値ポリシーの設定は保持されません。それらのしきい値ポリシーが必要な場合は、パートナー クラスタに移動されたボリュームおよびLUNに適用できます。オブジェクトが元のクラスタに戻ると、それらのユーザ定義のしきい値ポリシーが自動的に再適用されます。

詳細については、"[スイッチオーバーおよびスイッチバックの発生時のボリュームの動作](#)"。

パフォーマンスイベントを分析する

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）か廃止のイベントか、関連するワークロードとクラスタ コンポーネント、およびイベントを解決するためのオプションを特定できます。

パフォーマンスイベントに関する情報を表示する

[イベント管理]インベントリ ページを使用して、Unified Managerで監視されているクラスタ上のすべてのパフォーマンス イベントのリストを表示できます。この情報を表示することにより、最も重大なイベントを特定し、詳細情報を確認してイベントの原因を特定できます。

開始する前に

- 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、[ステータス]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探している場合、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表示されます。イベントを選択すると、イベントに関する詳細を[イベントの詳細]ページで確認できます。

手順

1. 左側のナビゲーション ペインで、[イベント管理] をクリックします。
2. [表示] メニューから、[アクティブなパフォーマンス イベント] を選択します。

このページには、過去7日間に生成された「新規」と「確認済み」のすべてのパフォーマンス イベントが表示されます。

3. 分析するイベントを特定し、イベント名をクリックします。

イベントの詳細ページが表示されます。



[パフォーマンス エクスプローラ]ページおよびアラートEメールのイベント名のリンクをクリックして、イベントの詳細ページを表示することもできます。

ユーザー定義のパフォーマンスしきい値からイベントを分析する

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場合に発生します。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]ページを使用してパフォーマンス イベントを分析し、必要に応じてイベントに対処してパフォーマンスを正常な状態に戻します。

ユーザー定義のパフォーマンスしきい値イベントに応答する

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。

開始する前に

- 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。
- 新規または廃止のパフォーマンス イベントが存在する必要があります。

手順

1. イベントに関する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を説明する*説明*を確認します。

たとえば、「レイテンシ値 456 ms/op により、しきい値設定 400 ms/op に基づいて警告イベントがトリガーされました」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ます。

3. ポリシー名にカーソルを合わせて、イベントをトリガーしたしきい値ポリシーの詳細を表示します。

詳細には、ポリシー名、使用されるパフォーマンス カウンタ、超過した場合に重大または警告イベントが生成されるカウンタ値、および対象となる期間が含まれます。

4. イベント トリガー時間 をメモしておけば、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ていたかどうかを調査できます。
5. 次のどちらかのオプションを使用してイベントをさらに詳しく調査し、パフォーマンスの問題を解決するための操作を実行する必要があるかどうかを判断します。

オプション	考えられる調査措置
ソース オブジェクト名をクリックして[エクスプローラ]ページを表示する。	このページでは、オブジェクトの詳細を表示して他の同様のストレージ オブジェクトと比較し、他のストレージ オブジェクトに同じタイミングでパフォーマンスの問題が発生していないかを確認できます。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を確認できます。
クラスタ名をクリックして[クラスタ サマリ]ページを表示する。	このページでは、オブジェクトが格納されているクラスタの詳細を表示して、同じタイミングで他のパフォーマンスの問題が発生していないかを確認できます。

システム定義のパフォーマンスしきい値からイベントを分析する

システム定義のパフォーマンスしきい値で生成されたイベントは、特定のストレージ オブジェクトの1つまたは複数のパフォーマンス カウンタがシステム定義ポリシーのしきい値を超えたことを示しています。この場合、ストレージ オブジェクト（アグリゲートやノードなど）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]ページを使用してパフォーマンス イベントを分析し、必要に応じてイベントに対処してパフォーマンスを正常な状態に戻します。



システム定義のしきい値ポリシーは、Cloud Volumes ONTAP、ONTAP Edge、ONTAP Select の各システムでは無効です。

システム定義のパフォーマンスしきい値イベントに応答する

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。

開始する前に

- 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。
- 新規または廃止のパフォーマンス イベントが存在する必要があります。

手順

- イベントに関する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。
- イベントの原因となったしきい値違反を説明する*説明*を確認します。

たとえば、「ノード使用率の値が 90 % であるため、しきい値設定が 85 % に基づいて警告イベントが発生しました」というメッセージは、クラスター オブジェクトに対してノード使用率の警告イベントが発生したことを示します。

3. イベント トリガー時間 をメモしておけば、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ていたかどうかを調査できます。
4. システム診断 で、システム定義ポリシーがクラスター オブジェクトに対して実行している分析の種類の簡単な説明を確認します。

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 グラフにオブジェクトのパフォーマンスが表示されます。

5. 推奨アクション の下にある ヘルプして実行 リンクをクリックすると、パフォーマンス イベントを自分で解決するために実行できる推奨アクションが表示されます。

QoSポリシーグループのパフォーマンスイベントに応答する

ワークロードのスループット（IOPS、IOPS/TB、またはMBps）がONTAPで定義されているQoSポリシーの設定を超え、ワークロードのレイテンシに影響を及ぼしている場合、Unified ManagerでQoSポリシー警告イベントが生成されます。これらのシステム定義のイベントにより、多くのワークロードにレイテンシの影響が及ぶ前に潜在的な問題に対処することができます。

開始する前に

- 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、または廃止のパフォーマンス イベントが存在する必要があります。

Unified Managerでは、定義されているQoSポリシーの設定を超えるワークロードが過去1時間の各パフォーマンス収集期間で見つかった場合に、QoSポリシーの違反とみなして警告イベントを生成します。ワークロードのスループットは、各収集期間中に短時間のみ QoS しきい値を超えることがあります。Unified Managerは収集期間中の「平均」スループットのみをチャートに表示します。そのため、QoSのイベントを受け取った場合でも、グラフではワークロードのスループットがポリシーのしきい値を超えていないように見えることがあります。

System ManagerまたはONTAPコマンドを使用してポリシー グループを管理できます。これには次のタスクが含まれます。

- ワークロードに対する新しいポリシー 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
- 別のアグリゲートやノードへのワークロードの移動

手順

1. イベントに関する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を説明する*説明*を確認します。

たとえば、「vol1_NFS1 の IOPS 値 1,352 IOPS により、ワークロードの潜在的なパフォーマンスの問題を識別するための警告イベントがトリガーされました」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ます。

3. イベント情報 セクションで、イベントが発生した日時やイベントがアクティブになっている期間に関する詳細を確認します。

また、QoSポリシーのスループットを共有しているボリュームまたはLUNについて、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、2つのグラフを確認します。1つは合計平均 IOPS または MBps (イベントによって異なります) を示し、もう1つはレイテンシを示します。これらのグラフを確認することで、ワークロードがQoSの上限に達したときのレイテンシに影響しているクラスタ コンポーネントを特定することができます。

共有QoSポリシーのイベントについては、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、追加のワークロードは「その他のワークロード」カテゴリにまとめて追加されます。また、QoSポリシーに含まれるすべてのワークロードの平均レイテンシがレイテンシ グラフに表示されます。

アダプティブQoSポリシーのイベントの場合、IOPSおよびMBpsのグラフには、割り当てられたIOPS/TBのしきい値ポリシーをボリュームのサイズに基づいてIOPSまたはMBpsに換算した値が表示されます。

5. 推奨アクション セクションで提案を確認し、ワークロードのレイテンシの増加を避けるために実行する必要があるアクションを決定します。

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 イベントを解決するために実行できる推奨アクションの詳細を表示します。

定義されたブロックサイズを持つ適応型**QoS**ポリシーからのイベントを理解する

アダプティブQoSポリシー グループでは、ボリューム サイズに基づいてスループットの上限と下限が自動的に調整され、TBまたはGBあたりのIOPSが一定に維持されます。ONTAP 9.5以降では、QoSポリシーにブロック サイズを指定することでMB/sのしきい値も同時に適用できます。

アダプティブQoSポリシーにIOPSのしきい値を割り当てた場合、各ワークロードで発生する処理数にのみ制限だけが適用されます。ワークロードを生成するクライアントに設定されているブロック サイズによっては、一部のIOPSにはるかに多くのデータが含まれ、処理を実行するノードの負荷はるかに大きくなる場合があります。

ワークロードのMB/sは次の式を使用して算出されます。

$$\text{MB/s} = (\text{IOPS} * \text{Block Size}) / 1000$$

平均IOPSが3,000のワークロードについて、クライアントのブロック サイズが32KBに設定されている場合、このワークロードの実効MB/sは96です。平均IOPSが3,000の同じワークロードについて、クライアントのブロック サイズが48KBに設定されている場合は、このワークロードの実効MB/sは144になります。この場合、ブロック サイズが大きい方がノードでの処理データが50%多くなることがわかります。

次に、アダプティブQoSポリシーにブロック サイズが定義されている場合について、クライアントで設定されているブロック サイズに基づいてどのようにイベントがトリガーされるかを見てみましょう。

ポリシーを作成し、ピーク サイズを2,500IOPS/TB、ブロック サイズを32KBに設定します。この場合、使用

容量が1TBのボリュームに対するMB/sのしきい値は80MB/s ($(2500\text{IOPS} * 32\text{KB}) / 1000$) に設定されます。Unified Managerでは、スループットの値が定義されたしきい値の90%に達すると警告イベントが生成されます。イベントが生成される状況は次のとおりです。

使用容量	スループットがこの数値を超えるとイベントが生成されます。	
	IOPS	MB/秒
1 TB	2,250 IOPS	72MB/s
2 TB	4,500 IOPS	144MB/s
5 TB	11,250 IOPS	360MB/s

ボリュームの使用可能なスペースが2TB、IOPSが4,000、クライアントで設定されているQoSブロック サイズが32KBである場合、スループットは128MB/s ($(4,000\text{ IOPS} * 32\text{KB}) / 1000$) になります。この場合、4,000 IOPSと128MB/sのどちらについても、ボリュームで2TBのスペースを使用する場合のしきい値を超えていないため、イベントは生成されません。

ボリュームの使用可能なスペースが2TB、IOPSが4,000、クライアントで設定されているQoSブロック サイズが64KBである場合、スループットは256MB/s ($(4,000\text{ IOPS} * 64\text{KB}) / 1000$) になります。この場合、4,000 IOPSについてはイベントは生成されませんが、MB/sの値については256MB/sでしきい値の144MB/sを超えているためイベントが生成されます。

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、[イベントの詳細]ページの[システム診断]セクションにはMBpsのグラフが表示されます。アダプティブ QoS ポリシーの IOPS 違反に基づいてイベントがトリガーされた場合、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MB/sの両方に違反がある場合は、2つのイベントが表示されます。

QoS設定の調整の詳細については、以下を参照してください。 ["パフォーマンス管理の概要"](#)。

ノードリソースの過剰利用パフォーマンスイベントに応答する

1つのノードが運用効率の上限を超えて稼働していて、ワークロードのレイテンシに影響を及ぼしている可能性がある場合、Unified Managerでノード リソース過剰使用警告イベントが生成されます。これらのシステム定義のイベントにより、多くのワークロードにレイテンシの影響が及ぶ前に潜在的な問題に対処することができます。

開始する前に

- 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。
- 新規または廃止のパフォーマンス イベントが存在する必要があります。

Unified Managerでは、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。

このタイプのパフォーマンスの問題には、System ManagerまたはONTAPコマンドを使用して次のように対処できます。

- QoSポリシーを作成してシステム リソースの使用率が高いボリュームやLUNに適用する。

- ワークロードが適用されているポリシー グループのQoSの最大スループット制限を小さくする。
- 別のアグリゲートやノードへのワークロードの移動
- ノードにディスクを追加するか、ノードのCPUやRAMをアップグレードして、ノードの容量を増やす。

手順

1. イベントに関する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を説明する*説明*を確認します。

たとえば、メッセージ「Perf.シンプルさ-02 の使用済み容量値が 139% であるため、データ処理ユニットの潜在的なパフォーマンスの問題を識別するための警告イベントがトリガーされました。」は、ノード シンプルさ-02 のパフォーマンス容量が過剰に使用されており、ノードのパフォーマンスに影響を与え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のレイテンシです。これらのグラフを確認することで、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特定することができます。

どのワークロードにQoSポリシーが適用されていて、どのワークロードに適用されていないかを表示するには、IOPSグラフにカーソルを合わせます。

4. 推奨アクション セクションで提案を確認し、ワークロードのレイテンシの増加を避けるために実行する必要があるアクションを決定します。

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 イベントを解決するために実行できる推奨アクションの詳細を表示します。

クラスターの不均衡なパフォーマンスイベントに応答する

Unified Managerは、クラスタ内の1つのノードの負荷が他のノードよりもはるかに高く、ワークロードのレイテンシに影響を及ぼしている可能性がある場合、クラスタ不均衡警告イベントを生成します。これらのシステム定義のイベントにより、多くのワークロードにレイテンシの影響が及ぶ前に潜在的な問題に対処することができます。

開始する前に

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%を超えるノードが見つかった場合、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. イベントに関する情報を表示するには、「イベント」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を説明する*説明*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、クラスター Dallas-1-8 上のノード間の負荷差が 62% で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がトリガーされました」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が過剰に使用されており、ノードのパフォーマンスに影響を与えていることを示します。

3. 推奨アクション のテキストを確認して、高パフォーマンスのボリュームを、使用済みパフォーマンス容量値の高いノードから、使用済みパフォーマンス容量値が最低のノードに移動します。
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 クラスターの名前をクリックします。
 - b. クラスターパフォーマンス サマリー ページで、管理対象オブジェクト 領域の ノード をクリックします。
 - c. ノード インベントリ ページで、使用済みパフォーマンス容量 列でノードを並べ替えます。
 - 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 エクスプローラー ページで、表示と比較 メニューから このノードの集計 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 エクスプローラー ページで、表示と比較 メニューから このアグリゲートのボリュームを選択します。
 - e. ボリュームを **IOPS** 列で並べ替え、最も多くの IOPS を使用するボリュームの名前と、そのボリュームが存在するアグリゲートの名前を書き留めます。
6. 使用済みパフォーマンス容量の値が最も低いノードの使用率が最も低いボリュームを特定します。
 - a. ストレージ > アグリゲート をクリックして、アグリゲート インベントリ ページを表示します。
 - b. パフォーマンス: すべての集計 ビューを選択します。
 - c. フィルター ボタンをクリックし、「Node」が手順 4 で書き留めた使用済みパフォーマンス容量値が最も低いノードの名前と等しいフィルターを追加します。
 - 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メモします。
7. 新しいノードの使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の組み合わせを使用して実行できます。

数日後、このクラスターから同じクラスター不均衡イベントを受け取っていないかを確認します。

動的パフォーマンスしきい値からイベントを分析する

動的なしきい値によるイベントは、ワークロードの実際の応答時間（レイテンシ）と想

定範囲との差が大きい場合に生成されます。[イベントの詳細]ページを使用してパフォーマンス イベントを分析し、必要に応じてイベントに対処してパフォーマンスを正常な状態に戻します。



動的なパフォーマンスしきい値は、Cloud Volumes ONTAP、ONTAP Edge、ONTAP Selectの各システムでは無効です。

動的パフォーマンス イベントに関係する被害ワークロードを特定する

Unified Managerでは、競合状態のストレージ コンポーネントが原因の応答時間（レイテンシ）の偏差が最も高いボリューム ワークロードを特定できます。このようなワークロードを特定すると、そのワークロードにアクセス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通常よりも遅い理由を把握できます。

開始する前に

- 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、または廃止の動的なパフォーマンス イベントが存在する必要があります。

[イベントの詳細]ページには、コンポーネントのアクティビティまたは使用量の偏差が大きい順、またはイベントの影響が大きい順に、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. イベントに関する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. ワークロードのレイテンシとワークロード 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。

動的パフォーマンスイベントに関係するワークロードを特定する

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。

開始する前に

- 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、または廃止の動的なパフォーマンス イベントが存在する必要があります。

[イベントの詳細]ページには、コンポーネントの使用量が多い順、またはイベントの影響が大きい順に、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. ワークロードのレイテンシとワークロード 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。

動的パフォーマンスイベントに関係するシャークワークロードを特定する

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。

開始する前に

- 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、または廃止の動的なパフォーマンス イベントが必要です。

[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. イベントに関する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. ワークロードのレイテンシとワークロード アクティビティのグラフで、**Shark** ワークロード 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、クラスタ間のスイッチ間リンク (ISL) を過剰に使用している *bully* ワークロード、またはリンクの健全性の問題が原因である可能性があります。Unified Manager は、パートナー クラスタのパフォーマンス イベントを考慮せずに、MetroCluster構成内の各クラスタを個別に監視します。

MetroCluster構成内の両方のクラスタのパフォーマンス イベントは、Unified Managerの[ダッシュボード]ページにも表示されます。また、Unified Manager のヘルス ページを表示して、各クラスターのヘルスをチェックし、それらの関係を表示することもできます。

MetroCluster構成のクラスタ上の動的パフォーマンスイベントを分析する

Unified Managerを使用して、パフォーマンス イベントが検出されたMetroCluster構成のクラスタについて分析することができます。クラスター名、イベント検出時間、関連する *bully* および *victim* ワークロードを識別できます。

開始する前に

- 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構成についての新規、確認済み、または廃止のパフォーマンス イベントが検出されている必

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. イベントに関する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. イベントの説明を参照して、関連するワークロードの名前と数を確認します。

この例では、[MetroCluster Resources]アイコンが赤色で表示されており、MetroClusterのリソースが競合状態にあることがわかります。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す。

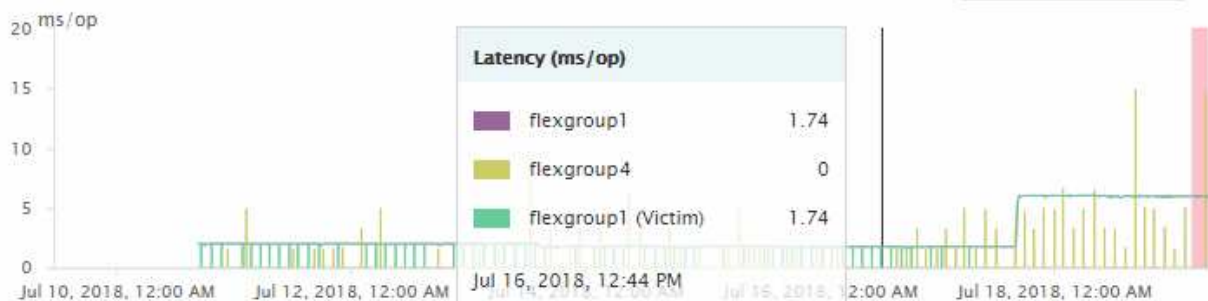


3. クラスタの名前とイベントの検出時刻を書き留めます。この情報は、パートナー クラスタのパフォーマンス イベントを分析するときに使用します。
4. グラフで、*victim* ワークロードを確認し、その応答時間がパフォーマンスしきい値よりも高いことを確認します。

この例では、マウスオーバーで表示される情報にVictimワークロードが表示されています。[レイテンシ]グラフを確認すると、関連するVictimワークロードの全体的なレイテンシのパターンは一貫していることがわかります。Victimワークロードの異常なレイテンシによってイベントがトリガーされた場合でも、レイテンシのパターンが一貫していれば、ワークロードのパフォーマンスは想定範囲内に収まっており、I/Oの一時的な上昇によってレイテンシが増加したことでイベントがトリガーされた可能性が考えられます。

System Diagnosis (Jul 9, 2018, 11:09 AM - Jul 19, 2018, 7:39 AM) ?

Workload Latency



これらのボリュームのワークロードにアクセスするアプリケーションでクライアントに最近インストールしたものがある場合は、そのアプリケーションから大量のI/Oが送信されたことが原因でレイテンシが増加した可能性があります。ワークロードのレイテンシが想定範囲内に戻ってイベントの状態が廃止に変わり、その状態が30分以上続くようであれば、このイベントは無視しても問題がないと考えられます。イベントが新規の状態のまま継続する場合は、イベントの原因となった問題が他にないかどうかをさらに詳しく調べます。

5. ワークロード スループット チャートで、**Bully** ワークロード 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のリソースを過剰に消費しているためにイベントが発生した可能性が考えられます。Bullyワークロードの書き込みスループット（MBps）の偏差が大きくなっています。

このグラフから、ワークロードの全体的な書き込みスループット（MBps）のパターンがわかります。書き込みMBpsのパターンからスループットの異常が認められるため、ワークロードがMetroClusterのリソースを過剰に使用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やパートナー クラスタのパフォーマンスの問題がイベントの原因として考えられます。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構成上のリモート クラスタの動的パフォーマンス イベントを分析する

Unified Managerを使用して、MetroCluster構成のリモート クラスタの動的なパフォーマンス イベントを分析できます。この分析によって、リモート クラスタのイベントがそのパートナー クラスタのイベントの原因となったかどうかを判断できます。

開始する前に

- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- MetroCluster構成内のローカル クラスタのパフォーマンス イベントを分析し、イベント検出時刻を確認しておく必要があります。
- パフォーマンス イベントに関連したローカル クラスタとそのパートナー クラスタの健全性を確認し、パートナー クラスタの名前を確認しておく必要があります。

手順

1. パートナー クラスタを監視しているUnified Managerインスタンスにログインします。
2. 左側のナビゲーション ペインで [イベント] 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*セクターから*過去1時間*を選択し、*範囲の適用*をクリックします。
4. *フィルタリング*セクターで、左側のドロップダウン メニューから*クラスター*を選択し、テキスト フィールドにパートナー クラスターの名前を入力して、*フィルターの適用*をクリックします。

選択したクラスタのイベントが過去1時間ない場合は、パートナーでイベントが検出されたときにこのクラスタではパフォーマンスの問題は発生していません。

5. 選択したクラスタで過去1時間にイベントが検出された場合は、イベントの検出時刻をローカル クラスタのイベントの検出時刻と比較します。

これらのイベントにデータ処理コンポーネントの競合を引き起こしているBullyワークロードが関係している場合は、これらのBullyワークロードが原因でローカル クラスタのイベントが発生した可能性があります。イベントをクリックし、[イベントの詳細] ページで分析して推奨される解決方法を確認できます。

これらのイベントにBullyワークロードが関係していない場合、ローカル クラスタのパフォーマンス イベントの原因はBullyワークロードではありません。

QoS ポリシー グループのスロットリングによって発生する動的なパフォーマンス イベントに応答する

Unified Managerを使用して、ワークロードのスループット (MBps) を調整しているサービス品質 (QoS) ポリシー グループが原因のパフォーマンス イベントを調査できます。この調整によって、ポリシー グループ内のボリューム ワークロードの応答時間 (レイテンシ) が増大することがあります。イベント情報を使用して、ポリシー グループに新しい制限値を設定して調整を停止する必要があるかどうかを判断できます。

開始する前に

- 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、または廃止のパフォーマンス イベントが存在する必要があります。

手順

1. イベントに関する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. 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る 説明 をお読みください。



調整の結果、あるワークロードは自身の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. ワークロードのレイテンシとワークロード使用率のグラフで、**Bully Workloads** を選択します。
5. グラフにカーソルを合わせると、ポリシー グループに影響を与えている上位のユーザ定義ワークロードが表示されます。

偏差が最も大きく、調整の原因となったワークロードがリストの最上位に表示されます。アクティビティは、ポリシー グループ制限に対して各ワークロードが使用している割合です。

6. *推奨アクション*領域で、上位のワークロードの*ワークロードの分析*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. レイテンシ チャートの QoS 制限を比較して、イベント発生時にどの程度の調整がレイテンシに影響を与えたかを確認します。

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。イベントの発生時、ポリシー グループ内のワークロードの合計スループットが1,200op/secを超えたため、ポリシー グループのアクティビティが1,000op/secに調整されました。

9. 読み取り/書き込みレイテンシ の値を 読み取り/書き込み/その他 の値と比較します。

どちらのグラフも、待ち時間が長い読み取り要求の数が多いことを示していますが、書き込み要求の要求数と待ち時間は低くなっています。これらの値は、スループットが高いか、またはレイテンシを増加させる操作の数が多い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

ループの制限を設定するかどうかを決定する際に使用できます。

10. ONTAP System Manager を使用して、ポリシー グループの現在の制限を 1,300 op/sec に増やします。
11. 1 日後、Unified Manager に戻り、手順 3 で記録したワークロードを ワークロード分析 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. ページ上部の変更イベントアイコン (●) をクリックして、ポリシー グループの制限を変更します。
14. *読み取り/書き込み/その他*チャートを*待ち時間*チャートと比較します。

読み取り要求と書き込み要求は同じですが、スロットルが停止し、レイテンシが減少しました。

ディスク障害によって発生する動的なパフォーマンスイベントに対応する

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。

開始する前に

- 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、または廃止のパフォーマンス イベントが存在する必要があります。

手順

1. イベントに関する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. *説明*を読んでください。そこには、イベントに関係するワークロードと競合しているクラスター コンポーネントが説明されています。

競合状態のクラスター 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ー コンポーネントです。[競合しているコンポーネント]の下にアグリゲート アイコンが赤で強調表示され、かっこ内にアグリゲートの名前が表示されます。

3. ワークロード使用率チャートで、*Bully ワークロード*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ワークロードとこのアグリゲートの他のワークロードが組み合わされて、アグリゲートでの競合および関連するイベントを引き起こした可能性があります。

5. Disk Healthワークロードのアクティビティがイベントの原因であることを確認したら、再構築が完了し、Unified Managerがイベントを分析してアグリゲートが引き続き競合状態にあるかを検出するまで約30分待ちます。

6. *イベントの詳細*を更新します。

RAIDの再構築が完了したら、[状態]が「廃止」になったことを確認します。これは、イベントが解決されたことを示します。

7. ワークロード使用率チャートで、「Bully ワークロード」を選択し、ピーク使用率別に集計上のワークロードを表示します。
8. *推奨アクション*領域で、上位のワークロードの*ワークロードの分析*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) のデータが表示されるように時間範囲を設定します。

イベントタイムラインでは、赤い点 (●) 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、ノード統計の行を非表示にし、アグリゲートの行だけを表示します。
11. このグラフのデータを、**Latency** グラフのイベント発生時のデータと比較します。

[アグリゲート利用率]では、イベント発生時にRAIDの再構築プロセスが原因の多数の読み取り / 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テイクオーバーによって発生する動的なパフォーマンスイベントに対応する

Unified Managerを使用して、ハイアベイラビリティ (HA) ペアを構成するクラスタ ノードでの大量のデータ処理が原因のパフォーマンス イベントを調査できます。また、Unified Managerを使用してノードの健全性を確認し、ノードで検出された最近の健全性イベントがパフォーマンス イベントに関与しているかどうかを判断できます。

開始する前に

- 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、または廃止のパフォーマンス イベントが存在する必要があります。

手順

1. イベントに関する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. *説明*を読んでください。そこには、イベントに関係するワークロードと競合しているクラスター コンポーネントが説明されています。

競合状態のクラスタ コンポーネントによってレイテンシが影響を受けたVictimボリュームが1つあります。パートナー ノードからすべてのワークロードをテイクオーバーしてデータを処理中のノードが、競合状態のクラスタ コンポーネントです。[競合しているコンポーネント]の下に[データ処理]アイコンが赤で強調表示され、イベント発生時にデータを処理していたノードの名前がカッコ内に表示されます。

3. *説明*で、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。ページ上部のイベントタイムラインに、イベント変更アイコン (●) 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ます。HAテイクオーバーの詳細がホバーテキストで表示されます。

[レイテンシ]グラフに表示されたイベントから、HAテイクオーバーと同じタイミングで発生した高レイテンシが原因で、選択したボリュームでパフォーマンスしきい値を超えたことがわかります。

5. *ズーム表示*をクリックすると、新しいページにレイテンシ チャートが表示されます。
6. [表示] メニューで [クラスター コンポーネント] を選択して、クラスター コンポーネントごとの合計レイテンシを表示します。
7. HAテイクオーバーの開始を示す変更イベント アイコンにマウス カーソルを合わせ、データ処理のレイテンシを合計レイテンシと比較します。

HAテイクオーバーの実行時に、データ処理ノードでワークロード需要が増加したためにデータ処理のレイテンシが急増しています。CPU利用率の増加によってレイテンシが増加し、イベントがトリガーされました。

8. 障害が発生したノードを修復したあと、ONTAP System Managerを使用してHAギブバックを実行します。ワークロードはパートナー ノードから修復されたノードに移動します。
9. HA ギブバックが完了したら、Unified Manager で次の構成検出 (約 15 分後) を行った後、イベント管理インベントリ ページで 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見つけます。

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確認できます。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を解決する

推奨される対処方法を使用して、パフォーマンス イベントを解決することができます。最初の3つの推奨策は常に表示され、表示されたイベントに固有の推奨策が4つ目以降に表示されます。

ヘルプ リンクでは、特定のアクションを実行するための手順など、提案された各アクションに関する追加情報が提供されます。一部の対処方法では、Unified Manager、ONTAP System Manager、OnCommand Workflow Automation、ONTAP CLIコマンド、またはこれらのツールの組み合わせを使用する場合があります。

レイテンシが予想範囲内であることを確認する

クラスター コンポーネントが競合状態にある場合、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) が減少する可能性があります。競合しているコンポーネント上の各被害者ワークロードのレイテンシを確認し、実際のレイテンシが予想範囲内であ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

ディスク障害、HAフェイルオーバー、ボリリューム移動などを原因とするクラスタの構成変更が、ボリ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、最新の構成変更がいつ行われたかを確認し、処理やレイテンシ（応答時間）と比較して、選択したボリリュームのワークロードのアクティビティに変化が生じたかどうかを確認できます。

Unified Manager のパフォーマンス ページでは、限られた数の変更イベントのみを検出できます。健全性のページには、構成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 でボリリュームを検索して、イベント履歴を表示できます。

クライアント側からワークロード パフォーマンスを改善するためのオプション

パフォーマンス イベントに関係するボリリュームに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）を確認して、クライアント側の変更によってイベントを修正できるかどうかを判断できます。

クラスタ上のボリリュームに接続されたクライアントのI/O要求が増加すると、その要求に対応するためにクラスタの負荷が増大します。クラスタの特定のボリリュームに大量のI/O要求を送信しているクライアントがわかれば、そのボリリュームにアクセスするクライアントの数を調整するか、またはボリリュームに送信されるI/Oの量を減らすことで、クラスタのパフォーマンスを改善できます。また、このボリリュームが属しているQoSポリシー グループに上限を適用したり、上限を引き上げたりすることもできます。

クライアントとそのアプリケーションを調査して、クライアントが通常よりも多くのI/Oを送信していることがクラスタ コンポーネントでの競合の原因となっていないかを確認できます。[イベントの詳細]ページの[システム診断]セクションには、競合状態にあるコンポーネントを使用する上位のボリリューム ワークロードが表示されます。特定のボリ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 クラスタ上のボリリュームへの書き込み要求が、リモート クラスタ上のボリリュームにミラーされます。ローカル クラスタ上のソース ボリリュームとリモート クラスタ上のデスティネーション ボリリュームの同期を維持することで、MetroCluster構成での両クラスタの要求が増加する可能性もあります。このようなミラー ボリリュームへの書き込み要求を減らすことで、クラスタが実行する同期処理が減り、他のワークロードのパフォーマンスに与える影響を軽減できます。

クライアントまたはネットワークに問題がないかどうかの確認

クラスタ上のボリリュームに接続されたクライアントのI/O要求が増加すると、その要求に対応するためにクラスタの負荷が増大します。クラスタの需要が増加すると、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遅延が増加し、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、競合状態にあるコンポーネントを使用する上位のボリリューム ワークロードが表示されます。特定のボリリュームにアクセスしているクライアントがわかった場合は、そのクライアントに移動して、クライアントのハードウェアまたはアプリケーションが正常に動作しているか、あるいは通常より負荷が増えていないかを確認できます。クライアント管理者またはアプリケーション

ンベンダーにサポートを依頼しなければならない場合があります。

ネットワークインフラを確認することで、クラスタと接続されているクライアントとの間のI/O要求の実行速度が想定よりも遅くなる原因となるハードウェアの問題、ボトルネック、またはワークロードの競合が発生しているかどうかを判断できます。ネットワーク管理者にサポートを依頼しなければならない場合があります。

QoSポリシーグループ内の他のボリュームのアクティビティが異常に高いかどうかを確認します

アクティビティの変化が最も大きいQoSポリシーグループ内のワークロードを確認すると、複数のワークロードがイベントの原因となったかどうかを判断できます。また、他のワークロードがスループット制限を超えているかどうか、またはアクティビティの想定範囲内に戻ったかどうかを確認することもできます。

[イベントの詳細]ページの[システム診断]セクションで、ワークロードをアクティビティのピーク偏差でソートして、アクティビティの変化が最も大きいワークロードをテーブルの先頭に表示することができます。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可能性のある「bullies」である可能性があります。

各ボリュームワークロードの[ワークロード分析]ページに移動して、そのIOPSアクティビティを確認できます。処理のアクティビティが非常に高い期間が存在するワークロードは、イベントの原因となった可能性があります。ワークロードのポリシーグループの設定を変更したり、ワークロードを別のポリシーグループに移動したりできます。

ONTAP System ManagerまたはONTAP CLIコマンドを使用して、ポリシーグループを次のように管理できます。

- ポリシーグループを作成します。
- 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します。
- ポリシーグループのスループット制限を変更します。

論理インターフェイス（LIF）の移動

論理インターフェイス（LIF）を負荷の低いポートに移動すると、負荷分散を改善できるほか、メンテナンス処理やパフォーマンスの調整、間接アクセスの軽減に役立ちます。

間接アクセスは、システムの効率を低下させる可能性があります。間接アクセスは、ボリュームワークロードでネットワーク処理とデータ処理に別々のノードが使用されている場合に発生します。間接アクセスを軽減するにはLIFを再配置します。つまり、ネットワーク処理とデータ処理に同じノードが使用されるようにLIFを移動します。負荷の高いLIFが自動的に別のポートに移動されるようにONTAPで負荷分散を設定することも、LIFを手動で移動することもできます。

利点	考慮事項
• 負荷分散が改善されます。 • 間接アクセスが軽減されます。	 CIFS共有に接続されているLIFを移動すると、CIFS共有にアクセスするクライアントが切断されます。CIFS共有に対する読み取り要求や書き込み要求はすべて中断されます。

負荷分散の設定にはONTAPコマンドを使用します。詳細については、ONTAPのネットワークに関するドキュメントを参照してください。

LIFを手動で移動する場合は、ONTAP System ManagerとONTAP CLIコマンドを使用します。

負荷の低い時間帯でのStorage Efficiency処理の実行

Storage Efficiency処理に適用されるポリシーやスケジュールを変更して、影響を受けるボリューム ワークロードの負荷が低いときにStorage Efficiency処理を実行するように設定できます。

Storage Efficiency処理では、大量のクラスタCPUリソースが使用されて、処理を実行するボリュームの負荷が高くなることがあります。Storage Efficiency処理の実行中に、影響を受けるボリュームでアクティビティレベルが上がると、レイテンシが高くなってイベントがトリガーされる可能性があります。

[イベントの詳細]ページの[システム診断]セクションには、Bullyワークロードを特定できるように、QoSポリシー グループのワークロードがアクティビティのピーク偏差の順に表示されます。表の上部近くに「ストレージ効率」が表示されている場合は、これらの操作が被害者のワークロードを圧迫しています。これらのワークロードがあまり忙しくないときに実行す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ことで、ストレージ効率化操作によってクラスター上で競合が発生するのを防ぐことができます。

効率化ポリシーの管理には、ONTAP System Managerを使用できます。効率化ポリシーとスケジュールの管理には、ONTAPコマンドを使用できます。

Storage Efficiencyとは

Storage Efficiencyを使用すると、低コストで最大限のデータを格納し、スペースを節約しつつ、急増するデータに対応することができます。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。

ストレージ効率には、シン プロビジョニング、スナップショット コピー、重複排除、データ圧縮、FlexClone、SnapVaultとボリュームSnapMirrorによるシン レプリケーション、RAID-DP、Flash Cache、Flash Pool アグリゲート、FabricPool対応アグリゲートなどのテクノロジーの使用が含まれ、これらはストレージ使用率の向上とストレージ コストの削減に役立ちます。

ユニファイド ストレージ アーキテクチャでは、Storage Area Network (SAN;ストレージ エリア ネットワーク)、Network-Attached Storage (NAS;ネットワーク接続型ストレージ)、および単一プラットフォーム上のセカンダリ ストレージを効率的に統合できます。

Flash Pool アグリゲート内で構成された、または Flash Cache と RAID-DP テクノロジーを使用して構成され

たシリアル SATA (Advanced Technology Attachment) ドライブなどの高密度ディスク ドライブは、パフォーマンスと復元力に影響を与えることなく効率を向上させます。

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）が、クラウド階層として指定した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）を管理するのに役立ちます。

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により、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配置

アグリゲートにディスクを追加すると、ストレージ容量を増やし、そのアグリゲートのパフォーマンスを高めることができます。ディスクを追加したあと、追加したディスクにデータを再配置するまでは読み取りパフォーマンスは向上しません。

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よってトリガーされた集計イベントを Unified Manager が受信した場合、次の手順を使用できます。

- 動的しきい値のイベントを受信した場合、[イベントの詳細]ページで、競合状態にあるアグリゲートを表すクラスタ コンポーネントのアイコンが赤でハイライト表示されます。

そのアイコンの下に、ディスクを追加できるアグリゲートの名前がかっこ内に表示されます。

- システム定義のしきい値のイベントを受信した場合、[イベントの詳細]ページで、問題があるアグリゲートの名前がイベントの説明のテキストに表示されます。

そのアグリゲートにディスクを追加してデータを再配置できます。

アグリゲートに追加できるのは、クラスタにすでに存在しているディスクだけです。クラスタに使用可能なディスクが残っていない場合は、必要に応じて管理者に問い合わせるか追加のディスクを購入してください。アグリゲートへのディスクの追加は、ONTAP System ManagerまたはONTAPのコマンドを使用して実行できます。



データの再配置を行うのは、HDDアグリゲートまたはFlash Poolアグリゲートを使用している場合だけです。SSDアグリゲートまたはFabricPoolアグリゲートにはデータを再配置しないでください。

ノードでFlash Cacheを有効にしてワークロード パフォーマンスを改善する仕組み

クラスタ内の各ノードでFlash Cache™インテリジェント データ キャッシングを有効にすることで、ワークロード パフォーマンスを改善できます。

Flash Cacheモジュール（PCIeベースのメモリ モジュールであるPerformance Acceleration Module）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して、ランダム リード中心のワークロードのパフォーマンスを最適化します。このハードウェアは、ONTAPのWAFL外部キャッシュ ソフトウェア コンポーネントと連携して機能します。

Unified Managerの[イベントの詳細]ページでは、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。このアイコンの下には、アグリゲートを特定するアグリゲート名がカッコ内に表示されます。このアグリゲートが配置されているノードでFlash Cacheを有効にすることができます。

ONTAP System ManagerまたはONTAPコマンドを使用して、Flash Cacheがインストールされて有効になっているかを確認でき、有効になっていない場合は有効にすることができます。次のコマンドは、特定のノードでFlash Cacheが有効になっているかどうかを示します。

```
cluster::> run local options flexscale.enable
```

Flash Cacheとその使用要件については、次のテクニカル レポートを参照してください。

["テクニカルレポート 3832: フラッシュキャッシュのベストプラクティスガイド"](#)

ストレージ アグリゲートでFlash Poolを有効にしてワークロード パフォーマンスを改善する仕組み

アグリゲート上でFlash Pool 機能を有効にすると、ワークロードのパフォーマンスを向上させることができます。フラッシュ プールは、HDD と SSD の両方を組み込んだアグリゲートです。プライマリ ストレージにはHDDを使用し、SSDを使用して読み取りと書き込みの高性能なキャッシュを実現することで、アグリゲートのパフォーマンスを向上させることができます。

Unified Managerの[イベントの詳細]ページには、競合状態にあるアグリゲートの名前が表示されます。ONTAP System ManagerまたはONTAPコマンドを使用して、アグリゲートでFlash Poolが有効になっているかどうかを確認できます。SSDを搭載している場合は、コマンドライン インターフェイスを使用して有効にすることができます。SSD がインストールされている場合は、アグリゲート上で次のコマンドを実行して、Flash Pool が有効になっているかどうかを確認できます。

```
cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled
```

このコマンドでは、`aggr\_name`競合中の集約などの集約の名前です。

Flash Pool とその使用要件の詳細については、『Clustered Data ONTAP物理ストレージ管理ガイド』を参照してください。

MetroCluster構成の健全性チェック

Unified Managerでは、MetroCluster over IP構成とMetroCluster over FC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。

電子メールアラートを送信するように Unified Manager を設定すると、パフォーマンス イベントの原因となっている可能性のあるローカル クラスタまたはリモート クラスタの健全性に関する問題を電子メールで確認できます。Unified Manager GUI では、イベント管理 を選択して現在のイベントの一覧を表示し、フィルターを使用してMetroCluster構成イベントのみを表示できます。

詳細については、["MetroCluster構成のクラスタの健全性チェック"](#)

MetroCluster構成の検証

MetroCluster over FC構成およびMetroCluster over IP構成でミラーされたワークロード

にパフォーマンスの問題が発生しないようにするには、MetroCluster構成が正しくセットアップされていることを確認します。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することで、ワークロードのパフォーマンスを向上させることもできます。

参照 ["MetroClusterのドキュメント"](#)ファイバ チャネル (FC) スイッチ、ケーブル、およびスイッチ間リンク (ISL) を含むMetroCluster構成でクラスタを設定する手順について説明します。このガイドは、ローカル クラスタとリモート クラスタがミラー ボリューム データと通信できるようにMetroClusterソフトウェアを設定する際にも役立ちます。 MetroCluster over IP セットアップに固有の情報については、以下を参照してください。 ["MetroCluster IP構成の設置"](#)。

MetroCluster構成を以下の要件と比較することができます。 ["MetroClusterのドキュメント"](#) MetroCluster構成内のコンポーネントを変更またはアップグレードすると、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します。この比較によって、次の点を確認できます。

- コントローラがワークロードに適しているか。
- スループットの処理能力を高めるために、ISLバンドルをより大きな帯域幅にアップグレードする必要があるか。
- 帯域幅を増やすためにスイッチ上でバッファ間クレジット（BBC）を調整できるか。
- ワークロードにSSDストレージへの大量の書き込みスループットがある場合、そのスループットに対応するためにFC-to-SASブリッジをアップグレードする必要があるか。

関連情報

- MetroClusterコンポーネントの交換またはアップグレードの詳細については、 ["MetroClusterのドキュメント"](#)。
- コントローラのアップグレードについては、以下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"](#)そして ["スイッチオーバーとスイッチバックを使用したMetroCluster IP 構成のコントローラのアップグレード"](#)

ワークロードを別のアグリゲートに移動する

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。

開始する前に

- 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、アグリゲートが存在するクラスター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*ペインから*集計*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. *使用率*列をクリックすると、集計を最も使用率の低い順に並べ替えることができます。

また、*空き容量*が最も大きい集計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*セレクターから*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時間より長い期間のパフォーマンス履歴を表示できます。過去72時間だけでなく常に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. *表示と比較*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およびFlexGroupコンスチチュエント ボリュームのリストが表示されます。

- d. ボリュームをMBpsの高い順に並べ替えたあとにIOPSの高い順に並べ替えることで、最も負荷の高いボリュームがわかります。

- e. 別のアグリゲートに移動するボリュームの名前を書き留めます。

3. 事前に特定した利用率の低いアグリゲートに負荷の高いボリュームを移動します。

移動処理は、ONTAP System Manager、OnCommand Workflow Automation、ONTAPコマンド、またはこれらのツールの組み合わせを使用して実行できます。

数日後に、移動先のノードまたはアグリゲートから同じタイプのイベントを受け取っていないかどうかを確認します。

ワークロードを別のノードに移動する

ワークロードが現在実行されているノードよりも負荷の低い別のノード上のアグリゲートをUnified Managerで特定し、選択したボリュームをそのアグリゲートに移動できま

す。負荷の低いノード上のアグリゲートに負荷の高いワークロードを移動すれば、両ノードでのワークロードの効率が向上します。

開始する前に

- 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. *イベントの詳細*ページで、ノードが存在するクラスター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 タブで、管理対象オブジェクト ペインから 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*列をクリックすると、使用率の最も低い順にノードを並べ替えることができます。

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. 別のノード上の最も利用率の低いアグリゲートを特定します。

- a. 左側のナビゲーション ペインで、[ストレージ] > [アグリゲート] をクリックし、[表示] メニューから [パフォーマンス] > [すべてのアグリゲート] を選択します。

「パフォーマンス: すべての集計」ビューが表示されます。

- b. *フィルタリング*をクリックし、左側のドロップダウンメニューから*ノード*を選択し、テキストフィールドにノードの名前を入力して、*フィルタの適用*をクリックします。

「パフォーマンス: すべての集計」ビューが再表示され、このノードで使用可能な集計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*列をクリックすると、集計が最も使用されていない順に並べ替えられます。

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*イベント詳細*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。

「パフォーマンス: すべてのボリューム」ビューには、そのノード上のボリュームのフィルターされたリストが表示されます。
 - c. *合計容量*列をクリックすると、割り当てられた最大のスペースでボリュームを並べ替えることができます。

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の組み合わせを使用して実行できます。

数日後に、このノードまたはアグリゲートから同じタイプのイベントを受け取っていないかどうかを確認します。

ワークロードを別のノードのアグリゲートに移動する

ワークロードが現在実行されているノードよりも負荷の低い別のノード上のアグリゲートをUnified Managerで特定し、選択したボリュームをそのアグリゲートに移動できます。負荷の低いノード上のアグリゲートに負荷の高いワークロードを移動すれば、両ノードでのワークロードの効率が向上します。

開始する前に

- 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、ノードが存在するクラスター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 ペインから 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. *使用率*列をクリックすると、使用率の最も低い順にノードを並べ替えることができます。

また、*空き容量*が最も大きい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. 別のノード上の最も利用率の低いアグリゲートを特定します。

- a. 左側のナビゲーション ペインで、[ストレージ] > [アグリゲート] をクリックし、[表示] メニューから [パフォーマンス] > [すべてのアグリゲート] を選択します。

「パフォーマンス: すべての集計」ビューが表示されます。

- b. *フィルタリング*をクリックし、左側のドロップダウンメニューから*ノード*を選択し、テキストフィールドにノードの名前を入力して、*フィルタの適用*をクリックします。

「パフォーマンス: すべての集計」ビューが再表示され、このノードで使用可能な集計のリストが表示されます。

- c. *使用率*列をクリックすると、集計を最も使用率の低い順に並べ替えることができます。

また、*空き容量*が最も大きい集計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*イベント*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。

「パフォーマンス: すべてのボリューム」ビューには、そのノード上のボリュームのフィルターされたリストが表示されます。

- c. *合計容量*列をクリックすると、割り当てられた最大のスペースでボリュームを並べ替えることができます。

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の組み合わせを使用して実行できます。

数日後に、移動先のノードまたはアグリゲートから同じタイプのイベントを受け取っていないかどうかを確認します。

ワークロードを別のHAペアのノードに移動する

現在ワークロードが実行されているハイアベイラビリティ（HA）ペアよりも空きパフォーマンス容量が大きい別のHAペアのノード上のアグリゲートをUnified Managerで特定し、その別のHAペア上のアグリゲートに選択したボリュームを移動できます。

開始する前に

- 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に問題がある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。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. *イベントの詳細*ページで、ノードが存在するクラスター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 ペインから ノード をクリックします。

このクラスター上のノードのリストは、「パフォーマンス: すべてのノード」ビューに表示されます。
 - c. 現在パフォーマンスに問題がある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、使用率の最も低い順にノードを並べ替えます。

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. この新たな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 ビューで、ノードをクリックします。

[パフォーマンス / ノード エクスプローラ] ページにノードの詳細が表示されます。

- b. [表示と比較] メニューで、[このノードの集計]*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*列をクリックすると、集計が最も使用されていない順に並べ替えられます。

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*イベント*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。

「パフォーマンス: すべてのボリューム」ビューには、そのノード上のボリュームのフィルターされたリストが表示されます。

- c. *合計容量*列をクリックすると、割り当てられた最大のスペースでボリュームを並べ替えることができます。

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の組み合わせを使用して実行できます。

数日後に、このノードまたはアグリゲートから同じタイプのイベントを受け取っていないかどうかを確認します。

ワークロードを別のHAペアの別のノードに移動する

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、その別のHAペア上のアグリゲートに選択したボリュームを移動できます。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。

開始する前に

- 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、この改善策を利用できません。
- 現在パフォーマンスに問題がある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。

以下に示す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ペアの利用率の低いノードに移動する際に役立ちます。

- 同じクラスタで別のHAペアを構成する利用率の低いノード
- この別のノードで最も利用率が低いアグリゲート
- 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、ストレージ > クラスタ をクリックし、[表示] メニューから パフォーマンス > すべてのクラスタ を選択します。

「パフォーマンス: すべてのクラスタ」ビューが表示されます。
 - b. 現在のクラスタの ノード数 フィールドの数字をクリックします。

「パフォーマンス: すべてのノード」ビューが表示されます。
 - c. 現在パフォーマンスに問題がある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ペアで最も利用率が低いノードを特定します。
 - a. *使用率*列をクリックすると、使用率の最も低い順にノードを並べ替えることができます。

また、*空き容量*が最も大きい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. 別のノード上の最も利用率の低いアグリゲートを特定します。
 - a. 左側のナビゲーション ペインで、[ストレージ] > [アグリゲート] をクリックし、[表示] メニューから [パフォーマンス] > [すべてのアグリゲート] を選択します。

「パフォーマンス: すべての集計」ビューが表示されます。
 - b. *フィルタリング*をクリックし、左側のドロップダウンメニューから*ノード*を選択し、テキストフィールドにノードの名前を入力して、*フィルタの適用*をクリックします。

「パフォーマンス: すべての集計」ビューが再表示され、このノードで使用可能な集計のリストが表示されます。
 - c. *使用率*列をクリックすると、集計を最も使用率の低い順に並べ替えることができます。

また、*空き容量*が最も大きい集計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*イベント*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。

「パフォーマンス: すべてのボリューム」ビューには、そのノード上のボリュームのフィルターされたリストが表示されます。

c. *合計容量*列をクリックすると、割り当てられた最大のスペースでボリュームを並べ替えることができます。

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の組み合わせを使用して実行できます。

数日後に、移動先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たノードでの作業の優先順位付け

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)、あるいは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にある場合、[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] ページでは、影響を受けたボリュームを IOPS と MBps で並べ替えて、イベントの原因となった可能性のある最も使用率の高いワークロードを確認できます。

ノード リソースを過剰に消費しているボリュームは、より制限の厳しいポリシー グループに割り当てます。これにより、ポリシー グループによる調整でワークロードのアクティビティが制限されて、そのノードでのリソースの使用が削減されます。

ONTAP System ManagerまたはONTAPコマンドを使用してポリシー グループを管理できます。これには次のタスクが含まれます。

- ポリシー グループの作成
- 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が問題であることがわかった場合は、使用されていないボリュームとLUNを検索してアグリゲートから削除できます。これによってディスク スペース不足の問題を解消できます。

アグリゲートでのパフォーマンス イベントの原因がディスク スペースの不足である場合は、使用されなくなったボリュームやLUNをいくつかの方法で特定できます。

使用されていないボリュームを特定する方法は次のとおりです。

- イベントの詳細ページの「影響を受けるオブジェクトの数」フィールドには、影響を受けるボリュームのリストを表示するリンクがあります。

リンクをクリックすると、「パフォーマンス: すべてのボリューム」ビューにボリュームが表示されます。そこから、影響を受けるボリュームを **IOPS** で並べ替えて、アクティブになっていないボリュームを確認できます。

使用されていないLUNを特定する方法は次のとおりです。

1. [イベントの詳細]ページで、イベントが発生したアグリゲートの名前を確認して書き留めます。
2. 左側のナビゲーション ペインで、ストレージ > **LUN** をクリックし、[表示] メニューから パフォーマンス > すべての **LUN** を選択します。
3. *フィルタリング*をクリックし、左側のドロップダウンメニューから*集計*を選択し、テキストフィールドに集計の名前を入力して、*フィルターの実用*をクリックします。
4. 影響を受ける LUN の結果リストを **IOPS** で並べ替えて、アクティブでない LUN を表示します。

使用されていないボリュームとLUNを特定したら、ONTAP System ManagerまたはONTAPコマンドを使用して、それらのオブジェクトを削除できます。

ディスクの追加およびアグリゲート レイアウトの再構築

アグリゲートにディスクを追加すると、ストレージ容量を増やし、そのアグリゲートのパフォーマンスを高めることができます。ディスクを追加してアグリゲートが再構築されると、パフォーマンスが改善します。

システム定義のしきい値イベントが発生すると、[イベントの詳細]ページのイベントの説明に問題が発生してい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

グリゲートへのディスクの追加は、ONTAP System ManagerまたはONTAPのコマンドを使用して実行できます。

["技術レポート 3838: ストレージサブシステム構成ガイド"](#)

Unified Manager サーバーと外部データ プロバイダー間の接続を設定する

Unified Manager サーバと外部データ プロバイダ間の接続により、クラスタ パフォーマンス データを外部サーバに送信できるため、ストレージ マネージャはサードパーティ ソフトウェアを使用してパフォーマンス メトリックをグラフ化できます。

Unified Manager サーバーと外部データ プロバイダー間の接続は、メンテナンス コンソールの「外部データ プロバイダー」というメニュー オプションを通じて確立されます。

外部サーバに送信可能なパフォーマンス データ

Unified Managerは、監視対象のすべてのクラスタからさまざまなパフォーマンス データを収集します。収集されたデータのうち、特定のデータ グループを外部サーバに送信することができます。

グラフ化するパフォーマンス データに応じて、次のいずれかの統計グループを選択して送信できます。

統計グループ	含まれるデータ	詳細
パフォーマンスモニター	以下のオブジェクトのパフォーマンスに関する総合的な統計データ。 • LUN • ボリューム	このグループは、監視対象の全クラスタ内のすべてのLUNとボリュームの合計IOPS / レイテンシを提供します。 提供する統計データが最も少ないグループです。
リソースの利用	以下のオブジェクトのリソース利用率の統計データ。 • ノード • アグリゲート	このグループは、監視対象の全クラスタのノードおよびアグリゲートの物理リソースの利用率に関する統計データを提供します。 また、パフォーマンス モニター グループで収集された統計も提供します。

統計グループ	含まれるデータ	詳細
ドリルダウン	以下の全追跡対象オブジェクトの読み取り / 書き込み、およびプロトコルごとの詳細な統計データ。 • ノード • アグリゲート • LUN • ボリューム • ディスク • LIF • ポート / NIC	このグループは、監視対象の全クラスターで追跡される7つのオブジェクト タイプのすべてについて、読み取り / 書き込みおよびプロトコルごとの内訳データを提供します。 また、パフォーマンス モニター グループとリソース使用率グループで収集された統計も提供します。 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 システムでクラスターまたはクラスター オブジェクトの名前が変更されると、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ー (「metric_path」と呼ばれる) のパフォーマンス データが含まれるようになります。2つのオブジェクトが同じオブジェクトとして関連付けられることはありません。たとえば、ボリュームの名前を「volume1_acct」から「acct_vol1」に変更すると、古いボリュームの古いパフォーマンス データと、新しいボリュームの新しいパフォーマンス データが表示されます。

外部データ プロバイダに送信可能なすべてのパフォーマンス カウンタの一覧については、ナレッジ ベースの記事30096を参照してください。

["What are the ActiveIQ Unified Manager performance counters that can be exported to an External Data Provider?"](#)

Unified Managerからパフォーマンスデータを受信できるようにGraphiteを設定する

Graphiteは、コンピュータ システムからパフォーマンス データを収集してグラフ化するオープン ソフトウェア ツールです。Unified Managerから統計データを受信するには、Graphiteサーバとソフトウェアを適切に設定する必要があります。

NetAppが、特定のバージョンのGraphiteまたはその他の他社製ツールをテストまたは検証することはありません。



Graphiteサーバは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から統計データを受信できるようにするために、次の変更を加える必要があります。

- の中で /opt/graphite/conf/carbon.conf` ファイルの場合、Graphiteサーバーで1分あたりに作成できるファイルの最大数を`_200_`に設定する必要があります。(MAX\_CREATES\_PER\_MINUTE = 200`)。

構成内のクラスター数や送信することを選択した統計オブジェクトによっては、最初に何千もの新しいファイルの作成が必要になる場合があります。そのため、1分あたりの作成ファイル数が200の設定でも、最初

の指標ファイルをすべて作成するのに15分以上かかることがあります。指標ファイルがすべて作成されれば、このパラメータは以降関係ありません。

- IPv6アドレスを使用して展開されたサーバーでGraphiteを実行している場合、`/opt/graphite/conf/carbon.conf` ファイルを「`0.0.0.0`」から「`:::`」に変更する必要があります(`LINE_RECEIVER_INTERFACE = :::`)
- の中で `/opt/graphite/conf/storage-schemas.conf` ファイル、``retentions`` パラメータを使用して、頻度を 5 分に設定し、保持期間を環境に適し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いくらでも長く設定できますが、頻度は最低1つの保持設定で5分に設定する必要があります。次の例では、Unified Managerのセクションは、`pattern`` パラメータ、値は初期頻度を 5 分、保持期間を 100 日に設定します。 ``[OPM]`

```
pattern = ^netapp-performance\..
```

```
retentions = 5m:100d
```



デフォルトのベンダータグが「`netapp-performance`」から別のものに変更された場合、その変更は ``pattern`` パラメータも同様です。



Unified Managerサーバがパフォーマンス データを送信する際にGraphiteサーバが使用できないとデータは送信されず、その間のデータは収集されません。

Unified Manager サーバから外部データ プロバイダへの接続を構成する

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別およびデータの送信頻度を指定できます。

開始する前に

- 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を用意しておく必要があります。
 - サーバの名前またはIPアドレス (IPv4またはIPv6)
 - サーバのデフォルト ポート (デフォルトポート2003を使用していない場合)
- Unified Managerサーバから統計データを受信できるようにリモート サーバと他社製ソフトウェアを設定しておく必要があります。
- 送信する統計データ グループを確定しておく必要があります。
 - `PERFORMANCE_INDICATOR`: パフォーマンスモニターの統計
 - `RESOURCE_UTILIZATION`: リソース使用率とパフォーマンスモニターの統計
 - `DRILL_DOWN`: すべての統計
- 統計を送信する時間間隔 (5分、10分、または15分) を知っておく必要があります。

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、1回に送信されるデータ量が、デフォルトの送信間隔 (5分) で送信する場合の2倍 (または3倍) になります。



Unified Managerのパフォーマンス収集間隔を10分または15分に変更した場合は、送信間隔もUnified Managerの収集間隔以上に変更する必要があります。

1台のUnified Managerサーバと1台の外部データ プロバイダ サーバ間の接続を設定できます。

手順

1. Unified Managerサーバのメンテナンス コンソールに、メンテナンス ユーザとしてログインします。

Unified Managerメンテナンス コンソールのプロンプトが表示されます。

2. メンテナンス コンソールで、外部データ プロバイダー 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、次のように入力します。`y`続行します。

5. プロンプトが表示されたら、接続先のサーバのIPアドレスまたは名前、サーバのポート情報を入力します（デフォルト ポート2003と異なる場合）。

6. プロンプトが表示されたら、次のように入力します。`y`入力した情報が正しいことを確認します。

7. いずれかのキーを押して[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、次のように入力します。`y`続行します。

10. プロンプトが表示されたら、送信する統計データの種類、統計データの送信間隔を入力し、統計データの送信を今すぐに有効にするかどうかを指定します。

のために..	入力する内容
Statistics group ID	0- PERFORMANCE_INDICATOR（デフォルト） 1- リソース使用率 2- ドリルダウン

のために..	入力する内容
Vendor tag	統計が外部サーバー上に保存されるフォルダーのわかりやすい名前。「netapp-performance」はデフォルト名ですが、別の値を入力することもできます。 フォルダ構造を指定するには、ピリオドを使用します。例えば、次のように入力すると `stats.performance.netapp`統計は stats > performance > netapp にあります。
Transmit interval	5（デフォルト）、10、または`15`分
Enable/disable	0- 無効にする 1- 有効（デフォルト）

11. プロンプトが表示されたら、次のように入力します。`y`入力した情報が正しいことを確認します。
12. いずれかのキーを押して[External Server Connection]メニューに戻ります。
13. タイプ`x`メンテナンス コンソールを終了します。

接続設定が完了すると、選択したパフォーマンス データが指定したサーバに指定した送信間隔で送信されます。送信された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）では、ONTAPソフトウェアを実行する多数のシステムを一元化されたユーザ インターフェイスで監視できます。Unified Managerサーバ インフラは拡張性とサポート性に優れ、高度な監視および通知機能を備えています。

Unified Managerの主な機能は、クラスタの可用性と容量の監視 / 通知 / 管理、保護機能の管理、診断データの収集とテクニカル サポートへの送信です。

Unified Managerを使用してクラスタを監視できます。クラスタで問題が発生すると、Unified Managerのイベントを通じて問題の詳細が通知されます。一部のイベントでは、問題を解消するための対応策も提示されます。問題が発生したときにEメールやSNMPトラップで通知されるように、イベントに対してアラートを設定できます。

Unified Managerでは、アノテーションを関連付けることで環境内のストレージ オブジェクトを管理できます。カスタム アノテーションを作成し、ルールに基づいて動的にクラスタ、Storage Virtual Machine（SVM）、およびボリュームを関連付けることができます。

また、それぞれのクラスタ オブジェクトについて、容量や健全性のグラフに表示される情報を使用してストレージ要件を計画することもできます。

物理容量と論理容量

Unified Managerは、ONTAPストレージ オブジェクトに使用される物理容量と論理容量の概念を利用します。

- **物理容量:** 物理スペースとは、ボリュームで使用されるストレージの物理ブロックを指します。Storage Efficiency機能（重複排除や圧縮など）によるデータの削減により、一般に「使用済み物理容量」は使用済み論理容量よりも小さくなります。
- **論理容量:** 論理スペースとは、ボリューム内の使用可能なスペース（論理ブロック）を指します。論理スペースとは、重複排除や圧縮の結果を考慮せずに、理論上のスペースの使用方法を指します。「使用済み論理容量」とは、使用済み物理容量に、設定されているStorage Efficiency機能（重複排除や圧縮など）による削減量を加えたものです。物理スペースの削減が反映されないため、通常は使用済み物理容量よりも大きくなります。したがって、合計論理容量はプロビジョニング済みスペースよりも大きくなる場合があります。

容量の測定単位

Unified Manager は、1024 (2¹⁰) 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、これらの単位がKB、MB、GB、TB、PBと表示されていました。ONTAP 9.10.1以降では、KiB、MiB、GiB、TiB、PiBと表示されます。



スループットに使用される単位は、すべてのリリースのONTAPについて、引き続きキロバイト/秒 (Kbps)、メガバイト/秒 (Mbps)、ギガバイト/秒 (Gbps)、テラバイト/秒 (Tbps) になります。

ONTAP 9.10.0 以前の Unified Manager に表示される容量単位	ONTAP 9.10.1 の Unified Manager に表示される容量単位	計算式	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 は、スケーラビリティ、サポート性、強化された監視および通知機能を提供するサーバー インフラストラクチャ上に構築されています。Unified Manager 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 には次の機能が含まれています。

- 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、ストレージ仮想マシン (SVM)、アグリゲート、ボリューム、LUN、ネームスペース、qtree、LIF、スナップショット コピー、ジャンクション パス、NFS 共有、SMB 共有、ユーザーおよびグループのクォータ、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: 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構成およびMetroCluster over IP構成：クラスタ コンポーネントの設定、問題、接続ステータスの表示と監視（MetroCluster over FC構成についてはMetroClusterのスイッチとブリッジを含む）
- アラート、イベント、およびしきい値インフラの強化
- LDAP / LDAPS / SAML認証とローカル 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
- ダッシュボードの強化：容量、可用性、保護、パフォーマンスなど、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
- 一部のディスク障害、MetroClusterアグリゲートミラーリングの劣化、MetroClusterスペアディスクの残置などのイベントの影響を受けるリソースをグラフィカルに表示する影響範囲領域

- MetroClusterイベントの影響を表示する可能性のある影響領域
- 一部のディスク障害、MetroClusterアグリゲートミラーリングの劣化、MetroClusterスペアディスクの残置などのイベントに対処するために実行できるアクションを表示する推奨修正アクション領域
- 影響を受ける可能性のあるリソース領域には、ボリューム オフライン イベント、ボリューム制限イベント、シン プロビジョニング ボリューム領域が危険にさらされているイベントなどのイベントによって影響を受ける可能性のあるリソースが表示されます。
- FlexVolまたはFlexGroupボリュームを備えた SVM のサポート
- ノードのルート ボリューム監視のサポート
- Snapshotコピーの監視強化（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 / 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との統合によるワークフローの実行

Storage Automation Storeで、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を提供しています。パックをダウンロードし、WFAにインポートして実行できます。自動化されたワークフローは、次の場所で入手できます。

["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**インターフェース

ここでは、Active IQ Unified Managerでデータ ストレージの容量、可用性、保護に関する問題をトラブルシューティングするための2種類のユーザ インターフェイスについて説明します。2 つの UI 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）を併せてインストールし、設定する必要があります。

Unified Manager Web UI

Unified Manager Web UI を使用すると、管理者はデータ ストレージの容量、可用性、および保護に関連するクラスターの問題を監視およびトラブルシューティングできます。

以降のセクションで、管理者がUnified Manager Web UIに表示されるストレージ容量、データの可用性、または保護に関する問題をトラブルシューティングする際に従う共通のワークフローについて説明します。

メンテナンス コンソール

Unified Manager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 が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形式となります。

この情報は、メンテナンス コンソールにアクセスしてUnified Managerサーバの機能に関連する問題を解決するのに役立ちます。

クラスターとクラスターオブジェクトの健全性の管理と監視

Unified Manager は、定期的な API クエリとデータ収集エンジンを使用して、クラスターからデータを収集します。クラスターを Unified Manager データベースに追加することで、これらのクラスターの可用性と容量のリスクを監視および管理できます。

クラスター監視を理解する

クラスターを Unified Manager データベースに追加して、クラスターの可用性、容量、および CPU 使用率、インターフェイス統計、空きディスク容量、qtree 使用率、シャーシ環境などのその他の詳細を監視できます。

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。設定されている場合、Unified Manager はイベントによってアラートがトリガーされたときに、指定された受信者に通知を送信します。

ノードルートボリュームを理解する

Unified Managerを使用して、ノードのルート ボリュームを監視できます。ノードの停止を防ぐための十分な容量をノードのルート ボリュームに確保しておくことを推奨します。

ノード ルート ボリュームの使用容量がノード ルート ボリュームの合計容量の 80% を超えると、ノード ルート ボリュームのスペースがほぼいっぱいであるイベントが生成されます。通知を受け取るようにこのイベントのアラートを設定することができます。ONTAP System ManagerまたはONTAP CLIを使用して、ノードの停止を防ぐための適切な処置を行うことができます。



クラスターで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。

ノードルート集計のイベントとしきい値を理解する

Unified Managerを使用して、ノードのルート アグリゲートを監視できます。ルート アグリゲート内のルート ボリュームをシックプロビジョニングしてノードの停止を防ぐことを推奨します。

デフォルトでは、ルート アグリゲートについては容量とパフォーマンスのイベントは生成されません。また、Unified Managerで使用するしきい値はノードのルート アグリゲートには適用されません。これらのイベントが生成されるように設定を変更できるのは、テクニカル サポート担当者だけです。テクニカル サポート担当者が設定を変更すると、容量のしきい値がノードのルート アグリゲートにも適用されるようになります。

ONTAP System ManagerまたはONTAP CLIを使用して、ノードの停止を防ぐための適切な処置を行うことができます。



クラスターで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。

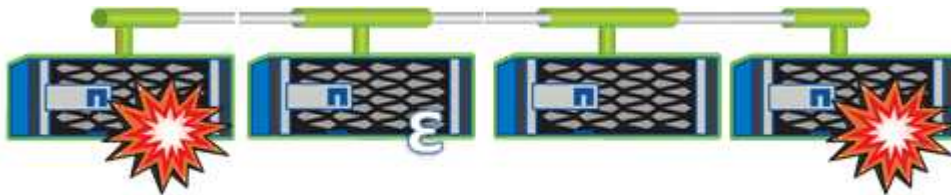
クォーラムとイプシロンを理解する

クォーラムとイプシロンは、クラスタの健全性と機能を判断するための重要な基準で、通信および接続に関する潜在的な問題へのクラスタの対応を決定します。

クォーラムは、クラスターが完全に機能するための前提条件です。クラスターがクォーラム状態にある場合、ノードの大多数は正常であり、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1つのまとまりとしてデータの単一のビューを共有するため、任意の時点において1つのノードの集まりだけがクォーラムを構成することができます。つまり、通信が確立されていない2つのノードが異なる方法でデータを変更できる場合には、データを1つのデータビューに表示できなくなります。

クラスター内の各ノードは、1つのノードマスターを選出する投票プロトコルに参加します。残りの各ノードはセカンダリになります。マスターノードは、クラスタ内に情報を同期する役割を担います。形成されたクォーラムは継続的な投票によって維持されます。マスターノードがオフラインになった場合、クラスタでクォーラムが維持されていれば、オンラインのノードの投票によって新しいマスターが選出されます。

偶数個のノードを持つクラスターでは同点になる可能性があるため、1つのノードにはイプシロンと呼ばれる追加の分数投票重みが与えられます。大規模クラスターの2つの等しい部分間の接続が失敗した場合、イプシロンを含むノードのグループは、すべてのノードが正常であると想定してクォーラムを維持します。たとえば、次の図では、4ノードクラスタの2つのノードで障害が発生しています。ただし、残りのノードの1つにイプシロンが設定されているため、健全なノードが過半数に満たなくてもクォーラムが維持されます。



クラスタが作成されると、自動的に最初のノードにイプシロンが割り当てられます。イプシロンを保持しているノードで障害が発生したり、ハイアベイラビリティパートナーをテイクオーバーしたり、ハイアベイラビリティパートナーにテイクオーバーされた場合、イプシロンは別のHAペアの健全なノードに自動的に割り当てられます。

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つのノード障害によってクォーラムが失われるような処理を実行しようとする、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。

一般的に、クラスタのノード間に信頼性のある接続が確立されている場合には、小規模のクラスタよりも大規模のクラスタの方が安定します。ノードの半数にイプシロンを加えた過半数のクォーラムの要件は、2ノードのクラスタよりも24ノードのクラスタの方が簡単に維持できます。

2ノードのクラスタでは、クォーラムの維持に独特な課題が存在します。2ノードクラスタはクラスタHAを使用します。クラスタHAでは、どちらのノードもイプシロンを保持しません。代わりに、両方のノードが継続的にポーリングされ、1つのノードに障害が発生した場合でも、もう1つのノードがデータへの完全な読み取り/書き込みアクセスと、論理インターフェイスおよび管理機能へのアクセスを確実に持つようにします。

クラスターのリストと詳細を表示する

「ヘルス: すべてのクラスター」ビューを使用して、クラスターのインベントリを表示で

きます。「容量: すべてのクラスター」ビューでは、すべてのクラスターのストレージ容量と使用率に関する概要情報を表示できます。

開始する前に

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]ページを使用して、個々のクラスターの健全性、容量、構成、LIF、ノード、ディスクなどの詳細を表示することもできます。

「ヘルス: すべてのクラスター」ビュー、「容量: すべてのクラスター」ビュー、および「クラスター/ヘルスの詳細」ページの詳細は、ストレージの計画に役立ちます。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、[ヘルス: すべてのクラスター]ビューから特定のクラスターを選択し、容量の詳細を取得して、クラスターに必要なスペースが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、ストレージ > クラスター をクリックします。
2. [表示] メニューで、[正常性: すべてのクラスター] ビューを選択して正常性情報を表示するか、[容量: すべてのクラスター] ビューを選択してすべてのクラスターのストレージ容量と使用率の詳細を表示します。
3. クラスターの名前をクリックすると、*クラスター/ヘルス*詳細ページでクラスターの完全な詳細が表示されます。

関連情報

- ["\[クラスタ / 健全性の詳細ページ\]"](#)
- ["パフォーマンス: すべてのクラスタービュー"](#)
- ["MetroCluster構成の監視"](#)
- ["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構成内のクラスターの健全性をチェックする

Active IQ Unified Manager (Unified Manager) を使用して、MetroCluster over FC構成およびMetroCluster over IP構成のクラスタとそのコンポーネントについて、健全性を確認することができます。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。

開始する前に

- 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、関連したクラスタの名前を取得しておく必要があります。
- MetroCluster構成 (FCおよびIP) 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。

MetroCluster over FC構成でクラスタの健全性を確認する

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

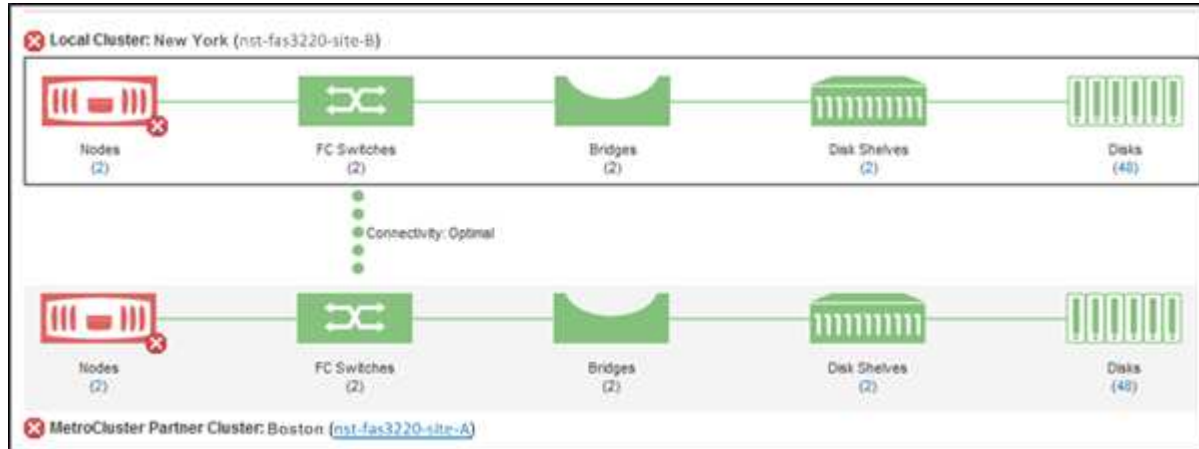
1. 左側のナビゲーション ペインで [イベント管理] をクリックして、イベント リストを表示します。
2. フィルター パネルで、ソース タイプ カテゴリの下にあるすべてのMetroClusterフィルターを選択します。すべてのMetroCluster構成について環境内で生成されたすべてのイベントが表示されます。
3. MetroClusterイベントの横にあるクラスタの名前をクリックします。



MetroClusterイベントが表示されない場合は、検索バーを使用して、MetroCluster over FC構成関連のイベントに関係しているクラスタの名前を検索できます。

「ヘルス: すべてのクラスター」ビューに、イベントの詳細情報が表示されます。

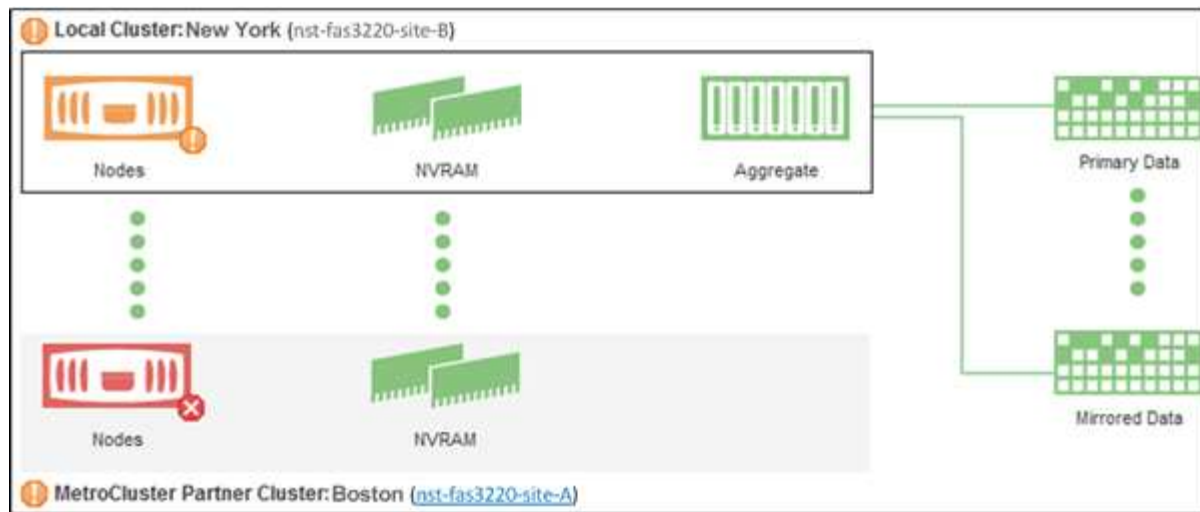
4. * MetroCluster接続 * タブを選択すると、選択したクラスターとそのパートナー クラスター間の接続の健全性が表示されます。



この例では、ローカル クラスターとそのパートナー クラスター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、クラスター間のリンクを表します。アイコンにマウス カーソルを合わせると、イベント情報を表示できます。アイコンをクリックすると、イベントを表示できます。どちらかのクラスターで発生した健全性の問題がパフォーマンス イベントの一因である可能性があります。

Unified Managerは、クラスター間のリンクのNVRAMコンポーネントを監視します。ローカル クラスターまたはパートナー クラスターの[FC スイッチ]アイコンまたは[接続]アイコンが赤の場合は、リンク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。

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に関する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。ページ上に赤または黄色のアイコンがない場合は、パートナー クラスタにおける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構成でクラスタの健全性を確認する

MetroCluster over IP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. フィルターパネルの*ソースタイプ*カテゴリで、`MetroCluster Relationship` フィルター。すべてのMetroCluster構成について環境内で生成されたすべてのイベントが表示されます。



レポートされたMetroClusterイベントが表示されない場合は、検索バーを使用して、MetroCluster over IP構成関連のイベントに関係しているクラスタの名前で検索できます。

3. 関連するMetroClusterイベントの横にあるクラスタの名前をクリックします。[クラスタ]ページが開き、そのクラスタの詳細が表示されます。健康上の問題の判断については、以下を参照してください。"[MetroCluster over IP構成の接続の問題の監視](#)"。

すべてのSANアレイクラスタの健全性と容量ステータスを表示します

[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。

開始する前に

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 クラスタの概要情報は、[ヘルス: すべてのクラスタ] ビューと [容量: すべてのクラスタ] ビューで表示できます。さらに、[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、ストレージ > クラスター をクリックします。
2. *「ヘルス: すべてのクラスター」ビューに「パーソナリティ」列が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 クラスターに対して「All SAN Array」が表示されます。

3. 情報を確認します。
4. これらのクラスターのストレージ容量に関する情報を表示するには、「容量: すべてのクラスター」ビューを選択します。
5. これらのクラスター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 クラスターの名前をクリックします。

[クラスター / 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します。

ノードリストと詳細を表示する

「ヘルス: すべてのノード」ビューを使用して、クラスター内のノードのリストを表示できます。[クラスター / 健全性の詳細]ページを使用すると、監視対象のクラスターに含まれるノードに関する詳細情報を表示できます。

開始する前に

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ー、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เปア容量、合計容量）などの詳細情報を参照できます。HAペア、ディスク シェルフ、およびポートに関する情報を取得することもできます。

手順

1. 左側のナビゲーション ペインで、ストレージ > ノード をクリックします。
2. ヘルス: 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[クラスター / 健全性の詳細]ページに表示されます。左側のペインには、HAペアのリストが表示されます。デフォルトでは、[HA の詳細]が開き、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、次のうち該当する操作を実行します。

表示する内容	操作
ディスク シェルフの詳細	ディスクシェルフ。
ポート関連の情報	ポート。

詳細については、以下を参照してください。

- ["パフォーマンス: すべてのノードビュー"](#)

- "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"

契約更新のためのハードウェア在庫レポートを生成する

ハードウェアのモデル番号とシリアル番号、ディスクのタイプと数、インストールされているライセンスなど、クラスターとノードのすべての情報を含むレポートを生成できます。このレポートは、NetAppActive IQ プラットフォームに接続されていない安全なサイト (「ダーク」 サイト) 内での契約更新に役立ちます。

開始する前に

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、ストレージ > ノード をクリックします。
2. ヘルス: すべてのノード ビューまたは パフォーマンス: すべてのノード ビューに移動します。
3. レポート > * > ハードウェア インベントリ レポート* を選択します。

ハードウェア インベントリ レポートは、.csvファイルとしてダウンロードされ、その時点における完全な情報を含みます。

4. この情報をNetAppのサポート担当者に提出して契約更新を申請します。

ストレージVMのリストと詳細を表示する

[健全性: すべてのストレージ VM] ビューから、ストレージ仮想マシン (SVM) のインベントリを監視できます。[Storage VM / 健全性の詳細]ページを使用して、監視対象のSVMに関する詳細情報を確認できます。

開始する前に

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、ストレージ > ストレージ **VM** をクリックします。
2. 次のいずれかの方法を選択してSVMの詳細を表示します。
 - すべてのクラスター内のすべての 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: すべてのストレージ 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。

最小限の詳細ダイアログ ボックスで [詳細の表示] をクリックして、完全な詳細を表示することもできます。

3. 最小限の詳細ダイアログ ボックスで [関連を表示] をクリックして、SVM に関連するオブジェクトを表示

します。

関連情報

- ["ストレージVM: ヘルス詳細ページ"](#)
- ["パフォーマンス: すべてのストレージVMビュー"](#)
- ["セキュリティ: ランサムウェア対策"](#)
- ["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"](#)

集計リストと詳細を表示する

「ヘルス: すべてのアグリゲート」ビューから、アグリゲートのインベントリを監視できます。「容量: すべてのアグリゲート」ビューでは、すべてのクラスター内のアグリゲートの容量と使用率に関する情報を表示できます。

開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

アグリゲートの容量と構成、ディスク情報などの詳細を[アグリゲート / 健全性の詳細]ページに表示できます。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、ストレージ > アグリゲート 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。
 - すべてのクラスター内のすべてのアグリゲートのヘルスに関する情報を表示するには、[表示] メニューで [ヘルス: すべてのアグリゲート ビュー] を選択します。
 - すべてのクラスター内のすべてのアグリゲートの容量と使用率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。

最小限の詳細ダイアログ ボックスで [詳細の表示] をクリックして、完全な詳細を表示することもできます。

3. 最小限の詳細ダイアログ ボックスから [関連を表示] をクリックして、集計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: すべての集計ビュー"](#)
- ["アグリゲート容量レポートのカスタマイズ"](#)

FabricPool の容量情報を表示する

クラスタ、アグリゲート、ボリュームのFabricPoolの容量の情報を、それらのオブジェクトの[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、および詳細ページに表示できます。ミラー階層が構成されている場合、これらのページに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。

クラウド層が別のクラウド プロバイダー (「ミラー層」) にミラーリングされている場合、両方のクラウド層が集計/ヘルス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。

容量情報を表示するには...	操作
クラスタ	a. [容量: すべてのクラスター] ビューで、クラスターをクリックします。 b. クラスター/ヘルスの詳細ページで、*構成*タブをクリックします。 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。
アグリゲート	a. [容量: すべてのアグリゲート] ビューで、[タイプ] フィールドに「SSD (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。 b. 集計 / ヘルスの詳細ページで、容量 タブをクリックします。 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。 c. *ディスク情報*タブをクリックします。 クラウド階層の名前と使用済み容量が表示されます。 d. *構成*タブをクリックします。 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。

容量情報を表示するには...	操作
ボリューム	a. 「容量: すべてのボリューム」ビューで、「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。 b. ボリューム/ヘルスの詳細ページで、*構成*タブをクリックします。 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。

- ワークロード分析 ページの 容量トレンド 領域で「クラウド層ビュー」を選択すると、前月にローカル パフォーマンス層とクラウド層で使用されていた容量を確認できます。

FabricPoolアグリゲートの詳細については、以下を参照してください。"[ディスクとアグリゲート - 概要](#)"。

ストレージプールの詳細を表示する

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。

開始する前に

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

- 左側のナビゲーション ペインで、ストレージ > アグリゲート をクリックします。
- 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。

- *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がストレージ プールを使用している場合にのみ表示されます。

- [キャッシュ]テーブルで、必要なストレージ プールの名前にカーソルを合わせます。

ストレージ プールの詳細が表示されます。

ボリュームリストと詳細を表示する

「健全性: すべてのボリューム」ビューから、ボリュームのインベントリを監視できます。「容量: すべてのボリューム」ビューでは、クラスター内のボリュームの容量と使用率に関する情報を表示できます。

開始する前に

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 / 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、構成、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、ストレージ > ボリューム 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。
 - クラスター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、[表示] 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。
 - クラスター内のボリュームの容量と使用率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。

最小限の詳細ダイアログ ボックスで [詳細の表示] をクリックして、完全な詳細を表示することもできます。

3. オプション: 最小限の詳細ダイアログ ボックスから [関連を表示] 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: ヘルス詳細ページ"](#)
- ["パフォーマンス: すべてのボリュームビュー"](#)
- ["セキュリティ: ランサムウェア対策"](#)
- ["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のグラフを表示するレポートの作成"](#)

NFS共有の詳細を表示する

すべてのNFS共有について、ステータス、ボリューム（FlexGroupボリュームまたはFlexVol）に関連付けられているパス、NFS共有に対するクライアントのアクセス レベル、エクスポートされているボリュームに定義されているエクスポート ポリシーなどの詳細情報を表示できます。監視対象のすべてのクラスター上のすべての NFS 共有を表示するには、「ヘルス: すべての NFS 共有」ビューを使用し、特定のストレージ仮想マシン (SVM) 上のすべての NFS 共有を表示するには、「ストレージ VM/ヘルスの詳細」ページを使用します。

開始する前に

- 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。

手順

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	次の手順に従ってください...
すべてのNFS共有を表示	ストレージ > *NFS共有*をクリックします
単一のSVMのNFS共有を表示	a. ストレージ > *ストレージ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. ストレージ VM / ヘルスの詳細ページで、NFS 共有 タブをクリックします。

詳細については、["ファイル共有ボリュームのプロビジョニング"](#)そして["APIを使用したCIFSおよびNFSファイル共有のプロビジョニング"](#)。

SMB/CIFS共有の詳細を表示する

すべてのSMB/CIFS共有について、共有名、ジャンクション パス、コンテナ オブジェクト、セキュリティ設定、共有に対して定義されているエクスポート ポリシーなどの詳細情報を表示できます。監視対象のすべてのクラスター上のすべての SMB 共有を表示するには、「ヘルス: すべての SMB 共有」ビューを使用し、特定のストレージ仮想マシン (SVM) 上のすべての SMB 共有を表示するには、「ストレージ VM/ヘルスの詳細」ページを使用します。

開始する前に

- 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。

手順

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	次の手順に従ってください...
すべてのSMB/CIFS共有を表示	ストレージ > *SMB共有*をクリックします

目的	次の手順に従ってください...
単一のSVMのSMB / CIFS共有を表示	a. ストレージ > *ストレージ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. ストレージ VM / ヘルスの詳細ページで、 SMB 共有 タブをクリックします。

詳細については、["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"](#)。

スナップショットコピーのリストを表示する

選択したボリュームのSnapshotコピーのリストを表示できます。Snapshotコピーのリストを使用すると、1つ以上のSnapshotコピーが削除された場合に再利用可能なディスクスペースの量を計算できます。また、必要に応じてSnapshotコピーを削除できます。

開始する前に

- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- Snapshotコピーを含むボリュームがオンラインになっている必要があります。

手順

1. 左側のナビゲーション ペインで、ストレージ > ボリューム をクリックします。
2. ヘルス: すべてのボリューム ビューで、表示するスナップショット コピーが含まれているボリュームを選択します。
3. *ボリューム/健全性*の詳細ページで、*容量*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、スナップショット コピー の横にあるリンクをクリックします。

Snapshotコピーの数はリンクになっており、クリックするとSnapshotコピーのリストが表示されます。

関連情報

["\[健全性/ボリュームページ\]"](#)

Snapshotコピーを削除する

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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

ボリュームはオンラインである必要があります。

使用中またはロック状態のSnapshotコピーを削除する場合は、Snapshotコピーを使用しているアプリケーションからそのコピーを解放しておく必要があります。

- FlexCloneボリュームが親ボリューム内のベースのSnapshotコピーを使用している場合、そのSnapshotコピーは削除できません。

ベーススナップショットコピーは、FlexCloneボリュームを作成するために使用されるスナップショットコピーであり、ステータスを表示します。`Busy`アプリケーション依存性として`Busy, Vclone`親ボリューム内。

- 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、ストレージ > ボリューム をクリックします。
2. ヘルス: すべてのボリューム ビューで、表示するスナップショット 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. *ボリューム/健全性*の詳細ページで、*容量*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、スナップショット コピー の横にあるリンクをクリックします。

Snapshotコピーの数はリンクになっており、クリックするとSnapshotコピーのリストが表示されます。

5. スナップショット コピー ビューで、削除するスナップショット コピーを選択し、選択した項目の削除 をクリックします。

スナップショットコピーの再利用可能なスペースを計算する

1つ以上のSnapshotコピーを削除した場合に再利用可能となるディスク スペースの量を計算できます。

開始する前に

- 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である必要があります。この機能はFlexGroupボリューム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、ストレージ > ボリューム をクリックします。
2. ヘルス: すべてのボリューム ビューで、表示するスナップショット 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. *ボリューム/健全性*の詳細ページで、*容量*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、スナップショット コピー の横にあるリンクをクリックします。

Snapshotコピーの数はリンクになっており、クリックするとSnapshotコピーのリストが表示されます。

5. スナップショット コピー ビューで、再利用可能なスペースを計算するスナップショット コピーを選択します。
6. *計算*をクリックします。

ボリューム上の再利用可能なスペース（割合、KB、MB、GBなど）が表示されます。

7. 再利用可能なスペースを再計算するには、必要なスナップショット 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

それぞれのストレージ オブジェクト ページから、すべてのクラスターとクラスター 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。インベントリのストレージと保護の次の各セクションからは、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。

- [クラスタのインベントリ]ページ、[クラスタの健全性]ページ、[クラスタのパフォーマンス]ページ
- [アグリゲートのインベントリ]ページ、[アグリゲートの健全性]ページ、[アグリゲートのパフォーマンス]ページ
- [ボリュームのインベントリ]ページ、[ボリュームの健全性]ページ、[ボリュームのパフォーマンス]ページ
- [ノードのインベントリ]ページ、[ノードのパフォーマンス]ページ
- [StorageVM のインベントリ]ページ、[StorageVM の健全性]ページ、[StorageVM のパフォーマンス]ページ
- [保護関係]ページ

Unified Managerの一般的な健全性関連のワークフローとタスク

Unified Managerに関連する一般的な管理ワークフローと管理タスクには、監視対象のストレージ クラスタの選択、データの可用性 / 容量 / 保護に悪影響を及ぼす状態の診断、消失したデータのリストア、ボリュームの設定と管理、診断データのバンドルとテクニカル サポートへの送信（必要時）などがあります。

Unified Manager を使用すると、ストレージ管理者はダッシュボードを表示し、管理対象ストレージ クラスタの全体的な容量、可用性、および保護の健全性を評価し、発生する可能性のある特定の問題を迅速に識別、検索、診断し、解決を割り当てることができます。

管理対象ストレージ オブジェクトのストレージ容量やデータ可用性に影響する、クラスタ、Storage Virtual Machine (SVM)、ボリューム、またはFlexGroupボリュームに関連した最も重要な問題が、[ダッシュボード]ページのシステムの健全性グラフおよびイベントに表示されます。重要な問題が特定されると、このペー

ジに適切なトラブルシューティング ワークフローをサポートするためのリンクが表示されます。

関連する管理ツール（OnCommand Workflow Automation（WFA）など）が含まれているワークフローにUnified Managerを組み込んで、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 リソース構成の問題に起因するデータ可用性イベントが[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、埋め込まれたリンクに従って、該当するストレージ リソースに関する接続情報を確認し、トラブルシューティングのアドバイスを参照し、他の管理者に問題の解決を割り振ることができます。

- パフォーマンス インシデントの設定と監視

管理者は、監視対象のストレージ システム リソースのパフォーマンスを監視し、管理することができます。詳細については、"[Active IQ Unified Managerによるパフォーマンス監視の概要](#)"を参照してください。

- ボリューム容量の問題の診断と管理

[ダッシュボード]ページにボリューム ストレージ容量の問題が表示された場合、ストレージ管理者はリンク先を参照して該当するボリュームのストレージ容量に関連する現在と過去の傾向を確認し、トラブルシューティングのアドバイスを参照して、他の管理者に問題の解決を割り振ることができます。

- 保護関係の設定、監視、問題の診断

保護関係を作成して設定したあと、ストレージ管理者は、保護関係に関連する潜在的な問題、保護関係の現在の状態、該当する関係に対して成功した現在と過去の保護ジョブの情報、およびトラブルシューティングのアドバイスを確認できます。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リストア

- ストレージ オブジェクトへのアノテーションの関連付け

ストレージ管理者は、ストレージ オブジェクトにアノテーションを関連付けることで、ストレージ オブジェクトに関連するイベントをフィルタリングして表示できます。これにより、イベントに関連する問題に優先順位を付けて解決することが可能となります。

- Unified Managerで収集された健全性、容量、パフォーマンスの情報をREST APIで表示して、クラスタの管理に利用できます。見る"[Active IQ Unified Manager REST APIでの作業の開始](#)"詳細についてはこちらをご覧ください。

- テクニカル サポートへのサポート バンドルの送信

ストレージ管理者は、メンテナンス コンソールを使用して、サポート バンドルを取得し、テクニカル サポートに送信することができます。AutoSupportメッセージよりも詳しい診断とトラブルシューティングが必要な問題が発生した場合は、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。

データの可用性を監視およびトラブルシューティングする

Unified Manager は、承認されたユーザーが保存されたデータにアクセスできる信頼性を

監視し、アクセスをブロックまたは妨害する状況を警告し、それらの状況を診断して解決策を割り当てて追跡できるようにします。

このセクションの可用性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およびソフトウェアの状態を検出し、診断し、解決のために割り当てる方法の例について説明します。

ストレージフェイルオーバー相互接続リンクのダウン状態をスキャンして解決する

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。

開始する前に

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。このため、一般的には、管理者がアップグレードの開始前にアップグレード対象のクラスタ ノードでストレージ フェイルオーバーの信頼性を監視して確認します。

手順

1. 左側のナビゲーション ペインで、[イベント管理] をクリックします。
2. イベント管理 インベントリ ページで、*アクティブな可用性イベント*を選択します。
3. *イベント管理*インベントリページの*名前*列の上部にある  入力してください ``failover`` テキスト ボックスで、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に制限します。

ストレージ フェイルオーバーの状態に関連する過去のイベントがすべて表示されます。

このシナリオでは、Unified Manager の可用性インシデント セクションにイベント「ストレージ フェイルオーバー インターコネクトの 1 つ以上のリンクがダウンしています」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 1 つ以上のイベントが表示される場合は、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して、そのイベントの詳細情報を表示します。

この例では、イベント タイトル「Storage Failover Interconnect One or More Links Down」 をクリックします。

そのイベントの[イベントの詳細]ページが表示されます。

- a. [イベントの詳細]ページで、次のタスクを1つ以上実行できます。
 - [原因]フィールドでエラー 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

"[イベントの詳細ページ]"

"Unified Managerのユーザ ロールと機能"

ストレージフェイルオーバー相互接続リンクのダウンに対する修正アクションを実行する

ストレージ フェイルオーバー関連イベントの[イベントの詳細]ページを表示し、ページの概要情報を確認して、イベントの緊急性や、問題の考えられる原因と解決策を特定できます。

開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

この例では、[イベントの詳細]ページに表示されるイベントの概要に、ストレージ フェイルオーバー インターコネクト リンクの停止状態に関する次の情報が表示されます。

```
Event: Storage Failover Interconnect One or More Links Down
```

```
Summary
```

```
Severity: Warning
```

```
State: New
```

```
Impact Level: Risk
```

```
Impact Area: Availability
```

```
Source: aardvark
```

```
Source Type: Node
```

```
Acknowledged By:
```

```
Resolved By:
```

```
Assigned To:
```

```
Cause: At least one storage failover interconnected link  
       between the nodes aardvark and bonobo is down.  
       RDMA interconnect is up (Link0 up, Link1 down)
```

このイベント情報から、HAペアのaardvarkノードとbonoboノードの間のストレージ フェイルオーバー インターコネクト リンクLink1が停止している一方で、AppleとBoyの間のLink0はアクティブであることがわかります。一方のリンクがアクティブであるため、Remote Dynamic Memory Access (RDMA) は引き続き機能し、ストレージ フェイルオーバー ジョブも正常に実行されます。

ただし、両方のリンクが停止してストレージのフェイルオーバー保護が完全に無効になる状態を防ぐために、Link1が停止した理由を詳しく診断することになります。

手順

1. *イベント*詳細ページで、ソース フィールドに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 フェイルオーバー相互接続リンク ダウン状態に関連する可能性のあるその他のイベントの詳細を取得できます。

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、該当するHAペア (aardvarkとbonobo) の[HAの詳細]が[クラスタ / 健全性の詳細]ページの[ノード]タブに表示さ

れ、その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. イベントに関する詳細については、**HA** の詳細 を確認してください。

この例では、[Events]表に関連情報が表示されます。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 ダウン」イベント、イベントが生成された時刻、そしてこのイベントの発生元ノードが表示されます。

[HA の詳細]で確認したノードの場所情報を使用して、該当するHAペア ノードで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、または自ら実施します。

関連情報

["\[イベントの詳細ページ\]"](#)

["Unified Managerのユーザ ロールと機能"](#)

ボリュームのオフライン問題を解決する

このワークフローでは、Unified Managerの[イベント管理]インベントリ ページに表示されるボリューム オフライン イベントを評価して解決する方法の例を示します。このシナリオでは、管理者がUnified Managerを使用してボリューム オフライン イベントを解決します。

開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ボリュームがオフライン状態と報告された場合は、いくつかの理由が考えられます。

- 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) のルート ボリュームをホストしているノードが停止したために、SVMが停止した。
- 2つのRAIDディスクで同時に障害が発生したために、ボリュームをホストしているアグリゲートが停止した。

[イベント管理]インベントリ ページ、および[クラスタ / 健全性]、[Storage VM / 健全性]、[ボリューム / 健全性]の各詳細ページを使用して、上記の可能性が1つ以上該当す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、[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。

可用性イベントの[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*の詳細ページでは、次の 1 つ以上のタスクの情報を確認できます。

- 実行可能な診断のガイダンスを得るために、[原因]フィールドに表示される情報を確認します。

この例では、[原因]フィールドの情報から、該当のボリュームのみがオフラインになっていることがわかります。

- SVM 管理者が問題のボリュームを意図的にオフラインにしたことを示す兆候がないか、「メモと更新」領域を確認します。
- イベントのソース（ここではオフライン状態と報告されたボリューム）をクリックして、ボリュームの詳細情報を参照します。
- 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、またはイベントを解決済みとマークします（該当する場合）。

ボリュームのオフライン状態に対する診断アクションを実行する

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。

開始する前に

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解決することができます。

- ボリューム/ヘルス 詳細ページ リンクをクリックして、ホスト ノードがダウンし、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ためにボリュームがオフラインになっているかどうかを確認します。

見る"[ボリュームのオフライン状態がダウンノードによって引き起こされたかどうかを判断する](#)"。

- ボリューム/健全性 の詳細ページ リンクをクリックすると、ボリュームがオフラインになっていて、その SVM のルート ボリュームをホストしているノードがダウンしているためにホスト ストレージ仮想マシン (SVM) が停止しているかどうかを確認できます。

見る"[ボリュームがオフラインで、ノードがダウンしているために SVM が停止しているかどうかを判断する](#)"。

- ボリューム / ヘルス 詳細ページ リンクをクリックして、ホスト アグリゲート内のディスクが壊れているためにボリュームがオフラインになっているかどうかを確認します。

見る"[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"](#)

ホストノードがダウンしているためにボリュームがオフラインになっているかどうかを判別します

Unified Manager Web UIを使用して、ボリュームがオフラインになっている原因が、ボリュームのホスト 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。

開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ボリュームのオフライン状態の原因が、ホスト ノードの障害とその後のストレージ フェイルオーバーの失敗であるかどうかを判別するには、次の手順を実行します。

手順

1. オフライン ボリュームの **ボリューム / 健全性** 詳細ページの **関連デバイス** ペインで、SVM の下に表示されるハイパーテキスト リンクを見つけてクリックします。

[Storage VM / 健全性の詳細]ページに、オフライン ボリュームのホストStorage Virtual Machine (SVM) に関する情報が表示されます。

2. ストレージ **VM / ヘルス** 詳細ページの **関連デバイス** ペインで、ボリュームの下に表示されるハイパーテキスト リンクを見つけてクリックします。

「ヘルス: すべてのボリューム」ビューには、SVM によってホストされているすべてのボリュームに関する情報の表が表示されます。

3. ヘルス: すべてのボリューム*ビューの状態列ヘッダーで、フィルターシンボルをクリックします。☰をクリックし、[*オフライン] オプションを選択します。

オフライン状態のSVMボリュームのみが一覧表示されます。

4. 「ヘルス: すべてのボリューム」ビューで、グリッドシンボルをクリックします  をクリックし、クラスター ノード オプションを選択します。

クラスター ノード オプションを見つけるには、グリッド選択ボックスをスクロールする必要がある場合があります。

クラスター ノード列がボリューム 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. [正常性: すべてのボリューム] ビューで、オフライン ボリュームのリストを見つけて、その [クラスター ノード] 列で、そのホスティング 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、ホスト ノードが属しているノードのHAペアの状態が表示されます。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果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。

ボリュームがオフラインで、ノードがダウンしているために **SVM** が停止しているかどうかを判別します。

Unified Manager Web UIを使用して、ボリュームがオフラインになっている原因が、そのホストStorage Virtual Machine (SVM) のルート ボリュームをホストするノードの停止に起因してSVMが停止したためであるかどうかを確認することができます。

開始する前に

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 ボリューム / ヘルス 詳細ページの 関連デバイス ペインで、SVM の下に表示されるハイパーテキスト リンクを見つけてクリックします。

ストレージ VM / ヘルスの詳細ページには、ホスティング SVM の「実行中」または「停止済み」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、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 のステータスが停止している場合は、**[SVM の表示]** をクリックして、ホスティング SVM が停止している原因をさらに特定します。
3. *健全性: すべてのストレージVM*ビューのSVM列ヘッダーで、フィルターシンボルをクリックします。  停止した SVM の名前を入力します。

指定したSVMの情報が表形式で表示されます。

4. *ヘルス: すべてのストレージVM*ビューで、次に、[ルート ボリューム] オプションを選択します。

[ルート ボリューム]列がSVMインベントリに追加され、停止したSVMのルート ボリュームの名前が表示されます。

5. [ルート ボリューム] 列で、ルート ボリュームの名前をクリックすると、そのボリュームの ストレージ **VM / ヘルス** 詳細ページが表示されます。

SVMルート ボリュームのステータスが「(オンライン)」である場合は、元のボリュームのオフライン状態の原因が、そのSVMルート ボリュームをホストするノードの停止ではないことがわかります。

6. SVMルート ボリュームのステータスが「(オフライン)」の場合は、SVMルート ボリュームの[ボリューム / 健全性の詳細]ページの[関連デバイス]ペインで[アグリゲート]に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. アグリゲートの アグリゲート / ヘルス 詳細ページの 関連デバイス ペインで、ノードの下に表示されるハイパーテキスト リンクを見つけてクリックします。

[クラスタ / 健全性の詳細]ページの[ノード]タブに、SVMルート ボリュームのホスト ノードが属しているノードのHAペアの状態が表示されます。ノードの状態が画面に示されます。

ボリュームのオフライン状態の原因が、そのボリュームのホストSVMのオフライン状態であり、さらにその状態の原因がSVMのルート ボリュームをホストするノードの停止であることを確認したら、適切な管理者またはオペレータに連絡して、停止したノードを手動で再起動するように依頼します。

アグリゲート内のディスクの破損によりボリュームがオフラインになっているかどうかを確認する

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。

開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ボリュームのオフライン状態の原因が、RAIDディスクの問題によりホスト アグリゲートがオフラインになったためであるかどうかを判別するには、次の手順を実行します。

手順

1. *ボリューム/健全性*詳細ページの*関連デバイス*ペインで、アグリゲートの下に表示されるハイパーテキスト リンクを見つけてクリックします。

[アグリゲート / 健全性の詳細]ページに、ホスト アグリゲートのステータスが「オンライン」または「オフライン」と表示されます。アグリゲートのステータスがオンラインである場合、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. 集約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] リストで破損したディスク イベントを探します。
3. 破損したディスクをさらに識別するには、[関連デバイス] ペインの [ノード] の下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、*フィルター*ペインで*破損*を選択して、破損状態にある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である場合は、[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よるホスト アグリゲートのオフライン状態であることを確認したら、適切な管理者またはオペレータに連絡し、手動による破損ディスクの交換とアグリゲートをオンラインに戻す処理を依頼します。

容量の問題を解決する

このワークフローでは、容量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[ダッシュボード]ページにアクセスして、監視対象のストレージ オブジェクトに容量の問題が発生してい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します。

開始する前に

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、イベント ドロップダウン リストの下に容量パネルで「ボリューム スペースがいっぱい」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 スペースがいっぱいのエラー 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*の詳細ページから、次の 1 つ以上のタスクを実行できます。
 - 「原因」フィールドのエラー メッセージを確認し、「推奨される修復アクション」の下のおすすめをクリックして、可能な修復の説明を確認します。
 - [ソース]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情報を表示します。
 - このイベントに関して追加されたメモを確認します。
 - イベントにメモを追加します。
 - イベントを別のユーザに割り当てます。
 - イベントに応答します。
 - イベントを解決済みとマークします。

関連情報

["\[イベントの詳細ページ\]"](#)

ボリューム全体に対して推奨される修復アクションを実行する

「ボリューム スペースがいっぱいです」というエラー イベントを受信した後、イベントの詳細ページで推奨される修復アクションを確認し、推奨されるアクションの 1 つを実行することにします。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

Unified Managerを使用するこのワークフロー内のタスクは、どのロールのユーザでも実行できます。

この例では、Unified Managerの[イベント管理]インベントリ ページに「ボリューム スペースがフル」イベントが表示されたので、その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。

- ボリュームに対して自動拡張、重複排除、または圧縮を有効にする。
- ボリュームをサイズ変更するか、移動する。
- ボリュームのデータを削除するか、移動する。

いずれの修正策もONTAP System ManagerまたはONTAP CLIから実施する必要がありますが、実施する修正策を決め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、影響を受けるボリュー

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、構成 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. 関連デバイス ペインで、ホスティング アグリゲートの名前をクリックして、アグリゲートがより大きなボリュームに対応できるかどうかを確認します。
4. アグリゲート / ヘルス の詳細ページで、完全なボリュームをホストしているアグリゲートに十分な未コミット容量があることがわかったので、ONTAP System Manager を使用してボリュームのサイズを変更し、容量を増やします。

関連情報

["\[イベントの詳細ページ\]"](#)

健康閾値を管理する

すべてのアグリゲート、ボリューム、およびqtreeに適用されるグローバル健全性しきい値を設定して、健全性しきい値の違反を追跡することができます。

ストレージ容量の健全性しきい値とは

ストレージ容量の健全性しきい値は、Unified Manager サーバーがストレージ オブジェクトの容量の問題を報告する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。必要に応じて、オブジェクトまたはオブジェクトのグループに対するそれらの設定を変更できます。

グローバルヘルスしきい値設定を構成する

アグリゲート、ボリューム、およびqtreeのサイズを効果的に監視できるように、容量、増加率、Snapshotリザーブ、クォータ、およびinodeについて、グローバル健全性しきい値の条件を設定することができます。また、遅延しきい値を超えた場合にイベントを生成する設定を編集することもできます。

グローバル健全性しきい値の設定は、アグリゲートやボリュームなど、関連付けられているすべてのオブジェクトに適用されます。しきい値を超えるとイベントが生成され、アラートが設定されている場合はアラート通知も送信されます。しきい値はデフォルトで推奨値に設定されていますが、それらの値を変更することでイベントが生成される間隔をニーズに合わせて調整することができます。しきい値を変更した場合、次の監視サイクルから反映され、その値に基づいてイベントが生成または廃止されます。

グローバルヘルスしきい値設定には、左側のナビゲーションメニューの [イベントしきい値] セクションからアクセスできます。また、個々のオブジェクトのインベントリ ページまたは詳細ページから、そのオブジェクトのしきい値の設定を変更することもできます。

- 詳細については、["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、"[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、"[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、"[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。

グローバル集計ヘルスしきい値を構成する

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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

オプションをグローバル レベルで設定すると、オブジェクトのデフォルト値が変更されます。ただし、オブジェクト レベルでデフォルト値が変更されている場合、グローバルな値は変更されません。

しきい値のオプションは、効果的に監視できるようにデフォルトで値が設定されています。ただし、それぞれの環境の要件に合わせて値を変更することができます。

アグリゲートに配置されているボリュームで自動拡張が有効になっている場合は、元のボリューム サイズではなく、自動拡張で設定された最大ボリューム サイズに基づいて、アグリゲートの容量のしきい値を超えているかどうか判定されます。



ノードのルート アグリゲートには健全性しきい値の値は適用されません。

手順

1. 左側のナビゲーション ペインで、イベントしきい値 > 集計 をクリックします。
2. 容量、増加率、およびSnapshotコピーのしきい値を必要に応じて設定します。
3. *保存*をクリックします。

関連情報

"ユーザの追加"

グローバルボリュームの健全性しきい値を構成する

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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

ほとんどのしきい値のオプションは、効果的に監視できるようにデフォルト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。

ボリュームで自動拡張が有効になっている場合は、元のボリューム サイズではなく、自動拡張で設定された最大ボリューム サイズに基づいて、容量のしきい値を超えているかどうか判定されることに注意してください。



Snapshotコピー数のデフォルト値1000は、ONTAPバージョン9.4以降ではFlexVolのみに、ONTAPバージョン9.8以降ではFlexGroupボリュームのみに適用されます。それより古いバージョンの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コピー数の上限は250です。古いバージョンの場合、1000（および250～1000の間の数）を設定してもUnified Managerはこれを250と解釈するため、Snapshotコピーの数が250を超えるとイベントが送信されます。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、[ヘルス: すべてのボリューム] ビューまたは [ボリューム/ヘルスの詳細] ページでしきい値を 250 以下に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 > ボリューム をクリックします。
2. 容量、Snapshotコピー、qtreeクォータ、ボリューム増加率、およびinodeのしきい値を必要に応じて設定します。
3. *保存*をクリックします。

関連情報

"ユーザの追加"

グローバルqtreeヘルスしきい値を設定する

すべてのqtreeに対するグローバル健全性しきい値を設定して、しきい値の違反を追跡することができます。健全性しきい値の違反が発生すると該当するイベントが生成されるため、それらのイベントに基づいて予防策を講じることが可能です。監視対象のすべてのqtreeに適用されるしきい値について、ベストプラクティスの設定に基づいてグローバルな値を設定することができます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

しきい値のオプションは、効果的に監視できるようにデフォルトで値が設定されています。ただし、それぞれの環境の要件に合わせて値を変更することができます。

qtreeについてのイベントが生成されるのは、qtreeに対してqtreeクォータまたはデフォルト クォータが設定されている場合だけです。ユーザ クォータまたはグループ クォータで定義されているスペースがしきい値を超えてもイベントは生成されません。

手順

1. 左側のナビゲーション ペインで、イベントしきい値 > **Qtree** をクリックします。
2. 容量のしきい値を必要に応じて設定します。
3. *保存*をクリックします。

管理されていない保護関係の遅延しきい値設定を構成する

管理対象外の保護関係に対する遅延健全性しきい値（警告およびエラー）のグローバルなデフォルト設定を編集することで、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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

遅延時間は定義されている転送スケジュールの間隔よりも短い必要があります。たとえば、転送スケジュールが1時間ごとの場合、遅延時間は1時間未満でなければなりません。遅延しきい値では、遅延時間が超えてはならない割合を指定します。たとえば、上記の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。管理対象外のいずれかの保護関係に対して、設定を個別に指定して適用することはできません。

手順

1. 左側のナビゲーション ペインで、イベントしきい値 > 関係 をクリックします。
2. 警告またはエラーの遅延時間を増減して、デフォルトのグローバル設定を変更します。
3. 遅延しきい値の量から警告またはエラー イベントがトリガーされないようにするには、[有効] の横にあるボックスのチェックを外します。
4. *保存*をクリックします。

関連情報

["ユーザの追加"](#)

個々の集計ヘルスしきい値設定を編集する

1つ以上のアグリゲートの容量、増加率、およびSnapshotコピーについての健全性しきい値の設定を編集することができます。しきい値を超えると、アラートが生成されて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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

しきい値の値を変更すると、次の監視サイクルから、その値に基づいてイベントが生成または廃止されます。

アグリゲートに配置されているボリュームで自動拡張が有効になっている場合は、元のボリューム サイズではなく、自動拡張で設定された最大ボリューム サイズに基づいて、アグリゲートの容量のしきい値を超えているかどうか判定されます。

手順

1. 左側のナビゲーション ペインで、ストレージ > アグリゲート をクリックします。
2. 「ヘルス: すべての集計」*ビューで、1 つ以上の集計を選択し、「しきい値の編集」*をクリックします。
3. 集計しきい値の編集 ダイアログ ボックスで、適切なチェック ボックスをオンにして設定を変更することで、容量、増加、またはスナップショット コピーのいずれかのしきい値設定を編集します。
4. *保存*をクリックします。

関連情報

["ユーザの追加"](#)

個々のボリュームの健全性しきい値設定を編集する

1 つ以上のボリュームの容量、増加率、クォータ、およびスペース リザーベーションについての健全性しきい値の設定を編集することができます。しきい値を超えると、アラートが生成されて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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

しきい値の値を変更すると、次の監視サイクルから、その値に基づいてイベントが生成または廃止されます。

ボリュームで自動拡張が有効になっている場合は、元のボリューム サイズではなく、自動拡張で設定された最大ボリューム サイズに基づいて、容量のしきい値を超えているかどうか判定されることに注意してください。



Snapshotコピー数のデフォルト値1000は、ONTAPバージョン9.4以降ではFlexVolのみに、ONTAPバージョン9.8以降ではFlexGroupボリュームのみに適用されます。それより古いバージョンの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コピー数の上限は250です。古いバージョンの場合、1000（および250～1000の間の数）を設定してもUnified Managerはこれを250と解釈するため、Snapshotコピーの数が250を超えるとイベントが送信されます。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、[ヘルス: すべてのボリューム] ビューまたは [ボリューム/ヘルスの詳細] ページでしきい値を 250 以下に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、ストレージ > ボリューム 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、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、適切なチェック ボックスを選択して設定を変更することで、容量、スナップショット コピー、qtree クォータ、増加、または inode のいずれかのしきい値設定を編集します。
4. *保存*をクリックします。

関連情報

"ユーザの追加"

個々のqtreeの健全性しきい値設定を編集する

1つ以上のqtreeの容量についての健全性しきい値の設定を編集することができます。しきい値を超えると、アラートが生成されて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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

しきい値の値を変更すると、次の監視サイクルから、その値に基づいてイベントが生成または廃止されます。

手順

1. 左側のナビゲーション ペインで、ストレージ > **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. **[qtree しきい値の編集]** ダイアログ ボックスで、選択した qtree の容量しきい値を変更し、[保存] をクリックします。



[Storage VM / 健全性の詳細]ページの[qtree]タブで個々のqtreeのしきい値を設定することもできます。

クラスターのセキュリティ目標を管理する

Unified Manager には、『NetApp セキュリティ強化ガイド for ONTAP 9』で定義された推奨事項に基づいて、ONTAP クラスタ、ストレージ仮想マシン (SVM)、およびボリュームのセキュリティがどの程度確保されてい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 NetApp 推奨のガイドラインに従っていない領域を提示して、潜在的な問題を修正できるようにすることです。ほとんどの場合、問題は ONTAP System Manager または ONTAP CLI を使用して解決します。組織がすべての推奨事項に従うとはかぎらないため、変更が不要な場合もあります。

参照 ["NetApp ONTAP 9 セキュリティ強化ガイド"](#) 詳細な推奨事項と解決策については、(TR-4569) を参照してください。

Unified Managerは、セキュリティ ステータスを報告するだけでなく、セキュリティ違反があるクラスタまたはSVMに対してセキュリティ イベントを生成します。これらの問題は[イベント管理]インベントリ ページで追跡できます。また、イベントにアラートを設定して、新たなセキュリティ イベントが発生したときにストレージ管理者が通知を受け取るようにすることができます。

詳細については、"[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、ストレージ仮想マシン (SVM)、およびボリュームのセキュリティ基準は、『NetApp セキュリティ強化ガイド for ONTAP 9』で定義されている推奨事項に照らして評価されます。

セキュリティ チェックには、次のようなものがあります。

- クラスタがSAMLなどのセキュアな認証方式を使用しているかどうか
- ピア クラスタの通信が暗号化されているかどうか
- Storage VMの監査ログが有効になっているかどうか
- ボリュームでソフトウェアまたはハードウェアの暗号化が有効になっているかどうか

コンプライアンスカテゴリと "[NetApp ONTAP 9 セキュリティ強化ガイド](#)"詳細情報については。



Active IQプラットフォームから報告されるアップグレード イベントもセキュリティ イベントとみなされます。これらのイベントは、ONTAPソフトウェア、ノード ファームウェア、またはオペレーティング システム ソフトウェア（セキュリティ アドバイザリ用）のアップグレードが必要な問題を示します。これらのイベントは[セキュリティ]パネルには表示されませんが、[イベント管理]インベントリ ページから確認できます。

詳細については、"[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

この表では、Unified Manager が評価するクラスタ セキュリティ コンプライアンス パラメータ、NetApp の推奨事項、およびパラメータがクラスタが準拠しているかどうかの全体的な判断に影響するかどうかについて説明します。

クラスター上に非準拠の SVM があると、クラスターのコンプライアンス値に影響します。そのため、クラスタのセキュリティが準拠とみなされるためには、事前にSVMのセキュリティ問題の修正が必要となる場合があります。

以下のパラメータは、すべてのインストール環境で表示されるわけではありません。たとえば、ピア クラスタがない場合やクラスタでAutoSupportを無効にしている場合、「クラスタ ピアリング」や「AutoSupport HTTPS転送」の項目は表示されません。

パラメータ	説明	推奨事項	クラスターコンプライアンスに影響
グローバル FIPS	グローバルFIPS（連邦情報処理標準）140-2準拠モードが有効になっているかどうかを示します。FIPSを有効にすると、TLSv1とSSLv3は無効になり、TLSv1.1とTLSv1.2のみが許可されます。	有効	はい
Telnet	システムへのTelnetアクセスが有効になっているかどうかを示します。セキュアなリモートアクセスを確立するために、Secure Shell（SSH）を推奨します。	無効	はい
安全でない SSH 設定	SSH が安全でない暗号（たとえば *cbc で始まる暗号）を使用するかどうかを示します。	いいえ	はい
ログイン バナー	システムにアクセスするユーザに対してログインバナーが有効になっているかどうかを示します。	有効	はい
クラスタ ピアリング	ピア クラスタ間の通信が暗号化されているかどうかを示します。このパラメータが準拠とみなされるためには、ソースとデスティネーションの両方のクラスタで暗号化が設定されている必要があります。	暗号化	はい
ネットワーク タイム プロトコル	クラスタにNTPサーバが1つ以上設定されているかどうかを示します。冗長性と最適なサービスを確保するために、NetApp少なくとも 3 台の NTP サーバーをクラスタに関連付けることをお勧めします。	設定	はい

パラメータ	説明	推奨事項	クラスターコンプライアンスに影響
OCSP	9.14.1 以降、Active IQ Unified Manager は、ストレージ仮想マシン (SVM、旧称 Vserver) レベルでオンライン証明書ステータス プロトコル (OCSP) ステータス情報を提供します。つまり、SVM へのすべての SSL/TLS 接続に OCSP 検証が適用され、これらの接続で使用する証明書の整合性と有効性が保証されます。	有効	いいえ
リモート監査ログ	ログ転送 (syslog) が暗号化されるかどうかを示します。	暗号化	はい
AutoSupport HTTPS 転送	AutoSupportメッセージをNetAppサポートに送信するためのデフォルトのトランスポート 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。NetApp、不要な組み込みアカウントをロック (無効化) することを推奨しています。	無効	はい
SAML ユーザ	SAMLが設定されているかどうかを示します。SAMLを使用すると、シングル サインオンのログイン方法として多要素認証 (MFA) を設定できます。	いいえ	いいえ

パラメータ	説明	推奨事項	クラスターコンプライアンスに影響
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、クラスターにアクセスするユーザに対して推奨される認証メカニズムです。	いいえ	いいえ
LDAP ユーザ	LDAPが設定されているかどうかを示します。Active DirectoryとLDAPは、ローカルユーザよりもクラスターを管理するユーザに対して推奨される認証メカニズムです。	いいえ	いいえ
証明書ユーザ	証明書ユーザがクラスターにログインするように設定されているかどうかを示します。	いいえ	いいえ
ローカル ユーザ	ローカル ユーザがクラスター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は無効にしてください。セキュアなリモート アクセスを確立するために、Secure Shell (SSH) が推奨されます。	無効	はい
MD5 の使用	ONTAPユーザ アカウントに安全性が低いMD5ハッシュ関数が使用されているかどうかを示します。MD5ハッシュを使用したユーザ アカウントについては、より安全なSHA-512などの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

パラメータ	説明	推奨事項	クラスターコンプライアンスに影響
証明書発行者タイプ	使用されているデジタル証明書のタイプを示します。	CA署名	いいえ

Storage VMのコンプライアンス 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各条件（パラメータ）、NetAppの推奨設定、およびSVMが準拠しているかどうかの総合的な判断にその条件が影響するかどうかを示します。

パラメータ	説明	推奨事項	SVMコンプライアンスに影響
監査ログ	監査ログが有効になっているかどうかを示します。	有効	はい
安全でない SSH 設定	SSHが安全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*。	いいえ	はい
ログイン バナー	システム上の SVM にアクセスするユーザーに対してログイン バナーが有効か無効かを示します。	有効	はい
LDAP 暗号化	LDAP暗号化が有効になっているかどうかを示します。	有効	いいえ
NTLM 認証	NTLM認証が有効になっているかどうかを示します。	有効	いいえ
LDAP ペイロードの署名	LDAPペイロードの署名が有効になっているかどうかを示します。	有効	いいえ
CHAP 設定	CHAPが有効になっているかどうかを示します。	有効	いいえ
Kerberos V5	Kerberos V5認証が有効になっているかどうかを示します。	有効	いいえ

パラメータ	説明	推奨事項	SVM コンプライアンスに影響
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 のステータスがアクティブ	FPolicyが作成されているかどうかを示します。	はい	いいえ
SMB 暗号化が有効	SMBの署名と封印が有効になっているかどうかを示します。	はい	いいえ
SMB 署名が有効	SMBの署名が有効になっている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

この表は、Unified Manager がボリューム上のデータが不正なユーザー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するために評価するボリューム暗号化パラメータを示しています。

ボリューム暗号化パラメータは、クラスタまたはStorage VMが準拠しているとみなされるかどうかには影響しません。

パラメータ	説明
ソフトウェア暗号化	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の暗号化	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

クラスタおよびストレージ仮想マシン (SVM) は、『NetApp セキュリティ強化ガイド for ONTAP 9』で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基準のいずれ

かが満たされていない場合、準拠していないと見なされます。また、非準拠と判断されたSVMが1つでもある場合も、クラスタは非準拠とみなされます。

セキュリティ カードの各ステータス アイコンとその意味は次のとおりです。

-  - パラメータは推奨どおりに設定されています。
-  - パラメータが推奨どおりに設定されていません。
-  - クラスター上で機能が有効になっていないか、パラメーターが推奨どおりに構成されていませんが、このパラメーターはオブジェクトのコンプライアンスに寄与しません。

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。

クラスターとストレージVMのセキュリティステータスを表示する

Active IQ Unified Managerでは、環境内のストレージ オブジェクトのセキュリティ ステータスをインターフェイスのさまざまなポイントで確認できます。定義したパラメータに基づいて情報とレポートを収集および分析し、監視対象のクラスタおよびStorage VMについて、不審な挙動や不正なシステム変更を検出することができます。

セキュリティに関する推奨事項については、["NetApp ONTAP 9 セキュリティ強化ガイド"](#)

[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 レベルでのONTAPクラスタとストレージ 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. 監視対象のすべてのクラスターのセキュリティ ステータスを表示するか、単一のクラスターのセキュリティ ステータスを表示するかに応じて、ドロップダウン メニューから [すべてのクラスター] を選択するか、単一のクラスターを選択します。
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、`View Reports`リンクをクリックすると、ボリューム、クラスター、またはストレージ VM 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。

[セキュリティ]ページには、次のパネルが表示されます。

- クラスタコンプライアンス: データセンター内のすべてのクラスタのセキュリティステータス (準拠しているクラスタと準拠していないクラスタの数)
- ストレージ VM コンプライアンス: データセンター内のすべてのストレージ VM のセキュリティ ステータス (準拠しているストレージ VM と準拠していないストレージ VM の数)
- ボリューム暗号化: 環境内のすべてのボリュームの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と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ステータス: 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)

- クラスター認証と証明書: SAML、Active Directory、証明書とローカル認証など、各タイプの認証方法を使用しているクラスターの数。証明書の有効期限が切れているか60日以内に切れるクラスターの数も表示されます。

[クラスター]ページでのすべてのクラスターのセキュリティの詳細表示

クラスター / セキュリティ 詳細ページでは、クラスター レベルでのセキュリティ コンプライアンスの状態を表示できます。

手順

1. 左側のナビゲーション ペインで、ストレージ > クラスター をクリックします。
2. *表示 > セキュリティ > すべてのクラスター*を選択します。

グローバルFIPS、Telnet、安全でない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、クラスターの証明書の有効期限のステータスなど、デフォルトのセキュリティ パラメータが表示されます。

クリックすると  その他のオプション ボタンをクリックし、Unified Manager または System Manager の セキュリティ ページでセキュリティの詳細を表示することを選択します。System Managerで詳細を確認するには、有効なクレデンシャルが必要です。



クラスターに期限切れの証明書がある場合は、expired *クラスター証明書の有効性*の下で、System Manager (9.10.1 以降) から更新します。クリックできません `expired` System Manager インスタンスが 9.10.1 より前のリリースの場合。

[Storage VM]ページでのすべてのクラスターのセキュリティの詳細の表示

ストレージ VM / セキュリティ 詳細ページでは、ストレージ VM レベルでのセキュリティ コンプライアンスの状態を表示できます。

手順

1. 左側のナビゲーション ペインで、ストレージ > ストレージ VM をクリックします。
2. 表示 > セキュリティ > すべてのストレージ VM を選択します。クラスターとセキュリティ パラメータのリストが表示されます。

Storage VMのセキュリティ コンプライアンスのデフォルトのビューで、Storage VM、クラスター、ログイン バナー、監査ログ、安全でないSSH設定などのセキュリティ パラメータを確認できます。

クリックすると  その他のオプション ボタンをクリックし、Unified Manager または System Manager の セキュリティ ページでセキュリティの詳細を表示することを選択します。System Managerで詳細を確認するには、有効なクレデンシャルが必要です。

ボリュームとストレージ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、以下を参照してください。"[すべてのボリュームとストレージVMのランサムウェア対策ステータスの表示](#)"。

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 イベントを表示します

「アップグレード」の影響領域を持つ特定のセキュリティ イベントがあります。これらはActive IQプラットフォームから報告されるイベントで、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。

開始する前に

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、通知が不要なアップグレード セキュリティ イベントがある場合は、このリストを利用して無効にするイベントを特定できます。

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。

[イベント管理]インベントリ ページには、デフォルトではすべてのアクティブなイベント（新規と確認済みのイベント）が表示されます。

2. [表示] メニューから [アップグレード イベント] を選択します。

アクティブなすべてのアップグレード セキュリティ イベントが表示されます。

すべてのクラスターでユーザー認証がどのように管理されているかを表示します

[セキュリティ]ページには、各クラスターでユーザの認証に使用されている認証タイプと、各タイプを使用してクラスターにアクセスしているユーザ数が表示されます。このページを使用して、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にあるドロップダウン メニューから [すべてのクラスター] 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. クラスター認証 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ーの数を確認します。
5. クラスター セキュリティ カードを表示して、各クラスターでユーザーを認証するために使用されている認証メカニズムを表示します。

安全でない方法やNetAppが推奨していない方法を使用してシステムにアクセスしているユーザーがいる場合は、その方法を無効にすることができます。

すべてのボリュームの暗号化ステータスを表示する

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。

開始する前に

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、ストレージ > ボリューム 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. 健全性: ボリュームの暗号化 ビューで、暗号化タイプ フィールドで並べ替えるか、フィルターを使用して、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 (暗号化タイプが「なし」) を表示します。

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) 、およびそれらの現在のランサムウェア対策ステータスのリストを表示して、ボリュームおよびSVM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。

開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

ランサムウェア対策ステータスの詳細については、以下を参照してください。["ONTAP: ランサムウェア対策を有効にする"](#)。

ランサムウェア対策検出機能による全ボリュームのセキュリティの詳細表示

手順

1. 左側のナビゲーション ペインで、ストレージ > ボリューム をクリックします。
2. 表示メニューで、ヘルス > セキュリティ > *ランサムウェア対策*を選択します。
3. セキュリティ: ランサムウェア対策 ビューでは、さまざまなフィールドで並べ替えたり、フィルターを使用したりできます。



ランサムウェア対策は、オフライン ボリューム、制限状態のボリューム、SnapLockボリューム、FlexGroupボリューム、FlexCacheボリューム、SANのみのボリューム、停止中の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に対してはサポートされていません。

ランサムウェア対策の検出機能による全Storage VMのセキュリティの詳細表示

手順

1. 左側のナビゲーション ペインで、ストレージ > ストレージ 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*を選択します。SVMとランサムウェア対策ステータスのリストが表示されます。



ランサムウェア対策による監視は、NASプロトコルが有効になっていないStorage VMではサポートされていません。

すべてのアクティブなセキュリティイベントを表示

アクティブなセキュリティ イベントをすべて表示し、問題を解決できるユーザに各イベントを割り当てることができます。また、受信不要なセキュリティ イベントがある場合は、このリストを利用して無効にするイベントを特定できます。

開始する前に

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。

[イベント管理]インベントリ ページには、デフォルトでは新規と確認済みのイベントが表示されます。

2. [表示] メニューから、[アクティブなセキュリティ イベント] を選択します。

このページには、過去7日間に生成された「新規」と「確認済み」のすべてのセキュリティ イベントが表示されます。

セキュリティイベントのアラートを追加する

セキュリティ イベントのアラートは、Unified Managerで受信する他のイベントと同様に、イベントごとに個別に設定することができます。または、すべてのセキュリティ イベントを同じように扱い、同じユーザにEメールを送信する場合は、セキュリティ イベントがトリガーされたときに通知する共通のアラートを作成することもできます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

以下の例は、「Telnet プロトコルが有効」セキュリティ イベントのアラートを作成する方法を示しています。クラスタへのリモート管理アクセス用にTelnetアクセスが設定されると、アラートが送信されます。同じ手順で、すべてのセキュリティ イベントに対してアラートを作成できます。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > アラート設定 をクリックします。
2. *アラート設定*ページで、*追加*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、アラートの名前と説明を入力します。
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ーを選択します。
5. *イベント*をクリックし、次のアクションを実行します。
 - a. イベントの重大度リストで、*警告*を選択します。

- b. 一致するイベント リストで、**Telnet** プロトコルが有効 を選択します。
6. ***アクション***をクリックし、***これらのユーザーに警告***フィールドで警告メールを受信するユーザーの名前を選択します。
7. 通知頻度、SNMPトラップの発行、スクリプトの実行など、このページの他のオプションを設定します。
8. ***保存***をクリックします。

特定のセキュリティイベントを無効にする

デフォルトでは、すべてのイベントが有効になっています。環境で重要でないイベントは、無効にして通知が生成されないようにすることができます。無効にしたイベントの通知を再開するには、該当するイベントを有効にします。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

イベントを無効にすると、システムで以前に生成されたイベントは「廃止」とマークされ、それらのイベントに設定されたアラートはトリガーされなくなります。無効にしたイベントを有効にすると、それらのイベントの通知の生成が次の監視サイクルから再開されます。

手順

1. 左側のナビゲーション ペインで、**ストレージ管理 > イベント設定** 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	a. *無効*をクリックします。 b. [イベントの無効化] ダイアログ ボックスで、重大度として 警告 を選択します。これはすべてのセキュリティ イベントが該当するカテゴリです。 c. [一致イベント]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[イベントの無効化]列に移します。 d. *[保存して閉じる]*をクリックします。 e. 無効にしたイベントが[イベント セットアップ] 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。
イベントを有効にする	a. 無効になっているイベントのリストで、再び有効にするイベント（複数可）のチェックボックスをオンにします。 b. *有効*をクリックします。

セキュリティ イベント

セキュリティ イベントは、『NetApp セキュリティ強化ガイド for ONTAP 9』で定義されたパラメータに基づいて、ONTAP クラスタ、ストレージ仮想マシン (SVM)、およびボリュームのセキュリティ ステータスに関する情報を提供します。これらのイベントは潜在的な問題を通知するものです。管理者はその重大度を評価し、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 タイプ別にまとめられ、イベント名とトラップ名、影響レベル、および重大度が表示されます。これらのイベントは、クラスタおよびStorage VMのイベント カテゴリに表示されます。

バックアップと復元操作を管理する

Active IQ Unified Managerのバックアップを作成し、システム障害やデータ損失が発生した場合に、リストア機能を使用して同じ（ローカル）システムまたは新しい（リモート）システムにバックアップをリストアできます。

Unified Managerをインストールしたオペレーティング システム、および管理対象のクラスタとノードの数に応じて、バックアップとリストアの方法は3種類あります。

オペレーティング システム	展開規模	推奨バックアップ方法
VMware vSphere	any	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	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プロトコルによるUnified ManagerデータベースのNetApp Snapshot

これらのそれぞれの方法について、以降のセクションで説明します。

仮想アプライアンスでのUnified Managerのバックアップとリストア

仮想アプライアンスにインストールされたUnified Managerのバックアップ / リストア 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。

仮想アプライアンスのバックアップを完了するには、次のタスクを実行します。

1. VM の電源をオフにし、Unified Manager 仮想アプライアンスの VMware スナップショットを取得しま

す。

2. VMware スナップショットをキャプチャするには、データストアにNetAppスナップショット コピーを作成します。

ONTAPソフトウェアを実行しているシステム以外でデータストアをホストしている場合は、ストレージベンダーのガイドラインに従ってVMwareスナップショットを作成します。

3. NetAppスナップショット コピーまたはスナップショットと同等のものを代替ストレージに複製します。
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する必要があります。

VMをリストアする際は、作成したVMwareスナップショットを使用して、VMをバックアップの作成時点の状態に戻すことができます。

MySQLデータベース ダンプを使用したバックアップとリストア

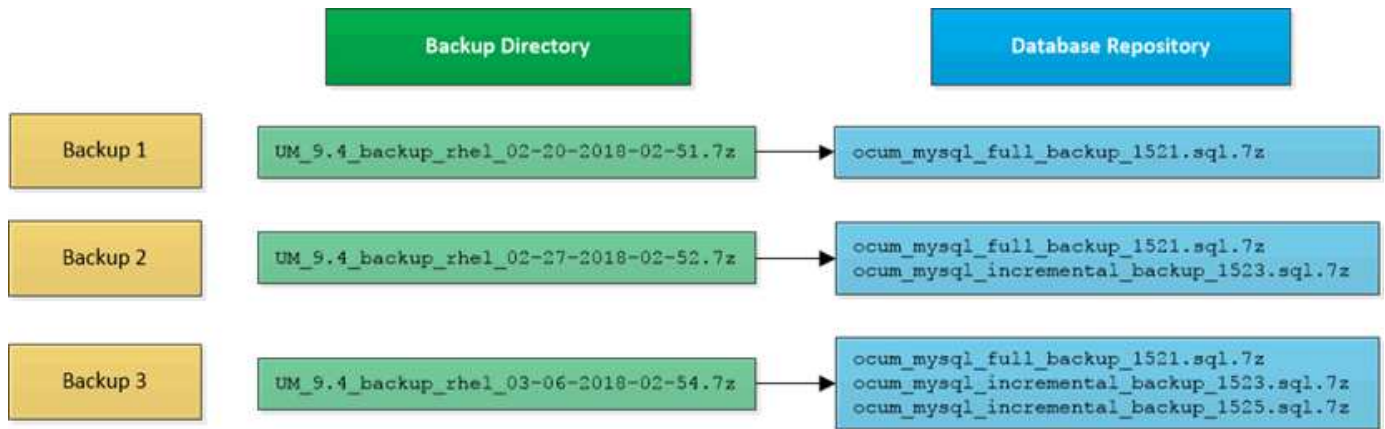
MySQL データベース ダンプ バックアップとは、システム障害やデータ損失が発生した場合に利用できるActive IQ Unified Managerデータベースと構成ファイルのコピーです。バックアップはローカルにもリモートにも保存できますが、Active IQ Unified Managerホスト システムとは別のリモートの場所を定義することを推奨します。



LinuxサーバおよびWindowsサーバにUnified Managerをインストールしている場合、デフォルトのバックアップ メカニズムはMySQLデータベース ダンプです。ただし、Unified Managerで管理しているクラスターやノードの数が多い場合や、MySQLバックアップが完了するまでに何時間もかかる場合は、Snapshotコピーを使用してバックアップを実行できます。この機能は、Red Hat Enterprise LinuxおよびWindowsで使用できます。

データベース ダンプ バックアップでは、バックアップ ディレクトリに1つのファイルとデータベース リポジトリ ディレクトリに1つ以上のファイルが作成されます。バックアップ ディレクトリ内のファイルは非常に小さく、バックアップを再作成するために必要なデータベース リポジトリ ディレクトリ内のファイルへのポインタのみが含まれます。

データベース バックアップの初回生成時は、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。それ以降のバックアップの生成時は、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 ファイルとの差分を含む増分バックアップ ファイルが作成されます。追加のバックアップを作成すると、次の図に示すように、最大保持設定までこのプロセスが繰り返されます。



これらの2つのディレクトリ内のバックアップ ファイルは、名前を変更したり削除したりしないでください。それらの処理を行うと、以降のリストア処理が失敗します。

バックアップ ファイルをローカル システムに保存する場合は、完全なリストアを必要とするシステムの問題が発生したときに使用できるように、それらのバックアップ ファイルをリモートにコピーする処理が必要になります。

バックアップ処理を開始する前に、Active IQ Unified Managerで整合性チェックが実行され、必要なすべてのバックアップ ファイルとバックアップ ディレクトリが存在し、書き込み可能であることが確認されます。また、バックアップ ファイルを作成できるだけの十分なスペースがシステムにあるのかも確認されます。

データベースダンプバックアップの保存先とスケジュールを設定する

Unified Managerのデータベース ダンプ バックアップ設定で、データベースのバックアップ パス、保持数、およびバックアップ スケジュールを設定できます。日単位または週単位のスケジュールされたバックアップを有効にすることができます。スケジュールされたバックアップはデフォルトでは無効になっていますが、設定することを推奨します。

開始する前に

- 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定義することを推奨します。

- Unified ManagerをLinuxシステムにインストールし、MySQLバックアップを使用する場合は、バックアップ ディレクトリに対して次の権限と所有権が設定されていることを確認してください。

権限: 0750、所有権: jboss:maintenance

- Unified ManagerをWindowsシステムにインストールし、MySQLバックアップを使用する場合は、バックアップ ディレクトリにアクセスできるのが管理者だけであることを確認してください。

初回のバックアップではフル バックアップが実行されるため、2回目以降のバックアップよりも時間がかかります。フル バックアップは1GBを超えることもあり、3〜4時間かかる場合があります。2回目以降は増分バックアップとなるため、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スペースに対して多すぎる場合は、定期的にフル バックアップを実行して、古いバックアップとその増分ファイルを置き換えることができます。別の方法として、Snapshotコピーを使用してバックアップを作成することもできます。
- 新しいクラスタを追加してから最初の15日間に作成されたバックアップについては、過去のパフォーマンス データが正確でないことがあります。

手順

1. 左側のナビゲーション ペインで、[全般] > [データベース バックアップ] 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*をクリックします。

スケジュールに基づいてデータベース ダンプ バックアップ ファイルが作成されます。使用可能なバックアップ ファイルは[データベース バックアップ]ページで確認できます。

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 ファイルを同一または異なるUnified Managerサーバにリストアする処理です。リストア処理はUnified Managerメンテナンス コンソールから実行します。

同じ（ローカル）システムでリストア処理を実行する場合、バックアップ ファイルがすべてローカルに保存されていれば、デフォルトの場所を使用してリストア オプションを実行できます。別のUnified Managerシステム（リモート システム）でリストア処理を実行する場合は、リストア オプションを実行する前に、バックアップ ファイルをセカンダリ ストレージからローカル ディスクにコピーする必要があります。

復元プロセス中は、Unified Manager からログアウトされます。リストア処理が完了したら、システムにログインできます。

バックアップ イメージを新しいサーバにリストアする場合は、リストア処理の完了後に新しいHTTPSセキュリティ証明書を生成してUnified Managerサーバを再起動する必要があります。また、バックアップ イメージを新しいサーバにリストアするときに求められた場合は、SAML認証を再設定する必要があります。



Unified Manager が新しいバージョンのソフトウェアにアップグレードされた後は、古いバックアップ ファイルを使用してイメージを復元することはできません。Unified Managerをアップグレードすると、スペースを節約するために、最新のファイルを除く古いバックアップ ファイルがすべて自動的に削除されます。

関連情報

["HTTPSセキュリティ証明書の生成"](#)

["SAML認証の有効化"](#)

WindowsでMySQLデータベースのバックアップを復元する

データ損失やデータ破損が発生した場合、リストア機能を使用してUnified Managerを以前の安定した状態にリストアすることで損失を最小限に抑えることができます。Unified Manager 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。

開始する前に

- Windowsの管理者権限が必要です。
- リストア処理を実行するシステムにUnified Managerのバックアップ ファイルとデータベース リポジトリ ディレクトリの内容をコピーしておく必要があります。

バックアップファイルをデフォルトのディレクトリにコピーすることをお勧めします。

`\ProgramData\NetApp\OnCommandAppData\ocum\backup`。データベースリポジトリファイルは、`\database_dumps_repo\サブディレクトリの下 \backup\ディレクトリ`。

- バックアップファイルは `.7z` タイプ。

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 MySQL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。また、Windowsのバックアップは、Windowsプラットフォームにのみリストアできます。



フォルダ名にスペースが含まれている場合は、バックアップ ファイルの絶対パスまたは相対パスを二重引用符で囲む必要があります。

手順

1. 新しいサーバへのリストアを実行する場合は、Unified Managerのインストールの完了後に、UIを起動したり、クラスタ、ユーザ、または認証設定を設定したりしないでください。これらの情報は、リストア プロセスでバックアップ ファイルから取り込みます。
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. コマンドを入力してください ``maintenance_console`` Enter キーを押します。
5. メンテナンス コンソールの メイン メニュー で、 バックアップの復元 オプションの番号を入力します。
6. *MySQL バックアップの復元*の番号を入力します。
7. プロンプトが表示されたら、バックアップ ファイルの絶対パスを入力します。

Bundle to restore from:

```
\ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_backup_windows_02-20-2020-02-51.7z
```

リストア処理が完了したら、Unified Managerにログインできます。

バックアップをリストアしたあとにOnCommand Workflow Automationサーバが動作しなくなった場合は、次

の手順を実行します。

1. Workflow Automationサーバで、Unified ManagerサーバのIPアドレスを最新のマシンを参照するように変更します。
2. 手順1で取得に失敗した場合は、Unified Managerサーバでデータベース パスワードをリセットします。

NetApp Snapshotを使用したバックアップとリストア

NetApp Snapshotコピーは、システム障害やデータ損失が発生した場合にリストアに利用できるUnified Managerデータベースと構成ファイルのポイントインタイム イメージを作成する機能です。SnapshotコピーをいずれかのONTAPクラスタ上のボリュームに定期的に書き込むようにスケジュールすることで、常に最新のコピーを保持することができます。



この機能は、仮想アプライアンスにインストールされたActive IQ Unified Managerでは使用できません。

Linuxでバックアップを構成する

Active IQ Unified ManagerがLinuxマシンにインストールされている場合は、NetApp Snapshotを使用してバックアップとリストアを設定できます。

Snapshotコピーにかかる時間はごくわずかで、通常は数分で完了します。Unified Managerデータベースがロックされる時間も非常に短く、インストール環境の中断はほとんどありません。イメージにはSnapshotコピーが最後に作成されたあとに発生したファイルへの変更だけが記録されるため、ストレージ スペースは最小限しか消費せず、パフォーマンスのオーバーヘッドもわずかです。SnapshotはONTAPクラスタに作成されるため、必要に応じて、SnapMirrorなどのNetAppの他の機能を利用して保護を追加できます。

バックアップ処理を開始する前に、Unified Managerは整合性チェックを実行して、デスティネーション システムが使用可能であることを確認します。



- 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 9.16で作成したバックアップは、Unified Manager 9.16のシステムにのみリストアできます。

- Snapshot設定に変更があると、Snapshotが無効になることがあります。

スナップショットコピーの場所を構成する

ONTAP System ManagerまたはONTAP CLIを使用して、いずれかのONTAPクラスタでSnapshotコピーを格納するボリュームを設定できます。

開始する前に

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

- 地理的にUnified Managerサーバに近い場所に設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：
 - 名前スイッチと名前マッピングは「files」を使用するように設定する必要があります
 - クライアント側のユーザーに対応するために作成されたローカルユーザー
 - 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てください
 - エクスポートポリシーでスーパーユーザーアクセスが「any」に設定されていることを確認してください。
 - Linux 向けNetAppスナップショットの NFS
 - NFSサーバーでNFSv4が有効になっており、クライアントとストレージVMでNFSv4 IDドメインが指定されている必要があります。
 - ボリュームはUnified Manager/opt/netapp/dataディレクトリの2倍以上のサイズである必要があります。

現在のサイズを確認するには、`du -sh /opt/netapp/data/`コマンドを使用します。

- ボリュームの要件：
 - ボリュームはUnified Managerの/opt/netapp/dataディレクトリの2倍以上のサイズである必要があります。
 - セキュリティスタイルはUNIXに設定する必要があります
 - ローカルスナップショットポリシーを無効にする必要があります
 - ボリュームの自動サイズ設定を有効にする必要がある
 - パフォーマンスサービスレベルは、「Extreme」など、IOPSが高くレイテンシが低い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、["ONTAP 9でNFSv4を設定する方法"](#)そして["ONTAP 9 NFS 構成エクスペンスガイド"](#)。

スナップショットコピーの保存先を指定する

Active IQ Unified Manager Snapshotコピーのデスティネーションには、いずれかのONTAPクラスタですでに設定済みのボリュームを指定する必要があります。デスティネーションはメンテナンス コンソールを使用して定義します。

- 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. Secure Shellを使用して、Active IQ Unified ManagerシステムのIPアドレスまたはFQDNに接続します。
2. メンテナンス ユーザ（umadmin）の名前とパスワードでシステムにログインします。
3. コマンドを入力してください `maintenance\_console` Enter キーを押します。
4. メンテナンス コンソールの メイン メニュー で、 バックアップの復元 オプションの番号を入力します。
5. * NetAppスナップショット バックアップの構成*の番号を入力します。
6. NFSを設定するオプションの番号を入力します。
7. 提供する必要のある情報を確認して、「バックアップ構成の詳細を入力」の番号を入力します。
8. Snapshotを書き込むボリュームを指定するには、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の名前、ストレージ システムのユーザ名とパスワード、およびマウント パスを入力します。
9. この情報を確認して入力してください y。

システムで次のタスクが実行されます。

- クラスタへの接続を確立する
 - すべてのサービスを停止します
 - ボリューム内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てActive IQ Unified Managerインターフェイスを起動し、まだ作成していない場合はSnapshotコピーのスケジュールを作成します。

Windowsでバックアップを構成する

Active IQ Unified Managerは、Windowsオペレーティング システムでのNetApp Snapshotを使用したバックアップとリストアを、iSCSIプロトコルを使用するLUNを利用してサポートします。

Snapshotベースのバックアップは、Unified Managerのすべてのサービスの実行中に作成できます。このバックアップでは、データベース全体にグローバルな読み取りロックが適用されて同時書き込みが回避されるため、Snapshotには整合性が取れた状態のデータベースがキャプチャされます。Windows OSにインストールされたUnified ManagerでNetApp Snapshotを使用した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のバックアップをSnapshotベースに設定します。

Unified ManagerでSnapshotコピーの作成を設定する前に、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のバックアップ場所を設定する

WindowsでUnified ManagerをバックアップしたあとにSnapshotコピーを格納するための

ボリュームを設定する必要があります。

開始する前に

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
 - 地理的にUnified Managerサーバに近い場所に設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クラスタ上の iSCSI 接続
 - 構成されたマシンでiSCSIプロトコルを有効にする必要があります
 - バックアップ構成には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はLUNを1つだけ配置し、それ以外は何も含めないでください。
 - LUN のサイズは、9.9 Active IQ Unified Managerで処理されると予想されるデータ サイズの 2 倍以上である必要があります。
- 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てください
 - エクスポートポリシーでスーパーユーザーアクセスが「any」に設定されていることを確認してください。
- ボリュームとLUNの要件：
 - ボリュームは、Unified Manager MySQL データ ディレクトリの少なくとも 2 倍のサイズである必要があります。
 - セキュリティスタイルはWindowsに設定する必要があります
 - ローカルスナップショットポリシーを無効にする必要があります
 - ボリュームの自動サイズ設定を有効にする必要がある
 - パフォーマンスサービスレベルは、「Extreme」など、IOPSが高くレイテンシが低いポリシーに設定する必要があります。

ONTAPクラスタの設定

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、事前にいくつかの設定手順をONTAPクラスタで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、Storage VMにiSCSI LIFとして割り当てることができるようにデータLIFを設定します。次に、System Managerユーザ インターフェイスを使用してiSCSI対応のStorage VMを設定します。このStorage VMに静的ネットワーク ルートを設定し、LIFが発信トラフィックにネットワークを使用する方法を制御する必要があります。



バックアップ設定専用のボリュームとLUNが必要です。使用するボリュームにはLUNを1つだけ配置します。LUNのサイズは、Active IQ Unified Managerでの処理が想定されるデータ サイズの2倍以上にする必要があります。

次の設定を行う必要があります。

手順

1. iSCSI対応のStorage VMを設定するか、同じ設定の既存のStorage VMを使用します。
2. 設定したStorage VMにネットワーク ルートを設定します。
3. 単一のLUNを含むボリュームを適切な容量で設定し、そのLUN専用になるようにします。



System Managerで作成されたLUNの場合、LUNのマッピングを解除するとigroupが削除されてリストアが失敗することがあります。この状況を回避するには、LUNを明示的に作成し、LUNのマッピングが解除されても削除されないようにします。

4. Storage VMにイニシエータ グループを設定します。
5. ポートセットを設定します。
6. igroupをポートセットと統合します。
7. LUNをigroupにマップします。

Windowsホスト マシンの設定

NetApp Snapshotを使用してActive IQ Unified Managerをバックアップおよびリストアする前に、Windowsホスト マシンを設定する必要があります。Windows ホスト マシンでMicrosoft iSCSI イニシエーターを起動するには、検索バーに「iscsi」と入力し、**iSCSI** イニシエーター をクリックします。

開始する前に

ホスト マシン上の以前の設定をすべて消去する必要があります。

Windowsの新規インストール時にiSCSIイニシエータを起動しようとする、確認のプロンプトが表示され、確認すると[iSCSIイニシエーターのプロパティ]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、[iSCSIイニシエーターのプロパティ]ダイアログ ボックスが開き、非アクティブまたは接続しようとしているターゲットが表示されます。そのため、Windowsホスト上の以前の設定をすべて削除する必要があります。

手順

1. ホスト マシン上の以前の設定をすべて消去します。
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. 検出された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 でスナップショットコピーの保存先を指定する

Active IQ Unified Manager Snapshotコピーのデスティネーションには、いずれかのONTAPクラスタですでに設定済みのボリュームを指定する必要があります。デスティネーションはメンテナンス コンソールを使用して定義します。

- Active IQ Unified ManagerがインストールされているWindowsホストの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. Power Shell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. コマンドを入力してください `maintenance\_console` Enter キーを押します。
4. メンテナンス コンソールの メイン メニュー で、 バックアップの復元 オプションの番号を入力します。
5. * NetAppスナップショット バックアップの構成*の番号を入力します。
6. iSCSIを設定するオプションの番号を入力します。
7. 提供する必要のある情報を確認して、「バックアップ構成の詳細を入力」の番号を入力します。
8. Snapshotを書き込むボリュームを指定するには、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の名前、ストレージ システムのユーザ名とパスワード、およびマウント ドライブを入力します。
9. この情報を確認して入力してください y。

システムで次のタスクが実行されます。

- ストレージVMが検証されました
- ボリュームが検証されました
- ドライブをマウントし、ステータスを検証します
- LUNの存在とステータス
- 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スペース（mysqlデータディレクトリの2倍以上）が存在することが検証されています
- 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との通信に使用されるiSCSIイニシエータ

10. メンテナンス コンソールを終了してActive IQ Unified Managerインターフェイスを起動し、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スナップショットコピーによるバックアップを構成する

Snapshotコピーを使用してActive IQ Unified Managerバックアップを作成するには、メンテナンス コンソールからいくつかの設定手順を実行する必要があります。

開始する前に

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 name
- マウント パス
- ストレージ システムのクレデンシャル

手順

1. Unified Managerのメンテナンス コンソールにアクセスします。
2. 4 を入力して バックアップの復元 を選択します。
3. 2 を入力して、* NetAppスナップショットを使用したバックアップと復元*を選択します。



バックアップ設定を変更する場合は、3 を入力して * NetAppスナップショット バックアップ構成の更新* を選択します。更新できるのはパスワードのみです。

4. メニューから 1 を入力して、* NetAppスナップショット バックアップの構成*を選択します。
5. 「1」と入力して必要な情報を入力します。
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ていることを確認します。

指定した情報（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）に間違いがないかがチェックされます。バックグラウンドで実行される処理は次のとおりです。

- サービスは停止しています
- データベースディレクトリは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
- サービスが再起動されます。Active Active IQ Unified Managerインターフェイスで構成が完了すると、バックアップ タイプがNetAppスナップショットに変更され、ユーザー インターフェイスにデータベース バックアップ (スナップショット ベース) として反映されます。

Snapshotが無効になる可能性があるため、バックアップ処理を開始する前にSnapshot設定に変更がないかどうかを確認する必要があります。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。そのあとにバックアップをEドライブに再設定した場合、データは新しい設定に従ってEドライブに保存されます。Gドライブに作成された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で失

敗します。

LinuxとWindowsのバックアップスケジュールを定義する

Unified Manager 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。

開始する前に

- オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。
- メンテナンス コンソールからSnapshotコピーを作成するための設定を行って、Snapshotを作成するデスティネーションを特定しておく必要があります。

Snapshotコピーは数分で作成され、Unified Managerデータベースがロックされるのは数秒だけです。



新しいクラスタを追加してから最初の15日間に作成されたバックアップについては、過去のパフォーマンス データが正確でないことがあります。

手順

1. 左側のナビゲーション ペインで、[全般] > [データベース バックアップ] 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. 保持数 フィールドに、保持するスナップショット コピーの最大数を入力します。

保持数のデフォルト値は10です。Snapshotコピーの最大数は、クラスタのONTAPソフトウェアのバージョンによって決まります。このフィールドを空白のままにすると、ONTAPのバージョンに関係なく最大値を実装できます。

4. *毎日スケジュール*または*毎週スケジュール*ボタンを選択し、スケジュールの詳細を指定します。
5. *適用*をクリックします。

スケジュールに基づいてSnapshotコピーが作成されます。使用可能なバックアップ ファイルは[データベース バックアップ]ページで確認できます。

このボリュームとSnapshotは重要であるため、次のいずれかの場合に通知を受けるように、このボリュームについて1つまたは2つのアラートを作成できます。

- ボリューム スペースの90%に達している場合。アラートを設定するには、ボリューム スペースがいっぱい イベントを使用します。

ONTAP System ManagerまたはONTAP CLIを使用してボリュームに容量を追加し、Unified Managerデータベースのスペースが不足しないようにすることができます。

- Snapshotが最大数に近づいている場合。アラートを設定するには、イベント「スナップショット コピーが多すぎます」を使用します。

ONTAP System ManagerまたはONTAP CLIを使用して古いSnapshotを削除し、新しいSnapshotコピー用の空きスペースを常に確保することができます。

アラートの設定は[アラート セットアップ]ページで行います。

スナップショットコピーを使用して**Unified Manager**を復元する

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。

開始する前に

- 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とWindowsホストマシンの管理者権限が必要です。
- Unified Managerサーバのメンテナンス コンソールへのログインが許可されているユーザIDとパスワードが必要です。

リストア機能は、プラットフォームおよびバージョンに固有の機能です。Unified Managerのバックアップは、同じバージョンのUnified Managerにのみリストアできます。

手順

1. Unified ManagerシステムのIPアドレスまたは完全修飾ドメイン名に接続します。
 - Linux: セキュアシェル
 - Windows: Power Shell
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. コマンドを入力してください `maintenance\_console` Enter キーを押します。
4. メンテナンス コンソールの メイン メニュー で、 バックアップの復元 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復元*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。* NetApp Snapshot Backup の構成* を選択するには 1 を入力し、元のシステムと同じように Snapshot コピーの設定を構成します。

6. * NetApp Snapshot を使用して復元*を選択するには、3 を入力します。
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. リストア処理が完了したら、Unified Managerユーザ インターフェイスにログインします。

バックアップをリストアしたあとにWorkflow Automationサーバが動作しなくなった場合は、次の手順を実行します。

1. Workflow Automationサーバで、Unified ManagerサーバのIPアドレスを最新のマシンを参照するように変更します。
2. 手順1で取得に失敗した場合は、Unified Managerサーバでデータベース パスワードをリセットします。

バックアップの種類を変更する

Active IQ Unified Managerシステムのバックアップ タイプを変更するには、メンテナンス コンソールのオプションを使用します。* NetAppスナップショット バックアップの構成解除* 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。

開始する前に

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. バックアップと復元を行うには、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スナップショット バックアップの構成解除* で 4 を選択します。

実行される処理が表示されます。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、サービスの再開の順に実行されます。

バックアップ方式を変更すると、バックアップ メカニズムがSnapshotコピーからデフォルトのMySQLバックアップに変更されます。この変更は、[一般設定]の[データベース バックアップ]セクションに表示されます。

Unified Managerのオンデマンド バックアップ

Active IQ Unified Managerのユーザ インターフェイスを使用して、必要なときにいつでもオンデマンド バックアップを生成することができます。オンデマンド バックアップを使用すると、既存のバックアップ方法で瞬時にバックアップを作成できます。オンデマンド バックアップでは、MySQLベースとNetApp Snapshotベースのバックアップが区別されません。

データベース バックアップ ページの 今すぐバックアップ ボタンを使用して、オンデマンド バックアップを実行できます。オンデマンド バックアップはActive IQ Unified Manager用に設定したスケジュールに依存しません。

Unified Manager仮想アプライアンスをLinuxシステムに移行する

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 MySQLデータベース ダンプ バックアップを仮想アプライアンスからRed Hat Enterprise Linuxシステムにリストアすることができます。

開始する前に

- 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。
 - 復元操作を行うには、Unified Manager メンテナンス ユーザーの名前を知っておく必要があります。
- Linuxシステム：
 - 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"](#)。
 - このサーバ上の Unified Manager のバージョンは、バックアップ ファイルを使用している仮想アプライアンスのバージョンと同じである必要があります。

- インストールが完了しても、UIを起動したり、クラスタ、ユーザ、または認証設定を設定したりしないでください。これらの情報は、リストア プロセスでバックアップ ファイルから取り込みます。
- Linuxホストのrootユーザのクレデンシャルが必要です。

ここでは、仮想アプライアンスにバックアップ ファイルを作成し、そのバックアップ ファイルをRed Hat Enterprise Linux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、[管理] > [データベース バックアップ] 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. [スケジュール] セクションで、[毎日スケジュール] を選択し、現在の時刻から数分後の時刻を入力すると、すぐにバックアップが作成されます。
5. *適用*をクリックします。
6. バックアップが生成されるまで数時間待ちます。

フル バックアップは1GBを超えることもあり、完了までに3〜4時間かかる場合があります。

7. Unified ManagerがインストールされているLinuxホストにルートユーザーとしてログインし、SCPを使用して仮想アプライアンスの/supportから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たことを確認してください。

8. コマンドプロンプトで、バックアップを復元します。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。

次のタスクを実行します。

- 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システムには/jail/supportパスはないため、バックアップ パスをLinuxシステムのデフォルトの設定 (/data/ocum-backup) が任意の新しいパスに変更します。
- Workflow Automation接続を両サイドで再設定します (WFAを使用する場合)。
- 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。

スクリプトを管理する

スクリプトを使用して、Unified Manager 内の複数のストレージ 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。イベントでアラートがトリガーされるとスクリプトが実行されます。カスタム スクリプトをアップロードし、アラートが生成されたときの動作をテストできます。

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により組織がこの機能を許可したくない場合は、ストレージ管理 > 機能設定 からこの機能を無効にすることができます。

スクリプトとアラートの連携方法

Unified Managerでイベントに対するアラートが発生したときにスクリプトが実行されるように、アラートにスクリプトを関連付けることができます。スクリプトを使用して、ストレージ オブジェクトの問題を解決したり、イベントの生成元のストレージ オブジェクトを特定したりできます。

Unified Manager でイベントのアラートが生成されると、指定された受信者にアラート メールが送信されます。アラートをスクリプトに関連付けた場合は、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のEメールで確認できます。



カスタム スクリプトを作成し、それを特定のイベント 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アクションが実行され、修正 アクションは [管理アクション] ページまたは Unified Manager ダッシュボードでデフォルトでは使用できなくなります。

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、関連するイベントの情報を収集したり、ストレージ オブジェクトを変更したりできます。

スクリプトから引数を取得する例

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

アラートが生成されると、このスクリプトが実行されて次のような出力が表示されます。

```
-eventID : 290
-eventSourceID : 4138
```

スクリプトを追加する

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。

開始する前に

- 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ているファイル形式は、Perl、Shell、PowerShell、Python、および`.bat`ファイル。

Unified Managerがインストールされているプラットフォーム	サポートされる言語
VMware	Perl / シェル スクリプト
Linux	Perl / Python / シェル スクリプト
Windows	PowerShell / Perl / Python / .batスクリプト

- Perl スクリプトの場合、Unified Manager サーバーに Perl がインストールされている必要があります。VMware環境にはPerl 5がデフォルトでインストールされ、Perl 5のサポート対象のみがスクリプトでサポートされます。Unified ManagerのあとにPerlをインストールした場合は、Unified Managerサーバを再起動する必要があります。
- PowerShellスクリプトを使用するには、スクリプトを実行するための適切なPowerShell実行ポリシーがWindowsサーバで設定されている必要があります。



スクリプトでログ ファイルを作成してアラート スクリプトの進捗を追跡する場合は、ログ ファイルがUnified Managerのインストール フォルダ内に作成されないようにする必要があります。

- アプリケーション管理者またはストレージ管理者のロールが必要です。

カスタム スクリプトをアップロードし、アラートに関するイベントの詳細を収集できます。



この機能がユーザ インターフェイスに表示されない場合は、管理者によって無効にされています。必要に応じて、ストレージ管理 > 機能設定 からこの機能を有効にできます。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > スクリプト 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。

スクリプトを削除する

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。

開始する前に

- アプリケーショ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、ストレージ管理 > スクリプト 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。

テストスクリプトの実行

ストレージ オブジェクトに対してアラートが生成されたときにスクリプトが正しく実行されるかどうかを確認することができます。

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- サポートされるファイル形式のスクリプトをUnified Managerにアップロードしておく必要があります。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > スクリプト をクリックします。
2. [スクリプト]ページで、テスト スクリプトを追加します。
3. 左側のナビゲーション ペインで、ストレージ管理 > アラート設定 をクリックします。
4. *アラート設定*ページで、次のいずれかのアクションを実行します。

目的	操作
アラートを追加する	a. *[追加]*をクリックします。 b. [操作]セクションで、テスト スクリプトにアラートを関連付けます。

目的	操作
アラートを編集する	a. アラートを選択し、[編集] をクリックします。 b. [操作]セクションで、テスト スクリプトにアラートを関連付けます。

5. *保存*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」引数で実行され、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。

グループを理解する

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、異機種ストレージ オブジェクト (クラスター、SVM、ボリューム) の動的なコレクションです。Unified Manager でグループを作成して、ストレージ オブジェクトのセットを簡単に管理できます。グループ内のメンバーは、Unified Manager によってある時点で監視されているストレージ オブジェクトに応じて変更される可能性があります。

- グループごとに一意の名前を付けます。
- 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。
- 1つのグループに複数の種類のストレージ オブジェクト (クラスター、SVM、またはボリューム) 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時点、または Unified Manager が監視サイクルを完了した時点に基づいて、グループに動的に追加されます。
- グループ内のすべてのストレージ オブジェクトに同じ処理 (ボリュームのしきい値の設定など) 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、クラスター、またはSVM) を特定のグループに追加する基準を定義したものです。グループのグループ ルール

は、条件グループまたは条件を使用して定義します。

- グループには必ずグループ ルールを関連付ける必要があります。
- グループ ルールにはオブジェクト タイプを関連付ける必要があります。関連付けることができるオブジェクト タイプは1つだけです。
- グループに対してストレージ オブジェクトが追加または削除されるのは、各監視サイクルの完了後、およびルール作成、編集、削除時です。
- グループ ルールには1つ以上の条件グループを、各条件グループには1つ以上の条件を含めることができます。
- ストレージ オブジェクトは、作成されたグループ ルールに基づいて複数のグループに属することができます。

条件

複数の条件グループを作成し、各条件グループに1つ以上の条件を含めることができます。グループのグループ ルールに定義されたすべての条件グループを適用して、グループに含めるストレージ オブジェクトを指定することができます。

条件グループに含まれる条件は論理ANDを使用して実行され、条件グループのすべての条件を満たす必要があります。条件はグループ ルールを作成または変更すると作成され、条件グループのすべての条件を満たすストレージ オブジェクトのみが適用、選択、およびグループの対象となります。グループに含めるストレージ オブジェクトの範囲を限定するには、条件グループで複数の条件を使用します。

次のオペランドと演算子を使用して必要な値を指定することで、ストレージ オブジェクトの条件を作成できます。

ストレージオブジェクトタイプ	適用可能なオペランド
Volume	• オブジェクト名 • 所有クラスタ名 • 所有SVM名 • アノテーション
SVM	• オブジェクト名 • 所有クラスタ名 • アノテーション
クラスタ	• オブジェクト名 • アノテーション

任意のストレージ オブジェクトのオペランドとして注釈を選択すると、「Is」演算子が使用可能になります。その他のすべてのオペランドについては、演算子として「Is」または「Contains」のいずれかを選択できます。

- オペランド

Unified Manager のオペランドのリストは、選択したオブジェクト タイプに基づいて変わります。リストには、Unified Manager で定義したオブジェクト名、所有クラスタ名、所有 SVM 名、注釈が含まれます。

- オペレーター

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 でサポートされている演算子は、「Is」と「Contains」です。

「Is」演算子を選択すると、選択したオペランドに指定された値とオペランド値が完全に一致するかどうか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基準を満たすかどうか評価されます。

- 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。

- Value

値のフィールドは、選択したオペランドによって変わります。

条件を使用したグループ ルールの例

ボリュームに対する条件グループで、次の2つの条件が定義されているとします。

- 名前に「vol」が含まれています
- SVM名は「data_svm」です

この条件グループは、名前に「vol」が含まれ、「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を選択します。

条件グループ

条件グループは論理ORを使用して実行され、ストレージ オブジェクトに適用されます。ストレージ オブジェクトがグループに追加されるためには、いずれかの条件グループを満たす必要があります。いずれかの条件グループを満たすすべてのストレージ オブジェクトがグループにまとめられます。条件グループを使用して、グループに含めるストレージ オブジェクトの範囲を広げることができます。

条件グループを使用したグループ ルールの例

ボリュームに対する2つの条件グループで、各グループにそれぞれ次の2つの条件が定義されているとします。

- 条件グループ1
 - 名前に「vol」が含まれています
 - SVM 名は「data_svm」です。条件グループ 1 は、名前に「vol」が含まれ、名前が「data_svm」の SVM でホストされているすべてのボリュームを選択します。
- 条件グループ2
 - 名前に「vol」が含まれています

- ・データ プライオリティの注釈値は「critical」です。条件グループ 2 は、名前に「vol」が含まれ、データ プライオリティ注釈値が「critical」として注釈されているすべてのボリュームを選択します。

これらの2つの条件グループを含むグループ ルールをストレージ オブジェクトに適用した場合、選択したグループに次のストレージ オブジェクトが追加されます。

- ・名前に「vol」が含まれ、「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」が含まれ、データ優先度注釈値「critical」が付けられているすべてのボリューム。

ストレージ オブジェクトでのグループ操作の仕組み

グループ アクションは、グループ内のすべてのストレージ オブジェクトに対して実行される操作です。たとえば、ボリュームしきい値グループ アクションを構成して、グループ内のすべてのボリュームのボリュームしきい値を同時に変更できます。

グループは、固有のグループ アクション タイプをサポートします。ボリューム ヘルスしきい値グループ アクション タイプを 1 つだけ持つグループを作成できます。ただし、同じグループに対して、異なるタイプのグループ アクション (使用可能な場合) を構成することもできます。グループ アクションのランクによって、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が決まります。ストレージ オブジェクトの詳細ページには、ストレージ オブジェクトに適用されているグループ アクションに関する情報が表示されます。

ユニークなグループアクションの例

グループ G1 および G2 に属するボリューム A があり、これらのグループに対して次のボリューム ヘルスしきい値グループ アクションが構成されているとします。

- ・`Change\_capacity\_threshold`ボリュームの容量を設定するためのランク1のグループアクション
- ・`Change\_snapshot\_copies`ボリュームのスナップショットコピーを構成するための、ランク2のグループアクション

その`Change\_capacity\_threshold`集団行動は常に`Change\_snapshot\_copies`グループアクションが実行され、ボリュームAに適用されます。Unified Managerが監視の1サイクルを完了すると、ボリュームAのヘルスしきい値関連イベントは、`Change\_capacity\_threshold`集団行動。G1 グループまたは G2 グループに対して、別のボリュームしきい値タイプのグループ アクションを構成することはできません。

グループを追加する

クラスタ、ボリューム、およびStorage Virtual Machine (SVM) を管理しやすいように、グループを作成して1つにまとめることができます。

開始する前に

アプリケーショ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、ストレージ管理 > グループ 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、グループの名前と説明を入力します。
4. *[追加]*をクリックします。

グループを編集する

Unified Managerで作成したグループの名前と説明を編集できます。

開始する前に

アプリケーショ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。既存のグループの名前は使用できません。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > グループ 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、説明、またはその両方を変更します。
4. *保存*をクリックします。

グループを削除する

不要になったグループは、Unified Managerから削除できます。

開始する前に

- 削除するグループのグループ ルールに関連付けられたストレージ オブジェクト（クラスタ、SVM、またはボリューム）がないことを確認する必要があります。
- アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > グループ 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が、マッピングは解除されます。

グループルールを追加する

グループのグループ ルールを作成して、ボリューム、クラスタ、Storage Virtual Machine (SVM) などのストレージ オブジェクトを動的にグループに追加することができます。グループ ルールを作成するには、1つ以上の条件を含む条件グループを少なくとも1つ設定する必要があります。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

監視中のストレージ オブジェクトは、グループ ルールを作成後すぐにグループに追加されます。新しいオブジェクトは、監視サイクルの完了後にグループに追加されます。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > グループ 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な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。

作成するには....	操作
条件	a. オペランドのリストからオペランドを選択します。 b. 演算子として「含む」または「である」のいずれかを選択します。 c. 値を入力するか、使用可能な値のリストから選択します。
条件グループ	a. *条件グループを追加*をクリックします b. オペランドのリストからオペランドを選択します。 c. 演算子として「含む」または「である」のいずれかを選択します。 d. 値を入力するか、使用可能な値のリストから選択します。 e. 必要に応じて「条件を追加」をクリックしてさらに条件を作成し、条件ごとに手順 a ～ d を繰り返します。

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 ルールを作成し、条件の設定と条件グループの追加を行うには、[グループ 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. 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「含む」を選択します。
6. 値を入力してください `svm_data`。
7. *条件グループを追加*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「含む」を選択します。
10. 値を入力してください `vol`。
11. *条件を追加*をクリックします。
12. 手順 8 でオペランドとして **data-priority** を選択し、手順 9 で演算子として **Is** を選択し、手順 10 で値として **critical** を選択して、手順 8 ～ 10 を繰り返します。
13. グループ ルールの条件を作成するには、[追加] をクリックします。

グループルールを編集する

グループ ルールを編集して条件グループと条件グループ内の条件を変更し、特定のグループに対してストレージ オブジェクトを追加または削除することができます。

開始する前に

アプリケーショ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 > グループ 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. グループ ルールの編集 ダイアログ ボックスで、必要に応じてグループ ルール名、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*をクリックします。

グループルールを削除する

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。

開始する前に

アプリケーショ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、ストレージ管理 > グループ 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。

グループアクションを追加する

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、そ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。

開始する前に

アプリケーショ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 > グループ 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 ダイアログボックスで、アクションの名前と説明を入力します。
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、選択した操作タイプの必須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。

グループアクションを編集する

グループ操作の名前、説明、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。

開始する前に

アプリケーショ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 > グループ 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 ダイアログ ボックスで、必要に応じて、グループ アクション名、説明、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変更します。
4. *保存*をクリックします。

グループのボリューム健全性しきい値を構成する

ボリュームの容量、Snapshotコピー、qtreeクォータ、増加率、およびinodeについて、グループレベルで健全性しきい値を設定することができます。

開始する前に

アプリケーショ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、ストレージ管理 > グループ 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 アクションを構成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「アクション タイプ」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。

グループアクションを削除する

不要になったグループ操作は、Unified Managerから削除できます。

開始する前に

アプリケーショ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、そのグループのストレージ オブジェクトにグローバルしきい値が適用されます。ストレージ オブジェクトに対して設定されたオブジェクトレベルの健全性しきい値には影響はありません。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > グループ 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。

グループアクションの順序を変更する

グループ操作をグループ内のストレージ オブジェクトに適用する順序を変更することができます。グループ操作は、ランクに基づいてストレージ オブジェクトに順番に適用されます。グループ操作には、設定した時点では最も低いランクが割り当てられます。要件に応じてグループ操作のランクを変更することができます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

単一の行または複数の行を選択し、ドラッグ アンド ドロップ操作を繰り返し行って、グループ操作のランクを変更することができます。ただし、変更後の優先順序は変更を保存するまでグループ操作のグリッドに反映されません。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > グループ をクリックします。
2. *グループアクション*タブで、*並べ替え*をクリックします。
3. グループ アクションの順序変更 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、必要に応じてグループ アクションの順序を並べ替えます。
4. *保存*をクリックします。

アノテーションを使用してストレージ オブジェクト イベントを優先順位付けする

アノテーション ルールを作成してストレージ オブジェクトに適用すると、適用されたアノテーションのタイプとその優先順位に基づいてオブジェクトを識別し、フィルタリングできるようになります。

注釈についてさらに詳しく

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

アノテーションとは、あるテキスト文字列（名前）と別のテキスト文字列（値）の組み合わせです。各注釈の名前と値のペアは、注釈ルールを使用してストレージ オブジェクトに動的に関連付けることができます。事前定義されたアノテーションにストレージ オブジェクトを関連付けると、そのアノテーションに関連するイベントをフィルタリングして表示できます。アノテーションは、クラスタ、ボリューム、およびStorage Virtual Machine (SVM) に適用できます。

アノテーションの名前には、それぞれ複数の値を割り当てることが可能です。それらの名前と値の各ペアをルールに基づいてストレージ オブジェクトに関連付けることができます。

たとえば、「data-center」という名前の注釈を作成し、その値を「Boston」と「Canada」にすることができます。次に、値「Boston」を持つ注釈「data-center」をボリューム v1 に適用できます。「data-center」という注釈が付けられたボリューム v1 上のイベントに対してアラートが生成されると、生成された電子メールにはボリュームの場所「Boston」が示され、これにより、問題を優先順位付けして解決できるようになります。

Unified Managerでのアノテーション ルールの仕組み

注釈ルールは、ストレージ オブジェクト (ボリューム、クラスター、またはストレージ 仮想マシン (SVM)) に注釈を付けるために定義する基準です。アノテーション ルールは、条件グループまたは条件のいずれかを使用して定義できます。

- アノテーションには必ずアノテーション ルールを関連付ける必要があります。
- アノテーション ルールにはオブジェクト タイプを関連付ける必要があります。関連付けることができるオブジェクト タイプは1つだけです。
- Unified Manager は、各監視サイクルの後、またはルールが作成、編集、削除、または並べ替えられたと

きに、ストレージ オブジェクトに注釈を追加または削除します。

- アノテーション ルールには1つ以上の条件グループを、各条件グループには1つ以上の条件を含めることができます。
- ストレージ オブジェクトには複数のアノテーションを適用できます。特定のアノテーションに対するアノテーション ルールの条件で別のアノテーションを使用して、すでにアノテートされているオブジェクトに別のアノテーションを追加することもできます。

条件

複数の条件グループを作成し、各条件グループに1つ以上の条件を含めることができます。アノテーションのアノテーション ルールに定義されたすべての条件グループを適用して、ストレージ オブジェクトをアノテートすることができます。

条件グループに含まれる条件は論理ANDを使用して実行され、条件グループのすべての条件を満たす必要があります。条件はアノテーション ルールを作成または変更すると作成され、条件グループのすべての条件を満たすストレージ オブジェクトのみが適用、選択、およびアノテートの対象となります。アノテートするストレージ オブジェクトの範囲を限定するには、条件グループで複数の条件を使用します。

次のオペランドと演算子を使用して必要な値を指定することで、ストレージ オブジェクトの条件を作成できます。

ストレージオブジェクトタイプ	適用可能なオペランド
Volume	• オブジェクト名 • 所有クラスタ名 • 所有SVM名 • アノテーション
SVM	• オブジェクト名 • 所有クラスタ名 • アノテーション
クラスタ	• オブジェクト名 • アノテーション

任意のストレージ オブジェクトのオペランドとして注釈を選択すると、「Is」演算子が使用可能になります。その他のすべてのオペランドについては、演算子として「Is」または「Contains」のいずれかを選択できます。「Is」演算子を選択すると、オペランド値と選択したオペランドに指定された値が完全に一致するかどうか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基準を満たすかどうか評価されます。

- 選択したオペランドの値が指定した値と完全に一致する。
- 選択したオペランドの値に指定した値が含まれる。

条件を使用したアノテーション ルールの例

ボリュームに対して条件グループが1つ設定されたアノテーション ルールで、次の2つの条件が定義されているとします。

- 名前に「vol」が含まれています
- SVM名は「data_svm」です

この注釈ルールは、名前に「vol」が含まれ、「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に、選択した注釈と注釈タイプを注釈付けします。

条件グループ

条件グループは論理ORを使用して実行され、ストレージ オブジェクトに適用されます。ストレージ オブジェクトがアノテートされるためには、いずれかの条件グループの要件を満たす必要があります。いずれかの条件グループの条件を満たすすべてのストレージ オブジェクトがアノテートされます。条件グループを使用して、アノテートするストレージ オブジェクトの範囲を広げることができます。

条件グループを使用したアノテーション ルールの例

ボリュームに対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、各グループにそれぞれ次の2つの条件が定義されているとします。

- 条件グループ1
 - 名前に「vol」が含まれています
 - SVM 名は「data_svm」です。この条件グループは、名前に「vol」が含まれ、名前が「data_svm」の SVM でホストされているすべてのボリュームに注釈を付けます。
- 条件グループ2
 - 名前に「vol」が含まれています
 - データ プライオリティの注釈値は「critical」です。この条件グループは、名前に「vol」が含まれ、データ プライオリティ注釈値が「critical」として注釈付けされているすべてのボリュームに注釈を付けます。

これらの2つの条件グループを含むアノテーション ルールをストレージ オブジェクトに適用した場合、次のストレージ オブジェクトがアノテートされます。

- 名前に「vol」が含まれ、「data_svm」という名前で SVM にホストされているすべてのボリューム。
- 名前に「vol」が含まれ、データ優先度注釈値が「critical」として注釈付け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、low という値を持つ定義済みの注釈です。これらの値を使用して、格納されているデータの優先度に基づいて、ストレージ オブジェクトをアノテートすることができます。事前定義されたアノテーションの値を編集または削除することはできません。

- データ優先度: ミッションクリティカル

このアノテーションは、ミッション クリティカルなデータが格納されたストレージ オブジェクトに適用されます。たとえば、本番用アプリケーションを含むオブジェクトなどが考えられます。

- データ優先度:高

このアノテーションは、優先度の高いデータが格納されたストレージ オブジェクトに適用されます。たとえば、ビジネス アプリケーションをホストしているオブジェクトなどが考えられます。

- データ優先度:低

このアノテーションは、優先度の低いデータが格納されたストレージ オブジェクトに適用されます。たとえば、バックアップやミラーのデスティネーションなど、セカンダリ ストレージにあるオブジェクトなどが考えられます。

動的に注釈を追加する

Unified Managerでカスタム アノテーションを作成すると、クラスタ、Storage Virtual Machine (SVM)、およびボリュームがルールに基づいてアノテーションに動的に関連付けられます。ルールにより、ストレージ オブジェクトにアノテーションが自動的に割り当てられます。

開始する前に

アプリケーショ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 > 注釈 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 ダイアログボックスで、注釈の名前と説明を入力します。
4. オプション: *注釈値*セクションで、*追加*をクリックして注釈に値を追加します。
5. *保存*をクリックします。

注釈に値を追加する

アノテーションに値を追加し、その後、アノテーションの名前と値の特定のペアにストレージ オブジェクトを関連付けることができます。アノテーションに値を追加することで、より効率的にストレージ オブジェクトを管理できるようになります。

開始する前に

アプリケーショ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値を追加することはできません。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > 注釈 をクリックします。
2. *注釈*ページで、値を追加する注釈を選択し、*値*セクションで*追加*をクリックします。
3. 注釈値の追加 ダイアログボックスで、注釈の値を指定します。

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。

注釈を削除する

不要になったカスタム アノテーションとその値を削除できます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- アノテーションの値が他のアノテーションやグループ ルールで使用されていないことを確認する必要があります。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > 注釈 をクリックします。
2. *注釈*タブで、削除する注釈を選択します。

選択したアノテーションの詳細が表示されます。

3. 選択した注釈とその値を削除するには、[アクション] > [削除] 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。

注釈リストと詳細を表示する

クラスタ、ボリューム、およびStorage Virtual Machine (SVM) に動的に関連付けられるアノテーションのリストを確認することができます。説明、作成者、作成日、値、ルール、オブジェクトなど、アノテーションに関連する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、ストレージ管理 > 注釈 をクリックします。
2. *注釈*タブで注釈名をクリックすると、関連する詳細が表示されます。

注釈から値を削除する

カスタム アノテーションに関連付けられている値がそのアノテーションに当てはまらなくなった場合は、値を削除することができます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- アノテーションの値がアノテーション ルールやグループ ルールに関連付けられていないことを確認する必要があります。

事前定義されたアノテーションから値を削除することはできません。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > 注釈 をクリックします。

2. *注釈*タブの注釈リストで、値を削除する注釈を選択します。
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*ダイアログボックスで*はい*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。

注釈ルールを作成する

Unified Managerがボリューム、クラスタ、Storage Virtual Machine (SVM) などのストレージ オブジェクトを動的にアノテートするために使用するアノテーション ルールを作成できます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

監視中のストレージ オブジェクトは、アノテーション ルールの作成後すぐにアノテートされます。新しいオブジェクトは、監視サイクルの完了後にアノテートされます。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > 注釈 をクリックします。
2. *注釈ルール*タブで*追加*をクリックします。
3. 注釈ルールの追加 ダイアログボックスで、注釈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、注釈を付けるストレージ オブジェクトのタイプを選択します。
5. *注釈の適用*フィールドで、使用する注釈と注釈値を選択します。
6. [条件]セクションで、該当する操作を実行して条件、条件グループ、またはその両方を作成します。

作成するには...	操作
条件	a. オペランドのリストからオペランドを選択します。 b. 演算子として「含む」または「である」のいずれかを選択します。 c. 値を入力するか、使用可能な値のリストから選択します。

作成するには...	操作
条件グループ	a. *条件グループの追加*をクリックします。 b. オペランドのリストからオペランドを選択します。 c. 演算子として「含む」または「である」のいずれかを選択します。 d. 値を入力するか、使用可能な値のリストから選択します。 e. 必要に応じて「条件を追加」をクリックしてさらに条件を作成し、条件ごとに手順 a ～ d を繰り返します。

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を行うには、[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「含む」を選択します。
6. 値を入力してください `svm_data`。
7. *条件グループを追加*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「含む」を選択します。
10. 値を入力してください `vol`。
11. *条件を追加*をクリックします。
12. 手順 8 でオペランドとして **data-priority** を選択し、手順 9 で演算子として **Is** を選択し、手順 10 で値として **mission-critical** を選択して、手順 8 ～ 10 を繰り返します。
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に手動で注釈を追加する

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、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、必要なアノテーションの名前と値のペアを指定できます。

開始する前に

アプリケーショ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。

注釈を追加するには...	操作
クラスタ	a. ストレージ > *クラスター*をクリックします。 b. 1つ以上のクラスタを選択します。
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 > *SVM*をクリックします。 b. 1つ以上のSVMを選択します。

2. *注釈*をクリックし、名前と値のペアを選択します。
3. *適用*をクリックします。

注釈ルールを編集する

アノテーション ルールを編集して条件グループおよび条件グループに含まれる条件を変更することで、ストレージ オブジェクトに対してアノテーションを追加または削除できます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

関連するアノテーション ルールを編集すると、ストレージ オブジェクトへのアノテーションの関連付けが解除されます。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > 注釈 をクリックします。
2. 注釈ルール*タブで、編集する注釈ルールを選択し、*アクション > *編集*をクリックします。
3. 注釈ルールの編集 ダイアログ ボックスで、必要に応じてルール名、注釈名と値、条件グループ、条件を変更します。

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*をクリックします。

注釈ルールの条件を設定する

1つ以上の条件を設定して、Unified Managerがストレージ オブジェクトに対して適用す

るアノテーション ルールを作成できます。アノテーション ルールに一致するストレージ オブジェクトに、ルールで指定した値がアノテートされます。

開始する前に

アプリケーショ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 > 注釈 をクリックします。
2. *注釈ルール*タブで*追加*をクリックします。
3. 注釈ルールの追加 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]リストからいずれかのオブジェクト タイプを選択し、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 セクションで、リストからオペランドと演算子を選択し、条件値を入力するか、条件の追加 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

オブジェクト名に「svm_data」が含まれるオブジェクト タイプ SVM の条件を考えてみましょう。

条件を設定するには、[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 フィールドで、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「含む」を選択します。
6. 値を入力してください svm_data。
7. *[追加]*をクリックします。

注釈ルールを削除する

不要になったアノテーション ルールは、Active IQ Unified Managerから削除できます。

開始する前に

アプリケーショ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、ストレージ管理 > 注釈 をクリックします。
2. *注釈ルール*タブで、削除する注釈ルールを選択し、*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。

注釈ルールの並べ替え

Unified Managerで、アノテーション ルールをストレージ オブジェクトに適用する順序を変更することができます。アノテーション ルールは、ランクに基づいてストレージ オブジェクトに順番に適用されます。アノテーション ルールには、設定した時点では最も低いランクが割り当てられます。ただし、要件に応じてアノテーション ルールのランクを変更することができます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

単一の行または複数の行を選択し、ドラッグ アンド ドロップ操作を繰り返し行って、アノテーション ルールのランクを変更することができます。ただし、変更後の優先順序は変更を保存するまで[アノテーション ルール]タブに表示されません。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > 注釈 をクリックします。
2. *注釈ルール*タブで、*並べ替え*をクリックします。
3. 注釈ルールの順序変更 ダイアログ ボックスで、1 行または複数の行をドラッグ アンド ドロップして、注釈ルールの順序を並べ替えます。
4. *保存*をクリックします。

変更後の順序は表示するには、変更内容を保存する必要があります。

Web UI とメンテナンス コンソールからサポート バンドルを送信する

サポート バンドルの送信が必要となるのは、問題についてAutoSupportメッセージよりも詳しい診断とトラブルシューティングが必要な場合です。Unified Manager Web UIおよびメンテナンス コンソールを使用して、サポート バンドルをテクニカル サポートに送信できます。

Unified Managerは、完全なサポート バンドルを最大2つ、軽量のサポート バンドルを3つ保存します。

関連情報

["Unified Managerのユーザ ロールと機能"](#)

AutoSupportメッセージとサポート バンドルをテクニカル サポートに送信する

[AutoSupport]ページでは、定期的またはオンデマンドでAutoSupportメッセージをテクニカル サポート チームに送信することができます。サポート チームは、受け取った情報に基づいて、環境を正しく運用したり、環境の整合性を維持する手助けをすることができます。AutoSupportはデフォルトで有効になっており、NetApp Active IQのメリットを活用するためには有効にしておく必要があります。

Unified Managerサーバに関するシステム診断情報と詳細なデータを必要に応じてメッセージで送信したり、メッセージを定期的に送信するようにスケジュールしたり、さらにはサポート 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 サーバの設定」セクションの説明に従ってHTTP設定を設定したりできるのは、管理者またはメンテナンス ユーザだけです。HTTPプロキシ サーバを使用する必要がある環境では、ストレージ管理者がオンデマンドのAutoSupportメッセージとサポート バンドルをテクニカル サポートに送信する前に設定を完了しておく必要があります。

オンデマンドの**AutoSupport**メッセージを送信する

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、オンデマンド メッセージを生成して送信できます。

手順

1. *[一般] > * [AutoSupport]*に移動し、次のいずれかまたは両方のアクションを実行します。
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*をクリックします。
5. * AutoSupport の生成と送信*をクリックします。

定期的な**AutoSupport**を有効にする

問題の診断と解決のために、事前定義された特定のメッセージを定期的にテクニカル サポートに送信することができます。この機能は、デフォルトで有効に設定されています。無効になっている場合、管理者またはメンテナンス ユーザが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AutoSupport」セクションで、「 AutoSupportデータをActive IQに定期的に送信する」チェックボックスをオンにします。
3. 必要に応じて、「HTTPプロキシ サーバの設定」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*をクリックします。

オンデマンドサポートバンドルをアップロードする

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。

一部のタイプのサポート データは、クラスタ リソースを大量に使用したり、完了までに時間がかかるため、完全なサポート バンドルを選択した場合は、どのデータ タイプをバンドルに含めるか、または含めないかを指定してサポート バンドルのサイズを削減できます。30日分のログと構成データベース レコードのみを含む

軽量のサポート バンドル（パフォーマンス データ、取得記録ファイル、サーバ ヒープ ダンプは含まれない）を作成することもできます。

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. ライト 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、[ライト 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. あるいは、完全なサポート バンドルを送信するには、[完全なサポート バンドルを生成する] チェック ボックスをオンにします。それぞれのデータ タイプについて、サポート バンドルに含めるか除外するかを選択します。



データ タイプを1つも選択しなかった場合も、その他のUnified Managerデータを含むサポート 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、[バンドルをテクニカル サポートに送信する] チェック ボックスをオンにします。このチェック ボックスをオフにすると、バンドルが生成されてUnified Managerサーバのローカルに格納されます。生成されたサポートバンドルは、VMwareシステム の/supportディレクトリで後から使用できます。 /opt/netapp/data/support/ Linuxシステムでは、ProgramData\NetApp\OnCommandAppData\ocum\support Windows システムの場合。
6. *送信*をクリックします。

HTTPプロキシサーバーを設定する

Unified Managerサーバからサポートに直接アクセスできない環境では、AutoSupportのコンテンツをサポート に送信するためのインターネット アクセスを提供するプロキシを指定できます。このセクションは、管理者 およびメンテナンス ユーザのみが使用できます。

• HTTPプロキシを使用する

HTTPプロキシとして使用するサーバを識別するには、このチェック ボックスをオンにします。

プロキシ サーバのホスト名またはIPアドレス、およびサーバへの接続に使用するポート番号を入力します。

• 認証を使用する

HTTPプロキシとして使用するサーバにアクセスするための認証情報を提供する場合がある場合は、この チェック ボックスをオンにします。

HTTPプロキシでの認証に必要なユーザ名とパスワードを入力します。



ベーシック認証のみ提供するHTTPプロキシはサポートされていません。

メンテナンス コンソールへのアクセス

Unified Managerユーザ インターフェイスが動作状態でない場合、またはこのユーザ インターフェイスにない機能を実行する必要がある場合は、メンテナンス コンソールにア

クセスしてUnified Managerシステムを管理できます。

開始する前に

Unified Managerをインストールして設定しておく必要があります。

15分間操作しないと、メンテナンス コンソールからログアウトされます。



VMwareにインストールした場合、VMwareコンソールからメンテナンス ユーザとしてすでにログインしているときは、Secure Shellを使用して同時にログインできません。

手順

1. 次の手順に従ってメンテナンス コンソールにアクセスします。

このオペレーティング システムでは...	次の手順に従ってください...
VMware	a. Secure Shellを使用して、Unified Manager仮想アプライアンスのIPアドレスまたは完全修飾ドメイン名に接続します。 b. メンテナンス ユーザ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。
Linux	a. Secure Shellを使用して、Unified ManagerシステムのIPアドレスまたは完全修飾ドメイン名に接続します。 b. メンテナンス ユーザ (umadmin) の名前とパスワードでシステムにログインします。 c. コマンドを入力してください `maintenance_console` Enter キーを押します。
Windows	a. 管理者のクレデンシャルでUnified Managerシステムにログインします。 b. Windows管理者としてPowerShellを起動します。 c. コマンドを入力してください `maintenance_console` Enter キーを押します。

Unified Managerメンテナンス コンソール メニューが表示されます。

サポートバンドルを生成してアップロードする

トラブルシューティングのサポートを受ける際に、診断情報を含むサポート バンドルを生成し、テクニカル サポートに送信することができます。

Unified Manager 9.8以降では、Unified Managerサーバがインターネットに接続されていれば、メンテナンス コンソールからNetApp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。

開始する前に

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、クラスタ リソースを大量に使用したり、完了までに時間がかかるため、完全なサポート バンドルを選択した場合は、どのデータ タイプをバンドルに含めるか、または含めないかを指定してサポート バンドルのサイズを削減できます。30日分のログと構成データベース レコードのみを含む軽量なサポート バンドル（パフォーマンス データ、取得記録ファイル、サーバ ヒープ ダンプは含まれない）を作成することもできます。

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。

手順

1. メンテナンス コンソールの 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レベルに応じて、「ライト サポート バンドルの生成」または「サポート バンドルの生成」を選択します。
3. 完全なサポート バンドルを選択した場合は、次のデータ タイプを選択または選択解除してサポート バンドルに含めるか除外するかを指定します。

- 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

主要なUnified Managerサーバ プロセスの状態のSnapshot。このオプションはデフォルトでは無効になっており、カスタマー サポートから要求された場合にのみ選択します。

- 取得記録

Unified Managerと監視対象クラスタの間の全通信の記録。



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. タイプ `g`を入力し、Enter キーを押してサポート バンドルを生成します。

サポート バンドルの生成ではメモリが大量に消費されるため、この時点でサポート バンドルを生成するかどうかを確認するプロンプトが表示されます。

5. タイプ `y`を入力し、Enter キーを押してサポート バンドルを生成します。

現時点でサポートバンドルを生成したくない場合は、次のように入力します。`n`と入力し、Enter キーを押します。

6. 完全なサポート バンドルにデータベース ダンプ ファイルを含めるように指定した場合は、パフォーマンス統計の対象期間を指定するためのプロンプトが表示されます。パフォーマンス統計の取り込みには多くの時間とスペースが必要になることがあるため、取り込ま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。

例えば、次のように入力します `20210101` 2021年1月1日現在。入力 `n` パフォーマンス統計を含めない場合は、

- 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から10まで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、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。タイプ `y` と入力し、Enter キーを押します。

サポート ケース番号を入力するように求められます。

- 8. ケース番号がすでにある場合は、その番号を入力してEnterキーを押します。それ以外の場合は、そのまま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何らかの理由でサポート バンドルをアップロードできない場合は、手動で取得して送信できます。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、リモート デスクトップ (RDP) を使用してサポート バンドルを取得することができます。

生成されたサポート バンドルは、VMwareシステムの場合は/supportディレクトリ、Linuxシステムの場合は/opt/netapp/data/support/、Windowsシステムの場合はProgramData\NetApp\OnCommandAppData\ocum\supportに格納されます。

関連情報

"Unified Managerのユーザ ロールと機能"

Windows クライアントを使用してサポート バンドルを取得する

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。このサポート バンドルをテクニカル サポートに送信して、問題の詳しい診断を受けることができます。使用可能なツールには、FilezillaやWinSCPなどがあります。

開始する前に

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、既存のサポート バンドルをすべて確認できます。

4. サポート バンドルのコピー先となるディレクトリを選択します。
5. コピーするサポート バンドルを選択し、ツールを使用してUnified Managerサーバからローカル システムにファイルをコピーします。

UNIX または **Linux** クライアントを使用してサポート バンドルを取得します。

UNIXまたはLinuxを使用している場合は、Linuxクライアント サーバでコマンドライン インターフェイス（CLI）を使用して、vAppからサポート バンドルを取得することができます。サポート バンドルの取得には、SCPまたはSFTPを使用します。

開始する前に

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きます。

手順

1. Linuxクライアント サーバを使用して、Telnetまたはコンソール経由でCLIにアクセスします。
2. アクセス`support`ディレクトリ。
3. 次のコマンドを使用して、サポート バンドルを取得してローカル ディレクトリにコピーします。

...を使用している場合	使用するコマンド
SCP	<code>scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>
SFTP	<code>sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>

サポート バンドルの名前は、メンテナンス コンソールを使用してサポート バンドルを生成するときに自動的に付けられます。

4. maintenanceユーザのパスワードを入力します。

例

次の例では、SCPを使用してサポート バンドルを取得します。

```
`$ scp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
support_bundle_20160216_145359.7z   100%  119MB  11.9MB/s   00:10
```

次の例では、SFTPを使用してサポート バンドルを取得します。


```
`$ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

サポートバンドルをテクニカルサポートに送信する

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である場合は、テクニカル サポートにサポート バンドルを送信します。

開始する前に

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サポート サイトにログインします。
2. ファイルをアップロードします。

["How to upload a file to NetApp"](#)

複数のワークフローに関連するタスクと情報

Unified Managerの多くのワークフローに、共通のタスク、およびワークフローの理解と実行に役立つ共通の参照情報があります。たとえば、イベントに関するメモの追加と確認、イベントの割り当て、イベントへの応答と解決などのタスクや、ボリューム、Storage Virtual Machine (SVM)、アグリゲートに関する詳細情報などです。

クラスタ コンポーネントとその競合要因

クラスタ コンポーネントの競合の原因となるクラスタのパフォーマンスの問題を特定することができます。コンポーネントを使用するワークロードのパフォーマンスが低下し、クライアント要求に対する応答時間 (遅延) が長くなり、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、犠牲者と呼ばれる他のクラスター コンポーネントとワークロードのパフォーマンスのレイテンシが増加する可能性があります。コンポーネントの競合状態を解消するには、ワークロードを減らすか処理能力を高めることでパフォーマンスを通常のレベルまで戻す必要があります。Unified Managerでは、ワークロード パフォーマンスの収集と分析が5分間隔で行われるため、クラスタ コンポーネントの利用率が高い状態が長時間続いたときにのみ検出されます。利用率が高い状態が5分間のうちの短時間しか続かないような一時的な利用率の急増は検出されません。

ストレージ アグリゲートが競合状態になる原因としては、たとえば、1つ以上のワークロードがそれぞれのI/O要求に対応するために競合する場合などがあります。アグリゲートの他のワークロードに影響し、それらのワークロードのパフォーマンスが低下する可能性があります。アグリゲートのアクティビティを減らす方法はいくつかありますが、たとえば、1つ以上のワークロードを負荷の低いアグリゲートまたはノードに移動し、現在のアグリゲートに対する全体的なワークロードの負荷を低くするなどの方法が効果的です。QoSポリシー グループの場合は、スループット制限を調整したりワークロードを別のポリシー グループに移動したりすることで、ワークロードが抑制されないようにすることができます。

Unified Manager は次のクラスタ コンポーネントを監視し、競合が発生したときに警告を発します。

- ネットワーク

クラスター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。待機時間は、クラスターが I/O 要求に応答する前に、「転送準備完了」トランザクションが完了するのを待機するために費やされる時間です。ネットワーク コンポーネントが競合状態にある場合、ブロック プロトコル レイヤでの長い待機時間は、1つ以上のワークロードのレイテンシに影響していることを意味します。

- ネットワーク処理

プロトコル レイヤとクラスタ間のI/O処理に関与する、クラスタ内のソフトウェア コンポーネントを表します。イベントが検出されてから、ネットワーク処理を実行するノードが変更されている可能性があります。ネットワーク処理コンポーネントが競合状態にある場合、ネットワーク処理ノードでの高利用率は、1つ以上のワークロードのレイテンシに影響していることを意味します。

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、ネットワーク処理のレイテンシの値が両方のノードについて表示され、ノードで負荷を適切に共有していることを確認できます。

- QoS 制限最大値

ワークロードに割り当てられたストレージQoSポリシー グループの最大スループット（ピーク）設定を表します。ポリシー グループ コンポーネントが競合状態にある場合、ポリシー グループ内のすべてのワークロードに、スループットの制限によってスロットルが適用され、1つ以上のワークロードのレイテンシに影響していることを意味します。

- QoS 制限の最小値

他のワークロードに割り当てられた QoS スループットの最小（予想）設定によって発生するワークロードの遅延を表します。特定のワークロードに設定された QoS の最小値が、約束されたスループットを保証するために帯域幅の大部分を使用する場合、他のワークロードは調整され、より多くの遅延が発生します。

- クラスター相互接続

クラスタ ノードを物理的に接続するケーブルとアダプタを表します。クラスタ インターコネクト コンポーネントが競合状態にある場合は、クラスタ インターコネクトでのI/O要求の長い待機時間がワークロードのレイテンシに影響していることを意味します。

- Data Processing

クラスタとストレージ アグリゲート間でワークロードを含むI/O処理に関与する、クラスタ内のソフトウェア コンポーネントを表します。イベントが検出されてから、データ処理を実行するノードが変更されている可能性があります。データ処理コンポーネントが競合状態にある場合、データ処理ノードでの高利用率は、1つ以上のワークロードのレイテンシに影響していることを意味します。

- ボリュームアクティベーション

すべてのアクティブ ボリュームの使用状況を追跡するプロセスです。1,000 を超えるボリュームがアクティブな大規模環境では、このプロセスは、ノードを介してリソースに同時にアクセスする必要の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最大しきい値を超えると、ここで特定されているように、重要でないボリュームの一部で遅延が発生します。

- * MetroClusterリソース*

NVRAMとインタースイッチ リンク (ISL) を含むMetroClusterリソースを表します。MetroCluster構成のクラスタ間でデータをミラーリングするのに使用します。MetroClusterコンポーネントが競合状態にある場合は、ローカル クラスタのワークロードによる大量の書き込みスループットまたはリンクの不具合が、ローカル クラスタの1つ以上のワークロードのレイテンシに影響していることを意味します。クラスタがMetroCluster構成に含まれていない場合は、このアイコンは表示されません。

- アグリゲートまたは **SSD** アグリゲート オペレーション

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。「SSD アグリゲート」は、すべて SSD (オールフラッシュ アグリゲート) で構成されるか、SSD とクラウド層 (FabricPoolアグリゲート) の組み合わせで構成されます。

- クラウドレイテンシ

クラスタとユーザ データ格納先のクラウド階層の間のI/O処理に関与する、クラスタ内のソフトウェア コンポーネントを表します。クラウド レイテンシ コンポーネントが競合状態にある場合、クラウド階層でホストされたボリュームからの大量の読み取りが1つ以上のワークロードのレイテンシに影響していることを意味します。

- SnapMirrorを同期

SnapMirror同期関係でプライマリ ボリュームからセカンダリ ボリュームにユーザー データを複製する際に関与するクラスター内のソフトウェア 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している場合は、 SnapMirror同期操作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を与えていることを意味します。

[ボリューム / 健全性の詳細]ページ

[ボリューム / 健全性の詳細]ページでは、選択したボリュームについて、容量、ストレージ効率、設定、保護、アノテーション、生成されたイベントなどの情報を確認できます。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る

[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。

- 守る

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。

- アボート

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。

- 静止

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。

- 解除

ソース ボリュームとデスティネーション ボリュームの間の関係を解除し、デスティネーションを読み書き可能ボリュームに変更します。

- 削除

選択したソースとデスティネーションの間の関係を完全に削除します。ボリュームが破棄されるわけではなく、ボリューム上のSnapshotコピーは削除されません。この処理を元に戻すことはできません。

- 再開

休止中の関係のスケジュールによる転送を有効にします。スケジュールされた次回の転送時、再開チェックポイントがある場合はそこから再開されます。

- 再同期

以前に解除した関係を再同期できます。

- 初期化 / 更新

新しい保護関係の場合は最初のベースライン転送を実行し、すでに初期化された関係の場合は手動更新を実行できます。

- 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、"[\[ボリューム / 健全性の詳細\]](#)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。

- 巻数を見る

「ヘルス: すべてのボリューム」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。

- 物理容量

ボリュームの物理容量の詳細：

- Snapshot オーバーフロー

Snapshotコピーで使用されているデータ スペースが表示されます。

- 使用済み

ボリュームでデータに使用されているスペースが表示されます。

- 警告

ボリュームのスペースがほぼフルであることを示します。このしきい値を超えると、「スペースがほぼフル」イベントが生成されます。

- エラー

ボリュームのスペースがフルであることを示します。このしきい値を超えると、「スペースがフル」イベントが生成されます。

- 使用不可

「シンプロビジョニング ボリュームにスペース リスクあり」イベントが生成され、シンプロビジョニング ボリュームのスペースがアグリゲートの容量の問題が原因で確保できないことを示します。使用不可の容量は、シンプロビジョニング ボリュームの場合のみ表示されます。

- [データ]グラフ

ボリュームの合計データ容量と使用済みデータ容量が表示されます。

自動拡張が有効になっている場合は、アグリゲートの使用可能なスペースも表示されます。このグラフには、ボリュームのデータに使用できる実質的なストレージ スペースとして、次のいずれかが表示されます。

- 次の場合は実際のデータ容量：
 - 自動拡張が無効になっている。
 - ボリュームで自動拡張が有効になっており、最大サイズに達している。
 - シックプロビジョニング ボリュームで自動拡張が有効になっており、それ以上拡張できない。
- 最大ボリューム サイズを考慮したボリュームのデータ容量（シンプロビジョニング ボリュームおよびシックプロビジョニング ボリュームでボリュームの最大サイズに対応するスペースがアグリゲートにある場合）
- 次回の自動拡張のサイズを考慮したボリュームのデータ容量（シックプロビジョニング ボリュームで自動拡張の割合のしきい値に対応できる場合）

- [Snapshot コピー]グラフ

このグラフは、Snapshot使用容量またはSnapshotリザーブが0でない場合にのみ表示されます。

どちらのグラフにも、Snapshot使用容量がSnapshotリザーブを超えている場合には超過分の使用容量が表示されます。

- 論理容量

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の場合は、「該当なし」と表示されます。

- 使用済み

ボリュームでデータに使用されている論理スペースの量と合計データ容量に対する使用済みの論理ス

ペースの割合が表示されます。

- 論理スペースの適用

シンプロビジョニング ボリュームに対して論理スペースの適用が設定されているかどうかが表示されます。[有効]に設定されている場合、ボリュームの使用済み論理サイズが現在設定されている物理ボリューム サイズを超えることはできません。

- 自動成長

スペースが不足したときにボリュームが自動で拡張されるかどうか。

- スペース保証

FlexVolがアグリゲートから空きブロックを削除するタイミングを制御する設定が表示されます。削除されたブロックは、ボリューム内のファイルへの書き込み用に確保されます。スペース ギャランティの設定は次のいずれかです。

- なし

ボリュームにスペース ギャランティが設定されていません。

- ファイル

データが書き込まれていないファイル（LUNなど）のフルサイズが確保されます。

- Volume

ボリュームのフルサイズが確保されます。

- 部分的

FlexCacheボリュームのサイズに基づいてスペースが確保されます。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 ギャランティはそのままです。



ボリュームのタイプが「データ キャッシュ」の場合、スペース ギャランティは「一部」です。

- 詳細（物理的）

ボリュームの物理仕様が表示されます。

- 総容量

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、ボリュームの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。

- スナップショットリザーブ

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。それぞれについて、Snapshotリザーブ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Snapshotコピーに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（使用不可の容量）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

ボリュームを自動で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。

- 部分準備金

オーバーライト リザーブのサイズを制御します。フラクショナル リザーブのデフォルト設定は100であり、必要なリザーブ スペースが実際に100%リザーブされ、オブジェクトの上書きが完全に保証されます。フラクショナル リザーブが100%未満の場合、そのボリューム内のすべてのスペース リザーブ ファイル用にリザーブされるスペースがその割合まで縮小されます。

- Snapshot の日次増加率

選択したボリューム内のSnapshotコピーの24時間ごとの変化（割合またはKB、MB、GBなど）が表示されます。

- Snapshot のフルまでの日数

ボリューム内のSnapshotコピー用にリザーブされたスペースが、指定のしきい値に達するまでの推定日数が表示されます。

[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や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する場合にSnapshotコピーを自動で削除するかどうかを示します。

- 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]ダイアログ ボックスが開き、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リストに表示されるSnapshotコピーの数は一致しないことがあります。

- ボリューム移動

ボリュームで実行された現在または前回のボリューム移動処理のステータスが表示されます。ボリューム移動処理の現在実行中のフェーズ、ソース アグリゲート、デスティネーション アグリゲート、開始時刻、終了時刻、推定終了時刻などの詳細も表示されます。

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。*ボリューム移動履歴*リンクをクリックすると、ボリューム移動操作の詳細情報を表示できます。

設定タブ

[設定]タブには、選択したボリュームについて、エクスポート ポリシー、RAIDタイプ、容量やストレージ効率化の関連機能に関する詳細が表示されます。

- 概要

- フルネーム

ボリュームの完全な名前が表示されます。

- アグリゲート

ボリュームが配置されているアグリゲートの名前、またはFlexGroupボリュームが配置されているアグリゲートの数が表示されます。

- 階層化ポリシー

ボリュームがFabricPool対応アグリゲートに導入されている場合に、ボリュームに対して設定されている階層化ポリシーが表示されます。「なし」、「Snapshot のみ」、「バックアップ」、「自動」、「すべて」のいずれかになります。

- Storage VM

ボリュームが含まれているSVMの名前が表示されます。

- ジャンクション パス

パスのステータス（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。**履歴**リンクをクリックすると、ジャンクション パスの最新の5つの変更を表示できます。

- エクスポート ポリシー

ボリューム用に作成されたエクスポート ポリシーの名前が表示されます。リンクをクリックすると、そのエクスポート ポリシーについて、SVMに属するボリュームで有効になっている認証プロトコルやアクセス権限などの詳細を確認できます。

- 形式

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」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。「RAID0」、「RAID4」、「RAID-DP」、「RAID-TEC」のいずれかです。



FlexGroupボリュームの場合、コンスティチュエント ボリュームを異なるタイプのアグリゲートに配置できるため、RAIDタイプが複数表示されることがあります。

- SnapLockタイプ

ボリュームが含まれているアグリゲートのSnapLockタイプが表示されます。

- SnapLock 有効期限

SnapLockボリュームの有効期限が表示されます。

- 容量

- シンプロビジョニング

ボリュームにシンプロビジョニングが設定されているかどうかが表示されます。

- 自動拡張

アグリゲート内でフレキシブル ボリュームが自動的に拡張されるかどうかが表示されます。

- Snapshot の自動削除

アグリゲートのスペース不足が原因でボリュームへの書き込みが失敗する場合にSnapshotコピーを自動で削除するかどうかを示します。

- 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

- 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。SnapVault関係が確立されたボリュームには「SnapVault」と表示されます。それ以外のボリュームには「標準」と表示されます。

- ストレージ効率ポリシー

このボリュームに対してUnified Managerから割り当てられているストレージ効率化ポリシーの名前を示します。このポリシーを使用して、圧縮と重複排除の設定を制御できます。

- 保護

- Snapshot コピー

Snapshotコピーの自動作成が有効か無効かを示します。

【保護】タブ

【保護】タブには、選択したボリュームの保護に関する詳細について、遅延の情報、関係のタイプ、関係のトポロジなどの情報が表示されます。

- まとめ

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。他の関係タイプについては、[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関係およびSnapVault関係について表示されるプロパティは次のとおりです。

- ソース ボリューム

選択したボリュームがデスティネーションの場合、選択したボリュームのソースの名前が表示されます。

- 遅延ステータス

保護関係の更新または転送の遅延ステータスが表示されます。「エラー」、「警告」、「重大」のいずれかです。

同期関係については、遅延ステータスは適用されません。

- 遅延時間

ミラーのデータがソースより遅延している時間が表示されます。

- 前回の更新成功日時

保護の更新に最後に成功した日時が表示されます。

同期関係については、前回の更新成功日時は適用されません。

- ストレージ サービス メンバー

ボリュームがストレージ サービスに属しており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

「はい」、「はい（バックアップ オプションあり）」、「なし」のいずれかが表示されます。「はい」の場合は、ソース ボリュームとデスティネーション ボリュームで異なるバージョンのONTAPソフトウェアを実行している場合でもSnapMirrorレプリケーションが可能です。「はい（バックアップ オプションあり）」の場合は、SnapMirror保護の実装で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。「なし」の場合は、バージョンに依存しないレプリケーションが有効になっていません。

- 関係機能

保護関係に使用できるONTAPの機能を示します。

- 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、保護サービスの名前が表示されます。

- 関係タイプ

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、およびSync）が表示されます。

- 関係の状態

SnapMirror関係またはSnapVault関係の状態が表示されます。「未初期化」、「SnapMirror 済

み」、「切断」のいずれかです。ソース ボリュームを選択した場合は、関係の状態は適用されず表示されません。

◦ 転送ステータス

保護関係の転送ステータスが表示されます。転送ステータスは、次のいずれかです。

- 中止中

SnapMirror転送が有効になっていますが、転送を中止する処理（チェックポイントの削除など）を実行中です。

- 確認中

デスティネーション ボリュームの診断チェックを実行中で、実行中の転送はありません。

- 最終処理中

SnapMirror転送が有効になっています。現在SnapVault増分転送の転送後のフェーズです。

- アイドル

転送が有効になっていますが、実行中の転送はありません。

- 同期

同期関係にある2つのボリュームのデータが同期されています。

- 非同期

デスティネーション ボリュームのデータがソース ボリュームと同期されていません。

- 準備中

SnapMirror転送が有効になっています。現在SnapVault増分転送の転送前のフェーズです。

- キューに登録

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。転送中ではありません。

- 休止中

SnapMirror転送を実行中です。増分転送が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のデータ転送が完了し、同期処理への移行が開始されています。

- 待機中

SnapMirror転送は開始されていますが、一部の関連タスクのキュー登録を待っています。

- 最大転送速度

関係の最大転送速度が表示されます。最大転送速度は、1秒あたりのキロバイト数 (Kbps)、1秒あたりのメガバイト数 (Mbps)、1秒あたりのギガバイト数 (Gbps)、1秒あたりのテラバイト数 (Tbps) のいずれかで示されます。関係間のベースライン転送に制限がない場合は「無制限」と表示されます。

- SnapMirror ポリシー

ボリュームの保護ポリシーが表示されます。「DPDefault」はデフォルトの非同期ミラー保護ポリシー、「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。ポリシーの名前をクリックすると、そのポリシーに関連付けられた詳細について次の情報を確認できます。

- 転送の優先順位
- アクセス時間を無視するかどうかの設定
- 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
- 保持設定のないスナップショット コピー ソースがデータ保護 (DP) ボリュームであるカスケード SnapVault関係では、ルール “sm_created” 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。「デフォルト」、「なし」、またはカスタムポリシーの名前のいずれかです。

- 保護されている

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、ボリュームが整合性グループ関係とSnapMirrorボリューム関係で保護されている場合、このフィールドには「SnapMirror」と「整合性グループ」の両方が表示されます。また、このフィールドには、統合された

関係ステータスを表示する[関係]ページへのリンクもあります。このリンクは、コンスティチュエント関係にのみ表示されます。

- 整合性グループ

SnapMirrorアクティブ同期関係で保護されているボリュームは、この列に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付けられているすべてのボリュームが図で示されます。選択したボリュームはダークグレーの線で囲んで示され、トポロジ内のボリュームをつなぐ線は保護関係のタイプを示しています。トポロジ内の関係の方向は左から右で、各関係の左側がソースで右側がデスティネーションです。

太線の二重線は非同期ミラー関係、太線の一重線は非同期バックアップ関係、細線の二重線は非同期ミラーバックアップ関係、太線と細線の二重線は同期関係です。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、表示されたメニューからボリュームを保護したりデータをリストアしたりできます。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。

このメニューは、以下に該当する場合は表示されません。

- RBACの設定で許可されていない場合：オペレータの権限しかない場合など
- ボリュームが同期保護関係にある場合
- ボリューム ID が不明な場合、たとえば、クラスター間関係があり、宛先クラスターがまだ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選択されて表示されます。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。

トポロジがいくつかある一般的なトポロジ テンプレートのいずれかに一致している場合、ボリュームの容量、遅延、Snapshotコピー、および前回成功したデータ転送に関する情報が表示されます。いずれのテンプレートにも一致していない場合は、ボリュームの遅延と前回成功したデータ転送に関する情報がトポロジの下の関係テーブルに表示されます。その場合、選択したボリュームの行が強調表示され、トポロジ ビューには、選択したボリュームとそのソース ボリュームの間の関係が太線と青色の点で示されます。

トポロジ ビューには次の情報が表示されます。

- 容量

ボリュームで使用されている合計容量が表示されます。トポロジ内のボリュームにカーソルを合わせると、そのボリュームに設定されている警告と重大のしきい値が[現在のしきい値設定]ダイアログ ボックスに表示されます。また、[現在のしきい値設定] ダイアログ ボックスの [しきい値の編集] 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オフにすると、トポロジ内のすべてのボリュームの容量情報がすべて非表示になります。

- 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。ラグ 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ラグ情報がすべて非表示になります。 ラグ チェックボックスが淡色表示

になっている場合、選択したボリュームのラグ情報と、関連するすべてのボリュームのラグ情報がトポロジの下の関係テーブルに表示されます。

- 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。スナップショット 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スナップショットコピー情報がすべて非表示になります。

スナップショットコピーアイコン () には、ボリュームのスナップショット 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リストに表示されるSnapshotコピーの数は一致しないことがあります。

- 前回成功した転送

前回成功したデータ転送の量、所要時間、日時が表示されます。最後に成功した転送 チェックボックスが淡色表示になっている場合、選択したボリュームの最後に成功した転送情報がトポロジの下の関係テーブルに表示されます。また、関連するすべてのボリュームの最後に成功した転送情報も表示されます。

- 歴史

選択したボリュームについてのSnapMirrorおよびSnapVaultの受信保護関係の履歴がグラフで表示されます。表示されるのは、受信関係の遅延時間、転送時間、および転送サイズの3種類の履歴グラフです。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関係およびSnapMirror同期関係で保護されている場合、転送時間と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 リストからグラフの種類を選択することができます。1週間、1カ月、または1年のいずれかの期間を選択して、その期間の詳細を表示することも可能です。履歴グラフは傾向を確認するのに役立ちます。たとえば、毎日または毎週同じ時間に大量のデータが転送されていたり、遅延警告や遅延エラーのしきい値を継続的に超過していれば、それに応じた措置を講じることができます。さらに、[エクスポート] ボタンをクリックすると、表示しているグラフのレポートを CSV 形式で作成できます。

保護の履歴グラフには次の情報が表示されます。

- 関係ラグ期間

縦軸 (y軸) には時間 (秒数、分数、または時間数) が、横軸 (x軸) には選択した期間 (日数、月数、または年数) が表示されます。y軸の最大値はx軸の期間における最大遅延時間を示しています。オレンジ色の線は遅延エラーのしきい値、黄色の線は遅延警告のしきい値を示しています。これらの線にカーソルを合わせると、しきい値の設定が表示されます。青色の線は遅延時間を示しています。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。

- 関係移行期間

縦軸 (y軸) には時間 (秒数、分数、または時間数) が、横軸 (x軸) には選択した期間 (日数、月数、または年数) が表示されます。y軸の最大値はx軸の期間における最大転送時間を示しています。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。



このグラフは、同期保護関係にあるボリュームについては表示されません。

- 転送された関係のサイズ

縦軸（y軸）には転送サイズ（バイト、KB、MB）が、横軸（x軸）には選択した期間（日数、月数、または年数）が表示されます。y軸の最大値はx軸の期間における最大転送サイズを示しています。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。



このグラフは、同期保護関係にあるボリュームについては表示されません。

【履歴】領域

【履歴】領域には、選択したボリュームの容量とスペース リザーベーションに関する情報がグラフで表示されます。さらに、[エクスポート] ボタンをクリックすると、表示しているグラフのレポートを CSV 形式で作成できます。

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 リストからグラフの種類を選択することができます。1週間、1カ月、または1年のいずれかの期間を選択して、その期間の詳細を表示することも可能です。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。

- 使用済みボリューム容量

折れ線グラフの形式で、ボリュームの使用容量（バイト、KB、MBなど）とボリュームの容量の使用履歴に基づく使用状況が縦軸（y軸）に表示されます。横軸（x軸）は期間です。期間は、1週間、1カ月、または1年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、グラフの線の表示と非表示を切り替えることが可能です。たとえば、凡例で[ボリューム - 使用済み容量]をクリックすると、ボリュームの使用済み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の比較

折れ線グラフの形式で、ボリュームの容量の使用履歴に基づく使用状況と使用済み容量、合計容量、および重複排除や圧縮によるスペース削減量（バイト、KB、MBなど）が縦軸（y軸）に表示されます。横軸（x軸）は期間です。期間は、1週間、1カ月、または1年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、グラフの線の表示と非表示を切り替えることが可能です。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、使用済み容量の推移を示す線が非表示になります。

- ボリューム使用容量（%）

折れ線グラフの形式で、ボリュームの使用率（%）とボリュームの容量の使用履歴に基づく使用状況が縦軸（y軸）に表示されます。横軸（x軸）は期間です。期間は、1週間、1カ月、または1年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、グラフの線の表示と非表示を切り替えることが可能です。たとえば、凡例で[ボリューム - 使用済み容量]をクリックすると、ボリュームの使用済み容量を示す線が非表示になります。

- スナップショット使用容量 (%)

面積グラフの形式で、SnapshotリザーブとSnapshotの警告しきい値、およびSnapshotコピーに使用されている容量の割合（%）が縦軸（y軸）に表示されます。Snapshotオーバーフローは別の色で示されます。横軸（x軸）は期間です。期間は、1週間、1カ月、または1年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、グラフの線の表示と非表示を切り替えることが可能です。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。

[イベント]リスト

[イベント]リストには、新規のイベントと応答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

イベントの名前が表示されます。

- トリガー時間

イベントが生成されてからの経過時間が表示されます。1週間を過ぎたイベントには、生成時のタイムスタンプが表示されます。

[関連するアノテーション]ペイン

[関連するアノテーション]ペインでは、選択したボリュームに関連付けられているアノテーションの詳細を確認できます。これには、ボリュームに適用されているアノテーションの名前と値などの情報が含まれます。[関連するアノテーション]ペインから、手動のアノテーションを削除することもできます。

[関連デバイス]ペイン

[関連デバイス]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。

- ストレージ仮想マシン

選択したボリュームが含まれるSVMの容量と健全性ステータスが表示されます。

- 集計

選択したボリュームが含まれるアグリゲートの容量と健全性ステータスが表示されます。FlexGroupボリュームの場合は、FlexGroupを構成するアグリゲートの数が表示されます。

- 総量

選択したボリュームの親アグリゲートに属するすべてのボリュームの数と容量が表示されます。最も高い重大度レベルに基づいて、ボリュームの健全性ステータスも表示されます。たとえば、アグリゲートに10個のボリュームがあり、5つのステータスが「警告」で残りの5つが「重大」の場合、ステータスは「重大」と表示されます。このコンポーネントは、FlexGroupボリュームに対しては表示されません。

- Qtrees

選択したボリュームに含まれるqtreeの数と、クォータが適用されたqtreeの容量が表示されます。クォータが適用されたqtreeの容量はボリュームのデータ容量に対する割合で示されます。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シェア**

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。

- **中小企業株**

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の総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。

- **ユーザーとグループのクォータ**

ボリュームとそのqtreeに関連付けられているユーザおよびユーザ グループ クォータの数とステータスが表示されます。

- *** FlexCloneボリューム***

選択したボリュームのすべてのクローン ボリュームの数と容量が表示されます。選択したボリュームにクローン ボリュームが含まれている場合にのみ表示されます。

- **親巻**

選択したFlexCloneボリュームの親ボリュームの名前と容量が表示されます。選択したボリュームがFlexCloneボリュームの場合にのみ表示されます。

[関連するグループ]ペイン

[関連するグループ]ペインでは、選択したボリュームに関連付けられているグループのリストを確認できます。

[関連するアラート]ペイン

[関連するアラート]ペインでは、選択したボリュームに対して作成されたアラートのリストを確認できます。[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。

[Storage VM / 健全性の詳細]ページ

[Storage VM / 健全性の詳細]ページでは、選択したStorage VMについて、健全性、容量、構成、データ ポリシー、論理インターフェイス（LIF）、LUN、qtree、ユーザ、ユーザ グループ クォータ、保護の詳細などの情報を表示できます。また、そのStorage VMに関連するオブジェクトやアラートに関する情報も表示できます。



監視できるのはデータStorage VMだけです。

コマンド ボタン

選択したStorage VMについて、各コマンド ボタンを使用して次のタスクを実行できます。

- パフォーマンスビューに切り替える

[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。

- ストレージ**VM**を表示

「健全性: すべてのストレージ VM」ビューに移動できます。

【健全性】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共有などのさまざまなオブジェクトのデータ可用性、データ容量、および保護の問題に関する詳細な情報が表示されます。

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が表示されます。たとえば、警告が表示されているボリューム容量グラフをクリックすると、重大度が警告である容量の問題があるボリュームのリストを表示できます。

- 可用性の問題

可用性の問題があるオブジェクトと可用性に関連する問題がないオブジェクトを含むオブジェクトの合計数をグラフで表示します。このグラフでは、問題が重大度レベル別に色分けされます。グラフの下には、Storage VM内のデータの可用性に影響を及ぼす可能性がある、またはすでに影響を及ぼしている問題について、その詳細が表示されます。たとえば、停止しているNAS LIFおよびSAN LIFやオフラインになっているボリュームの情報が表示されます。

現在実行中の関連するプロトコルやサービスに関する情報のほか、NFS共有やCIFS共有の数とステータスも確認できます。

- 容量の問題

容量の問題があるオブジェクトと容量関連の問題が発生していないオブジェクトを含むオブジェクトの合計数をグラフで表示します。このグラフでは、問題が重大度レベル別に色分けされます。グラフの下には、Storage VM内のデータの容量に影響を及ぼす可能性がある、またはすでに影響を及ぼしている問題について、その詳細が表示されます。たとえば、設定されたしきい値を超える可能性があるアグリゲートの情報が表示されます。

- 保護の問題

Storage VMの保護関連の健全性について、保護の問題がある関係とない関係、および両方の合計数がダイアログ ボックスに表示されます。選択したStorage VMのStorage VM DR関係のステータスも確認できます。Storage VM DR関係のイベントが表示され、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存在する場合、リンクをクリックすると、「健全性: すべてのボリューム」ビューに移動し、ストレージ VM 上の保護されていないボリュームのフィルターされたリストを表示できます。このグラフでは、問題が重大度レベル別に色分けされます。グラフをクリックすると、「関係: すべての関係」ビューに移動し、保護関係の詳細のフィルタリングされたリストを表示できます。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、またはすでに影響を及ぼしている問題について、その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が表示されます。

FlexVol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容量について、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。

- 総容量

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スペースのうち、データに使用可能な残りのスペースが表示されます。

- 容量の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に関する詳細が表形式で表示されます。

- ステータス

ボリュームに、容量に関するなんらか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。***詳細を表示***ボタンを使用すると、イベントの詳細情報を表示できます。

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。***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。

- Volume

ボリュームの名前が表示されます。

- 使用済みデータ容量

ボリュームの容量の使用率（％）に関する情報がグラフで表示されます。

- フルまでの日数

ボリュームの容量がフルに達するまでの推定日数が表示されます。

- シンプロビジョニング

選択したボリュームにスペース ギャランティが設定されているかどうかが表示されます。「はい」または「いいえ」のいずれかです。

- アグリゲート

FlexVolの場合は、ボリュームを含む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。

設定タブ

[設定]タブには、選択したStorage VMについて、所属するクラスタ、ルート ボリューム、含まれるボリュームのタイプ（FlexVol）、ポリシー、保護など、設定に関する詳細が表示されます。

- 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で設定できるプロトコルのタイプが表示されます。また、プロトコルが稼働中かどうかを示します（）、下（）、または設定されていない（）。

- データ ネットワーク インターフェース

- 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、インターフェースが稼働中かどうかを示します（）または下（）。

- 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、インターフェースが稼働中かどうかを示します（）または下（）。

- 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、インターフェースが稼働中かどうかを示します（）または下（）。

- 管理ネットワークインターフェース

- 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、管理インターフェースが稼働中かどうかを示します（）または下（）。

- ポリシー

- Snapshot 数

Storage VMで作成されたSnapshotポリシーの名前が表示されます。

- エクスポート ポリシー

エクスポート ポリシーが1つ作成されている場合はその名前が表示され、複数作成されている場合はその数が表示されます。

- 保護

- Storage VM DR

選択したStorage VMが保護されているか、デスティネーションであるか、保護されていないかが表示され、Storage VMが保護されている場合はデスティネーションの名前が表示されます。選択したStorage VMがデスティネーションの場合、ソースStorage VMの詳細が表示されます。ファンアウトの場合は、Storage VMが保護されているデスティネーションStorage VMの合計数が表示されます。個数のリンクをクリックすると、ソースStorage VMに関係するStorage VM関係のリストが表示されます。

- 保護されているボリューム

選択したStorage VMの全ボリュームのうち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 ボリュームの数が表示されます。

- 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で設定されているサービスのタイプが表示されます。「Domain Name System (DNS)」または「Network Information Service (NIS)」のいずれかです。

- 州

サービスの状態を表示します。状態は Up (●)、下 (●)、または未構成 (●)。

- ドメイン名

DNSサービスのDNSサーバまたはNISサービスのNISサーバの完全修飾ドメイン名 (FQDN) が表示されます。NISサーバが有効になっている場合は、アクティブなNISサーバのFQDNが表示されます。NISサーバが無効になっている場合は、すべてのFQDNのリストが表示されます。

- IP アドレス

DNSサーバまたはNISサーバのIPアドレスが表示されます。NISサーバが有効になっている場合は、アクティブなNISサーバのIPアドレスが表示されます。NISサーバが無効になっている場合は、すべてのIPアドレスのリストが表示されます。

【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ース

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。

- 動作状況

インターフェースの動作ステータスを表示します。これは Up (↑)、下 (↓)、または不明 (?)。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

インターフェースの管理ステータスを表示します。これは、アップ (↑)、下 (↓)、または不明 (?)。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。

- **母港**

インターフェイスが最初に関連付けられていた物理ポートが表示されます。

- **現在のポート**

インターフェイスが現在関連付けられている物理ポートが表示されます。インターフェイスが移行された場合、現在のポートがホーム ポートと同じでなくなることがあります。

- **ポートセット**

インターフェイスがマッピングされているポートセットが表示されます。

- **フェイルオーバーポリシー**

インターフェイスに設定されているフェイルオーバー ポリシーが表示されます。NFSインターフェイス、CIFSインターフェイス、およびFlexCacheインターフェイスの場合、デフォルトのフェイルオーバーポリシーは「次に使用可能」です。FCインターフェイスおよびiSCSIインターフェイスには、フェイルオーバー ポリシーは適用できません。

- **ルーティンググループ**

ルーティング グループの名前が表示されます。ルーティング グループの名前をクリックすると、ルートやデスティネーション ゲートウェイに関する詳細を確認できます。

ルーティング グループはONTAP 8.3以降ではサポートされないため、それらのクラスタの列は空白になります。

- **フェイルオーバーグループ**

フェイルオーバー グループの名前が表示されます。

Qtreesタブ

[qtree]タブには、qtreeとそのクォータに関する詳細が表示されます。1 つ以上の qtree の qtree 容量のヘルスしきい値設定を編集する場合は、[しきい値の編集] ボタンをクリックできます。

エクスポート ボタンを使用して、監視対象のすべての qtree の詳細を含むコンマ区切り値 (.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のいずれを対象にするかを選択できます。エクスポートしたCSVファイルには、qtreeに関する追加のフィールドもいくつか表示されます。

- 状態

qtreeの現在のステータスが表示されます。ステータスはクリティカル (❌)、エラー (❗)、警告 (⚠)、または通常 (✅)。

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。**詳細を表示**を使用して、イベントの詳細情報を表示できます。

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。**すべてのイベントを表示**を使用して、生成されたイベントのリストを表示することもできます。



qtreeには、重大度が同じまたは異なる容量関連のイベントが複数ある場合もあります。ただし、表示されるのは最も高い重大度だけです。たとえば、重大度が「エラー」と「警告」の2つのイベントがqtreeにある場合、表示される重大度は「エラー」だけです。

- Qツリー

qtreeの名前が表示されます。

- クラスタ

qtreeを含むクラスタの名前が表示されます。エクスポートしたCSVファイルにのみ表示されます。

- ストレージ仮想マシン

qtree を含むストレージ仮想マシン (SVM) の名前を表示します。エクスポートしたCSVファイルにのみ表示されます。

- 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。

- 割り当て設定

qtreeでクォータが有効になっているかどうかを示します。

- クォータタイプ

ユーザ、ユーザ グループ、またはqtreeのいずれのクォータであるかを示します。エクスポートしたCSV

ファイルにのみ表示されます。

- ユーザーまたはグループ

ユーザまたはユーザ グループの名前が表示されます。ユーザおよびユーザ グループごとに複数の行が表示されます。クォータのタイプがqtreeの場合やクォータが設定されていない場合は空になります。エクスポートしたCSVファイルにのみ表示されます。

- ディスク使用率 %

ディスク スペースの使用率が表示されます。ディスクのハード リミットが設定されている場合は、そのハード リミットに基づく値です。ディスクのハード リミットなしでクォータが設定されている場合は、ボリュームのデータ スペースに基づきます。クォータが設定されていない場合、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、グリッド ページに「該当なし」と表示され、CSV エクスポート データのフィールドは空白になります。

- ディスクハード制限

qtreeに対するディスク スペースの最大割り当て容量が表示されます。この制限に達すると、Unified Manager は重大なイベントを生成し、それ以上のディスク書き込みは許可されません。ディスクのハード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、値は「Unlimited」と表示されます。

- ディスクソフト制限

qtreeに対するディスク スペースの割り当て容量について、警告イベントを生成する容量が表示されます。ディスク 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、値は「Unlimited」と表示されます。デフォルトでは、この列は表示されません。

- ディスクしきい値

ディスク スペースについて設定されているしきい値が表示されます。ディスクしきい値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、値は「Unlimited」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。

- 使用されたファイル %

qtreeで使用されているファイルの割合が表示されます。ファイルのハード リミットが設定されている場合は、そのハード リミットに基づく値です。ファイルのハード リミットなしでクォータが設定されている場合は、値は表示されません。クォータが設定されていない場合、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、グリッド ページに「該当なし」と表示され、CSV エクスポート データのフィールドは空白になります。

- ファイルのハード制限

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、値は「Unlimited」と表示されます。

- ファイルソフト制限

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。クォータがファイル ソフト リミットなしで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、値は「Unlimited」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。

ユーザーとグループのクォータタブ

選択したStorage VMに対するユーザおよびユーザ グループのクォータに関する詳細が表示されます。クォータのステータス、ユーザまたはユーザ グループの名前、ディスクおよびファイルのソフト リミットとハード リミット、使用されているディスク スペースとファイル数、ディスクのしきい値などの情報を確認できます。また、ユーザやユーザ グループに関連付けられているEメール アドレスを変更することもできます。

• メールアドレス編集コマンドボタン

選択したユーザーまたはユーザー グループの現在の電子メール アドレスを表示する [電子メール アドレスの編集] ダイアログ ボックスを開きます。Eメール アドレスを変更することができます。 [電子メール アドレスの編集] フィールドが空白の場合、選択したユーザーまたはユーザー グループの電子メール アドレスを生成するためにデフォルトのルールが使用されます。

クォータが同じユーザが複数存在する場合は、ユーザの名前がカンマで区切って表示されます。また、デフォルトのルールを使用してEメール アドレスが生成されることはないため、通知を送信するにはEメール アドレスを指定する必要があります。

• 電子メールルールの設定コマンドボタン

Storage VMで設定されているユーザまたはユーザ グループ クォータについて、Eメール アドレスを生成するルールを作成または変更できます。クォータに違反が発生すると、指定したEメール アドレスに通知が送信されます。

• 状態

クォータの現在のステータスが表示されます。ステータスはクリティカル (❌)、警告 (⚠️)、または通常 (✅)。

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。*詳細を表示*を使用して、イベントの詳細情報を表示できます。

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。*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」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存在する場合は、ユーザの名前がカンマで区切って表示されます。

SecD エラーのためにONTAP が有効なユーザー名を提供しない場合、値は「Unknown」と表示されます。

- タイプ

ユーザまたはユーザ グループのどちらのクォータであるかを示します。

- ボリュームまたは**Qtree**

ユーザまたはユーザ グループのクォータが指定されているボリュームまたはqtreeの名前が表示されます。

ボリュームまたはqtreeの名前にカーソルを合わせると、それらに関する詳細を確認できます。

- ディスク使用率 %

ディスク スペースの使用率が表示されます。ディスクのハード制限なしでクォータが設定されている場合、値は「該当なし」と表示されます。

- ディスクハード制限

クォータに対するディスク スペースの最大割り当て容量が表示されます。この制限に達すると、Unified Manager は重大なイベントを生成し、それ以上のディスク書き込みは許可されません。ディスクのハード制限なしでクォータが設定されている場合、値は「Unlimited」と表示されます。

- ディスクソフト制限

クォータに対するディスク スペースの割り当て容量について、警告イベントを生成する容量が表示されます。ディスク ソフト リミットなしでクォータが設定されている場合、値は「Unlimited」と表示されます。デフォルトでは、この列は表示されません。

- ディスクしきい値

ディスク スペースについて設定されているしきい値が表示されます。ディスクしきい値制限なしでクォータが設定されている場合、値は「Unlimited」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。

- 使用されたファイル %

qtreeで使用されているファイルの割合が表示されます。ファイルのハード制限なしでクォータが設定されている場合、値は「該当なし」と表示されます。

- ファイルのハード制限

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。ファイルのハード制限なしでクォータが設定されている場合、値は「Unlimited」と表示されます。

- ファイルソフト制限

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。ファイルのソフト制限なしでクォー

タが設定されている場合、値は「Unlimited」と表示されます。デフォルトでは、この列は表示されません。

- 電子メールアドレス

クォータに違反が発生した場合に通知が送信されるユーザまたはユーザ グループのEメール アドレスが表示されます。

NFS共有タブ

[NFS 共有]タブには、NFS共有について、ステータス、ボリューム（FlexGroupボリュームまたはFlexVol）に関連付けられたパス、NFS共有に対するクライアントのアクセス レベル、エクスポートされているボリュームに対して定義されているエクスポート ポリシーなどの情報が表示されます。NFS共有は、ボリュームがマウントされていない場合、またはボリュームのエクスポート ポリシーに関連付けられているプロトコルにNFS共有が含まれていない場合は表示されません。

- 状態

NFS共有の現在のステータスが表示されます。ステータスはエラー (❗) または通常 (✅)。

- ジャンクションパス

ボリュームがマウントされているパスが表示されます。qtreeに明示的なNFSエクスポート ポリシーが適用されている場合、qtreeにアクセスできるボリュームのパスが表示されます。

- ジャンクションパスアクティブ

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。

- 混合

FlexGroupボリュームに状態の異なるコンスティチュエントが混在しています。

- セキュリティスタイル

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 スタイルは、UNIX、統合、NTFS、または混合のいずれかになります。

- UNIX (NFSクライアント)

ボリューム内のファイルおよびディレクトリにUNIX権限が設定されています。

- Unified

ボリューム内のファイルおよびディレクトリにunifiedセキュリティ形式が設定されています。

- NTFS (CIFSクライアント)

ボリューム内のファイルおよびディレクトリにWindows NTFS権限が設定されています。

- 混合

ボリューム内のファイルおよびディレクトリにUNIX権限またはWindows NTFS権限のどちらかを設定できます。

- **UNIX**パーミッション

エクスポートされているボリュームに設定されたUNIX権限ビット（8進数の文字列）が表示されます。UNIX形式の権限ビットと同様の形式です。

- 輸出ポリシー

エクスポートされているボリュームのアクセス権限を定義するルールが表示されます。リンクをクリックすると、エクスポート ポリシーに関連付けられているルールについて、認証プロトコルやアクセス権限などの詳細を確認できます。

SMB共有タブ

選択したStorage VMにある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 ボリュームのステータス、共有のセキュリティのデータ、共有に対して定義されているエクスポート ポリシーなどの情報を参照できます。SMB 共有と同等の NFS パスが存在するかどうかを確認することもできます。



[SMB 共有]タブにはフォルダ内の共有は表示されません。

- ユーザーマッピングの表示コマンドボタン

ユーザー マッピング 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することができます。

- **ACL** コマンド ボタンを表示

共有のアクセス制御ダイアログ ボックスを起動します。

選択した共有のユーザおよび権限の詳細を確認することができます。

- 状態

共有の現在のステータスが表示されます。ステータスは「正常」 (✓) またはエラー (⚠)。

- 共有名

SMB 共有の名前を表示します。

- 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。

- 包含オブジェクト

共有が属するコンテナ オブジェクトの名前が表示されます。コンテナ オブジェクトは、ボリュームまたはqtreeのいずれかです。

リンクをクリックすると、それぞれの詳細ページで、含まれている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。

- 混合

FlexGroupボリュームに状態の異なるコンスティチュエントが混在しています。

- 安全

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 スタイルは、UNIX、統合、NTFS、または混合のいずれかになります。

- UNIX (NFSクライアント)

ボリューム内のファイルおよびディレクトリにUNIX権限が設定されています。

- Unified

ボリューム内のファイルおよびディレクトリにunifiedセキュリティ形式が設定されています。

- NTFS (CIFSクライアント)

ボリューム内のファイルおよびディレクトリにWindows NTFS権限が設定されています。

- 混合

ボリューム内のファイルおよびディレクトリにUNIX権限またはWindows NTFS権限のどちらかを設定できます。

- 輸出ポリシー

共有に適用されているエクスポート ポリシーの名前が表示されます。Storage VMにエクスポート ポリシーが指定されていない場合は、「無効」と表示されます。

リンクをクリックすると、エクスポート ポリシーに関連付けられているルールについて、アクセス プロトコルや権限などの詳細を確認できます。このリンクは、選択したStorage VM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 相当

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 グループの詳細は[イニシエータ グループ]タブ、イニシエータの詳細は[イニシエータ]タブで確認できます。

- LUNタブ

選択したStorage VMに属するLUNに関する詳細が表示されます。LUNの名前、LUNの状態（オンラインまたはオフライン）、LUNが含まれているファイルシステム（ボリュームまたはqtree）の名前、ホスト オペレーティング システムのタイプ、LUNの合計データ容量とシリアル番号などの情報を参照できます。[LUN のパフォーマンス]列に[LUN / パフォーマンスの詳細]ページへのリンクが表示されます。

LUNでシンプロビジョニングが有効になっているかどうかや、LUNがイニシエータ グループにマッピングされているのかも確認できます。イニシエータにマッピングされている場合は、選択したLUNにマッピングされているイニシエータ グループとイニシエータを確認できます。

- イニシエーターグループタブ

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、グループのすべてのイニシエータで使用されているホスト オペレーティング システムのタイプ、サポートされるプロトコルなどの情報を参照できます。アクセス状態の列のリンクをクリックすると、イニシエータ グループの現在のアクセス状態を確認できます。

- 普通

イニシエータ グループは複数のアクセス パスに接続されています。

- シングルパス

イニシエータ グループは単一のアクセス パスに接続されています。

- パスなし

イニシエータ グループにアクセス パスが接続されていません。

イニシエータ グループがすべてのインターフェイスにマッピングされているか、ポートセットを介して特定のインターフェイスにマッピングされているかを確認することができます。[マッピングされたインターフェイス]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どちらかが表示されます。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の合計数が表示されます。

選択したイニシエータ グループにマッピングされているLUNとイニシエータも確認できます。

- イニシエータータブ

選択したStorage VMのイニシエータの名前とタイプ、およびそのイニシエータにマッピングされているイニシエータ グループの合計数が表示されます。

```
initiator groups that are mapped to the selected initiator group.
```

[関連するアノテーション]ペイン

[関連するアノテーション]ペインでは、選択したStorage VMに関連付けられているアノテーションの詳細を確認できます。これには、Storage VMに適用されるアノテーションの名前と値などの情報が含まれます。[関連するアノテーション]ペインから、手動のアノテーションを削除することもできます。

[関連デバイス]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。

- 集計

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る場合、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」であれば、ステータスは「重大」と表示されます。

- 割り当てられた集計

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。

- 巻

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ボリュームがある場合は、FlexGroupの数も含まれます。FlexGroupコンスチチュエントは含まれません。

[関連するグループ]ペイン

[関連するグループ]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。

[関連するアラート]ペイン

[関連するアラート]ペインでは、選択したStorage VMに対して作成されたアラートのリストを確認できます。*アラートを追加*リンクをクリックしてアラートを追加したり、アラート名をクリックして既存のアラートを編集したりすることもできます。

[クラスタ / 健全性の詳細]ページ

[クラスタ / 健全性の詳細]ページには、選択したクラスタについて、健全性、容量、設定の詳細などの情報が表示されます。クラスタのネットワーク インターフェイス (LIF)、ノード、ディスク、関連するデバイス、および関連するアラートに関する情報も確認できます。

クラスタ名の横にあるステータス（「問題なし」など）は通信ステータスで、Unified Managerがクラスタと通信できるかどうかを示します。クラスタのフェイルオーバー ステータスや全体的なステータスではありません。

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る

[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 ボックスを開き、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を開始し、Unified Manager がクラスタの最近の変更を検出できるようにします。

Unified ManagerをOnCommand Workflow Automationと組み合わせて使用している場合、再検出処理にはWFAのキャッシュ データがあればそれが必要です。

再検出処理が開始されると、関連付けられているジョブの詳細へのリンクが表示され、ジョブ ステータスを追跡できるようになります。

◦ 注釈: 選択したクラスターに注釈を付けることができます。

- クラスターを表示

「ヘルス: すべてのクラスター」ビューに移動できます。

[健全性]タブ

ノード、SVM、アグリゲートなどのさまざまなクラスター オブジェクトのデータ可用性とデータ容量の問題に関する詳細な情報が表示されます。可用性の問題は、クラスター オブジェクトのデータ処理機能に関連した問題です。容量の問題は、クラスター オブジェクトのデータ格納機能に関連した問題です。

オブジェクトのグラフをクリックすると、フィルタリングされたオブジェクトのリストを表示できます。たとえば、警告が表示されたSVMの容量のグラフをクリックすると、フィルタリングされたSVMのリストを表示できます。このリストには、重大度レベルが「警告」の容量の問題があるボリュームまたはqtreeを含むSVMが表示されます。また、警告が表示されたSVMの可用性のグラフをクリックすると、重大度レベルが「警告」の可用性の問題があるSVMのリストが表示されます。

可用性の問題

可用性の問題があるオブジェクトとないオブジェクトの両方を含むオブジェクトの合計数が図で表示されます。このグラフでは、問題が重大度レベル別に色分けされます。グラフの下には、クラスター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 シェルフやオフラインになっているアグリゲートの情報が表示されます。



SFOの棒グラフに表示されるデータは、ノードのHAの状態に基づきます。それ以外の棒グラフに表示されるデータは、生成されたイベントに基づいて計算されます。

容量の問題

容量の問題があるオブジェクトとないオブジェクトの両方を含むオブジェクトの合計数が図で表示されます。このグラフでは、問題が重大度レベル別に色分けされます。グラフの下には、クラスター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

選択したクラスター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。

- データ削減率

Snapshotコピーを含まない比率が、有効数字2桁で表示されます（例：1.8:1）。この比率は、ONTAPのStorage Efficiency設定に基づいています。

- 使用済み

すべてのアグリゲート上の、データに使用されている物理容量。これには、パリティ、ライトサイジング、リザーベーション用に割り当てられた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な情報が表示されます。ルート アグリゲートのデータは計算から除外されます。

- 総容量

クラスタの合計容量が表示されます。これには、パリティ用に割り当てられた容量は含まれません。

- 使用済み

データに使用されている容量が表示されます。これには、パリティ、ライトサイジング、リザーベーション用に割り当てられた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

クラスタのFabricPool対応アグリゲートについて、クラウド階層の合計使用済み容量と接続されている各クラウド階層の使用済み容量が表示されます。FabricPoolライセンスの有無は問われません。

ディスク タイプ別の物理容量内訳

[ディスク タイプ別の物理容量内訳]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、そのディスク タイプに関する詳細を[ディスク]タブで確認できます。

- 合計使用可能容量

データ ディスクの使用可能容量とスペア容量が表示されます。

- HDD

クラスタ内のすべてのHDDデータ ディスクの使用済み容量と使用可能容量が図で表示されます。HDDのデータ ディスクのスペア容量は点線で表されます。

- フラッシュ

- SSD Data

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。

- 未割り当てのディスク

クラスタ内の未割り当てのディスク数が表示されます。

[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なんらか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。詳細を表示 ボタンをクリックすると、イベントの詳細情報を表示できます。

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。*すべてのイベントを表示*リンクをクリックして、生成されたイベントのリストを表示することもできます。



アグリゲートには、重大度が同じまたは異なる容量関連のイベントが複数ある場合もあります。ただし、表示されるのは最も高い重大度だけです。たとえば、重大度が「エラー」と「重大」の2つのイベントがアグリゲートにある場合、表示される重大度は「重大」だけです。

- Aggregate

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。

設定タブ

選択したクラスタについて、IPアドレス、連絡先、場所などの詳細が表示されます。

クラスタの概要

- 管理インターフェース

Unified Managerからクラスタへの接続に使用されるクラスタ管理LIFが表示されます。インターフェイスの動作ステータスも表示されます。

- ホスト名または IP アドレス

Unified Managerからクラスタへの接続に使用されるクラスタ管理LIFのFQDN、短縮名、またはIPアドレスが表示されます。

- FQDN

クラスタの完全修飾ドメイン名（FQDN）が表示されます。

- OSバージョン

クラスタで実行されているONTAPのバージョンが表示されます。クラスタ内の各ノードで異なるバージョンのONTAPが実行されている場合は、最も古いONTAPのバージョンが表示されます。

- 担当者

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。

- Location

クラスタの場所が表示されます。

- パーソナリティ

オールSANアレイ構成のクラスタかどうかを示します。

リモート クラスタの概要

MetroCluster構成のリモート クラスタに関する詳細が表示されます。この情報は、MetroCluster構成に対してのみ表示されます。

- クラスタ

リモート クラスタの名前が表示されます。クラスタ名をクリックすると、クラスタの詳細ページに移動できます。

- 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。

- Location

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構成とMetroCluster over IP構成についてのみ表示されます。

- タイプ

MetroClusterのタイプ（2ノードまたは4ノード）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

MetroCluster構成（FCおよびIP）が表示されます。値は次のとおりです。

FC向け

- 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ノードの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す。

IPの場合

- イーサネット スイッチを使用した IP 構成（クラスタの構成に応じてL2またはL3）
 - 自動計画外スイッチオーバー（AUSO）

ローカル クラスタで自動計画外スイッチオーバーが有効になっているかどうかが表示されます。Unified Managerのデフォルトの設定では、2ノードのMetroCluster構成の場合、すべてのクラスタでAUSOが有効になります。AUSOの設定はコマンドライン インターフェイスを使用して変更できます。これは、MetroCluster over FCでのみサポートされます。

- スイッチオーバー モード

MetroCluster over IP構成のスイッチオーバー モードが表示されます。使用可能な値は次のとおりです。Active、Negotiated Switchover、そして Automatic Unplanned Switchover。

ノード

- 可用性

稼働中のノードの数を表示します（●）または下（●）をクラスター内に配置します。

- 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、そのバージョンのONTAPを実行しているノードの数が表示されます。たとえば、「9.6 (2), 9.3 (1)」は、2つのノードでONTAP 9.6が実行され、1つのノードでONTAP 9.3が実行されていることを示します。

Storage Virtual Machine

- 可用性

稼働中のSVMの数を表示します（●）または下（●）をクラスター内に配置します。

ネットワークインターフェース

- 可用性

稼働中の非データLIFの数を表示します（●）または下（●）をクラスター内に配置します。

- クラスタ管理インターフェース

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ース

ノード管理LIFの数が表示されます。

- クラスタ インターフェース

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

クラスタでメディエーターがサポートされているかどうか、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、および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

クラスタでメディエーターがサポートされているが、設定されていない場合に表示されます。

- IP アドレス

クラスタでメディエーターがサポートされており、設定されている場合に表示されます。メディエーターのステータスは色で示されます。緑は、メディエーターが到達可能であることを示します。赤は、メディエーターが到達不能であることを示します。

クラウド階層

このクラスタが接続されているクラウド階層のリストが表示されます。それぞれのクラウド階層のタイプ（Amazon S3、Microsoft Azureクラウド、IBM Cloud Object Storage、Google Cloud Storage、Alibaba Cloud Object Storage、またはStorageGRID）と状態（「使用可能」または「利用不可」）も表示されます。

[MetroCluster 接続]タブ

MetroCluster over FC構成のクラスタ コンポーネントの問題と接続ステータスが表示されます。ディザスタリカバリ パートナーに問題があるクラスタは赤い線で囲んで示されます。



[MetroCluster 接続]タブは、MetroCluster over FC構成のクラスタに対してのみ表示されます。

リモート クラスタの名前をクリックすると、リモート クラスタの詳細ページに移動できます。コンポーネント数のリンクをクリックして、コンポーネントの詳細を確認することもできます。たとえば、クラスタ内のノード数のリンクをクリックすると、クラスタの詳細ページにノード タブが表示されます。リモート クラスタのディスク数のリンクをクリックすると、リモート クラスタの詳細ページにディスク タブが表示されます。



8ノードのMetroCluster構成に対してディスク シェルフ コンポーネント数のリンクをクリックした場合、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。他のHAペアのローカル シェルフを表示する方法はありません。

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に加え、その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に関する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が表示されます。

コンポーネント間の接続に関する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。*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 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することができます。ディザスタ リカバリ パートナーに問題があるクラスタは赤い線で囲んで示されます。



[MetroCluster レプリケーション]タブは、MetroCluster over FC構成のクラスタに対してのみ表示されます。

MetroCluster環境では、このタブを使用して、ローカル クラスタとリモート クラスタの間の論理接続やピア関係を検証できます。クラスタ コンポーネントとその論理接続を客観的に捉えることができるため、メタデータやデータのミラーリングで発生する可能性がある問題を特定するのに役立ちます。

[MetroCluster レプリケーション]タブでは、選択したクラスタをローカル クラスタ、そのMetroClusterパートナーをリモート クラスタとして、詳しい図が表示されます。

[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を表示します。これは Up (↑)、下 (↓)、または不明 (?)。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を表示します。これは、アップ (↑)、下 (↓)、または不明 (?)。設定を変更する際やメンテナンスを実施する際には、インターフェイスの管理ステータスを変更することができます。管理ステータスは、動作ステータスとは異なる場合があります。ただし、LIFの管理ステータス

が「停止」の場合、動作ステータスはデフォルトで「停止」になります。

IP アドレス

インターフェイスのIPアドレスが表示されます。

ロール

インターフェイスのロールが表示されます。「クラスタ管理 LIF」、「ノード管理 LIF」、「クラスタ LIF」、「クラスタ間 LIF」のいずれかです。

ホーム ポート

インターフェイスが最初に関連付けられていた物理ポートが表示されます。

現在のポート

インターフェイスが現在関連付けられている物理ポートが表示されます。LIFの移行後は、現在のポートがホーム ポートと同じでなくなることがあります。

フェイルオーバー ポリシー

インターフェイスに設定されているフェイルオーバー ポリシーが表示されます。

ルーティング グループ

ルーティング グループの名前が表示されます。ルーティング グループの名前をクリックすると、ルートやデスティネーション ゲートウェイに関する詳細を確認できます。

ルーティング グループはONTAP 8.3以降ではサポートされないため、それらのクラスタの列は空白になります。

フェイルオーバー グループ

フェイルオーバー グループの名前が表示されます。

[ノード]タブ

選択したクラスタ内のノードに関する情報が表示されます。HAペア、ディスク シェルフ、およびポートについて、次の情報を確認できます。

HA の詳細

HAペアのノードのHAの状態と健全性ステータスが図で表示されます。ノードの健全性ステータスは次の色で示されます。

- 緑

ノードは稼働しています。

- 黄色

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、環境に何らかの問題があります。

- 赤

ノードは停止しています。

HAペアの可用性に関する情報を確認して、リスクを回避するための必要な措置を講じることができます。たとえば、テイクオーバー操作の可能性がある場合には、次のメッセージが表示されます: ストレージ フェイルオーバーが可能です。

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することができます。イベントがトリガーされた時刻も確認できます。

モデル番号など、ノード関連のその他の情報を確認することができます。

シングルノード クラスタがある場合は、ノードに関する詳細も確認できます。

ディスク シェルフ

HAペアのディスク シェルフに関する情報が表示されます。

ディスク シェルフや環境コンポーネントに対して生成されたイベントも表示され、それらのイベントがトリガーされた時刻も確認できます。

- 棚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 シェルフの環境に関する詳細が表示されます。環境の詳細は、次の色のアイコンで示されます。

- 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。

- 州

ディスク シェルフの状態が表示されます。「オフライン」、「オンライン」、「ステータスなし」、「初期化が必要」、「見つからない」、「不明」のいずれかです。

- モデル

ディスク シェルフのモデル番号が表示されます。

- ローカル ディスク シェルフ

ディスク シェルフがローカル クラスタとリモート クラスタのどちらに配置されているかを示します。この列は、MetroCluster構成のクラスタに対してのみ表示されます。

- 固有ID

ディスク シェルフの一意的識別子が表示されます。

- ファームウェアバージョン

ディスク シェルフのファームウェア バージョンが表示されます。

ポート

関連付けられたFC、FCoE、およびイーサネット ポートに関する情報が表示されます。ポートのアイコンをクリックすると、ポートとそれに関連付けられたLIFに関する詳細を確認できます。

ポートに対して生成されたイベントを確認することもできます。

ポートに関する次の詳細を確認できます。

- ポートID

ポートの名前が表示されます。たとえば、e0M、e0a、e0bなどです。

- ロール

ポートのロールが表示されます。「クラスタ」、「データ」、「クラスタ間」、「ノード管理」、「未定義」のいずれかです。

- 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。「イーサネット」、「Fibre Channel」、「FCoE」のいずれかです。

- 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 リビジョンを表示します。

- ステータス

ポートの現在の状態が表示されます。状態は、アップ、ダウン、リンク未接続、不明 (?)。

[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の詳細について、LIFの名前、動作ステータス、IPアドレスまたはWWPN、プロトコル、LIFに関連付けられているSVMの名前、現在のポート、フェイルオーバー ポリシー、フェイルオーバー グループなどの情報も確認できま

す。

[ディスク]タブ

選択したクラスタ内のディスクに関する詳細が表示されます。使用しているディスク、スペア ディスク、破損ディスク、未割り当てディスクの数など、ディスク関連の情報を確認できます。また、ディスク名、ディスク タイプ、ディスクの所有者ノードなどの詳細も確認できます。

ディスク プール サマリ

実質的タイプ (FCAL、SAS、SATA、MSATA、SSD、NVMe SSD、SSD CAP、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、その他の詳細を確認することもできます。実質的ディスク タイプの個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。未割り当てのディスクの場合、この列に値は表示されません。

州

ディスクの状態を表示します: アグリゲート、共有、スペア、破損、未割り当て、サポートなし、または不明。デフォルトでは、この列は、破損、未割り当て、サポート対象外、スペア、集約、共有の順序で状態が表示されるように並べ替えられています。

ローカル ディスク

ディスクがローカル クラスタに配置されている場合は「はい」、リモート クラスタに配置されている場合は「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 タイプに基づいてディスクの位置が表示されます。「コピー」、「データ」、「パリティ」などになります。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。集計数をクリックして、「ヘルス: すべての集計」ビューで影響を受ける集計のリストを表示することもできます。

次に該当する場合、この列に値は表示されません。

- 破損したディスクを含むクラスタがUnified Managerに追加された場合
- 障害が発生したディスクがない場合

ストレージ プール

SSDが属するストレージ プールの名前が表示されます。ストレージ プールの名前にカーソルを合わせると、ストレージ プールの詳細を確認できます。

格納可能な容量

使用可能なディスク容量が表示されます。

物理容量

ライトサイジングやRAID構成でフォーマットする前のrawディスクの容量が表示されます。デフォルトでは、この列は表示されません。

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、その作成とアグリゲートへの追加、およびスペア管理において同じタイプとみなされます。ONTAPIは、各ディスク タイプに実質的ディスク タイプを割り当てます。

使用済みスペア ブロック (%)

SSDディスクの使用済みのスペア ブロックの割合が表示されます。この列は、SSDディスク以外のディスクについては空白になります。

使用済み寿命 (%)

SSDの実際の使用状況とメーカーの想定寿命に基づいて、SSDの推定される使用済み寿命の割合が表示されます。この値が99を超えた場合、想定される耐久度に達したと考えられますが、必ずしもSSDで障害が発生しているとはかぎりません。値が不明なディスクについては省略されます。

ファームウェア

ディスクのファームウェア バージョンが表示されます。

rpm

ディスクの回転速度（rpm）が表示されます。デフォルトでは、この列は表示されません。

モデル

ディスクのモデル番号が表示されます。デフォルトでは、この列は表示されません。

ベンダー

ディスク ベンダーの名前が表示されます。デフォルトでは、この列は表示されません。

Shelf ID

ディスクが配置されているシェルフのIDが表示されます。

ベイ

ディスクが配置されているベイのIDが表示されます。

[関連するアノテーション]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。[関連するアノテーション]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。

[関連デバイス]ペイン

選択したクラスタに関連付けられているデバイスの詳細を確認できます。

これには、クラスタに接続されたデバイスのタイプ、サイズ、数、健全性ステータスなどのプロパティが含まれます。個数のリンクをクリックすると、特定のデバイスについて詳しく分析できます。

[MetroCluster パートナー]ペインを使用して、リモートの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）の数と詳細も確認できます。[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。

[関連デバイス]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、それらに移動することができます。

MetroCluster パートナー

MetroClusterパートナーの健全性ステータスが表示されます。個数のリンクを使用して詳細に移動し、クラスタ コンポーネントの健全性や容量に関する情報を確認できます。

ノード

選択したクラスタに属するノードの数、容量、および健全性ステータスが表示されます。容量は、総容量のうちの使用可能な合計容量を示します。

Storage Virtual Machine

選択したクラスタに属するSVMの数が表示されます。

アグリゲート

選択したクラスタに属するアグリゲートの数、容量、および健全性ステータスが表示されます。

【関連するグループ】ペイン

選択したクラスタを含むグループのリストを確認できます。

【関連するアラート】ペイン

【関連するアラート】ペインでは、選択したクラスタに対するアラートのリストを確認できます。[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。

関連情報

["【ボリュームページ】" クラスタ リストおよび詳細の表示](#)

【アグリゲート / 健全性の詳細】ページ

【アグリゲート / 健全性の詳細】ページでは、選択したアグリゲートについて、容量、ディスク情報、設定の詳細、生成されたイベントなどの情報を確認できます。また、そのアグリゲートに関連するオブジェクトやアラートに関する情報も参照できます。

コマンド ボタン



FabricPool対応アグリゲートを監視する場合、このページのコミット済み容量およびオーバーコミット容量の値はローカルのパフォーマンス階層の容量のみに基づきます。クラウド階層で使用可能なスペースの量は、オーバーコミット容量の値に反映されません。同様に、アグリゲートのしきい値もローカルのパフォーマンス階層のみに対する値となります。

選択したアグリゲートについて、各コマンド ボタンを使用して次のタスクを実行できます。

- パフォーマンスビューに切り替える

[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。

- 集計を表示

「ヘルス: すべての集計」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が表示されます。

デフォルトでは、ルート アグリゲートについては容量のイベントは生成されません。また、Unified Managerで使用されるしきい値は、ノード ルート アグリゲートには適用されません。これらのイベントが生成されるように設定を変更できるのは、テクニカル サポート担当者だけです。テクニカル サポート担当者が設定を変更すると、しきい値がノードのルート アグリゲートにも適用されるようになります。

• 容量

データ容量のグラフとSnapshotコピーのグラフに、アグリゲートの容量の詳細が表示されます。

◦ 使用済みの論理スペース

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地点（アグリゲートのスペースがほぼフルであるとみなされる地点）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地点（アグリゲートのスペースがフルであるとみなされる地点）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。

◦ スナップショットコピーグラフ

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リザーブを超えている場合には超過分の使用容量が表示されます。

• クラウド層

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ライセンスの有無は問われません。

クラウド層が別のクラウド プロバイダー（「ミラー層」）にミラーリングされている場合、両方のクラウド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。

- 総容量

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 オーバーコミットに関する情報が表示されます。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、アグリゲート内のボリュームの合計サイズがアグリゲートの総容量を超えるような割り当てが可能です。



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ライセンスの有無は問われません。クラウド階層が別のクラウド プロバイダ（ミラー階層）にミラーリングされている場合、両方のクラウド階層が表示されます。

- 合計キャッシュ スペース

Flash Poolアグリゲートに追加されているソリッド ステート ドライブ（SSD）の合計スペースが表示されます。アグリゲートに対して Flash Pool を有効にしたが、SSD を追加していない場合、キャッシュ スペースは 0 KB と表示されます。



アグリゲートに対して Flash Pool が無効になっている場合、このフィールドは非表示になります。

- アグリゲートのしきい値

アグリゲートの容量に関する次のしきい値が表示されます。

- ほぼフルのしきい値

アグリゲートがほぼフルであるとみなす割合を示します。

- フルのしきい値

アグリゲートがフルであるとみなす割合を示します。

- ほぼオーバーコミットのしきい値

アグリゲートが間もなくオーバーコミットされ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とみなす割合を示します。

- その他の詳細: 日次成長率

最後の2つのサンプル間の変更率が24時間続いた場合にアグリゲートで使用されるディスク容量が表示されます。

たとえば、アグリゲートのディスク スペースの使用量が午後2時に10GBで、午後6時に12GBであるとする、このアグリゲートの1日あたりの増加率は2GBです。

- ボリューム移動

現在実行中のボリューム移動処理の数が表示されます。

- 移動されたボリューム

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、ボリュームの使用可能なスペースのうちアグリゲートの容量の問題が原因で使用できないスペース（使用不可の容量）が表示されます。

表示するグラフはドロップダウン リストから選択できます。グラフに表示されるデータをソートして、使用済みサイズ、プロビジョニングされたサイズ、使用可能な容量、1日あたりの最大および最小増加率などの詳細を表示できます。アグリゲート内のボリュームを含むストレージ仮想マシン (SVM) に基づいて

データをフィルタリングできます。シンプロビジョニング ボリュームの詳細を表示することもできます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。デフォルトでは、アグリゲート内の上位30個のボリュームがフィルタリングされて表示されます。

[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ついて、RAIDタイプとサイズ、アグリゲートで使用されているディスクのタイプなど、詳細な情報が表示されます。このタブには、RAIDグループと使用されているディスクのタイプ（SAS、ATA、FCAL、SSD、VMDISKなど）を示す図も表示されます。パリティ ディスクやデータ ディスクにカーソルを合わせると、各ディスクのベイ、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ときは、共有ディスクの詳細が表示されます。専用ディスクと共有ディスクの両方が含まれているときは、両方のディスクの詳細が表示されます。

- RAIDの詳細

専用ディスクの場合のみ、RAIDの詳細が表示されます。

- 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グループに含めることができるディスクの最大数が表示されます。

- グループ

アグリゲート内のRAIDグループの数が表示されます。

- 使用ディスク

- 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ィスクの数と容量が表示されます。共有ディスクの詳細

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利用できるスペア データ ディスクの実質的タイプ、数、および容量が表示されます。



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ると、Unified Manager では、アグリゲートと互換性のあるスペア ディスクの一部が表示されません。

- **SSDキャッシュ**

専用キャッシュSSDディスクと共有キャッシュSSDディスクに関する詳細が表示されます。

専用キャッシュSSDディスクについては、次の情報が表示されます。

- **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グループに含めることができるディスクの最大数が表示されます。

- グループ

アグリゲート内のRAIDグループの数が表示されます。

- 使用ディスク

- 実質的タイプ

アグリゲート内でキャッシュに使用されているディスク タイプとして「SSD」が表示されます。

- データ ディスク

キャッシュ用にアグリゲートに割り当てられているデータ ディスクの数と容量が表示されます。

- パリティ ディスク

キャッシュ用にアグリゲートに割り当てられているパリティ ディスクの数と容量が表示されます。

- スペアディスク

選択したアグリゲートのノードでキャッシュに使用可能なスペア ディスクの実質的タイプ、数、および容量が表示されます。



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ると、Unified Manager では、アグリゲートと互換性のあるスペア ディスクの一部が表示されません。

共有キャッシュについては、次の情報が表示されます。

- ストレージプール

ストレージ プールの名前が表示されます。ストレージ プールの名前にカーソルを合わせると、次の情報を確認できます。

- ステータス

ストレージ プールのステータス (正常または異常) を表示します。

- 割り当て合計

ストレージ プール内の割り当て単位の総数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 プールの列に表示されるディスク数と[ディスク情報]タブに表示されるストレージ プールの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 プールが健全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。

- 割り当てられたキャッシュ

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。

- クラウド層

FabricPool対応アグリゲートを設定している場合にクラウド階層の名前が表示され、使用済みの合計スペースが表示されます。クラウド階層が別のクラウド プロバイダ（ミラー階層）にミラーリングされている場合、両方のクラウド階層の詳細が表示されます。

設定タブ

[設定]タブには、選択したアグリゲートについて、クラスター 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。

- クラウド層

FabricPool対応アグリゲートの場合、クラウド階層の詳細が表示されます。一部のフィールドはストレージ プロバイダに応じて異なります。クラウド層が別のクラウド プロバイダー（「ミラー層」）にミラーリングされている場合、両方のクラウド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。

- Name

ONTAPでの作成時に指定されたクラウド階層の名前が表示されます。

- サーバ

クラウド階層のFQDNが表示されます。

- ポート

クラウド プロバイダとの通信に使用されているポート。

- アクセス キー / アカウント

クラウド階層のアクセス キーまたはアカウントが表示されます。

- コンテナ名

クラウド階層のバケット名またはコンテナ名が表示されます。

- SSL

クラウド階層に対してSSL暗号化が有効になっているかどうかが表示されます。

【履歴】領域

【履歴】領域には、選択したアグリゲートの容量に関する情報がグラフで表示されます。さらに、[エクスポート] ボタンをクリックすると、表示しているグラフのレポートを CSV 形式で作成できます。

【履歴】ペインの上部にあるドロップダウン リストからグラフの種類を選択することができます。1週間、1カ月、または1年のいずれかの期間を選択して、その期間の詳細を表示することも可能です。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。

- 総使用容量 (%)

折れ線グラフの形式で、アグリゲートの使用率 (%) とアグリゲートの容量使用履歴が縦軸 (y軸) に表示されます。横軸 (x軸) は期間です。期間は、1週間、1カ月、または1年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、グラフの線の表示と非表示を切り替えることが可能です。たとえば、凡例で[使用済みパフォーマンス容量]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。

- 使用済み総容量と総容量の比較

折れ線グラフの形式で、アグリゲートの容量使用履歴と使用済み容量および合計容量 (バイト、KB、MB など) が縦軸 (y軸) に表示されます。横軸 (x軸) は期間です。期間は、1週間、1カ月、または1年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、グラフの線の表示と非表示を切り替えることが可能です。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、使用済み容量の推移を示す線が非表示になります。

- 総使用容量 (%) 対コミット容量 (%)

折れ線グラフの形式で、アグリゲートの容量使用履歴とコミット済みスペースの割合 (%) が縦軸 (y軸

）に表示されます。横軸（x軸）は期間です。期間は、1週間、1カ月、または1年のいずれかを選択できます。グラフの特定のポイントにカーソルを合わせると、その時点の詳細を確認できます。対応する凡例をクリックして、グラフの線の表示と非表示を切り替えることが可能です。たとえば、凡例で[コミット済みスペース]をクリックすると、コミット済みスペースを示す線が非表示になります。

【イベント】リスト

【イベント】リストには、新規のイベントと応答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

イベントの名前が表示されます。

- トリガー時間

イベントが生成されてからの経過時間が表示されます。1週間を過ぎたイベントには、生成時のタイムスタンプが表示されます。

【関連デバイス】ペイン

【関連デバイス】ペインでは、アグリゲートに関連するクラスター 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。

- ノード内の集約

選択したアグリゲートが含まれるクラスター ノード内のアグリゲートの総数と合計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、クラスター ノードに10個のアグリゲートがあり、5つのステータスが「警告」で残りの5つが「重大」の場合、ステータスは「重大」と表示されます。

- 巻

アグリゲート内のFlexVolおよびFlexGroupボリュームの数と容量が表示されます。FlexGroupコンスチ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付けられているリソース プールが表示されます。

- ディスク

選択したアグリゲート内のディスクの数が表示されます。

【関連するアラート】ペイン

【関連するアラート】ペインでは、選択したアグリゲートに対して作成されたアラートのリストを確認できます。[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。

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、トラブルシューティング

Unified Manager を使用すると、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 ボールト保護の監視とトラブルシューティング、上書きまたは失われたデータの復元を行うことができます。

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、複数の種類のSnapMirror保護関係をUnified Managerで設定できます。すべての種類のSnapMirror保護では、フェイルオーバーによるディザスタ リカバリ保護が提供されますが、パフォーマンス、バージョン依存性の解消、および複数のバックアップ コピーによる保護については、提供される機能が異なります。

従来型のSnapMirror非同期保護関係

従来型のSnapMirror非同期保護では、ソース ボリュームとデスティネーション ボリューム間のブロック レプリケーションによるミラー保護が提供されます。

従来型のSnapMirror関係では、ブロック レプリケーションに基づいてミラー処理が行われるため、他のSnapMirror関係よりも高速なミラー処理が可能です。ただし、従来型のSnapMirror保護では、デスティネーション ボリュームで実行されているONTAPソフトウェアのマイナー バージョンがソース ボリュームと同じかそれよりも新しい必要があります（バージョン8.xから8.x、9.xから9.xなど）。9.1のソースから9.0の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のメジャー バージョンがソースよりも古いい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を使用したSnapMirror非同期保護

バージョンに依存しないレプリケーションを使用したSnapMirror非同期保護では、ソース ボリュームとデスティネーション ボリュームでONTAP 8.3以降の異なるバージョンのソフトウェアを実行している場合でも（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）、これらのボリューム間に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。

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関係の場合、ミラー処理は従来型のブロック レプリケーションによるSnapMirrorほど高速ではありません。

そのため、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保護の実装は次の状況には適していません。

- 1,000万を超える保護対象のファイルがソース オブジェクトに含まれている。
- 保護対象データの目標復旧時点が2時間以下である（つまり、ソースのデータからの遅れが2時間未満のリカバリ可能なミラー データが常にデスティネーションに含まれている必要がある）。

これらのいずれかの状況では、デフォルトのSnapMirror保護をより高速なブロック レプリケーション ベースで実行する必要があります。

バージョンに依存しないレプリケーションとバックアップ オプションを使用した**SnapMirror**非同期保護

バージョンに依存しないレプリケーションとバックアップ オプションを使用した**SnapMirror**非同期保護では、ソース ボリュームとデスティネーション ボリューム間のミラー保護、およびミラー データの複数のコピーをデスティネーションに格納する機能が提供されます。

ストレージ管理者は、ソースからデスティネーションにミラーリングするSnapshotコピーを指定できます。また、それらのコピーをデスティネーションに（ソースのコピーが削除された場合でも）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**関係の場合、ミラー処理は従来型のブロック レプリケーションによる**SnapMirror**ほど高速ではありません。

SnapMirrorユニファイド レプリケーション（ミラー バックアップ）

SnapMirrorユニファイド レプリケーションを使用すると、同じデスティネーション ボリュームでディザスタリカバリとアーカイブを設定できます。**SnapMirror**と同様に、一元化されたデータ保護機能の初回起動時に、ベースライン転送が実行されます。デフォルトの統合データ保護ポリシー「MirrorAndVault」によるベースライン転送では、ソース ボリュームのスナップショット コピーが作成され、そのコピーとそれが参照するデータ ブロックが宛先ボリュームに転送されます。**SnapVault**と同様に、一元化されたデータ保護にはベースラインの古いSnapshotコピーが含まれません。

厳密な同期を使用した**SnapMirror**同期保護

「厳密な」同期による**SnapMirror**同期保護により、プライマリ ボリュームとセカンダリ ボリュームが常に互いの真のコピーであることが保証されます。セカンダリ ボリュームへのデータの書き込みでレプリケーション エラーが発生すると、プライマリ ボリュームに対するクライアントI/Oが中断されます。

通常の同期を使用した**SnapMirror**同期保護

「通常の」同期による**SnapMirror**同期保護では、プライマリ ボリュームとセカンダリ ボリュームが常に互いの真のコピーである必要はありません。これにより、プライマリ ボリュームの可用性が保証されます。セカンダリ ボリュームへのデータの書き込みでレプリケーション エラーが発生すると、プライマリ ボリュームとセカンダリ ボリュームが同期されていない状態のまま、プライマリ ボリュームに対するクライアントI/Oが継続されます。



[ヘルス: すべてのボリューム] ビューまたは [ボリューム/ヘルスの詳細] ページから同期保護関係を監視している場合、[復元] ボタンと [関係] 操作ボタンは使用できません。

SnapMirrorアクティブ同期

ONTAP 9.8以降では**SnapMirror**アクティブ同期機能が利用可能で、LUNを使用してアプリケーションを保護できるようになりました。アプリケーションが透過的にフェイルオーバーするため、災害発生時にもビジネス継続性を確保できます。

SM-BCを使用すると、クラスタおよびStorage Virtual Machineで使用可能な整合性グループ（CG）について、Unified Managerから同期**SnapMirror**関係を検出して監視できます。**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、AFFまたはASAのどちらかをプライマリクラスタとセカンダリ クラスタに設定できます。**SnapMirror**アクティブ同期は、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アクティブ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、保護関係をまとめて表示

し、ボリューム インベントリ内の整合性グループや、整合性グループ関係の保護トポロジ、および整合性グループ関係の最大1年分の履歴データを確認できます。レポートをダウンロードすることもできます。また、整合性グループ関係のサマリを表示したり、整合性グループ関係のサポートを検索したり、整合性グループで保護されているボリュームに関する情報を取得したりすることができます。

[関係]ページでは、整合性グループで保護されているソースとデスティネーションのストレージ オブジェクトおよびその関係をソート、フィルタリングしたり、保護を拡張したりできます。

SnapMirrorアクティブ同期の詳細については、以下を参照してください。"[ONTAP 9 Snapmirror Active Sync \(旧SM-BC\) に関するドキュメント](#)"。

Unified Managerで保護関係を設定する

Unified ManagerとOnCommand Workflow Automationを使用してデータを保護するためのSnapMirror関係とSnapVault関係をセットアップするには、いくつかの手順を実行する必要があります。

開始する前に

- アプリケーショ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を設定する](#)"。
 - "[Workflow AutomationでのUnified Managerデータ ソースのキャッシングの確認](#)"。

手順

1. 作成する保護関係のタイプに応じて、次のいずれかの処理を実行します。
 - "[SnapMirror保護関係を作成する](#)"。
 - "[SnapVault保護関係を作成する](#)"。
2. 関係のポリシーを作成する場合は、作成する関係タイプに応じて、次のいずれかの処理を実行します。
 - "[SnapVaultポリシーを作成する](#)"。
 - "[SnapMirrorポリシーを作成する](#)"。
3. "[SnapMirrorまたはSnapVaultスケジュールを作成する](#)"。

ワークフロー自動化とUnified Manager間の接続を構成する

OnCommand Workflow Automation (WFA) とUnified Managerの間にセキュアな接続を確立することができます。Workflow Automationに接続することで、SnapMirrorやSnapVaultの設定ワークフロー、SnapMirror関係の管理用コマンドなどの保護機能を使用できるようになります。

開始する前に

- Workflow Automationのバージョンが5.1.1P6以降である必要があります。



「Clustered Data ONTAP を管理するための WFA パック」は WFA 5.1.1P6 に含まれているため、従来のように NetAppStorage Automation Store からこのパックをダウンロードして WFA サーバーに個別にインストールする必要はありません。 ["WFA pack for managing ONTAP"](#)

- 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、全般 > ワークフロー自動化 をクリックします。
2. *ワークフロー自動化ページ*の*データベース ユーザー*領域で、Unified Manager とワークフロー自動化の接続をサポートするために作成したデータベース ユーザーの名前を選択し、パスワードを入力します。
3. ページの ワークフロー自動化資格情報 領域に、ワークフロー自動化セットアップのホスト名または IP アドレス (IPv4 または IPv6)、およびユーザー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*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. 「はい」 をクリックして Web UI を再読み込みし、ワークフロー自動化機能を追加します。

関連情報

["NetAppのマニュアル：OnCommand Workflow Automation（現在のリリース）"](#)

ワークフロー自動化における**Unified Manager**データソースのキャッシュを確認する

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作業を実行して、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。

開始する前に

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. ワークフロー自動化 UI から、実行 > データ ソース 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. 収集が正常に実行されてエラーが発生しないことを確認します。

Workflow AutomationをUnified Managerに統合するためには、収集エラーを解決する必要があります。

OnCommand Workflow Automationの再インストールまたはアップグレードの実行時の動作

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、まずOnCommand Workflow Automationと Unified Manager 間の接続を削除し、現在実行中またはスケジュールされているすべてのOnCommand Workflow Automationジョブが停止し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後は、Unified Manager との接続を再度設定する必要があります。

Unified Manager から**OnCommand Workflow Automation**セットアップを削除します。

OnCommand Workflow Automationが不要となった場合は、Unified ManagerからWorkflow Automationのセットアップを削除できます。

開始する前に

アプリケーショ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、左側の設定メニューの 一般 > ワークフロー自動化 をクリックします。
2. *ワークフロー自動化*ページで、*セットアップの削除*をクリックします。

保護関係のフェイルオーバーとフェイルバックを実行する

ハードウェア障害や災害が原因で保護関係のソース ボリュームが無効になっている場合は、Unified Managerの保護関係機能を使用して、保護デスティネーションに読み取り / 書き込みアクセスを設定し、ソースが再びオンラインになるまでそのボリュームにフェイルオーバーすることができます。さらに、元のソースがデータを提供できるようになった時点で、ソースにフェイルバックすることができます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- この処理を実行するには、OnCommand Workflow Automationをセットアップしておく必要があります。

手順

1. "[SnapMirror関係の解除](#)".

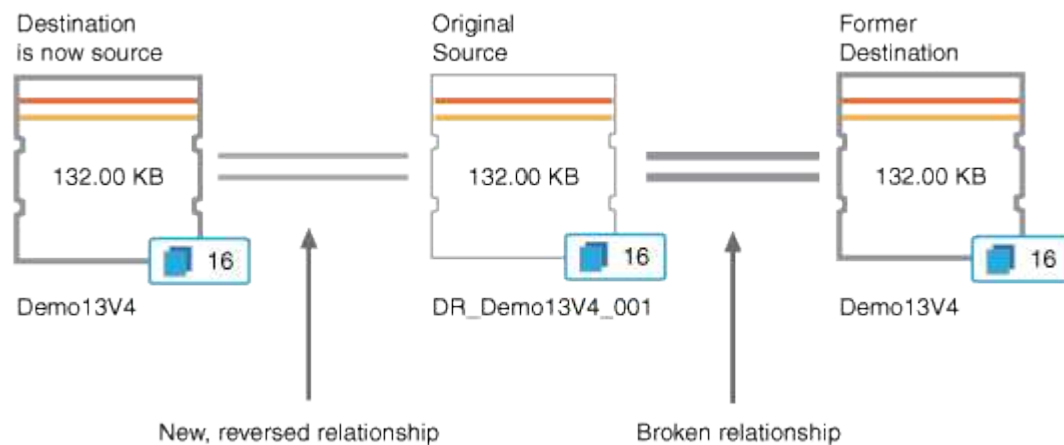
デスティネーションをデータ保護ボリュームから読み取り / 書き込みボリュームに変換する前、および関

係を反転する前に、関係を解除する必要があります。

2. "保護関係を逆転させる"。

元のソース ボリュームが再び使用可能になったら、ソース ボリュームをリストアして元の保護関係を再確立できます。ソースをリストアする前に、以前のデスティネーションに書き込まれたデータとソースを同期させる必要があります。逆再同期処理を使用して新しい保護関係を作成するには、元の関係のロールを反転し、ソース ボリュームと以前のデスティネーションを同期させます。新しい関係に対して新しいベースラインSnapshotコピーが作成されます。

反転関係は、カスケード関係に似ています。



3. "逆SnapMirror関係を解除する"。

元のソース ボリュームが再同期され、再びデータを提供できるようになったら、解除処理を使用して反転関係を解除します。

4. "関係を削除する"。

反転関係が不要になったときは、元の関係を再確立する前に反転関係を削除する必要があります。

5. "関係を再同期する"。

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/ヘルスの詳細ページから**SnapMirror**関係を解除する

[ボリューム / 健全性の詳細]ページで保護関係を解除することで、SnapMirror関係にあるソース ボリュームとデスティネーション ボリュームの間のデータ転送を停止することができます。関係の解除は、データを移行する場合のほか、ディザスタ リカバリやアプリケーションのテストなどの目的で行うことがあります。デスティネーション ボリュームは読み書き可能ボリュームに変わります。SnapVault関係を解除することはできません。

開始する前に

- アプリケーショ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*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. 宛先を右クリックし、メニューから [Break] を選択します。

[関係の解除]ダイアログ ボックスが表示されます。

3. 関係を解除するには、[続行] をクリックします。
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/ヘルスの詳細ページから保護関係を反転する

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。

開始する前に

- アプリケーショ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関係については実行できません。
- 保護関係がすでに存在している必要があります。
- 保護関係が解除されている必要があります。
- ソースとデスティネーションの両方がオンラインになっている必要があります。
- ソースが別のデータ保護ボリュームのデスティネーションになっている場合は実行できません。
- このタスクを実行すると、共通のSnapshotコピーのデータよりも新しいソースのデータは削除されます。
- 逆再同期した関係に対して作成されるポリシーとスケジュールは、元の保護関係と同じになります。

ポリシーとスケジュールが存在しない場合は作成されます。

手順

1. *ボリューム/ヘルス*詳細ページの*保護*タブから、ソースと宛先を逆にするSnapMirror関係をトポロジ内で見つけて、右クリックします。
2. メニューから*逆再同期*を選択します。

[逆再同期]ダイアログ ボックスが表示されます。

3. *[逆再同期] ダイアログ ボックスに表示されている関係が、逆再同期操作を実行する関係であることを確認し、[送信] をクリックします。

[逆再同期]ダイアログ ボックスが閉じて、[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: 各逆再同期ジョブのステータスを追跡するには、*ボリューム/ヘルス*詳細ページで*ジョブの

表示*をクリックします。

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、ボリューム/健全性 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/ヘルスの詳細ページから保護関係を削除します

保護関係を削除すると、選択したソースとデスティネーションの間の既存の関係を完全に削除することができます。これは、たとえば別のデスティネーションを使用して関係を作成する場合などに行います。この処理ではすべてのメタデータが削除され、元に戻すことはできません。

開始する前に

- アプリケーショ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*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. 宛先の名前を右クリックし、メニューから*削除*を選択します。

[関係の削除]ダイアログ ボックスが表示されます。

3. 関係を削除するには、[続行] をクリックします。

関係が[ボリューム / 健全性の詳細]ページから削除されます。

ボリューム/ヘルスの詳細ページから保護関係を再同期します

SnapMirror関係やSnapVault関係を解除してデスティネーションが読み書き可能になったあとに、ソースのデータとデスティネーションのデータが一致するようにデータを再同期することができます。再同期は、必要な共通のSnapshotコピーがソース ボリュームで削除されたためにSnapMirrorやSnapVaultの更新が失敗する場合にも実行することがあります。

開始する前に

- アプリケーショ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*詳細ページの*保護*タブから、トポロジ内で再同期する保護関係を見つけて右クリックします。
2. メニューから*再同期*を選択します。

または、[アクション] メニューから [関係] > [再同期] を選択して、現在詳細を表示している関係を再同期します。

[再同期]ダイアログ ボックスが表示されます。

3. *再同期オプション*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 スナップショット コピー をクリックし、スナップショット 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. デフォルトのスナップショット コピーを転送するのではなく、既存のスナップショット コピーを指定する場合は、[既存のスナップショット コピー] をクリックし、リストからスナップショット コピーを選択します。
6. *送信*をクリックします。

[再同期]ダイアログ ボックスに戻ります。

7. 再同期するソースを複数選択した場合は、既存のスナップショット コピーを指定する次のソースに対して [デフォルト] をクリックします。
8. 再同期ジョブを開始するには、[送信] をクリックします。

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: 各再同期ジョブのステータスを追跡するには、[ボリューム/ヘルスの詳細] ページで [ジョブの表示] をクリックします。

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、ボリューム/健全性 の詳細ページに戻ります。

すべてのタスクが正常に完了すれば再同期ジョブは終了です。

保護ジョブの失敗を解決する

このワークフローでは、Unified Managerのダッシュボードで保護ジョブの失敗を特定して解決する方法の例を示します。

開始する前に

このワークフローの一部のタスクは、管理者ロールでのログインを必要とするため、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「ジョブ停止」インシデントが表示されており、ボリュームで「保護ジョブ失敗」エラーが発生したことがわかります。このエラーを調べて、考えられる原因と解決策を特定します。

手順

1. ダッシュボードの未解決のインシデントとリスク領域の保護インシデント パネルで、保護ジョブが失敗しました 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次の形式で書かれています object_name:/object_name - Error Name、のような cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed。

失敗した保護ジョブの[イベントの詳細]ページが表示されます。

2. 概要 領域の [原因] フィールドにあるエラー メッセージを確認して、問題を特定し、考えられる修正アクションを評価します。

見る["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"](#)。

問題を特定し、失敗した保護ジョブの修正アクションを実行します

ジョブの失敗に関するエラー メッセージを[イベントの詳細]ページの[原因]フィールドで確認し、ジョブが失敗した原因がSnapshotコピー エラーであることを特定します。次に、[ボリューム / 健全性の詳細]ページに移動して詳細情報を収集します。

開始する前に

アプリケーション管理者のロールが必要です。

[イベントの詳細]ページの[原因]フィールドに表示されるエラー メッセージには、失敗したジョブに関する次のテキストが記載されています。

```
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
```

このメッセージから得られる情報は次のとおりです。

- 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なかった。

このジョブにはソースボリューム間の保護関係が含まれていました cluster2_src_vol2`仮想サーバー上 `cluster2_src_svm`宛先ボリューム `managed_svc2_vol3`仮想サーバー上の `cluster3_dst_svm`。

- スナップショットコピージョブが失敗しました 0426cluster2_src_vol2snap`ソースボリューム上 `cluster2_src_svm:/cluster2_src_vol2`。

このシナリオでは、ジョブが失敗した原因と考えられる対処策を特定できます。ただし、失敗を解決するには、System Manager Web UIまたはONTAP CLIコマンドを使用する必要があります。

手順

1. エラー メッセージを確認し、ソース ボリュームでSnapshotコピー ジョブが失敗していることから、おそらくソース ボリュームに問題があると判断します。

オプションで、エラー メッセージの最後にある ジョブの詳細 リンクをクリックすることもできますが、このシナリオでは、それを行わないことを選択します。

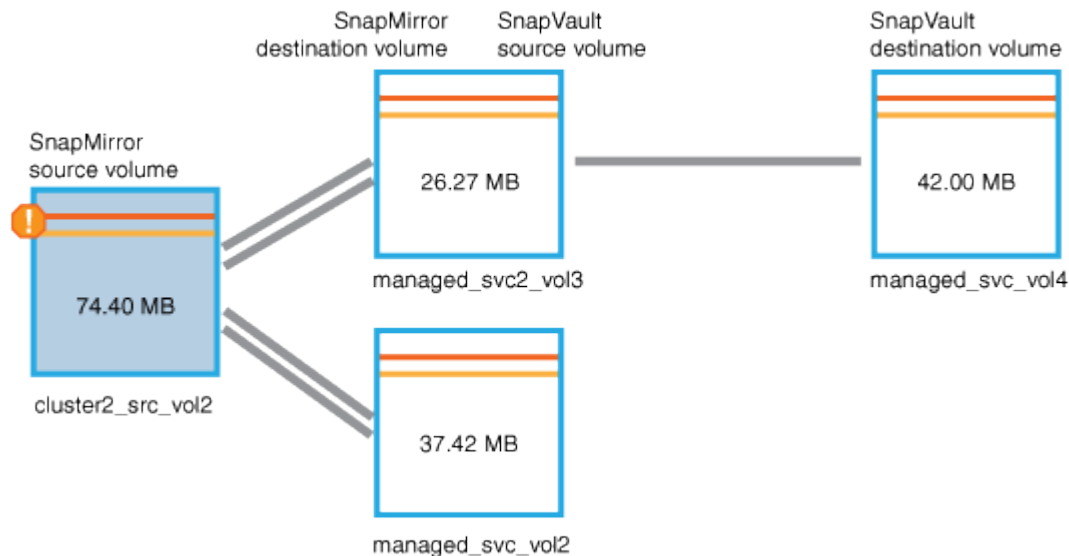
2. イベントを解決するために、次の作業を行います。
 - a. **【割り当て先】** ボタンをクリックし、メニューから **【自分】** を選択します。
 - b. イベントにアラートが設定されている場合は、アラート通知を繰り返し受信しないように、**【確認】** ボタンをクリックします。
 - c. 必要に応じて、イベントに関するメモを追加することもできます。
3. ソース ボリュームの詳細を表示するには、**【概要】** ペインの **【ソース】** フィールドをクリックします。

ソース フィールドには、ソース オブジェクトの名前が含まれます。この場合は、スナップショット コピー ジョブがスケジュールされたボリュームです。

ボリューム/健全性の詳細ページには、cluster2_src_vol2、保護タブの内容を表示します。

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。

また、そのボリュームに設定されている警告とエラーのしきい値を示す水平のバーが、ソース ボリューム アイコンに表示されています。



5. エラー アイコンにカーソルを合わせると、ポップアップ ダイアログが開いてしきい値の設定が表示され、ボリュームがエラーしきい値を超えて容量の問題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` 表示されます。
7. 容量 パネルの棒グラフにエラー アイコンが表示されています。これも、ボリューム容量がボリュームに設定されたしきい値レベルを超えたことを示しています。
8. 容量グラフの下には、ボリュームの自動拡張が無効になっていることと、ボリュームのスペース ガ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. イベント リストまで下にスクロールすると、保護ジョブの失敗、ボリュームがいっぱいになるまでの日数、ボリューム領域がいっぱいのイベントが生成されていることがわかります。
10. イベント リストで、ボリューム スペースがいっぱい イベントをクリックして詳細情報を取得し、このイベントが容量の問題に最も関連していると判断しました。

[イベントの詳細]ページには、ソース ボリュームに対して「ボリューム スペースがフル」イベントが表示されています。

11. 概要 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[推奨される対処方法]に、推奨される対処策が表示されます。



[推奨される対処方法]は一部のイベントだけに表示されるため、どのタイプのイベントでもこの領域が表示されるわけではありません。

「ボリューム スペースがフル」イベントを解決するために実施する推奨対処策をクリックしていきます。

- このボリュームの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します。
 - このボリュームで圧縮を有効にして実行します。
13. ボリュームの自動拡張を有効にすることにしたのですが、これを行うには、親アグリゲート上の空きスペースと現在のボリューム増加率を確認する必要があります。
 - a. 親集計を見てください。cluster2_src_aggr1 関連デバイス ペインで。



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情報を参照できます。

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. ページ上部に重要なインシデントを示すアイコンが表示されるので、アイコンの下テキストを確認します。

「完了までの日数: 1 日未満 | 1 日あたりの増加率: 5.4%」であると判断します。

14. システムマネージャに移動するか、ONTAP CLIにアクセスして有効にします。`volume autogrow`オプション。



ボリュームとアグリゲートの名前をメモしておいて、自動拡張を有効にするときに参照できるようにします。

15. 容量の問題を解決したら、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してマークします。

遅延問題を解決する

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[ダッシュボード]ページにアクセスして保護関係に問題がないかどうかを確認し、問題がある場合は解決策を探します。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

[ダッシュボード]ページで、[未解決のインシデントとリスク]領域を参照すると、[保護]ペインの[保護のリスク]の下にSnapMirror遅延エラーが表示されています。

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見つけてクリックします。

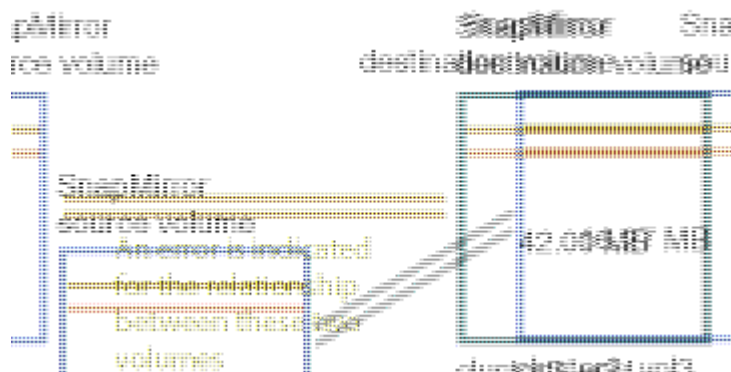
遅延エラー イベントの[イベントの詳細]ページが表示されます。

2. *イベント*の詳細ページから、次の 1 つ以上のタスクを実行できます。
 - 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、推奨される修正アクションがあるかどうかを確認します。
 - ボリュームの詳細を取得するには、[概要] 領域の [ソース] フィールドでオブジェクト名 (この場合はボリューム) をクリックします。
 - このイベントに関して追加されたメモを確認します。
 - イベントにメモを追加します。
 - イベントを特定のユーザに割り当てます。
 - イベントに応答するか、またはイベントを解決します。
3. このシナリオでは、*概要*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) をクリックして、ボリュームの詳細を取得します。

[ボリューム / 健全性の詳細]ページの[保護]タブが表示されます。

4. *保護*タブでは、トポロジ図を確認します。

3つのボリュームで構成されるSnapMirrorカスケードの最後のボリュームで遅延エラーが発生していることがわかりました。選択したボリュームがダークグレーの線で囲まれます。ソース ボリュームから延びるオレンジ色の二重線は、SnapMirror関係のエラーを示しています。



5. SnapMirrorカスケード内の各ボリュームをクリックします。

別のボリュームを選択すると、[Summary]、[Topology]、[History]、[Events]、[Related Devices]、[Related Alerts]の各領域に表示される保護情報が、そのボリュームに関連する詳細情報に変わります。

6. *概要*領域を確認し、各ボリュームの*更新スケジュール*フィールドの情報アイコンの上にカーソルを置きます。

このシナリオでは、SnapMirrorポリシーがDPDefaultであり、SnapMirrorスケジュールが毎時5分に更新されます。関係内のすべてのボリュームが同時にSnapMirror転送を試行することがわかりました。

7. 遅延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の2つのスケジュールを変更して、ソースが転送を完了してから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実行できます。

SnapMirror処理には、2つのレプリケーション タイプがあります。

- 非同期

プライマリ ボリュームからセカンダリ ボリュームへのレプリケーションがスケジュールに従って実行されます。

- 同期

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レプリケーションが実行されます。

保護ジョブは、10件までであれば、パフォーマンスに影響を及ぼすことなく同時に実行できます。11～30件のジョブを同時に実行すると、パフォーマンスが低下することがあります。30件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。

ボリューム保護ステータスの表示

[データ保護]ページには、データセンター内の1つまたはすべてのクラスタについて、保護対象のすべてのボリュームに関するデータ保護の詳細がまとめて表示されます。

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. 監視対象のすべてのクラスターのデータ保護ステータスを表示するか、単一のクラスターのデータ保護ステータスを表示するかに応じて、ドロップダウン メニューから [すべてのクラスター] を選択するか、単一のクラスターを選択します。
3. [データ保護]パネル上部の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。

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どちらを選択したかに応じて、このページには、SnapshotコピーまたはSnapMirrorポリシーで保護されているボリュームのデータ保護ステータス、およ

び保護されていないボリュームの数が表示されます。

個別のクラスター リストからクラスターを選択すると、そのクラスター内の保護されたボリュームのスナップショット保護とSnapMirror関係のステータスが表示されます。

このページでイベントをクリックすると、[イベントの詳細]ページが表示されます。*すべて表示*リンクをクリックすると、イベント管理インベントリ ページでアクティブな保護イベントをすべて表示できます。カーソルを合わせると、それぞれの数と凡例を確認できます。次のいずれかをクリックできます。

- Snapshotコピーで保護されていないボリュームおよびされているボリュームの棒グラフをクリックすると、[ボリューム]ページに移動して詳細を確認できます。
- すべての関係の棒グラフをクリックすると、ソース クラスターに基づいてフィルタされた詳細が[関係]ページに表示されます。

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

スナップショット コピーの概要: 次のようなスナップショット コピーによって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ボリュームと保護されていないボリュームの総数。
- Snapshotコピーのリザーブ スペースを使用している、または超えているボリュームの総数。

スナップショット コピー分析 には次の情報が詳細に表示されます。

- 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など）。
- 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なグラフ。
- Snapshotコピーのリザーブ スペースを使用している、使用していない、および超えているボリューム。
- Snapshotコピーの数に基づくボリューム数の内訳。

Snapshotコピーに関する注意事項

- Snapshotコピーで保護されているボリューム数には、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カウントされます。
- Snapshotコピーの数が返されるのは、オンラインかつ使用可能なボリュームのみです。
- Snapshotコピー数のグラフの範囲はそのつど変化します。このグラフは、選択したクラスター内のSnapshotの数に基づいて生成されます。
- ボリュームが保護対象とみなされるためには、ボリュームのSnapshotコピー スケジュールが有効になっている必要があります。
- Snapshotコピーのリザーブ スペースの値は、使用済みのディスク スペースを確認したり、1つ以上のSnapshotコピーが削除された場合に再利用可能なスペースを計算したりする際に重要となります。

SnapMirror関係の保護ステータスの表示

- SnapMirrorの概要*: 次のようなSnapMirrorポリシーによって保護されているボリュームの概要。
- ボリュームSnapMirror関係、Storage VMディザスタ リカバリ（SVM-DR）、およびこの2つの組み合わせなど、該当するSnapMirrorポリシーで保護されているボリュームの数。
- 目標復旧時点（RPO）の遅延が発生しているSnapMirror関係の総数（遅延ステータスに基づく）。

- SnapMirror分析* では次の情報が詳細に表示されます。
- SnapMirror関係に対して発生した個々のイベント（過去24時間に生成されたイベントなど）。
- それぞれのタイプのSnapMirrorポリシーで保護されているボリュームの数。
- 非同期ミラー、非同期バックアップ、非同期ミラー バックアップ、StrictSync、SnapMirrorアクティブ同期整合性グループ、同期など、各SnapMirror関係タイプで保護されている関係の数。
- 健全な関係と健全でない関係の数。
- ボリューム関係の数の内訳。RPOの遅延時間とステータスで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（）をクリックして、ラグしきい値設定を構成します。詳細については、["管理対象外の保護関係の遅延しきい値の設定"](#)。

SnapMirror関係に関する注意事項

- SnapMirror関係の数には、読み取りと書き込みが有効なソース ボリュームがカウントされます。デスティネーション ボリュームとルート ボリュームはカウントされません。
- SnapMirror関係の場合、ソース クラスタのイベントが表示されます。
- SnapMirror関係の数には、ソースとデスティネーションが同じクラスタまたは異なるクラスタにあるボリュームの数が含まれます。
- データ レプリケーションにおけるRPOの遅延時間は、SnapMirror関係に基づいています。ステータスは次のように分類されます ok、warning、または`error`設定された関係しきい値に基づきます。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、または問題に対処する必要があるかを判断できます。
- ボリュームに複数のSnapMirror関係が設定されている場合、RPO遅延は各関係タイプごとにカウントされます。
- ソースとデスティネーションの間でデータ レプリケーションに問題がある場合（関係が解除された場合など）、ボリューム関係は健全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の表示

データ保護 ページの * MetroCluster保護* パネルには、サイトでMetroCluster over FC または IP 構成によって保護されているクラスターと保護されていないクラスターの数が表示されます。このパネルの棒グラフをクリックすると[クラスタ]ページが開き、保護されているクラスタまたは保護されていないクラスタの詳細がフィルタされます。MetroCluster構成の監視の詳細については、以下を参照してください。["MetroCluster構成の監視"](#)。

ボリューム保護関係の表示

「関係: すべての関係」ビューおよび「ボリューム関係」ページから、既存のボリューム SnapMirrorおよびSnapVault関係のステータスを表示できます。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。

開始する前に

アプリケーショ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、ストレージ > ボリューム をクリックします。
2. [表示] メニューから、[リレーションシップ] > [すべてのリレーションシップ] 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最新情報を表示するには、デフォルトの「すべての関係」ページのままとします。
- 一定期間にわたる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 か月間の転送ステータス ビュー] を選択します。
- 日ごとのボリューム転送アクティビティ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 か月の転送率ビュー] 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のLUNを監視する

ONTAP環境で、LUN を含むアプリケーションを保護するためにSnapMirror Active Sync がサポートされている場合は、Active IQ Unified Managerでそれらの LUN を表示および監視できます。

SnapMirrorアクティブ同期は、SAN環境でフェイルオーバー時の目標復旧時間（RTO）ゼロを実現します。SnapMirrorアクティブ同期をサポートする一般的な環境では、ボリューム上のLUNが整合性グループ関係で保護されます。

これらのプライマリLUNとセカンダリLUNは、複合LUN（UUIDとシリアル番号が同じレプリカLUNのペア）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を表示するためには、整合性グループ関係に含まれるLUNを使用するプライマリ クラスタとセカンダリ クラスタの両方を、Unified Managerに追加して検出しておく必要があります。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、以下を参照してください。"[ONTAP 9 SnapMirror Active Sync \(旧SM-BC\) のドキュメント](#)"。

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、ストレージ > **LUN** 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。

「関係: すべての LUN」ビューが表示されます。

LUNの名前、ボリューム、LUNをホストしているStorage VM、クラスタ、整合性グループ、パートナーLUNなど、LUNの詳細を確認できます。これらの各コンポーネントをクリックすると、詳細ビューにドリルダウンできます。整合性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について、[SVMの詳細]ページの[SAN]タブで設定の詳細を確認できます。パートナーLUNのイニシエータやイニシエータグループなどの情報が表示されます。

環境内の保護対象のLUNのレポートをソート、フィルタ、生成、およびアップロードするためのグリッドレベルの標準機能を実行できます。

ヘルス: すべてのボリュームビューから**SnapVault**保護関係を作成します

「ヘルス: すべてのボリューム」ビューを使用して、同じストレージ VM 上の 1 つ以上のボリュームに対してSnapVault関係を作成し、保護目的でデータのバックアップを有効にすることができます。

開始する前に

- アプリケーショ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。

次の場合には、「保護」メニューは表示されません。

- この処理がRBACの設定で許可されていない場合：オペレータの権限しかない場合など
- ボリュームIDが不明な場合：クラスタ間関係が確立されているがデスティネーション クラスタが検出されていない場合など

手順

1. 左側のナビゲーション ペインで、ストレージ > ボリューム 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、同じストレージ仮想マシン (SVM) 上に複数の保護関係を作成するには、[健全性: すべてのボリューム] ビューで 1 つ以上のボリュームを選択し、ツールバーの [保護] をクリックします。

3. メニューから * SnapVault*を選択します。

[保護設定]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 ボリューム情報を構成します。
5. 詳細 をクリックして、必要に応じて重複排除、圧縮、自動拡張、およびスペース保証を設定し、適用 をクリックします。
6. * SnapVault* タブの * 宛先情報 * 領域と * 関係設定 * 領域を入力します。
7. *適用*をクリックします。

「健全性: すべてのボリューム」ビューに戻ります。

8. 健全性: すべてのボリューム ビューの上部にある保護構成ジョブ リンクをクリックします。

保護関係を1つだけ作成している場合は[ジョブの詳細]ページが表示されますが、複数の保護関係を作成している場合は、保護処理に関連するすべてのジョブがリストに表示されます。

9. 次のいずれかを実行します。

- ジョブが1つしかない場合は、[更新] をクリックして、保護構成ジョブに関連付けられているタスクリストとタスクの詳細を更新し、ジョブがいつ完了したかを確認します。
- ジョブが複数ある場合は、次の手順を実行します。
 - i. ジョブのリスト内のジョブをクリックします。
 - ii. 更新 をクリックすると、保護構成ジョブに関連付けられたタスク リストとタスクの詳細が更新され、ジョブが完了したかどうかを確認できます。
 - 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/ヘルスの詳細ページから**SnapVault**保護関係を作成します

ボリュームでデータ バックアップを有効にしてデータを保護するために、[ボリューム / 健全性の詳細]ページを使用してSnapVault関係を作成することができます。

開始する前に

- アプリケーショ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。

次の場合には、「保護」メニューは表示されません。

- この処理がRBACの設定で許可されていない場合：オペレータの権限しかない場合など
- ボリュームIDが不明な場合：クラスタ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. *ボリューム/健全性*詳細ページの*保護*タブで、トポロジ ビューで保護するボリュームを右クリックします。
2. メニューから*保護* > * SnapVault*を選択します。

[保護設定]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 リソース情報を構成します。
4. 詳細 をクリックして、必要に応じて重複排除、圧縮、自動拡張、およびスペース保証を設定し、適用 をクリックします。
5. 保護の構成 ダイアログボックスの 宛先情報 領域と 関係設定 領域を入力します。
6. *適用*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. *ボリューム/ヘルス*詳細ページの上部にある保護構成ジョブ リンクをクリックします。

[ジョブの詳細]ページが表示されます。

8. 更新 をクリックすると、保護構成ジョブに関連付けられたタスク リストとタスクの詳細が更新され、ジョブが完了したかどうかを確認できます。

ジョブのタスクが完了すると、新しい関係が[ボリューム / 健全性の詳細]ページのトポロジ ビューに表示されます。

ヘルス: すべてのボリュームビューから**SnapMirror**保護関係を作成します。

「ヘルス: すべてのボリューム」ビューを使用すると、同じストレージ VM 上の複数のボリュームを選択して、一度に複数のSnapMirror保護関係を作成できます。

開始する前に

- アプリケーショ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。

次の場合には、「保護」メニューは表示されません。

- この処理がRBACの設定で許可されていない場合：オペレータの権限しかない場合など
- ボリュームIDが不明な場合：クラスタ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. 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ます。

あるいは、同じ SVM 上に複数の保護関係を作成するには、[健全性: すべてのボリューム] ビューで 1 つ以上のボリュームを選択し、ツールバーの [保護] > [SnapMirror] をクリックします。

[保護設定]ダイアログ ボックスが表示されます。

2. * SnapMirror* をクリックして * SnapMirror* タブを表示し、宛先情報を設定します。
3. 必要に応じて、[詳細] をクリックしてスペース保証を設定し、[適用] をクリックします。
4. * SnapMirror* タブの * 宛先情報 * 領域と * 関係設定 * 領域を入力します。
5. *適用*をクリックします。

「健全性: すべてのボリューム」ビューに戻ります。

6. * 「健全性: すべてのボリューム」ビュー*の上部にある保護構成ジョブ リンクをクリックします。

保護関係を1つだけ作成する場合は、[ジョブの詳細]ページが表示されます。しかし、複数の保護関係を作成する場合は、保護処理に関連付けられているすべてのジョブのリストが表示されます。

7. 次のいずれかを実行します。

- ジョブが1つしかない場合は、[更新] をクリックして、保護構成ジョブに関連付けられているタスク リストとタスクの詳細を更新し、ジョブがいつ完了したかを確認します。
- ジョブが複数ある場合は、次の手順を実行します。
 - i. ジョブのリスト内のジョブをクリックします。

- ii. 更新 をクリックすると、保護構成ジョブに関連付けられたタスク リストとタスクの詳細が更新され、ジョブが完了したかどうかを確認できます。
- iii. フィルタリングされたリストに戻り、別のジョブを表示するには、[戻る] ボタンを使用します。

設定で指定したデスティネーションSVMと詳細設定で有効にしたオプションに応じて、次のいずれかのSnapMirror関係が作成されます。

- ソース ボリュームと同じかそれよりも新しいバージョンのONTAPで実行されているデスティネーションSVMを指定した場合、デフォルトではブロック レプリケーション ベースのSnapMirror関係が作成されます。
- ソース ボリュームと同じかそれよりも新しいバージョンのONTAPで実行されているデスティネーションSVMを指定し、詳細設定でバージョンに依存しないレプリケーションを有効にした場合、バージョンに依存しないレプリケーションに対応したSnapMirror関係が作成されます。
- ソース ボリュームよりも前のバージョンのONTAPで実行されているデスティネーションSVMを指定した場合、以前のバージョンでバージョンに依存しないレプリケーションがサポートされていれば、バージョンに依存しないレプリケーションに対応したSnapMirror関係が自動で作成されます。

ボリューム/ヘルスの詳細ページから**SnapMirror**保護関係を作成します。

データ レプリケーションを有効にしてデータを保護するために、[ボリューム / 健全性の詳細]ページを使用してSnapMirror関係を作成することができます。SnapMirrorレプリケーションを使用すると、ソースでデータ損失が発生した場合にデスティネーション ボリュームからデータをリストアできます。

開始する前に

- アプリケーショ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。

次の場合には、「保護」メニューは表示されません。

- この処理がRBACの設定で許可されていない場合：オペレータの権限しかない場合など
- ボリュームIDが不明な場合：クラスタ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

保護ジョブは、10件までであれば、パフォーマンスに影響を及ぼすことなく同時に実行できます。11～30件のジョブを同時に実行すると、パフォーマンスが低下することがあります。30件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. *ボリューム/健全性*詳細ページの*保護タブ*で、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ます。
2. メニューから*保護* > * SnapMirror*を選択します。

[保護設定]ダイアログ ボックスが表示されます。

3. * SnapMirror* をクリックして * SnapMirror* タブを表示し、宛先情報を設定します。
4. 必要に応じて、[詳細] をクリックしてスペース保証を設定し、[適用] をクリックします。

5. 保護の構成 ダイアログボックスの 宛先情報 領域と 関係設定 領域を入力します。

6. *適用*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. *ボリューム/ヘルス*詳細ページの上部にある保護構成ジョブ リンクをクリックします。

ジョブのタスクと詳細が[ジョブの詳細]ページに表示されます。

8. *ジョブ*の詳細ページで、*更新*をクリックして、保護構成ジョブに関連付けられているタスク リストとタスクの詳細を更新し、ジョブが完了するタイミングを確認します。

9. ジョブ タスクが完了したら、ブラウザの [戻る] をクリックして [ボリューム/ヘルス] の詳細ページに戻ります。

新しい関係が[ボリューム / 健全性の詳細]ページのトポロジ ビューに表示されます。

設定で指定したデスティネーションSVMと詳細設定で有効にしたオプションに応じて、次のいずれかのSnapMirror関係が作成されます。

- ソース ボリュームと同じかそれよりも新しいバージョンのONTAPで実行されているデスティネーションSVMを指定した場合、デフォルトではブロック レプリケーション ベースのSnapMirror関係が作成されます。
- ソース ボリュームと同じかそれよりも新しいバージョンのONTAPで実行されているデスティネーションSVMを指定し、詳細設定でバージョンに依存しないレプリケーションを有効にした場合、バージョンに依存しないレプリケーションに対応したSnapMirror関係が作成されます。
- ONTAPの以前のバージョン、またはソース ボリュームよりも新しいバージョンで実行されているデスティネーションSVMを指定した場合、以前のバージョンで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に対応したSnapMirror関係が自動で作成されます。

バージョンに柔軟性のあるレプリケーションで**SnapMirror**関係を作成する

バージョンに依存しないレプリケーションを使用してSnapMirror関係を作成できます。バージョンに依存しないレプリケーションを使用すると、ソース ボリュームとデスティネーション ボリュームが別のバージョンのONTAPで実行されている場合でも、SnapMirror保護を実装できます。

開始する前に

- アプリケーショ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同じバージョンのONTAPで実行されていない混在型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の場合、ミラー処理は従来型のブロック レプリケーションによるSnapMirrorほど高速ではありません。

手順

1. 保護するボリュームの*保護の構成*ダイアログ ボックスを表示します。
 - ボリューム/ヘルス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があるトポロジ 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。
 - [健全性: 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見つけて右クリックし、メニューから [保護] > [SnapMirror] を選択します。[保護設定]ダイアログ ボックスが表示されます。
2. * SnapMirror* をクリックすると、 * SnapMirror* タブが表示されます。
3. 保護の構成 ダイアログボックスの 宛先情報 領域と 関係設定 領域を入力します。

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、そ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で実行されるデスティネーション SVM を指定しても、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を設定する場合は、[詳細] 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*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. *ボリューム/ヘルス*詳細ページの上部にある保護構成ジョブ リンクをクリックします。

ジョブのタスクと詳細が[ジョブの詳細]ページに表示されます。

7. *ジョブ*の詳細ページで、*更新*をクリックして、保護構成ジョブに関連付けられているタスク リストとタスクの詳細を更新し、ジョブが完了するタイミングを確認します。
8. ジョブ タスクが完了したら、ブラウザの [戻る] をクリックして [ボリューム/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。

バックアップ オプションを備えたバージョンに柔軟なレプリケーションで**SnapMirror**関係を作成する

バージョンに依存しないレプリケーションとバックアップ オプション機能を使用してSnapMirror関係を作成できます。バックアップ オプション機能を使用すると、SnapMirror保護を実装できます。また、デスティネーションの場所でバックアップコピーの複数のバージョンを保持することもできます。

開始する前に

- アプリケーショ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、SnapMirrorディザスタ リカバリ機能（ボリュームのフェイルオーバーなど）によってデータを保護できます。同時に、SnapVault機能（複数のバックアップ コピーによる保護など）を提供することもできます。

手順

1. 保護するボリュームの*保護の構成*ダイアログ ボックスを表示します。
 - ボリューム/ヘルス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 保護 > * SnapMirror* を選択します。
 - [健全性: 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見つけて右クリックし、メニューから [保護] > [SnapMirror] を選択します。[保護設定]ダイアログ ボックスが表示されます。
2. * SnapMirror* をクリックすると、 * SnapMirror* タブが表示されます。
3. 保護の構成 ダイアログボックスの 宛先情報 領域と 関係設定 領域を入力します。
4. *詳細*をクリックすると、*詳細な宛先設定*ダイアログボックスが表示されます。
5. バージョンに柔軟なレプリケーション 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 ボックスをオンにし、[適用] をクリックします。
7. *適用*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. *ボリューム/ヘルス*詳細ページの上部にある保護構成ジョブ リンクをクリックします。

ジョブのタスクと詳細が[ジョブの詳細]ページに表示されます。

9. *ジョブ*の詳細ページで、*更新*をクリックして、保護構成ジョブに関連付けられているタスク リストとタスクの詳細を更新し、ジョブがいつ完了したかを確認します。
10. ジョブ タスクが完了したら、ブラウザの [戻る] をクリックして [ボリューム/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。

宛先効率設定を構成する

[詳細なデスティネーション設定]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に対する効率化設定（重複排除、圧縮、自動拡張、スペース ギャランティなど）を行うことができます。デスティネーションまたはセカンダリ ボリュームでスペースの利用率を最大限に高める場合にこれらの設定を使用します。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

デフォルトでは、効率化設定はソース ボリュームの設定に対応します。ただし、SnapVault関係の圧縮設定は例外で、この設定はデフォルトで無効になっています。

手順

1. 設定する関係のタイプに応じて、[保護の設定] ダイアログ ボックスで [SnapMirror] タブまたは [SnapVault] タブのいずれかをクリックします。
2. *宛先情報*領域で*詳細*をクリックします。

[詳細なデスティネーション設定]ダイアログ ボックスが開きます。

3. 必要に応じて、重複排除、圧縮、自動拡張、およびスペース ギャランティの効率化設定を有効または無効にします。
4. 適用 をクリックして選択内容を保存し、保護の構成 ダイアログボックスに戻ります。

SnapMirrorとSnapVaultのスケジュールを作成する

SnapMirrorおよびSnapVaultの基本または詳細スケジュールを作成して、ソース ボリュームまたはプライマリ ボリュームで自動データ保護転送を有効にすることができます。ボリュームでのデータ変更の頻度に応じて、転送の実行頻度を調整することができます。

開始する前に

- アプリケーショ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]領域に情報を入力しておく必要があります。
- 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. 保護の構成 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。

[スケジュールの作成]ダイアログ ボックスが表示されます。

2. スケジュール名 フィールドに、スケジュールに付ける名前を入力します。
3. 次のいずれかを選択します。

- 基本

間隔で指定する基本的なスケジュールを作成する場合に選択します。

- 高度な

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*をクリックします。

新しいスケジュールが[SnapMirrorスケジュール]または[SnapVaultスケジュール]のドロップダウン リストに表示されます。

既存の保護関係から保護を拡張するためにカスケードまたはファンアウト関係を作成します

既存の関係のソース ボリュームからのファンアウトまたはデスティネーション ボリュームからのカスケードを作成することで、既存の関係から保護を拡張できます。この処理は、1つのサイトから多数のサイトにデータをコピーする必要がある場合や、バックアップをさらに作成して追加の保護を提供する必要がある場合に実行します。

整合性グループ（複数のボリュームを保持するコンテナ）を使用して保護をボリュームに拡張することで、すべてのボリュームを1つのエンティティとして管理できます。Unified Managerの[Relationships]ページで、SnapMirrorアクティブ同期整合性グループと整合性グループの同期関係を確認できます。

開始する前に

- アプリケーショ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*をクリックします。または、[ボリュームの詳細]ページで関係を確認します。
2. *ボリューム関係*ページから、保護を拡張する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、宛先からカスケード関係を作成するかに応じて、[ソースから] または [宛先から] を選択します。
5. 作成する保護関係のタイプに応じて、「* SnapMirrorを使用*」または「* SnapVaultを使用*」のいずれかを選択します。

保護の構成 ダイアログ ボックスが表示されます。



この処理は、[関係 / ボリューム関係]と[ボリューム / 健全性の詳細]の統合ページから実行できます。

6. 保護の構成 ダイアログ ボックスに示されているように情報を入力します。

ボリューム関係ページから保護関係を編集する

既存の保護関係を編集して、最大転送速度、保護ポリシー、保護スケジュールを変更することができます。関係の編集は、転送に使用する帯域幅を制限したり、データが頻繁に変わるためにスケジュールされた転送の実行頻度を増やす場合などに行います。

開始する前に

アプリケーショ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 リレーションシップ ページで、ボリューム リストから、リレーションシップ設定を編集する同じ SVM 内の 1 つ以上の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***をクリックします。

選択した関係に変更内容が適用されます。

ボリューム/健全性の詳細ページから保護関係を編集する

既存の保護関係を編集して、現在の最大転送速度、保護ポリシー、保護スケジュールを変更することができます。関係の編集は、転送に使用する帯域幅を制限したり、データが頻繁に変わるためにスケジュールされた転送の実行頻度を増やす場合などに行います。

開始する前に

- アプリケーショ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をインストールして設定しておく必要があります。

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***詳細ページの***保護***タブから、トポロジ内で編集する保護関係を見つけ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] メニューから [関係] > [編集] 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 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***をクリックします。

選択した関係に変更内容が適用されます。

転送効率を最大化するために**SnapMirror**ポリシーを作成する

SnapMirrorポリシーを作成して、保護関係におけるSnapMirror転送の優先度を指定することができます。SnapMirrorポリシーで優先度を割り当てて、優先度が低い転送を通常の優先度の転送よりもあとに実行するようにスケジュールすることで、ソースからデスティネーションへの転送効率を最大化できます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automationのセットアップが完了している必要があります。
- このタスクでは、[保護設定]ダイアログ ボックスの[デスティネーション情報]領域に情報がすでに入力されていることを前提としています。

手順

1. 保護の構成 ダイアログボックスの * SnapMirror* 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。

[SnapMirror ポリシーの作成]ダイアログ ボックスが表示されます。

2. ポリシー名 フィールドに、ポリシーに付ける名前を入力します。
3. *転送優先度*フィールドで、ポリシーに割り当てる転送優先度を選択します。
4. コメント フィールドに、ポリシーに関するオプションのコメントを入力します。
5. *作成*をクリックします。

新しいポリシーが[SnapMirrorポリシー]ドロップダウン リストに表示されます。

転送効率を最大化するための**SnapVault**ポリシーを作成する

新しいSnapVaultポリシーを作成して、SnapVault転送の優先度を設定することができます。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。

開始する前に

- アプリケーショ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]領域に情報を入力しておく必要があります。

手順

1. 保護の構成 ダイアログボックスの * SnapVault* 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 フィールドに、ポリシーに関する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*をクリックします。

新しいポリシーが[Create Policy]ドロップダウン リストに表示されます。

ボリューム関係ページからアクティブなデータ保護転送を中止する

実行中のSnapMirrorレプリケーションを中止する場合、アクティブなデータ保護転送を中止することができます。ベースライン転送後の以降の転送については、再開チェックポイントを消去することも可能です。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。

開始する前に

- アプリケーショ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、以下に該当する場合は表示されません。

- この処理がRBACの設定で許可されていない場合：オペレータの権限しかない場合など
- ボリュームIDが不明な場合：クラスタ間関係が確立されているがデスティネーション クラスタが検出されていない場合など

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、ツールバーの [中止] をクリックします。

[転送の中止]ダイアログ ボックスが表示されます。

2. ベースライン転送ではない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. *続行*をクリックします。

[転送の中止]ダイアログ ボックスが閉じて、中止ジョブのステータスとジョブの詳細へのリンクが[ボリューム関係]ページの上部に表示されます。

4. オプション: [詳細を表示] リンクをクリックすると、ジョブ の詳細ページに移動し、追加の詳細やジョブの進行状況が表示されます。

ボリューム/ヘルス詳細ページからアクティブなデータ保護転送を中止します

実行中のSnapMirrorレプリケーションを中止する場合、アクティブなデータ保護転送を

中止することができます。ベースライン転送以外では、転送の再開チェックポイントを消去することも可能です。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。

開始する前に

- アプリケーショ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、以下に該当する場合は表示されません。

- この処理がRBACの設定で許可されていない場合：オペレータの権限しかない場合など
- ボリュームIDが不明な場合：クラスタ間関係が確立されているがデスティネーション クラスタが検出されていない場合など

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. *ボリューム/健全性*詳細ページの*保護*タブで、中止するデータ転送のトポロジビュー内の関係を右クリックし、*中止*を選択します。

[転送の中止]ダイアログ ボックスが表示されます。

2. ベースライン転送ではない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. *続行*をクリックします。

[転送の中止]ダイアログ ボックスが閉じて、中止処理のステータスとジョブの詳細へのリンクが[ボリューム / 健全性の詳細]ページの上部に表示されます。

4. オプション: [詳細を表示] リンクをクリックすると、ジョブ の詳細ページに移動し、追加の詳細やジョブの進行状況が表示されます。
5. ジョブの各タスクをクリックして詳細を確認します。
6. ブラウザの戻る矢印をクリックして、*ボリューム/健全性*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から保護関係を静止する

[ボリューム関係]ページでは、保護関係を休止してデータ転送を一時的に停止できます。関係の休止は、データベースを含むSnapMirrorデスティネーション ボリュームのSnapshotコピーを作成する場合に、Snapshotコピーの処理中にデータベース コンテンツの安定を確保する目的で行うことがあります。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automationのセットアップが完了している必要があります。

次の場合は休止操作が表示されません。

- RBACの設定で休止操作が許可されていない場合：オペレータの権限しかない場合など
- ボリュームIDが不明な場合：クラスタ間関係が確立されているがデスティネーション クラスタが検出されていない場合など
- Workflow AutomationとUnified Managerを連携させていない場合

手順

1. 1 つ以上の保護関係の転送を停止するには、[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、ツールバーの [停止] 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. *続行*をクリックします。

[ボリューム / 健全性の詳細]ページの上部に、休止ジョブのステータスがジョブの詳細へのリンクとともに表示されます。

3. *詳細を表示*リンクをクリックすると、*ジョブ*の詳細ページに移動し、追加の詳細とジョブの進行状況を確認できます。
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 リレーションシップ] 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/ヘルスの詳細ページから保護関係を休止する

保護関係を休止してデータ転送を一時的に停止できます。関係の休止は、データベースを含むSnapMirrorデスティネーション ボリュームのSnapshotコピーを作成する場合に、Snapshotコピーの実行中にデータベース コンテンツの安定を確保する目的で行うことがあります。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- Workflow Automationのセットアップが完了している必要があります。

次の場合は休止操作が表示されません。

- RBACの設定で許可されていない場合：オペレータの権限しかない場合など
- ボリュームIDが不明な場合：クラスタ間関係が確立されているがデスティネーション クラスタが検出されていない場合など
- Workflow AutomationとUnified Managerを連携させていない場合

手順

1. *ボリューム/健全性*詳細ページの*保護*タブで、停止する保護関係のトポロジ ビュー内の関係を右クリックします。
2. メニューから*静止*を選択します。
3. 続行するには、[はい] をクリックします。

[ボリューム / 健全性の詳細]ページの上部に、休止ジョブのステータスがジョブの詳細へのリンクとともに表示されます。

4. *詳細を表示*リンクをクリックすると、*ジョブ*の詳細ページに移動し、追加の詳細とジョブの進行状況を確認できます。
5. 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/健全性*の詳細ページに戻ります。

すべてのジョブ タスクが正常に完了すれば休止ジョブは終了です。

ボリューム関係ページからSnapMirror関係を解除する

保護関係を解除して、SnapMirror関係にあるソース ボリュームとデスティネーション ボリュームの間のデータ転送を停止することができます。関係の解除は、データを移行する場合のほか、ディザスタ リカバリやアプリケーションのテストなどの目的で行うことができます。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わります。SnapVault関係を解除することはできません。

開始する前に

- アプリケーショ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 リレーションシップ ページで、データ転送を停止する保護関係を持つ 1 つ以上のボリュームを選択し、ツールバーの 解除 をクリックします。

[関係の解除]ダイアログ ボックスが表示されます。

2. 関係を解除するには、[続行] をクリックします。
3. ボリューム リレーションシップ ページの リレーションシップの状態 列で、リレーションシップが解除されていることを確認します。

関係状態列はデフォルトでは非表示になっているため、表示/非表示列リストで選択する必要がある場合があります。 .

ボリューム関係ページから保護関係を削除します

[ボリューム関係]ページでは、保護関係を削除して、選択したソースとデスティネーションの間に存在する関係を完全に削除できます。この作業は、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。

開始する前に

- アプリケーショ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 リレーションシップ ページで、削除する保護関係を持つボリュームを 1 つ以上選択し、ツールバーの 削除 をクリックします。

[関係の削除]ダイアログ ボックスが表示されます。

2. 関係を削除するには、[続行] をクリックします。

関係が[ボリューム関係]ページから削除されます。

ボリューム関係ページから、休止関係でのスケジュールされた転送を再開します。

関係を静止してスケジュールされた転送を停止した後、**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 ボリューム上のデータが保護されるように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再開されます（チェックポイントが存在する場合はチェックポイントから）。

開始する前に

- アプリケーショ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. ボリューム 関係 ページで、静止関係を持つ 1 つ以上のボリュームを選択し、ツールバーの 再開 をクリックします。
2. *再開*ダイアログボックスで*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、その進行状況を追跡するには、ボリューム リレーションシップ ページの上部に表示されるジョブ 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、保護構成ジョブに関連付けられているタスク リストとタスクの詳細を更新し、ジョブがいつ完了したかを確認します。
 - 複数のジョブが表示される場合は、次の手順を実行します。
 - i. [ジョブ]ページで、詳細を表示するジョブをクリックします。
 - ii. ジョブの詳細ページで、[更新] をクリックして、保護構成ジョブに関連付けられているタスク リストとタスクの詳細を更新し、ジョブが完了するタイミングを確認します。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/ヘルスの詳細ページから、休止関係でのスケジュールされた転送を再開します。

関係を休止してスケジュールされた転送を停止した後、ボリューム/ヘルスの詳細ページで **再開** 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 ボリューム上のデータが保護されるように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再開されます（チェックポイントが存在する場合はチェックポイントから）。

開始する前に

- アプリケーショ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***詳細ページの***保護***タブで、再開する静止関係をトポロジ ビューで右クリックします。

または、[アクション]>[関係] メニューから [再開] を選択します。

2. ***再開***ダイアログボックスで***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、その進行状況を追跡するには、ボリューム/ヘルス 詳細ページの上部に表示されるジョブ 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、保護構成ジョブに関連付けられているタスク リストとタスクの詳細を更新し、ジョブが完了するタイミングを確認します。

ジョブが完了すると、次のスケジュールされた転送の実行時にデータ転送が再開されます。

ボリューム関係ページから保護関係を初期化または更新します

[ボリューム関係]ページでは、新しい保護関係で最初のベースライン転送を実行できます。また、すでに初期化された関係でスケジュールされていない増分更新を手動で実行してデータを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は初期化または更新できません。

開始する前に

- アプリケーショ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 リレーションシップ 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リレーションシップを持つ 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。

初期化/更新ダイアログ 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 スナップショット コピー をクリックし、スナップショット 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. デフォルトのスナップショット コピーを転送するのではなく、既存のスナップショット コピーを指定する場合は、[既存のスナップショット コピー] をクリックし、リストからスナップショット コピーを選択します。
5. *送信*をクリックします。

*初期化/更新*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、既存のスナップショット コピーを指定する次のソースに対して [デフォルト] をクリックします。
7. 初期化または更新ジョブを開始するには、[送信] をクリックします。

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: 各初期化ジョブまたは更新ジョブのステータスを追跡するには、[正常性: すべてのボリューム] ビューで [ジョブの表示] をクリックします。

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: 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 リレーションシップ] 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处理または更新処理は終了です。

ボリューム/ヘルスの詳細ページから保護関係を初期化または更新します

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できます。また、すでに初期化された関係でスケジュールされていない増分更新を手動で実行してデータをただちに転送する場合は、関係を更新できます。

注意: 整合性グループによって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。

開始する前に

- アプリケーショ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*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内で見つけて、右クリックします。
2. メニューから*初期化/更新*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]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 スナップショット コピー をクリックし、スナップショット 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. デフォルトのスナップショット コピーを転送するのではなく、既存のスナップショット コピーを指定する場合は、[既存のスナップショット コピー] をクリックし、リストからスナップショット コピーを選択します。
6. *送信*をクリックします。

[初期化 / 更新]ダイアログ ボックスに戻ります。

7. 初期化または更新するソースを複数選択した場合は、既存のスナップショット 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 [デフォルト] 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. 初期化または更新ジョブを開始するには、[送信] をクリックします。

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: 各初期化ジョブまたは更新ジョブのステータスを追跡するには、*ボリューム/ヘルス*詳細ページで*ジョブの表示*をクリックします。

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、*ボリューム/健全性*の詳細ページに戻ります。

すべてのタスクが正常に完了すれば初期化ジョブまたは更新ジョブは終了です。

ボリューム関係ページから保護関係を再同期します

[ボリューム関係]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か、または現在のソースを別のボリュームに変更するために、関係を再同期することができます。

開始する前に

- アプリケーショ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 リレーションシップ ページで、静止関係にある 1 つ以上のボリュームを選択し、ツールバーから **再同期** をクリックします。

[再同期]ダイアログ ボックスが表示されます。

2. *再同期オプション*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 スナップショット コピー をクリックし、スナップショット 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. デフォルトのスナップショット コピーを転送するのではなく、既存のスナップショット コピーを指定する場合は、[既存のスナップショット コピー] をクリックし、リストからスナップショット コピーを選択します。
5. *送信*をクリックします。

[再同期]ダイアログ ボックスに戻ります。

6. 再同期するソースを複数選択した場合は、既存のスナップショット コピーを指定する次のソースに対して [デフォルト] をクリックします。
7. 再同期ジョブを開始するには、[送信] をクリックします。

再同期ジョブが開始されると、[ボリューム関係]ページに戻り、ページの上部にジョブのリンクが表示されます。

8. オプション: 各再同期ジョブのステータスを追跡するには、[ボリューム リレーションシップ] ページで [ジョブの表示] をクリックします。

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 リレーションシップ] 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から保護関係を反転する

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。

開始する前に

- アプリケーショ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関係については実行できません。

- 保護関係がすでに存在している必要があります。
- 保護関係が解除されている必要があります。
- ソースとデスティネーションの両方がオンラインになっている必要があります。
- ソースが別のデータ保護ボリュームのデスティネーションになっている場合は実行できません。
- このタスクを実行すると、共通のSnapshotコピーのデータよりも新しいソースのデータは削除されます。
- 逆再同期した関係に対して作成されるポリシーとスケジュールは、元の保護関係と同じになります。

ポリシーとスケジュールが存在しない場合は作成されます。

手順

1. ボリューム リレーションシップ ページで、関係を元に戻すボリュームを 1 つ以上選択し、ツールバーの 逆再同期 をクリックします。

[逆再同期]ダイアログ ボックスが表示されます。

2. *[逆再同期] ダイアログ ボックスに表示される関係が逆再同期操作を実行する関係であることを確認し、[送信] をクリックします。

逆再同期処理が開始されると、[ボリューム関係]ページに戻り、ページの上部にジョブのリンクが表示されます。

3. オプション: 各逆再同期ジョブのステータスを追跡するには、[ボリューム リレーションシップ] ページで [ジョブの表示] をクリックします。

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 リレーションシップ] 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。

ボリュームとボリューム/ヘルスの詳細ページを使用してデータを復元します

[ボリューム]ページおよび[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、上書きまたは削除したファイルやディレクトリ、あるいはボリューム全体をSnapshotコピーからリストアすることができます。

開始する前に

アプリケーショ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、以下に該当する場合は使用できません。
 - ボリュームIDが不明な場合：クラスタ間関係が確立されているがデスティネーション クラスタが検出されていない場合など。

- 。ボリュームがSnapMirror同期レプリケーションの対象に設定されている場合。

手順

1. 左側のナビゲーション ペインから、ストレージ > ボリューム に移動します。
2. ボリュームを選択し、「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、*ボリューム/正常性の詳細 > アクション > 復元*に移動します。[リストア]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、"[リストアダイアログ ボックス](#)"。
3. デフォルトの設定と異なる場合は、データをリストアするボリュームとSnapshotコピーを選択します。
4. 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（元の場所 または 別の既存の場所）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。
 - 。 「復元パス」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。
 - 。 参照 をクリックしてディレクトリの参照ダイアログボックスを起動し、次の手順を実行します。
 - i. リストア先のデスティネーション クラスタ、Storage VM (SVM) 、およびボリュームを選択します。
 - ii. [名前]テーブルで、リストアする必要があるディレクトリ名を選択します。
 - iii. *ディレクトリを選択*をクリックします。
7. *復元*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. ジョブの進行状況を確認するには、左側のナビゲーション ペインで [保護] > [ジョブ] に移動し、ジョブのリストから復元ジョブのステータスを表示します。



Cloud Volumes ONTAPの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のルートを追加しなければならないことがあります。この構成手順は、NetApp Console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、バックアップ管理のためにパートナー アプリケーションにプロビジョニングを提供するために、ストレージ管理者が Unified Manager を使用して作成する集約のグループです。

リソースは、パフォーマンス、コスト、物理的な場所、可用性などの属性に基づいてプールにまとめることができます。関連するリソースをプールにグループ化すると、監視とプロビジョニングでそのプールを1つのユニットとして扱うことができます。これにより、リソースの管理が簡易化され、柔軟かつ効率的にストレージを使用できるようになります。

セカンダリ ストレージをプロビジョニングする際、Unified Managerでは、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。

- オンラインのデータ アグリゲート（ルート アグリゲートでない）。
- ONTAPのメジャー バージョンがソース クラスタと同じかそれ以降のデスティネーション クラスタ ノードにあるアグリゲート。
- リソース プールに含まれる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多いアグリゲート。
- デスティネーション ボリュームをプロビジョニングしたあとのスペースが、定義されているほぼフルと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いずれか該当する方）を超えないアグリゲート。
- デスティネーション ノードのFlexVolの数がプラットフォームの上限を超えない。

リソースプールを作成する

[リソース プールの作成]ダイアログ ボックスを使用すると、プロビジョニングのためにアグリゲートをグループ化できます。

開始する前に

アプリケーショ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. リソース プールの作成 ダイアログ ボックスの指示に従って、名前と説明を入力し、作成するリソース プールに集約をメンバーとして追加します。

リソースプールを編集する

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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

編集 ボタンは、リソース プールが 1 つ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 プールを選択した場合、[編集] ボタンは無効になります。

手順

1. 左側のナビゲーション ペインで、[保護] > [リソース プール] をクリックします。
2. リストから1つのリソース プールを選択します。
3. *編集*をクリックします。

[リソース プールの編集]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*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。

リソースプールのインベントリを表示する

[リソース プール]ページを使用すると、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。

開始する前に

アプリケーショ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] > [リソース プール] をクリックします。

リソース プールのインベントリが表示されます。

リソースプールのメンバーを追加する

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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

リソース プールに一度に追加できるアグリゲートの数は200個までです。[アグリゲート]ダイアログ ボックスに表示されるアグリゲートは他のリソース プールには属しません。

手順

1. 左側のナビゲーション ペインで、[保護] > [リソース プール] をクリックします。

2. リソース プール リストからリソース プールを選択します。

リソース プールのリストの下領域に、リソース プールのメンバーが表示されます。

3. リソース プール メンバー領域で、[追加] をクリックします。

[アグリゲート]ダイアログ ボックスが表示されます。

4. 1つ以上のアグリゲートを選択します。

5. *[追加]*をクリックします。

ダイアログ ボックスが閉じ、選択したリソース プールのメンバーのリストにアグリゲートが表示されます。

リソースプールから集約を削除する

アグリゲートを他の目的に使用したい場合などに、既存のリソース プールからアグリゲートを削除することができます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

リソース プールのメンバーは、リソース プールが選択されている場合にのみ表示されます。

手順

1. 左側のナビゲーション ペインで、[保護] > [リソース プール] をクリックします。
2. メンバー アグリゲートを削除するリソース プールを選択します。

[Members]ペインにメンバー アグリゲートのリストが表示されます。

3. 1つ以上のアグリゲートを選択します。

*削除*ボタンが有効になっています。

4. *削除*をクリックします。

警告のダイアログ ボックスが表示されます。

5. 続行するには、[はい] をクリックします。

選択したアグリゲートが[メンバー]ペインから削除されます。

リソースプールを削除する

不要になったリソース プールを削除できます。たとえば、1つのリソース プールから他の複数のリソース プールにメンバー アグリゲートを再配分したあと、元のリソース プールを廃止状態にすることができます。

開始する前に

アプリケーショ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*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。

ストレージ VM 災害復旧保護関係の監視

Active IQ Unified Managerでは、Storage VMレベルでのディザスタ リカバリを実現するStorage VMディザスタ リカバリ関係を監視できます。Storage VMディザスタ リカバリを使用すると、Storage VMのコンスチチュエント ボリューム内のデータをリカバリしたり、Storage VMの設定をリカバリしたりできます。

ソースStorage VMからデスティネーションStorage VMへのStorage VM DR関係は、非同期のディザスタ リカバリを実現するために作成されます。クラスタのセットアップに基づいて、データ ボリュームと一緒にすべてまたは一部のStorage VM設定（ネットワークとプロトコルの設定を除く）をレプリケートするかどうかを選択できます。

Storage VMディザスタ リカバリ関係を設定すると、ハードウェア障害や自然災害が原因でソースStorage VMを使用できなくなるとデスティネーションStorage VMが起動し、最小限のシステム停止でデータへのアクセスが再開されます。同様に、ソースStorage VMが使用可能になると、デスティネーションStorage VMと再同期され、ソースからのデータの提供が再開されます。SnapMirrorコマンドを使用して、Storage VMディザスタ リカバリ関係を設定および管理できます。

関係ページを使用してストレージ VM を監視する

Storage VMディザスタ リカバリ関係は、[インベントリ]の[保護]セクションにある[関係]ページで監視できます。デフォルトでは、コンスチチュエント関係のフィルタが適用されているため、[関係]ページには最上位の関係だけが表示されます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

フィルタを使用して、Storage VMディザスタ リカバリ関係を表示します。

手順

1. 左側のナビゲーション ペインで、保護 > 関係 をクリックします。

すべてのタイプ（ボリューム、整合性グループ、Storage VM）の関係が表示されます。

2. *フィルター*をクリックし、*関係オブジェクト タイプ*と*ストレージ VM*を選択して、ストレージ VMの災害復旧関係のみを表示します。
3. *フィルターを適用*をクリックします。



保護関係をすべて表示するには、コンスチチュエント関係のフィルタをクリアする必要があります。

Storage VMディザスタ リカバリ関係だけがページに表示されます。

ストレージVMページから保護関係を表示する

「ストレージ VM」ページを使用すると、既存のストレージ VM の災害復旧関係のステータスを表示できます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

転送と遅延のステータス、ソースとデスティネーションの詳細など、保護関係の詳細も確認できます。レポートのスケジュールを設定したり、既存のレポートを必要な形式でダウンロードしたりできます。***表示/非表示*** ボタンを使用すると、デフォルトでは表示されない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、**ストレージ > ストレージ VM** 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。

構成されたすべてのストレージ VM を含む「**関係: すべての関係**」ビューが表示されます。

保護ステータスに基づいてストレージ **VM** を表示する

[インベントリ]の[Storage VM]ページを使用すると、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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

[Storage VM]ビューに、Storage VMが保護されているかどうかを表示する[保護ルール]という新しい列が追加されました。



ソース クラスタがActive IQ Unified Managerに追加されていない場合は、そのクラスタに関連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、**ストレージ > ストレージ VM** をクリックします。
2. **表示** メニューから、**正常性 > すべてのストレージ VM** を選択します。

健全性: すべてのストレージ VM が表示されます。

3. **フィルター** をクリックすると、次のストレージ VM のいずれかが表示されます。

表示するには	フィルター値
保護されたストレージ VM	保護ルール*は*保護されています
保護されていないストレージ VM	保護ルール*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. ***フィルターを適用***をクリックします。

[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Storage VMまたは保護されていないStorage VMがすべて表示されます。

ストレージVMの関連付けを理解する

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と3次デスティネーションのどちらであるかに関係なく、関連付けはソースStorage VMとデスティネーションStorage VMの間で作成されます。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次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、保護 > ストレージ **VM** の関連付け ページで環境内のストレージ VM の関連付けを表示できます。

SVMを関連付ける方法は次の3とおりです。

- 任意のストレージ **VM** を関連付ける: 任意のプライマリ ソース ストレージ VM と 1 つ以上の宛先 SVM 間の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任意の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。
- 特定のストレージ **VM** を関連付ける: 特定のソース ストレージ VM と 1 つ以上の特定の宛先 SVM 間の関連付けを作成できます。たとえば、データを互いに分離する必要がある多数のクライアントにストレージ サービスを提供する場合は、このオプションを選択して、特定のソースStorage VMを、対象のクライアントにのみ割り当てられる特定のデスティネーションStorage VMに関連付けることができます。
- 外部ストレージ **VM** との関連付け: ソース ストレージ VM と宛先ストレージ VM の外部フレキシブル ボリューム間の関連付けを作成できます。

Storage VMの関連付けの作成

Storage Virtual Machineの関連付けの作成ウィザードでは、パートナーの保護アプリケーションがソース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関係で使うことができます。パートナー アプリケーションは、デスティネーション ボリュームの最初のプロビジョニングの際にこれらの関連付けを使用して、選択するリソースを特定します。

開始する前に

- 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。

あらゆるソースStorage VMと関係タイプについて、各デスティネーション クラスでデスティネーションStorage VMを1つだけ選択できます。

削除や作成の機能を使用した関連付けの変更は、以降のプロビジョニング処理にのみ反映されます。既存のデスティネーション ボリュームは移動されません。

手順

1. 左側のナビゲーション ペインで、保護 > ストレージ **VM** の関連付け をクリックします。

2. *ストレージ VM の関連付け*ページで、*作成*をクリックします。

*ストレージ仮想マシンの関連付けの作成*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。

◦ どれでも

すべてのプライマリ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に、このオプションを選択します。つまり、現時点で保護を必要とする既存のすべてのStorage VMおよび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に関連付ける特定のソースStorage VMを選択する場合に、このオプションを選択します。たとえば、データを互いに分離する必要のある多数のクライアントにストレージ サービスを提供する場合は、このオプションを選択して、特定のStorage VMソースを、対象のクライアントにのみ割り当てられる特定のStorage VMデスティネーションに関連付けます。

◦ なし（外部）

ソースStorage VMとデスティネーションStorage VMの外部のフレキシブル ボリュームの間で関連付けを作成する場合に、このオプションを選択します。

4. 作成する保護関係タイプとして、次のうちの1つまたは両方を選択します。

◦ **SnapMirror**

◦ **SnapVault**

5. *次へ*をクリックします。

6. 1つ以上のStorage VMの保護デスティネーションを選択します。

7. *[完了]*をクリックします。

Storage VMの関連付けの削除

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することができます。この処理は、たとえば、デスティネーションStorage VMがフルになり、Storage VMの保護の関連付けを新たに作成する場合などに行います。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

少なくとも1つのストレージ VM 関連付けが選択されるまで、削除 ボタンは無効になります。関連付けの削除と追加による変更は、以降のプロビジョニング処理にのみ反映されます。既存のデスティネーション ボリュームが移動されることはありません。

手順

1. 左側のナビゲーション ペインで、保護 > ストレージ **VM** の関連付け をクリックします。

2. Storage VMの関連付けを1つ以上選択します。

*削除*ボタンが有効になります。

3. *削除*をクリックします。

警告のダイアログ ボックスが表示されます。

4. 続行するには、[はい] をクリックします。

選択したStorage VMの関連付けがリストから削除されます。

ストレージ サービスをサポートするための **SVM** とリソース プールの要件

ストレージ サービスに固有の SVM の関連付けとリソース プールの要件を遵守すると、パートナー アプリケーションの準拠をより確実にすることができます。たとえば、パートナー アプリケーションによって提供されるストレージ サービスの保護トポロジをサポートするために、Unified Manager で SVM を関連付け、リソース プールを作成する場合などです。

一部のアプリケーションは、Unified Manager サーバーと連携して、ソース ボリュームとセカンダリまたは三次ロケーションの保護ボリューム間のSnapMirrorまたはSnapVaultバックアップ保護を自動的に構成および実行するサービスを提供します。これらの保護ストレージ 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またはカスケード構成の保護（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 / 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、以下の要件を確認してください。

- SVM の関連付けは、 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 ボリュームまたは三次ボリュームが存在する任意の SVM の間で設定する必要があります。
 - たとえば、ソース ボリューム Vol_A が SVM_1 上に存在し、 SnapMirror のセカンダリ デスティネーション ボリューム Vol_B が SVM_2 上に存在し、 3 次SnapVaultバックアップ ボリューム Vol_C が SVM_3 上に存在する保護トポロジをサポートするには、Unified Manager Web UI を使用して、SVM_1 と SVM_2 間のSnapMirror関連付けと、SVM_1 と SVM_3 間のSnapVaultバックアップ関連付けを設定する必要があります。

この例では、SVM_2 と SVM_3 間のSnapMirror関連付けまたはSnapVaultバックアップ関連付けは不要であり、使用されません。

- ソース ボリューム Vol_A とSnapMirror宛先ボリューム Vol_B の両方が SVM_1 上に存在す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集約リソースが含まれている必要があります。

Unified Manager Web UI を使用してリソース 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 ノードと三次ターゲット ノードを割り当てます。

ジョブとは

ジョブとは、Unified Manager を使用して監視できる一連のタスクです。ジョブとその関連タスクを表示すると、それらが正常に完了したかどうかを判断できます。

ジョブは、SnapMirror関係とSnapVault関係の作成時、関係の操作（解除、編集、休止、削除、再開、再同期、逆再同期）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。

ジョブを開始したら、[ジョブ]ページと[ジョブの詳細]ページを使用して、ジョブおよびジョブに関連するタスクの進捗状況を監視できます。

ジョブの監視

[ジョブ]ページでは、ジョブ ステータスを監視できるほか、ジョブのプロパティ（ストレージ サービス タイプ、状態、送信時刻、完了時刻など）を表示してジョブが正常に完了したかどうかを確認できます。

開始する前に

アプリケーショ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。

[ジョブ]ページが表示されます。

2. *状態*列を表示して、現在実行中のジョブのステータスを確認します。
3. 特定のジョブに関する詳細を表示する場合は、そのジョブ名をクリックします。

[ジョブの詳細]ページが表示されます。

求人の詳細を見る

ジョブの開始後に、[ジョブの詳細]ページからジョブの進捗状況を追跡し、関連タスクにエラーの可能性がないかどうかを監視できます。

開始する前に

アプリケーショ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すると、ジョブに関連付けられているタスクのリストが表示されます。
3. タスクをクリックすると、タスク リストの右側にある タスクの詳細 ペインと タスク メッセージ ペインに追加情報が表示されます。

ジョブを中止する

[ジョブ]ページでは、時間がかかりすぎているジョブ、多数のエラーが発生しているジョブ、あるいは不要となったジョブを中止できます。対象となるジョブは、ジョブの中止が可能なステータスとタイプのジョブに限られます。実行中のジョブはすべて中止できます。

開始する前に

アプリケーショ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 1 つのジョブを選択し、[中止] をクリックします。
3. 確認プロンプトで「はい」をクリックして、選択したジョブを中止します。

失敗した保護ジョブを再試行する

失敗した保護ジョブを修正するための対策を講じた後、「再試行」を使用してジョブを再度実行できます。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。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

失敗したジョブは一度に1つずつ再試行できます。複数のジョブを選択すると、[再試行] ボタンが無効になります。再試行できるのは、「保護構成」および「保護関係操作」タイプのジョブのみです。

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、失敗した保護構成または保護関係操作タイプのジョブを 1 つ選択します。

*再試行*ボタンが有効になっています。

3. *再試行*をクリックします。

ジョブが再実行されます。

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、保護ジョブなどの保護関連の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]ページを使用して、アグリゲート、ボリューム、関係に対してグローバルな健全性しきい値を設定できます。

[リソース プール]ページ

[リソース プール]ページには、既存のリソース プールとそのメンバーが表示され、プロ

ビジョニングのためにリソース プールを作成、監視、および管理できます。

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。

- 作成する

[リソース プールの作成]ダイアログ ボックスを表示します。このダイアログ ボックスでは、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。

- 消去

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。

- 説明

リソース プールの説明が表示されます。

- **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。有効な値は、Compliance、Enterprise、およびNon-SnapLockです。リソース プールには、同じSnapLockタイプのアグリゲートのみを含めることができます。

- 総容量

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。

- 利用可能な容量

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

リソース プールにメンバーを追加できます。

- 消去

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、選択したリソース 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。

- 状態

メンバー アグリゲートの現在のステータスが表示されます。ステータスはクリティカル (❌)、エラー (❗)、警告 (⚠)、または通常 (✅)。

- 集約名

メンバー アグリゲートの名前が表示されます。

- 州

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。

- 削除中

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。

- 凍った

アグリゲートが（一時的に）要求に応答していません。

- 不整合

アグリゲートが破損とマークされています。テクニカル サポートに連絡する必要があります。

- 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。

- 部分的

アグリゲート用のディスクが少なくとも1つ見つかりましたが、複数のディスクが不足しています。

- 休止中

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ています。

- 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

アグリゲートは検出されましたが、アグリゲート情報は Unified Manager サーバーによって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。

- 総容量

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。

- 利用可能な容量

アグリゲートで使用可能なスペース（MB、GBなど）が表示されます。

- 使用済み %

アグリゲートで使用されているスペースの割合が表示されます。

- ディスクタイプ

RAID構成タイプが表示されます。次のいずれかになります。

- RAID0：すべてのRAIDグループのタイプがRAID 0です。
- RAID4：すべてのRAIDグループのタイプがRAID 4です。
- RAID-DP: すべての RAID グループは RAID-DP タイプです。
- RAID-TEC: すべての RAID グループはRAID-TECタイプです。
- Mixed RAID：アグリゲートにRAIDタイプ（RAID 0、RAID 4、RAID-DP、RAID-TEC）の異なる複数のRAIDグループが含まれています。デフォルトでは、この列は表示されません。

[リソース プールの作成]ダイアログ ボックス

[リソース プールの作成]ダイアログ ボックスを使用すると、新しいリソース プールの名前と説明を指定して、そのリソース プールに対してアグリゲートを追加および削除することができます。

リソースプール名

テキスト ボックスを使用して、リソース プールを作成するための次の情報を追加できます。

リソース プール名を指定できます。

説明

リソース プールの説明を指定できます。

メンバー

リソース プールのメンバーが表示されます。メンバーを追加および削除することもできます。

コマンド ボタン

各コマンド ボタンを使用して次のタスクを実行できます。

- 追加

[アグリゲート]ダイアログ ボックスが開きます。ここでは、特定のクラスタのアグリゲートをリソース プールに追加できます。さまざまな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。

- 取り除く

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。

- 作成する

リソース プールを作成します。このボタンは、リソース プール名または説明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、[リソース プールの作成]ダイアログ ボックスを閉じます。

[リソース プールの編集]ダイアログ ボックス

[リソース プールの編集]ダイアログ ボックスを使用すると、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、元の名前や説明が正確でないか内容に誤りがある場合に、より正確な内容に変更することができます。

テキスト ボックス

各テキスト 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。

- 説明

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の変更内容を保存します。

- キャンセル

変更内容を破棄して、[リソース プールの編集]ダイアログ ボックスを閉じます。

【アグリゲート】ダイアログ ボックス

【アグリゲート】ダイアログ ボックスでは、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。少なくとも 1 つの集計が選択されるまで、[追加] ボタンは有効になりません。

- 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

集計リストには、監視対象の集計の名前とプロパティが (表形式で) 表示されます。

- 状態

ボリュームの現在のステータスが表示されます。ステータスはクリティカル (❌)、エラー (⚠️)、警告 (⚠️)、または通常 (✅)。

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。

- 集約名

アグリゲートの名前が表示されます。

- 州

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。

- 削除中

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。

- 凍った

アグリゲートが（一時的に）要求に応答していません。

- 不整合

アグリゲートが破損とマークされています。テクニカル サポートに連絡する必要があります。

- 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。

- 部分的

アグリゲート用のディスクが少なくとも1つ見つかりましたが、複数のディスクが不足しています。

- 休止中

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ています。

- 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

アグリゲートは検出されましたが、アグリゲート情報は Unified Manager サーバーによってまだ取得

されていません。

- クラスタ

アグリゲートが配置されているクラスタの名前が表示されます。

- ノード

アグリゲートが含まれるストレージ コントローラの名前が表示されます。

- 総容量

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

アグリゲート内の全ボリュームに対してコミットされたスペースの合計（MB、GBなど）が表示されます。デフォルトでは、この列は表示されません。

- 使用容量

アグリゲートで使用されているスペース（MB、GBなど）が表示されます。

- 利用可能な容量

アグリゲートでデータに使用できるスペース（MB、GBなど）が表示されます。デフォルトでは、この列は表示されません。

- 利用可能 %

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

[ジョブ]ページでは、実行中のすべてのパートナー アプリケーション保護ジョブの現在のステータスとその他の情報、および完了したジョブを表示できます。この情報から、まだ実行中のジョブや、ジョブが成功したかどうかを確認できます。

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。

- アボート

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選択できます。

- リトライ

保護構成または保護関係操作の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つずつ再試行できます。失敗したジョブを複数選択した場合、[再試行] ボタンは無効になります。ストレージ サービス ジョブは、失敗しても再試行できません。

- リフレッシュ

ジョブとその関連情報のリストを更新します。

[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、過去1週間に生成されたジョブのみが表示されます。列のソートやフィルタリングを使用して、表示されるジョブをカスタマイズできます。

- 状態

ジョブの現在のステータスが表示されます。ステータスはエラー (🚨) または通常 (✅)。

- ジョブID

ジョブのID番号が表示されます。デフォルトでは、この列は表示されません。

ジョブID番号は一意であり、ジョブの開始時にサーバによって割り当てられます。列フィルタのテキストボックスにジョブID番号を入力することで、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 タイプが表示されます。ジョブ タイプは次のとおりです。

- クラスター獲得

ワークフロー自動化ジョブがクラスターを再検出しています。

- 保護構成

保護ジョブは、cron スケジュール、 SnapMirrorポリシーの作成などのワークフロー自動化ワークフローを開始しています。

- 保護関係操作

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

ワークフロー自動化ジョブは複数のワークフローを実行しています。

- 復元する

リストア ジョブを実行しています。

- 掃除

リストアが不要となったストレージ 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。

- 破壊する

ジョブがストレージ サービスを削除しています。

- 輸入

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。

- 修正する

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。

- 購読する

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。

- 購読解除

ジョブがストレージ サービスからメンバーをサブスクライブ解除しています。

- アップデート

保護更新ジョブを実行しています。

- **WFA**構成

ワークフロー自動化ジョブはクラスター資格情報をプッシュし、データベース キャッシュを同期しています。

- 州

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

ジョブが中止されました。

- 中止

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。

- 提出時間

ジョブが送信された時刻が表示されます。

- 間隔

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。

求人詳細ページ

[ジョブの詳細]ページでは、特定の保護ジョブ タスクのステータスやその他の情報を確認できます。実行中のタスク、キューに登録されたタスク、完了したタスクの情報が表示されます。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
- 州
- 提出時間
- 完了時間
- 間隔

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。

- リフレッシュ

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。

- 求人を見る

[ジョブ]ページに戻ります。

[Job tasks]リスト

[Job tasks]リストには、特定のジョブに関連付けられているすべてのタスクと各タスクに関連するプロパティ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、この列に基づいて新しいタスクから古いタスクの順に情報が表示されます。

- タイプ

タスクのタイプが表示されます。

- 州

特定のタスクの状態が表示されます。

- 完了

完了したタスクです。

- キューに追加されました

実行待ちのタスクです。

- 実行中

実行中のタスクです。

- 待っている

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。

- 状態

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。

- 普通 ()

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。

- 間隔

タスクが開始されてからの経過時間が表示されます。

- 完了時間

タスクが完了した時刻が表示されます。デフォルトでは、この列は表示されません。

- タスクID

ジョブの個々のタスクを識別するGUIDが表示されます。この列はソートとフィルタリングが可能です。デフォルトでは、この列は表示されません。

- 依存関係の順序

グラフ内のタスクの順序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。

- タスク詳細ペイン

ジョブの各タスクについて、タスクの名前、タスクの説明、タスクが失敗した理由などの追加情報が表示されます。

- タスクメッセージペイン

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 メッセージは、すべてのタスクで表示されるとは限りません。

[詳細なセカンダリ設定]ダイアログ ボックス

[詳細なセカンダリ設定]ダイアログ ボックスでは、セカンダリ ボリュームのバージョンに依存しないレプリケーション、複数コピー バックアップ、およびスペース関連設定を有効にすることができます。[詳細なセカンダリ設定]ダイアログ ボックスは、現在の設定を変更して有効または無効にする場合に使用します。

スペース関連設定には、重複排除、データ圧縮、自動拡張、スペース ギャランティなど、格納できるデータの量を最大限に増やすための設定が含まれます。

このダイアログ ボックスには次のフィールドがあります。

- バージョンに柔軟なレプリケーションを有効にする

バージョンに依存しないレプリケーションを使用したSnapMirrorを有効にします。バージョンに依存しないレプリケーションでは、デスティネーション ボリュームでソース 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も、ソース ボリュームをSnapMirrorで保護することができます。

- Enable Backup

バージョンに依存しないレプリケーションが有効な場合に、SnapMirrorソースのデータの複数のSnapshotコピーをSnapMirrorデスティネーションに転送して保持することができます。

- 重複排除を有効にする

重複するデータ ブロックを排除してスペースを削減できるように、SnapVault関係のセカンダリ ボリュームで重複排除を有効にします。重複排除は、スペース削減率が10%以上で、データが頻繁には上書きされない場合に効果を期待できます。重複排除は、仮想環境、ファイル共有、およびバックアップのデータによく使用されます。この設定はデフォルトでは無効になっています。有効にすると、転送が完了するたびにこの処理が開始されます。

- 圧縮を有効にする

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、ピーク時以外の時間帯に圧縮を完了できるだけの十分なシステム リソースがある場合に効果を期待できます。SnapVault関係では、この設定はデフォルトで無効になっています。圧縮は、重複排除を選択した場合にのみ使用できます。

- インラインで圧縮

ディスクに書き込む前にデータを圧縮することで、スペース削減効果を即座に実現できます。インライン圧縮は、システムのピーク時の利用率が50%以下で、ピーク時に書き込みやCPUが多少増えても許容できる場合に効果を期待できます。この設定は、「圧縮を有効にする」が選択されている場合にのみ使用できます。

- 自動拡張を有効にする

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することができます。

- 最大サイズ

ボリュームを最大で何パーセントまで拡張できるようにするかを設定します。デフォルトでは、ソース ボリュームのサイズよりも20%まで大きくできます。現在のボリューム サイズがこの値以上の場合、そのボリュームは自動的に拡張されません。このフィールドは、自動拡張の設定を有効にした場合にのみ有効になります。

- サイズの増加

ボリュームの自動拡張で何パーセントずつ拡張するかを指定します。ソース ボリュームの割合で示した最大サイズに達するまで、この割合で自動的に拡張されます。

- スペース保証

データ転送が常に成功するようにセカンダリ ボリュームに十分なスペースを割り当てます。スペース ギランティの設定は次のいずれかです。

- ファイル

- Volume

- なし + たとえば、合計 50 GB のファイルを含む 200 GB のボリュームがあるとします。ただし、これらのファイルには 10 GB のデータしか保持されません。[Volume]を選択した場合、ソースの内容に関係なく、200GBのスペースがデスティネーション ボリュームに割り当てられます。[File]を選択した場合は、ソースのファイルに対応する十分なスペースを確保するために、デスティネーションに50GBの

スペースが割り当てられます。この状況で[None]を選択した場合は、ソースで実際にファイルのデータに使用されている10GBだけが割り当てられます。

スペース ギャランティは、デフォルトでは[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。

- 適用する

選択した効率設定を保存し、[保護の構成] ダイアログ ボックスで [適用] をクリックしたときに適用されます。

- キャンセル

変更内容を破棄して[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。

[詳細なデスティネーション設定]ダイアログ ボックス

[詳細なデスティネーション設定]ダイアログ ボックスを使用すると、デスティネーション ボリュームでスペース ギャランティの設定を有効にすることができます。詳細設定は、ソースではスペース ギャランティが無効になっている状況において、デスティネーションでスペース ギャランティを有効にする場合に使用します。SnapMirror関係の重複排除、圧縮、および自動拡張の設定はソース ボリュームから継承され、変更することはできません。

スペース ギャランティ

データ転送が常に成功するようにデスティネーション ボリュームに十分なスペースを割り当てます。スペース ギャランティの設定は次のいずれかです。

- ファイル
- Volume
- なし

たとえば、200GBのボリュームに合計50GBのファイルが格納されており、それらのファイルに実際に格納されているデータは10GBだけであるとします。[Volume]を選択した場合、ソースの内容に関係なく、200GBのスペースがデスティネーション ボリュームに割り当てられます。ファイル保証では、宛先のソース ファイル用に十分なスペースが確保されるように 50 GB 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 データによって使用される実際のスペースに対して宛先に 10 GB のみが割り当てられることになります。

スペース ギャランティは、デフォルトでは[Volume]に設定されています。

[リストア]ダイアログ ボックス

[リストア]ダイアログ ボックスを使用すると、特定のSnapshotコピーからボリュームにデータをリストアできます。

リストア元

[リストア元]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となるボリュームを指定します。デフォルトでは、リストア操作を開始したボリュームが選択されます。リストア操作を開始したボリュームと保護関係にあるすべてのボリュームを表示するドロップダウン リストから別のボリュームを選択することもできます。

- スナップショットコピー

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]リストの内容は、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リストします

デフォルトでは、最大995個のオブジェクトがリストに表示されます。選択したボリューム内のすべてのオブジェクトを表示する場合は、このチェックボックスを選択解除できます。アイテムの数が非常に多い場合は、この処理が完了するまでに時間がかかることがあります。

リストアする項目を選択

[リストアする項目を選択]領域では、リストアの対象として、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、または両者の組み合わせを選択できます。アイテムを最大数まで選択すると、アイテム選択チェック ボックスが無効になります。

- 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、またはパスを入力できます。パスを選択または入力するまで、このフィールドには何も表示されません。クリック  パスを選択すると、ディレクトリ構造内の 1 つのレベルが上に移動します。

- フォルダとファイルのリスト

入力したパスの内容が表示されます。デフォルトでは、最初にルート フォルダが表示されます。フォルダ名をクリックすると、そのフォルダの内容が表示されます。

リストアする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たパスを入力すると、指定したファイルが[フォルダ / 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 / 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、または両者の組み合わせをリストア対象として選択できます。

フォルダに995個を超えるアイテムが含まれている場合は、アイテムが多すぎて表示できないことを通知するメッセージが表示され、そのまま処理を続行すると、指定したフォルダ内のすべてのアイテムがリストアされます。選択したボリューム内のすべてのオブジェクトを表示する場合は、「最大 995 個のファイルとディレクトリを一覧表示する」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を復元する場所に移動するか、cluster://svm/volume/path の形式を使用してパスを手動で入力することができます。

- ディレクトリ階層を維持

このチェック ボックスをオンにすると、元のファイルまたはディレクトリの構造が維持されます。たとえば、ソースが /A/B/C/myFile.txt で、宛先が /X/Y/Z の場合、Unified Manager は宛先の次のディレクトリ構造を使用してデータを復元します：/X/Y/Z/A/B/C/myFile.txt。

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、[リストア]ダイアログ ボックスを閉じます。

- 復元する

選択した内容でリストア プロセスを開始します。

[ディレクトリの参照]ダイアログ ボックス

[ディレクトリの参照]ダイアログ ボックスは、元のソースとは別のクラスタおよびSVM上のディレクトリにデータをリストアする場合に使用します。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。

[ディレクトリの参照]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のリストが表示されます。デフォルトでは元のソース ボリュームのSVMが選択されます。

- 音量

選択したSVM内の読み書き可能なボリュームがすべて表示されます。ボリュームは、名前や使用可能なスペースでフィルタできます。最もスペースが大きいボリュームから順に一覧表示されます。デフォルトでは元のソース ボリュームが選択されます。

- ファイルパステキストボックス

データのリストア先となるファイル パスを入力できます。すでに存在する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、サブフォルダが表示されます（存在する場合）。フォルダ内のファイルは表示されません。クリック  フォルダーを選択すると、ディレクトリ構造内で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

選択内容を適用して、[ディレクトリの参照]ダイアログ ボックスを閉じます。ディレクトリを選択していない場合は、このボタンが無効になります。

- 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。

[保護設定]ダイアログ ボックス

[保護設定]ダイアログ ボックスを使用すると、クラスタ上の読み取り、書き込み、データ保護のすべてのボリュームに対してSnapMirror関係とSnapVault関係を作成して、ソース ボリュームまたはプライマリ ボリューム上のデータをレプリケートできます。

ソースタブ

- トポロジビュー

作成する関係が視覚的に表示されます。デフォルトでは、トポロジ内のソースが強調表示されます。

- 情報源

選択したソース ボリュームに関する詳細が表示されます。次の情報が含まれます。

- Source Cluster Name
- ソースSVM名
- Cumulative Volume Total Size

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。

- Cumulative Volume Used Size

選択したすべてのソース ボリュームの累積使用サイズが表示されます。

- ソース ボリューム

次の情報がテーブルに表示されます。

- 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。「Compliance」、「Enterprise」「Non-SnapLock」のいずれかです。

- Snapshot コピー

ベースライン転送に使用されるSnapshotコピーが表示されます。ソース ボリュームが読み取り/書き込みボリュームの場合、[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コピーを選択するための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、別のデフォルトのSnapshotコピーを選択することはできません。

SnapMirrorタブ

保護関係のデスティネーション クラスタ、Storage Virtual Machine (SVM)、アグリゲート、およびSnapMirror関係を作成する際のデスティネーションの命名規則を指定できます。SnapMirrorポリシーとスケジュールを指定することもできます。

- トポロジビュー

作成する関係が視覚的に表示されます。デフォルトでは、トポロジ内のSnapMirrorのデスティネーション リソースが強調表示されます。

- 目的地情報

保護関係のデスティネーション リソースを選択できます。

- 詳細リンク

SnapMirror関係の作成時に[詳細なデスティネーション設定]ダイアログ ボックスを表示します。

- クラスタ

保護デスティネーション ホストとして使用できるクラスタが表示されます。このフィールドは必須です。

- ストレージ仮想マシン (SVM)

選択したクラスターで使用可能な SVM を一覧表示します。SVM リストを入力する前にクラスター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

選択した SVM で使用可能なアグリゲートを一覧表示します。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。

- 順位

複数のアグリゲートがデスティネーションの要件をすべて満たす場合、この順位は、次の条件に従ってアグリゲートを表示する優先順位を示します。

- A. ソース ボリュームのノードとは異なるノードに配置されているアグリゲートが優先され、障害ドメインの分離が可能になります。
- B. ボリューム数が少ないノード上のアグリゲートが優先され、クラスタ内のノード全体での負荷分散が可能になります。
- C. 他のアグリゲートよりも空きスペースの多いアグリゲートが優先され、容量の分散が可能になります。順位1は、この3つの条件に従っているアグリゲートが最も優先されることを示します。

- アグリゲート名

アグリゲートの名前

- 使用可能容量

- データ用のアグリゲートで利用できるスペースの量

- リソース プール

アグリゲートが属するリソース プールの名前

- 命名規則

デスティネーション ボリュームに適用されるデフォルトの命名規則を指定します。用意されている命名規則をそのまま使用することも、カスタムの命名規則を作成することもできます。命名規則には、%C、%M、%V、%N の属性を指定できます。ここで、%C はクラスタ名、%M は SVM 名、%V はソース ボリューム、%N はトポロジの宛先ノード名です。

エントリが無効な場合は、[Naming Convention]フィールドが赤で強調表示されます。「Preview Name」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。関係が作成されると、デスティネーション名に001～999のサフィックスが追加され、プレビュー テキストのnnnがこのサフィックスに置き換わります。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が転送されるときに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スケジュールを示します。デフォルトはDPDefaultです。

- ポリシーを作成する

[SnapMirror ポリシーの作成]ダイアログ ボックスを表示します。このダイアログ ボックスでは、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スケジュールを示します。スケジュールは、「None」、「5min」、「8hour」、「daily」、「hourly」、「weekly」のいずれかに設定できます。デフォルトは「None」で、関係にスケジュールが関連付けられません。スケジュールが設定されていない関係については、ストレージ サービスに属している場合を除き、遅延ステータスの値は報告されません。

- スケジュールを作成

[スケジュールの作成]ダイアログ ボックスを表示します。このダイアログ ボックスでは、新しいSnapMirrorスケジュールを作成できます。

SnapVaultタブ

SnapVault関係を作成するときに、保護関係のセカンダリ クラスタ、SVM、アグリゲート、およびセカンダリ 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。

- トポロジービュー

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のセカンダリ 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

[詳細なセカンダリ設定]ダイアログ ボックスを表示します。

- クラスタ

保護のセカンダリ 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。

- ストレージ仮想マシン (SVM)

選択したクラスターで使用可能な SVM を一覧表示します。SVM リストを入力する前にクラスター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

選択した SVM で使用可能なアグリゲートを一覧表示します。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。

- 順位

複数のアグリゲートがデスティネーションの要件をすべて満たす場合、この順位は、次の条件に従ってアグリゲートを表示する優先順位を示します。

- A. プライマリ ボリュームのノードとは異なるノードに配置されているアグリゲートが優先され、障害ドメインの分離が可能になります。
- B. ボリューム数が少ないノード上のアグリゲートが優先され、クラスタ内のノード全体での負荷分散が可能になります。
- C. 他のアグリゲートよりも空きスペースの多いアグリゲートが優先され、容量の分散が可能になります。順位1は、この3つの条件に従っているアグリゲートが最も優先されることを示します。

- アグリゲート名

アグリゲートの名前

- 使用可能容量
 - データ用のアグリゲートで利用できるスペースの量
 - リソース プール

アグリゲートが属するリソース プールの名前

- 命名規則

セカンダリ ボリュームに適用されるデフォルトの命名規則を指定します。用意されている命名規則をそのまま使用することも、カスタムの命名規則を作成することもできます。命名規則には、%C、%M、%V、%N の属性を指定できます。ここで、%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、[Naming Convention]フィールドが赤で強調表示されます。「Preview Name」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、プレビュー領域では無効な情報に赤の疑問符が表示されます。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 テキストのnnnがこのサフィックスに置き換わります。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が転送されるときに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

関係に対するONTAPのSnapVaultポリシーを指定します。デフォルトは「XDPDefault」です。

- ポリシーを作成する

[SnapVault ポリシーの作成]ダイアログ ボックスを表示します。このダイアログ ボックスでは、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

関係に対するONTAPのSnapVaultスケジュールを指定します。スケジュールは、「None」、「5min」、「8hour」、「daily」、「hourly」、「weekly」のいずれかに設定できます。デフォルトは「None」で、関係にスケジュールが関連付けられません。スケジュールが設定されていない関係については、ストレージ サービスに属している場合を除き、遅延ステータスの値は報告されません。

- スケジュールを作成

[スケジュールの作成]ダイアログ ボックスを表示します。このダイアログ ボックスでは、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、[保護設定]ダイアログ ボックスを閉じます。

- 適用する

選択項目を適用して保護プロセスを開始します。

[スケジュールの作成]ダイアログ ボックス

[スケジュールの作成]ダイアログ ボックスでは、SnapMirror関係とSnapVault関係の転送について、基本的または詳細な保護スケジュールを作成できます。データが頻繁に更新されるため、データ転送の頻度を増やすために新しいスケジュールを作成したり、データの変更頻度が低い場合に頻度の低いスケジュールを作成したりすることができます。

SnapMirror同期関係に対してスケジュールを構成することはできません。

- 宛先クラスター

[保護設定]ダイアログ ボックスの[SnapVault]タブまたは[SnapMirror]タブで選択したクラスタの名前。

- スケジュール名

スケジュールに指定する名前。スケジュール名には、A～Z、a～z、0～9、および特殊文字 (! @ # \$ % { キャレット } & * () _ - . スケジュール名には次の文字を含めることはできません: < >。

- 基本または上級

使用するスケジュール モード。

「基本」モードには次の要素が含まれます。

- 繰り返し

スケジュールされた転送が発生する頻度。「毎時」、「毎日」、「毎週」のいずれかを選択できます。

- 日

毎週の繰り返しを選択した場合、転送が発生する曜日。

- Time

「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。

- 日数

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。

- 曜日

カンマで区切った数値のリスト。曜日を表します。有効な値は0～6です。0は日曜を表し、以降も同様です。この要素はオプションです。このフィールドを空にすると、指定した週に毎日転送が発生します。曜日を指定し、日にちを指定していない場合は、毎日ではなく指定した曜日にのみ転送が発生します。

- 営業時間

カンマで区切った数値のリスト。1日のうちの時間数を表します。有効な値は0～23です。0は午前0時を表します。この要素はオプションです。

- 分

カンマで区切った数値のリスト。1時間のうちの分数を表します。有効な値は0～59です。この要素

は必須です。

[SnapMirror ポリシーの作成]ダイアログ ボックス

[SnapMirror ポリシーの作成]ダイアログ ボックスでは、ポリシーを作成してSnapMirror 転送の優先度を設定できます。ポリシーを使用することで、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。

- 宛先クラスター

[保護設定]ダイアログ ボックスの[SnapMirror]タブで選択したクラスタの名前。

- 宛先SVM

[保護設定]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 (-)、およびアンダースコア (_) を使用できます。

- 転送の優先順位

非同期操作の転送を実行する優先順位。[標準]または[低]を選択できます。転送の優先順位として「標準」を指定したポリシーを使用する関係の転送は、「低」を指定したポリシーを使用する関係の転送の前に実行されます。

- コメント

オプションのフィールド。ポリシーに関するコメントを追加できます。

- 転送再開

転送が中止処理または何らかの障害（ネットワークの停止など）によって中断されたときに行う再開のアクションを示します。次のいずれかを選択できます。

- いつも

転送を再開する前に新しいSnapshotコピーを作成し、既存のSnapshotコピーが存在する場合は、チェックポイントから転送を再開して、そのあとに新しく作成したSnapshotコピーに基づく差分転送を実行するように指定します。

- 一度もない

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、[保護設定]ダイアログ ボックスを閉じます。

- 適用する

選択項目を適用して保護プロセスを開始します。

[SnapVault ポリシーの作成]ダイアログ ボックス

[SnapVault ポリシーの作成]ダイアログ ボックスでは、ポリシーを作成してSnapVault転送の優先度を設定できます。ポリシーを使用することで、プライマリからセカンダリ ボリュームへの転送効率を最大化できます。

- 宛先クラスター

[保護設定]ダイアログ ボックスの[SnapVault]タブで選択したクラスタの名前。

- 宛先**SVM**

[保護設定]ダイアログ ボックスの[SnapVault]タブで選択したSVMの名前。

- ポリシー名

新しいポリシーに指定する名前。ポリシー名には、A～Z、a～z、0～9、ピリオド (.)、ハイフン (-)、およびアンダースコア (_) を使用できます。

- 転送の優先順位

転送を実行する優先度。[標準]または[低]を選択できます。転送の優先順位として「標準」を指定したポリシーを使用する関係の転送は、「低」を指定したポリシーを使用する関係の転送の前に実行されます。デフォルト設定は「標準」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

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テーブルに表示します。このSnapshotコピーのポリシーには特定のレプリケーション ラベルが指定されています。次の情報とアクションを使用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の数値にする必要があります。すべてのルールすべての保持数の合計は251個以下でなければなりません。

- 削除

既存のSnapshotコピー ラベルを削除できます。

- Snapshot コピー ラベル

Snapshotコピー ラベルが表示されます。同じローカルSnapshotコピー ポリシーを使用する1個以上のボリュームを選択すると、ポリシー内の各ラベルのエントリが表示されます。2つ以上のローカルSnapshotコピー ポリシーを使用する複数のボリュームを選択すると、すべてのポリシーのすべてのラベルがテーブルに表示されます。

- スケジュール

各Snapshotコピー ラベルに関連付けられているスケジュールが表示されます。ラベルに複数のスケジュールが関連付けられている場合は、そのラベルのスケジュールがカンマで区切ったリストに表示されます。同じラベルを持ちながらスケジュールが異なる複数のボリュームを選択した場合、スケジュールには「Various」と表示され、選択したボリュームに複数のスケジュールが関連付けられていることが示されます。

- デスティネーションの保持数

SnapVaultセカンダリに保持されていて、指定したラベルを持つSnapshotコピーの数が表示されます。複数のスケジュールを使用するラベルの保持数として、各ラベルとスケジュールのペアの保持数の合計が表示されます。2つ以上のローカルSnapshotコピー ポリシーを使用する複数のボリュームを選択すると、保持数は空になります。

[関係の編集]ダイアログ ボックス

既存の保護関係を編集して、最大転送速度、保護ポリシー、保護スケジュールを変更することができます。

目的地情報

- 宛先クラスター

選択したデスティネーション クラスタの名前です。

- 宛先**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示します。選択すると、指定した値までにネットワーク帯域幅が制限されます。数値を入力してから、KBps（1秒あたりのキロバイト数）、MBps（1秒あたりのメガバイト数）、GBps（1秒あたりのギガバイト数）、TBps（1秒あたりのテラバイト数）のいずれかの単位を選択できます。最大転送速度は1KBps～4TBpsの範囲で指定する必要があります。最大転送速度を指定しない場合は、関係間でベースライン転送が制限されません。この設定は、プライマリ クラスタとセカンダリ クラスタが同じ場合は無効になります。

- SnapMirror ポリシー

関係のONTAP SnapMirrorスケジュールを示します。デフォルトはDPDefaultです。

- ポリシーを作成する

[SnapMirror ポリシーの作成]ダイアログ ボックスを表示します。このダイアログ ボックスでは、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スケジュールを示します。スケジュールは、「None」、「5min」、「8hour」、「daily」、「hourly」、「weekly」のいずれかに設定できます。デフォルトは「None」で、関係にスケジュールが関連付けられません。スケジュールが設定されていない関係については、ストレージ サービスに属している場合を除き、遅延ステータスの値は報告されません。

- スケジュールを作成

[スケジュールの作成]ダイアログ ボックスを表示します。このダイアログ ボックスでは、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、[保護設定]ダイアログ ボックスを閉じます。

- 提出する

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、新しい保護関係で最初のベースライン転送を実行できます。また、すでに初期化された関係でスケジュールされていない増分更新を手動で実行する場合は、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、初期化での転送の優先順位や、転送時に使用される帯域幅を変更できます。

- 転送の優先順位

転送を実行する優先度。[標準]または[低]を選択できます。通常の転送優先度を指定するポリシーとの関係は、低い転送優先度を指定するポリシーとの関係よりも先に実行されます。デフォルトでは「通常」が選択されています。

- 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が転送されるときにの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、次に示す最大転送速度設定のいずれかを指定できます。

- 個々の関係のセットアップまたは編集で指定した値を使用する

これを選択すると、各関係の作成時または編集時に指定された最大転送速度が、初期化処理と更新処理で使用されます。このフィールドは、転送速度が異なる複数の関係を初期化または更新する場合にのみ選択できます。

- 無制限

関係間の転送に帯域幅の制限がないことを示します。このフィールドは、転送速度が異なる複数の関係を初期化または更新する場合にのみ選択できます。

- 帯域幅を制限

選択すると、指定した値までにネットワーク帯域幅が制限されます。数値を入力してから、KBps（1秒あたりのキロバイト数）、MBps（1秒あたりのメガバイト数）、GBps（1秒あたりのギガバイト数）、TBps（1秒あたりのテラバイト数）のいずれかの単位を選択できます。最大転送速度は1KBps～4TBpsの範囲で指定する必要があります。

[ソース Snapshot コピー]タブ

[ソース Snapshot コピー]タブには、ベースライン転送に使用されるソースSnapshotコピーに関する次の情報が表示されます。

- ソースボリューム

対応するソース ボリュームの名前が表示されます。

- 宛先ボリューム

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。タイプは、[Read/write]または[Data Protection]のいずれかです。

- スナップショットコピー

データ転送に使用されるSnapshotコピーが表示されます。Snapshotコピーの値をクリックすると、[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 ボックスでは、使用する保護関係のタイプおよび実行する処理に応じて、転送に使用するSnapshotコピーを選択できます。データ保護タイプのソースについては、別のSnapshotコピーを指定できません。

コマンド ボタン

各コマンド ボタンを使用して次のタスクを実行できます。

- キャンセル

選択内容を破棄して、[初期化 / 更新]ダイアログ ボックスを閉じます。

- 提出する

選択内容を保存して、初期化ジョブまたは更新ジョブを開始します。

[再同期]ダイアログ ボックス

[再同期]ダイアログ ボックスでは、SnapMirror関係やSnapVault関係を解除してデスティネーションが読み書き可能ボリュームになったあとに、その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やSnapVaultの更新が失敗する場合にも実行することがあります。

再同期オプションタブ

[再同期オプション]タブでは、再同期する保護関係の転送の優先順位と最大転送速度を設定できます。

- 転送の優先順位

転送を実行する優先度。[標準]または[低]を選択できます。通常の転送優先度を指定するポリシーとの関係は、低い転送優先度を指定するポリシーとの関係よりも先に実行されます。

- 最大転送速度

ネットワークを介してクラスタ間でデータが転送されるときに最大速度を指定します。これを選択すると、ネットワーク帯域幅が指定した値に制限されます。数値を入力してから、KBps（1秒あたりのキロバイト数）、MBps（1秒あたりのメガバイト数）、GBps（1秒あたりのギガバイト数）、TBps（1秒あたりのテラバイト数）のいずれかの単位を選択できます。最大転送速度を指定しない場合は、関係間でベースライン転送が制限されません。

[ソース Snapshot コピー]タブ

[ソース Snapshot コピー]タブには、ベースライン転送に使用されるソースSnapshotコピーに関する次の情報が表示されます。

- ソースボリューム

対応するソース ボリュームの名前が表示されます。

- 宛先ボリューム

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

ボリュームの種類（読み取り/書き込みまたはデータ保護）を表示します。

- スナップショットコピー

データ転送に使用されるSnapshotコピーが表示されます。Snapshotコピーの値をクリックすると、[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 ボックスでは、使用する保護関係のタイプおよび実行する処理に応じて、転送に使用するSnapshotコピーを選択できます。

コマンド ボタン

- 提出する

再同期プロセスを開始し、[再同期] ダイアログ ボックスを閉じます。

- キャンセル

選択内容をキャンセルして、[再同期]ダイアログ ボックスを閉じます。

[ソース Snapshot コピーの選択]ダイアログ ボックス

[ソース Snapshot コピーの選択]ダイアログ ボックスを使用して、保護関係間でデータを転送するためのSnapshotコピーを選択するか、デフォルトの動作を選択します。選択するオプションは、関係を初期化、更新、再同期するかどうか、および関係がSnapMirrorとSnapVaultのどちらであるかによって異なります。

デフォルト

SnapVault関係およびSnapMirror関係の初期化、更新、転送の再同期に使用されるSnapshotコピーを決定する際のデフォルトの動作を選択できます。

SnapVault転送を実行する場合、各処理のデフォルトの動作は次のとおりです。

処理	ソースが読み取り/書き込みの場合のデフォルトの SnapVault の動作	ソースがデータ保護（DP）の場合のデフォルトの SnapVault 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すべてのSnapshotコピーを転送します。	ラベルが設定された最新のSnapshotコピーを転送します。

SnapMirror転送を実行する場合、各処理のデフォルトの動作は次のとおりです。

処理	デフォルトの SnapMirror 動作	SnapMirror から SnapMirror へのカスケード関係で 2 番目のホップである場合のデフォルトの SnapMirror 動作
初期化	新しいSnapshotコピーを作成して、そのSnapshotコピーおよびその前に作成されたすべてのSnapshotコピーを転送します。	ソースからSnapshotコピーをすべて転送します。
更新	新しいSnapshotコピーを作成して、そのSnapshotコピーおよびその前に作成されたすべてのSnapshotコピーを転送します。	すべてのSnapshotコピーを転送します。
再同期	新しいSnapshotコピーを作成して、ソースからSnapshotコピーをすべて転送します。	セカンダリ ボリュームから3番目のボリュームにすべてのSnapshotコピーを転送し、最も新しい共通のSnapshotコピーの作成後に追加されたデータを削除します。

既存のスナップショットコピー

リストから既存のSnapshotコピーを選択できます（Snapshotコピーの選択が許可されている場合）。

- スナップショットコピー

転送用に選択可能な既存のSnapshotコピーが表示されます。

- 作成日

Snapshotコピーが作成された日時が表示されます。最新のSnapshotコピーがリストの先頭に表示されます。

SnapVault転送の実行時に、ソースからデスティネーションに転送する既存のSnapshotコピーを選択する場合、各処理の動作は次のようになります。

処理	スナップショットコピーを指定する場合の SnapVault の動作	カスケードでスナップショットコピーを指定する場合の SnapVault 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に対しては、ソースSnapshotコピーの選択がサポートされません。
更新	指定したSnapshotコピーを転送します。	データ保護ボリュームに対しては、ソースSnapshotコピーの選択がサポートされません。

処理	スナップショットコピーを指定する場合の SnapVault の動作	カスケードでスナップショットコピーを指定する場合の SnapVault の動作
再同期	選択したSnapshotコピーを転送します。	データ保護ボリュームに対しては、ソースSnapshotコピーの選択がサポートされません。

SnapMirror転送の実行時に、ソースからデスティネーションに転送する既存のSnapshotコピーを選択する場合、各処理の動作は次のようになります。

処理	スナップショットコピーを指定する場合の SnapMirror の動作	カスケードでスナップショット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に対しては、ソースSnapshotコピーの選択がサポートされません。
更新	ソース上のすべてのSnapshotコピー（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に対しては、ソースSnapshotコピーの選択がサポートされません。
再同期	ソースからすべてのSnapshotコピー（選択したSnapshotコピーまで）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に対しては、ソースSnapshotコピーの選択がサポートされません。

コマンド ボタン

各コマンド ボタンを使用して次のタスクを実行できます。

- 提出する

選択内容を送信して、[ソース Snapshot コピーの選択]ダイアログ ボックスを閉じます。

- 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。

[逆再同期]ダイアログ ボックス

ソース ボリュームが機能しなくなったために保護関係を解除して、デスティネーションを読み書き可能なボリュームにした場合は、逆再同期によって関係の方向を反転させて、デスティネーションを新たなソースに、ソースを新たなデスティネーションにすることができます。

災害によって保護関係のソース ボリュームが機能しなくなった場合は、ソースの修理や交換、ソースの更

新、および関係の再確立を行う間、デスティネーション ボリュームを読み書き可能に変換してデータの提供を継続することができます。逆再同期操作を実行すると、共通スナップショット 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。

逆再同期前

逆再同期処理を実行する前の関係のソースとデスティネーションが表示されます。

- ソースボリューム

逆再同期処理を実行する前のソース ボリュームの名前と場所。

- 宛先ボリューム

逆再同期処理を実行する前のデスティネーション ボリュームの名前と場所。

逆再同期後

逆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。

- 宛先ボリューム

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。

- 提出する

逆再同期処理を開始します。

- キャンセル

逆再同期処理を開始せずに[逆再同期]ダイアログ ボックスを閉じます。

関係: すべての関係ビュー

「関係: すべての関係」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表示されるレポートには、ボリュームとStorage VMの両方の最上位の保護関係が含まれます。ページ上部にあるオプションを使用すると、特定のビューを選択したり、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たデータのリストを絞り込んだりすることができます。また、ページ上の列を追加 / 削除 / 順序変更したり、ページ上のデータを.csv、.pdf、.xlsxファイルにエクスポートしたりすることができます。カスタマイズしたページをカスタム ビューとして保存し、データのレポートを定期的に生成してEメールで送信するようにスケジュール設定できます。デフ

オルトでは、[関係] メニューを選択すると、表示されるレポートには、データセンター内のボリュームとストレージ VM の両方の保護関係が含まれます。フィルター オプションを使用すると、ボリュームのみ、ストレージ 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。同じレポートが[ストレージ]ページに表示されますが、選択したストレージの情報だけが含まれます。ボリュームまたはストレージ VM 関係を表示する場合は、[ストレージ] > [ボリューム] > [関係: すべての関係] ページにアクセスするか、[保護] > [関係] > [関係: すべての関係] にアクセスし、[フィルター] の [関係オブジェクト タイプ*] オプションを使用して、ボリュームまたはストレージ VM データのみをフィルター処理します。

すべての保護関係を一覧表示する [関係] ページには、宛先クラスタの **[System Manager で表示]** リンクがあり、これを使用してONTAP System Manager で同じオブジェクトを表示できます。

- 状態

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、エラー (❗)、警告 (⚠)、またはOK (✅)。

- ソースストレージ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。

クラスタ内のSVMがUnified Managerインベントリにまだ追加されていない場合、またはクラスタの前の更新後に作成された場合、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。

- ソース

選択内容に基づいて、保護されているソース ボリュームまたはソースStorage VMが表示されます。ソース ボリュームまたはStorage VMの名前をクリックすると、それらの詳細を表示できます。

メッセージが `Resource-key not discovered` が表示される場合、ボリュームはクラスタ上に存在しているが、Unified Manager インベントリにまだ追加されていないか、ボリュームがクラスタの最後の更新後に作成されたことを示している可能性があります。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。

- 宛先ストレージ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。

- 行き先

選択内容に基づいて、デスティネーション ボリュームまたはStorage VMの名前が表示されます。デスティネーション ボリュームまたはStorage VMの名前をクリックすると、それぞれのオブジェクトの詳細を表示できます。

- 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。整合性グループ関係にある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、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。ポリシーの名前をクリックすると、そのポリシーに関連付けられた詳細について次の情報を確認できます。

- 転送の優先順位

非同期操作の転送を実行する優先度を指定します。転送の優先順位は[標準]または[低]です。優先度が[標準]の転送は、優先度が[低]の転送よりも先に実行されます。デフォルトは[標準]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で実行する処理を指定します。StrictSync関係の場合、セカンダリ ボリュームとの同期に失敗すると、プライマリ ボリュームへのアクセスが制限されます。Sync関係の場合、セカンダリとの同期に失敗しても、プライマリへのアクセスは制限されません。

- 最大試行回数

SnapMirror関係の手動またはスケジュールされた各転送を試行する最大回数を指定します。デフォルトは8です。

- コメント

選択したポリシーに関するコメントを示すテキスト フィールドが表示されます。

- SnapMirrorラベル

Snapshotコピー ポリシーに関連付け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。

- 実際のスナップショットコピー

このボリューム上の、指定したラベルと一致するSnapshotコピーの数を指定します。

- スナップショットコピーを保存する

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。

- 保持の警告のしきい値

Snapshotコピー数の制限を指定します。この数に達すると、保持数の上限に近づいていることを通知する警告が送信されます。

- 遅延期間

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秒またはそれに近い値になります。

- ラグステータス

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。

- 最後の成功した更新

SnapMirrorまたはSnapVaultの処理に最後に成功した時刻が表示されます。

同期関係については、前回の更新成功日時は適用されません。

- 構成要素の関係

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。

- 関係の種類

ボリュームを複製するために使用される関係タイプが表示されます。次の関係タイプがあります。

- 非同期ミラー

- 非同期バックアップ

- 非同期ミラーボールド

- StrictSync

- 同期

- 転送状況

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、次のいずれかです。

- 中止中

SnapMirror転送が有効になっていますが、転送を中止する処理（チェックポイントの削除など）を実行中です。

- 確認中

デスティネーション ボリュームの診断チェックを実行中で、実行中の転送はありません。

- 最終処理中

SnapMirror転送が有効になっています。現在SnapVault増分転送の転送後のフェーズです。

- アイドル

転送が有効になっていますが、実行中の転送はありません。

- 同期

同期関係にある2つのボリュームのデータが同期されています。

- 非同期

デスティネーション ボリュームのデータがソース ボリュームと同期されていません。

- 準備中

SnapMirror転送が有効になっています。現在SnapVault増分転送の転送前のフェーズです。

- キューに登録

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。転送中ではありません。

- 休止中

SnapMirror転送を実行中です。増分転送が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のデータ転送が完了し、同期処理への移行が開始されています。

- 待機中

SnapMirror転送は開始されていますが、一部の関連タスクのキュー登録を待っています。

- 最終転送時間

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。

- 最終転送サイズ

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。

- 仲介者

メディア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SnapMirrorアクティブ同期がサポートされていません。

- 未設定

メディアエーターが設定されていないか、設定されているがUnified Managerにデスティネーション クラスタのみが追加されていてソース クラスタが追加されていません。

- メディアエーターの IP アドレス

メディアエーターが設定されていて、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に表示されます。

- 州

SnapMirror関係またはSnapVault関係の状態が表示されます。「未初期化」、「SnapMirror 済み」、「切断」のいずれかです。ソース ボリュームを選択した場合は、関係の状態は適用されず表示されません。

- 人間関係の健康

クラスタの関係の健全性が表示されます。

- 不健康な理由

関係が不健全な状態にある理由。

- 転送の優先順位

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[標準]の転送は、優先度が[低]の転送よりも先に実行されます。

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。

- バージョン柔軟なレプリケーション

「はい」、「はい（バックアップ オプションあり）」、「なし」のいずれかが表示されます。

- ソースクラスター

SnapMirror関係のソース クラスターのFQDN、短縮名、またはIPアドレスが表示されます。

- ソースクラスター**FQDN**

SnapMirror関係のソース クラスターの名前が表示されます。

- ソースノード

ボリュームの場合はSnapMirror関係のソース ノード名のリンクが、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、SnapMirrorアクティブ同期関係に属する整合性グループのボリュームについて、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。

ノード数リンクをクリックすると、該当する関係に関連付けられているノードをリストするノード 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。

ノード数リンクをクリックすると、該当する関係に関連付けられているノードをリストするノード 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。

- 宛先クラスター

SnapMirror関係のデスティネーション クラスターの名前が表示されます。

- 宛先クラスター**FQDN**

SnapMirror関係のデスティネーション クラスターのFQDN、短縮名、またはIPアドレスが表示されます。

- 保護

さまざまな関係が表示されます。この列には、クラスターおよびStorage Virtual Machineのボリュームと整合性グループの関係が次の順序で表示されます。

- SnapMirror
- Storage VM DR
- SnapMirror、ストレージVM DR
- 整合性グループ
- SnapMirror、整合性グループ。

関連情報

- *Relationship: MetroCluster*ビューの詳細については、"[MetroCluster構成の監視](#)"。
- *関係:過去1か月間の転送ステータス*ビューの詳細については、"[関係: 過去1か月間の転送ステータスビュー](#)"。
- *関係: すべての関係*ビューの詳細については、"[関係: 過去1か月間の転送率ビュー](#)"。

関係: 過去1か月間の転送ステータスビュー

「関係: 過去 1 か月間の転送ステータス」ビューでは、非同期関係にあるボリュームとストレージ VM の一定期間にわたる転送傾向を分析できます。また、転送が成功したか失敗したかどうか也表示されます。

ページ上部のコントロールを使用すると、特定のオブジェクトを検索したり、フィルターを作成して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エクスポートしたりできます。 .csv、.pdf、または.xlsxファイル。カスタマイズしたページをカスタムビューとして保存し、データのレポートを定期的に生成してEメールで送信するようにスケジュール設定できます。 フィルター オプションを使用すると、ボリュームのみ、またはストレージ 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。同じレポートが[ストレージ]ページに表示されますが、選択したストレージの情報だけが含まれます。たとえば、ボリューム関係を表示する場合は、「ストレージ」>「ストレージ VM」>「関係: 過去 1 か月間の転送ステータス」メニュー、または「保護」>「関係」>「関係: 過去 1 か月間の転送ステータス」メニューから、ストレージ VM の「関係: 過去 1 か月間の転送ステータス」レポートにアクセスし、「フィルター」を使用してボリュームのデータのみを表示できます。

• ソースボリューム

ソース ボリューム名が表示されます。

• 宛先ボリューム

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。

• 振替終了時間

ボリューム転送の終了時間が表示されます。

• 転送期間

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**

ストレージ仮想マシン (SVM) 名を表示します。

- ソースクラスター

ソース クラスター名が表示されます。

- 宛先**SVM**

宛先 SVM 名を表示します。

- 宛先クラスター

デスティネーション クラスター名が表示されます。

関連情報

- *関係: すべての関係*ビューの詳細については、"[関係: すべての関係ビュー](#)"。
- *Relationship: MetroCluster*ビューの詳細については、"[MetroCluster構成の監視](#)"。
- *関係: すべての関係*ビューの詳細については、"[関係: 過去1か月間の転送率ビュー](#)"。

関係: 過去1か月間の転送率ビュー

「関係: 過去 1 か月の転送率」ビューでは、非同期関係のボリュームについて、日々転送されるデータ量の量を分析できます。また、このページには、毎日の転送に関する詳細およびボリュームとStorage VMの転送処理を完了するために必要な時間が表示されます。

ページ上部にあるオプションを使用すると、特定のオブジェクトを検索したり、フィルタを作成および適用して表示されたデータのリストを絞り込んだりすることができます。また、ページ上の列を追加 / 削除 / 順序変更したり、ページ上のデータを.csv、.pdf、.xlsxファイルにエクスポートしたりすることができます。カスタマイズしたページをカスタム ビューとして保存し、データのレポートを定期的に生成してEメールで送信するようにスケジュール設定できます。たとえば、ボリュームの関係を表示する場合は、ストレージ > ボリューム > 関係: 過去 1 か月の転送速度 メニューにアクセスするか、保護 > 関係 > 関係: 過去 1 か月の転送速度 メニューにアクセスし、フィルター を使用してボリュームのデータのみを表示します。

- 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

- *Relationship: MetroCluster*ビューの詳細については、"[MetroCluster構成の監視](#)"。
- *関係:過去1か月間の転送ステータス*ビューの詳細については、"[関係: 過去1か月間の転送ステータスビュー](#)"。
- *関係: すべての関係*ビューの詳細については、"[関係: 過去1か月間の転送率ビュー](#)"

カスタム レポートの生成

Unified Managerレポート

Active IQ Unified Manager (旧称OnCommand Unified Manager) 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、スケジュールする機能を提供します。レポートには、ストレージシステムの容量、健全性、パフォーマンス、セキュリティ、保護関係に関する詳細を表示できます。

Active IQ Unified Manager 9.6 で導入された新しい Unified Manager レポートおよびスケジュール機能は、Unified Manager バージョン 9.5 で廃止された以前のレポート エンジンに代わるものです。

ネットワークをさまざまな側面（ビュー）から確認することで、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得ることができます。このビューは、列の表示 / 非表示の切り替えと並べ替え、データのフィルタリングとソート、結果の検索によってカスタマイズできます。カスタム ビューは、再利用できるように保存したり、レポートとしてダウンロードしたりできるほか、定期レポートとしてスケジュール設定してEメールで配布することができます。

Microsoft® Excel形式で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、フィルタ、ピボット テーブル、グラフなど、Excelの高度な機能を使用できます。カスタマイズしたExcelレポートに問題がなければ、Excelファイルをアップロードして、レポートの定期的な生成時や共有時に使用できます。

Unified Managerでは、ユーザ インターフェイスからレポートを生成する以外にも、以下の方法を使用して健全性、セキュリティ、パフォーマンスのデータを抽出できます。

- Open Database Connectivity (ODBC) およびODBCのツールを使用してデータベースに直接アクセスし、クラスタの情報を取得する。
- Unified Manager REST APIを実行して、確認したい情報を返します。

このリリース以降のActive IQ Unified Managerでは、レポート機能が次のように拡張されています。

- 設定したスケジュールに従ってレポートのEメールが送信されます。オンデマンド レポートを生成した場合も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。そのため、ファイル名が変更されても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

Unified Manager でクラスターに関する情報を収集し、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アクセスするには、次の 3 つの方法があります。

- UIのインベントリ ページからデータを直接抽出する。
- Open Database Connectivity (ODBC) およびODBCのツールを使用して、使用可能なすべてのオブジェクトにアクセスする。

- Unified Manager REST API を実行して、確認する情報を返します。

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。

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 は、監視対象のクラスタからのデータを保存するために MySQL データベースを使用します。データはMySQLデータベースのさまざまなスキーマに永続化されます。

次のデータベースからすべてのテーブルのデータを使用できます。

データベース	説明
netapp_model	ONTAPコントローラのオブジェクトに関するデータ。
netapp_model_view	ONTAPコントローラのオブジェクトに関するデータ。レポート ツールでの使用に適しています。
netapp_performance	クラスタ固有のパフォーマンス カウンタ。
ocum	UI のフィルタリング、並べ替え、および一部の派生フィールドの計算をサポートするための Unified Manager アプリケーション データと情報。
ocum_report	インベントリの構成と容量関連の情報のデータ。
ocum_report_birt	インベントリ設定と容量関連データのビュー。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。
scalemonitor	Unified Manager 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 ツールで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 ユーザ（レポート スキーマ ロールを持つデータベース ユーザ）は、これらのテーブル内のデータ

にアクセスできます。このユーザーには、Unified Manager データベースからのレポートやその他のデータベース ビューへの読み取り専用アクセス権が直接付与されます。ユーザ データやクラスターのクレデンシャル情報を含むテーブルにアクセスするための権限は付与されないことに注意してください。

レポートに使用できるUnified Manager REST API

REST API を使用すると、Unified Manager によってキャプチャされたヘルス、容量、パフォーマンス、およびセキュリティ情報を表示して、クラスターを管理できます。

REST APIはSwagger Webページから利用できます。Swagger Web ページにアクセスして、Unified Manager REST API ドキュメントを表示したり、API 呼び出しを手動で発行したりすることができます。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、以下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、アプリケーション管理者のいずれかのロールが必要です。

レポートを理解する

レポートにはストレージ、ネットワーク、サービス品質、および保護関係に関する詳細情報が表示されます。この情報を基に、潜在的な問題を発生前に特定して解決することができます。

ビューをカスタマイズした場合は、再利用できるように名前を付けて保存できます。カスタマイズしたビューに基づいてレポートを定期的に行うようにスケジュール設定し、他のユーザと共有できます。また、Excel形式でビューをダウンロードし、高度なExcel機能を使用してカスタマイズしたあとでファイルをUnified Managerに再度アップロードすることもできます。カスタマイズしたビューを使用してレポートをスケジュール設定すると、アップロードしたExcelファイルを使用してレポートを作成し、共有することができます。

スケジュール設定されたレポートは、すべて[レポート スケジュール]ページから管理できます。



レポートを操作するには、アプリケーション管理者またはストレージ管理者のロールが必要です。

レポートは、カンマ区切り値 (CSV) 、Excel、またはPDFファイルとしてダウンロードできます。

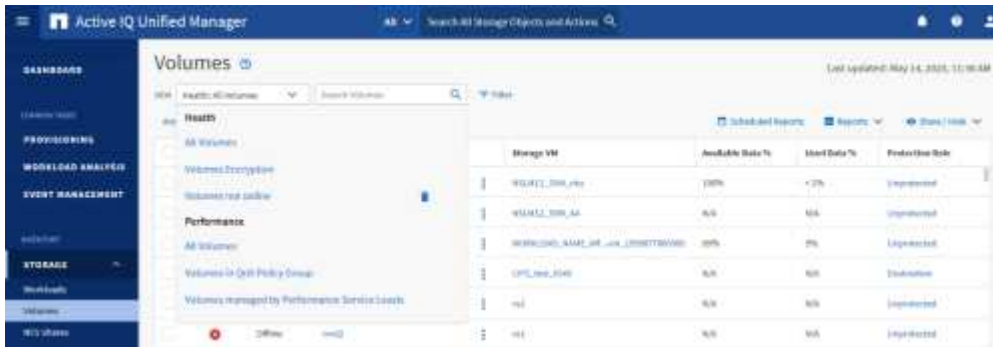
ビューとレポートの関係を理解する

ビューおよびインベントリ ページをダウンロードまたはスケジュール設定したものがレポートです。

ビューとインベントリ ページはカスタマイズして保存し、再利用することができます。Unified Managerで表示できるほぼすべての情報を、レポートとして保存、再利用、カスタマイズ、スケジュール設定、共有できます。

[表示]ドロップダウンで削除アイコンのある項目は、自分または他のユーザ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 ビューを変更または削除することはできません。

- 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すべて削除されます。
- カスタム ビューを変更した場合、そのビューを使用するレポートに変更が反映されるのは、レポート スケジュールに従って次回レポートが生成されてEメールで送信される時です。ビューを変更する場合は、変更内容がExcelで行ったレポートのカスタマイズに対応することを確認してください。必要であれば、Excelファイルをダウンロードして必要な変更を加え、ビューに対して再度アップロードすれば、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

次の表は、カスタマイズ、ダウンロード、およびスケジュール設定が可能なレポートとして使用できるビューとインベントリ ページの一覧です。

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
健康	クラスタ ノード アグリゲート Storage VM ボリューム SMB/CIFS共有 NFS 共有
パフォーマンス	クラスタ ノード アグリゲート Storage VM ボリューム LUN NVMeネームスペース ネットワーク インターフェイス (LIF) ポート
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）	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

新しいActive IQ Unified Managerレポート機能には、注意すべきいくつかの制限があります。

以前のバージョンの**Unified Manager**からの既存のレポート

スケジュールと受信者を編集できるのは、Unified Manager 9.5以前のリリースで作成およびインポートされた既存のレポート（.rptdesignファイル）のみです。Unified Manager 9.5以前の標準レポートをカスタマイズしたレポートは、新しいレポート ツールにインポートされません。

rptdesign ファイルからインポートした既存のレポートを編集する必要がある場合は、次のいずれかの操作を実行して、インポートしたレポートを削除してください。

- 新しいビューを作成し、作成したビューからレポートをスケジュールする（推奨）
- レポート上にカーソルを置き、SQLをコピーして、外部ツールを使用してデータを抽出する

デフォルト ビューは、カスタマイズしなくてもレポートとして生成できます。カスタム レポートは、新しいレポート機能を使用して再作成できます。

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、同じスケジュールを複数のレポートで再利用することはできません。

レポートの保護

適切な権限があるユーザであれば、誰でもレポートを編集または削除できます。保存したビューやスケジュールを、他のユーザが削除または変更できないようにする方法はありません。

イベント レポート

イベント ビューをカスタマイズしてレポートをCSV形式でダウンロードすることはできますが、イベント レポートを繰り返し生成して配信するようにスケジュール設定することはできません。

レポートの添付

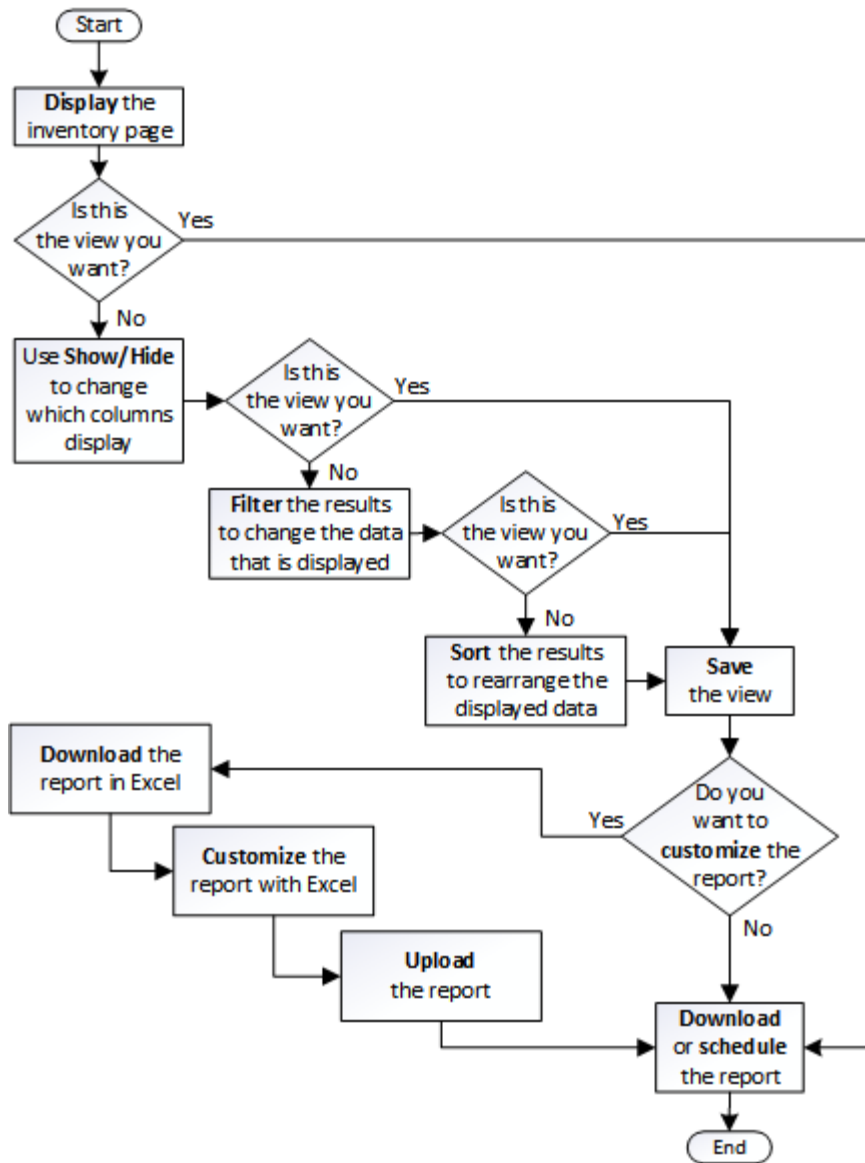
レポートをEメールの本文として送信することはできません。レポートはPDF、Excel、またはCSV形式の添付ファイルとして送信されます。

レポートの操作

必要なインベントリ ページのビューを見つけて、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

以下は、レポートのワークフローに関するデシジョン ツリーです。



レポートのクイック スタート

サンプルのカスタム レポートを作成して、各ビューの内容とレポートのスケジュール設定について学びます。このクイック スタートのレポートでは、アクセス頻度の低いコールド データが相当量あり、クラウド階層への移動を検討するボリュームを特定します。「パフォーマンス: すべてのボリューム」ビューを開き、フィルター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します。

開始する前に

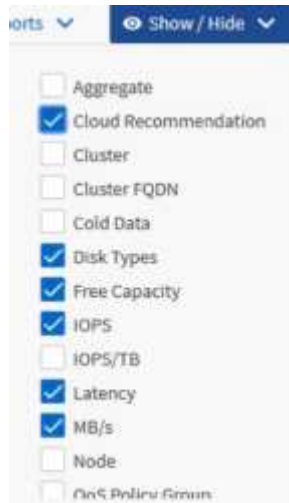
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- FabricPoolアグリゲートを設定しておく必要があります。また、それらのアグリゲート上にボリュームが必要です。

以下の手順に従って、次の操作を実行します。

- デフォルト ビューを開く
- データをフィルタおよびソートで列をカスタマイズする
- ビューを保存する
- カスタム ビューに対して生成されるようにレポートをスケジュール設定する

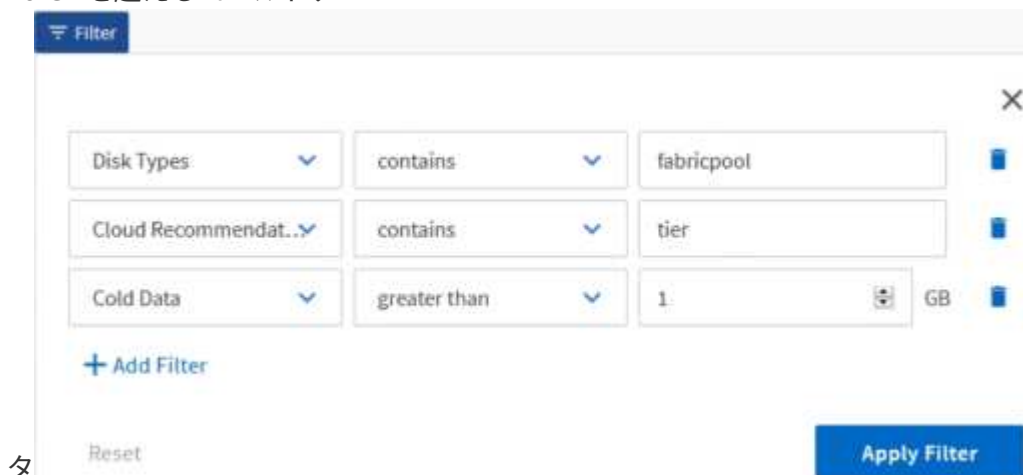
手順

1. 左側のナビゲーション ペインで、ストレージ > ボリューム 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. 表示/非表示 をクリックして、ビューに「ディスク タイプ」列が表示されることを確認します。



列を追加または削除して、レポートに必要なフィールドを含むビューを作成します。

4. 「ディスク タイプ」列を「クラウド推奨事項」列の横にドラッグします。
5. フィルター アイコンをクリックして次の 3 つのフィルターを追加し、[フィルターの適用] をクリックします。
 - ディスクタイプにFabricPoolが含まれる
 - クラウドに関する推奨事項に階層が含まれる
 - 10 GBを超えるコールドデー



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個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 データの量が最も多いボリュームがビューの先頭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、ビュー名が「保存されていないビュー」になります。ビューに表示されている内容を反映する名前を付けます (例: 「Vols change tiering policy」)。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、新しい名前でビューを保存します。

Volumes - Performance / Vols change tiering policy ⓘ Last updated: Feb 8, 2019, 12:26 PM ↻

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View Vols change tiering policy 🔍 Search Volumes ⚙️

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports Reports Show Hide

Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagntsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

- スケジュール設定や共有を行う前に、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て出力を確認してください。

Microsoft Excel (CSVまたはExcel) やAdobe Acrobat (PDF) などのインストールされているアプリケーションでファイルを開くか、またはファイルを保存します。



ビューをExcelファイルとしてダウンロードすると、複雑なフィルタ、並べ替え、ピボットテーブル、グラフを使用してレポートをさらにカスタマイズできます。Excelでファイルを開いてから、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内容は、レポートの実行時にビューに適用されます。

Excel を使用してレポートをカスタマイズする方法の詳細については、「サンプル *Microsoft Excel* レポート」を参照してください。

- インベントリページの*スケジュールされたレポート*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）に関連するすべてのスケジュール済みレポートがリストに表示されます。

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports

Volumes - Scheduled Reports View all Scheduled Reports

Add Schedule

Schedule Name	View	Recipients	Frequency	Format	
Weekly / Vols c... tiering policy	Performance / V... tiering policy	user@company.com	Weekly - Monday 1:00 PM	CSV	⋮

- スケジュールの追加 をクリックして、レポート スケジュール ページに新しい行を追加し、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します。
- レポートの名前を入力し、その他のレポートフィールドを入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

CSV形式のサンプル レポートを次に示します。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:52 PM - March 28, 2019, 12:52 PM)																
2	Generated At: March 28, 2019, 12:52 PM																
3																	
4	Status	Volume	Volume Id	Tiering Po	Cold Data	Free Capa	Total Capa	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id				
5	Ok	kjagnfsdst1	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040				
6	Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141				
	performance-volumes-28-Mar-2019																

PDF形式のサンプル レポートを次に示します。

Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:51 PM - March 28, 2019, 12:51 PM)
Generated At: March 28, 2019, 12:51 PM

Status	Volume	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	Cluster	Node	Aggregate
Ok	kjagnfsdst1	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る結果に基づいて、ONTAP 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する必要がある場合があります。

スケジュールされたレポートを検索する

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. *スケジュールされたレポートの検索*テキスト フィールドを使用します。

...別にレポートを検索するには	試す ...
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。

レポートをカスタマイズする

さまざまな方法でビューをカスタマイズすることで、ONTAP クラスターの管理に必要な情

報をすべて含んだレポートを作成することができます。

デフォルトのインベントリ ページまたはカスタム ビューをベースに、列の追加や削除、列の順序変更、データのフィルタリング、特定の列での昇順または降順のソートなどを行い、カスタマイズします。

Unified Manager 9.8以降では、ビューをExcel形式でダウンロードし、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。アップロードしたビューを使用してレポートをスケジュール設定すると、カスタマイズしたExcelファイルを使用してレポートを作成し、共有することができます。

Excel を使用してレポートをカスタマイズする方法の詳細については、「サンプル *Microsoft Excel* レポート」を参照してください。



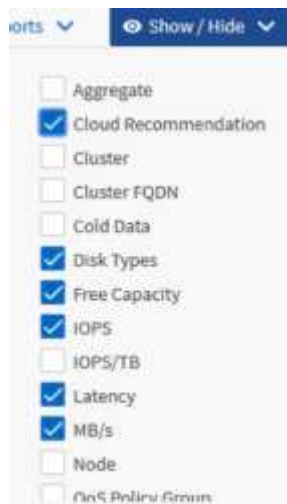
レポートを操作するには、アプリケーション管理者またはストレージ管理者のロールが必要です。

列をカスタマイズする

*表示/非表示*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 ページでは列をドラッグして並べ替えることができます。

手順

1. 列を追加または削除するには、[表示/非表示] をクリックします。



2. インベントリ ページで、列をドラッグしてレポートで必要な順序に並べ替えます。
3. ビューに名前を付けて変更を保存します。

データをフィルタリングする

要件を満たすレポートを作成するには、データをフィルタリングします。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. フィルター アイコンをクリックしてフィルターを追加し、表示する結果を絞り込んでから、[フィルターの適用] をクリックします。

The screenshot shows a 'Filter' panel with a close button (X) in the top right. It contains three filter rules, each with a field name, an operator, and a value:

- Rule 1: 'Disk Types' (dropdown) contains 'fabricpool' (text input).
- Rule 2: 'Cloud Recommendation' (dropdown) contains 'tier' (text input).
- Rule 3: 'Cold Data' (dropdown) is greater than '1' (text input) GB (unit dropdown).

Below the rules is a '+ Add Filter' button. At the bottom are 'Reset' and 'Apply Filter' buttons.

2. ビューに名前を付けて変更を保存します。

データの並べ替え

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. 列の見出しをクリックして、最も重要な情報がビューの先頭に表示されるように結果をソートします。
2. ビューに名前を付けて変更を保存します。

検索を使用したビューの絞り込み

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、レポートに必要な情報に合わせて結果をさら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. 検索フィールドを使用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の部分データを入力できます。たとえば、名前に「US_East」を含むノードを検索するには、全ノードのリストを絞り込むことができます。

検索結果はカスタム ビューに保存され、スケジュール済みレポートで使用されます。

3. ビューに名前を付けて変更を保存します。

Excelを使用してレポートをカスタマイズする

保存したビューをExcelワークブック形式（.xlsx）でダウンロードできます。Excelファイルを開くと、Excelの高度な機能を使用してレポートをカスタマイズできます。

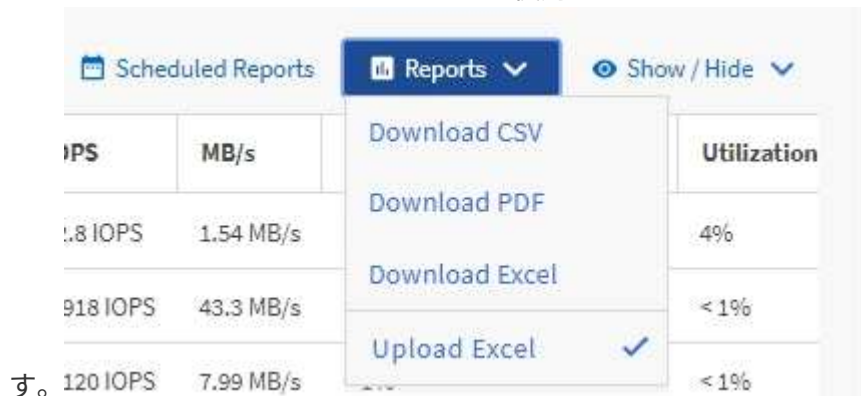
開始する前に

アップロードできるのは拡張子が.xlsxのExcelワークブック ファイルのみです。

たとえば、次に示すExcelの高度な機能をレポートで使用できます。

- 複数列の並べ替え
- 複雑なフィルタ
- ピボット テーブル
- グラフ

- ダウンロードしたExcelファイルには、保存した名前ではなくビューのデフォルトのファイル名が使用されます。
 - フォーマットは <View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx.
 - たとえば、カスタム保存ビューの名前は `Volumes-not online` ファイル名は `health-volumes-05-May-2020-19-18-00.xlsx` その日時に救われた場合。
- Excelファイルにはシートを追加できますが、既存のシートは変更しないでください。
 - 既存のシート、データ、情報は変更しないでください。代わりに、作成した新しいシートにデータをコピーします。
 - 上記のルールの唯一の例外は、「data」 ページで数式を作成できることです。dataページの式を使用して、新しいシートにグラフを作成します。
 - 新しいシートに「データ」または「情報」という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、または保存したビューを開きます。
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ファイルを元の場所に保存し直してください。
5. 複雑な並べ替え、フィルタ、ピボット テーブル、グラフなどのExcel機能を使用してファイルをカスタマイズします。詳細については、Microsoft® Excelのドキュメントを参照してください。
6. レポート > **Excel** のアップロード を選択し、変更したファイルを選択します。同じファイルの場所から、最後にダウンロードしたファイルがアップロードされます。

7. *スケジュールされたレポート*機能を使用して、自分自身にテスト レポートを送信します。

レポートをダウンロード

レポートをダウンロードして、データをカンマ区切り値（CSV）ファイル、Microsoft Excel（.XLSX）ファイル、またはPDFファイルとしてローカル ドライブや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. レポート ボタンをクリックして、次のいずれかの形式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 をダウンロード	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。

スケジュールレポート

再利用してレポートとして共有するビューができれば、Active IQ Unified Managerを使用してスケジュールを設定できます。スケジュールしたレポートに対しては、それぞれ受信者や配信頻度を変更するなどの管理操作を実行できます。

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できます。ただしイベントだけは例外で、CSVファイルとしてダウンロードすることはできませんが、スケジュール設定して再生成および共有することはできません。また、ダッシュボード、お気に入り、設定ページは、ダウンロードもスケジュール設定もできません。

Active IQ Unified Manager 9.8以降では、ビューをMicrosoft® Excel形式で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、フィルタ、ピボット テーブル、グラフなど、Excelの高度な機能を使用できます。カスタマイズしたExcelレポートに問題がなければ、Excelファイルをアップロードして、レポートの定期的な生成時や共有時に使用できます。

組み込みのビューとカスタマイズしたビューはスケジュール設定できます。送信するファイル タイプとしてCSV、PDF、またはXSLXを選択できます。初めてスケジュール設定したときにレポートをダウンロードして自身を唯一の受信者として割り当てると、受信者にレポートがどう表示されるかを確認できます。

レポートをスケジュールする

スケジュールを設定して定期的に生成および配布するビューまたはExcelファイルを決定したら、レポートのスケジュールを設定できます。

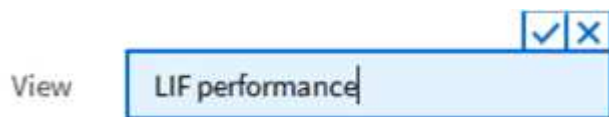
開始する前に

- アプリケーショ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 エンジンが Unified Manager サーバーから受信者リストに電子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、[全般] > [通知] ページで SMTP サーバー設定を構成する必要があります。
- 生成されたEメールによる添付ファイルの送信を許可するよう、Eメール サーバを設定する必要があります。

次の手順を実行して、ビューに対して生成するレポートをテストし、スケジュール設定します。使用するビューを選択またはカスタマイズします。こ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 ビューを使用します。左側のナビゲーション ペインで、ネットワーク > ネットワーク インターフェイス をクリックします。
2. Unified Managerに搭載されている機能を使用して、必要に応じてビューをカスタマイズします。
3. ビューをカスタマイズしたら、「ビュー」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します。



4. Microsoft® Excelの高度な機能を使用して、レポートをカスタマイズできます。詳細については、["Excelを使用したレポートのカスタマイズ"](#)。
5. レポートをスケジュール設定または共有する前に内容を確認するには、次の手順を実行します。

オプション	説明
Excel を使用してレポートをカスタマイズした場合	ダウンロードした既存のExcelファイルを表示します。
レポートをカスタマイズするために 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ているアプリケーションでファイルを開きます。

6. レポートに満足したら、「スケジュールされたレポート」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. ビュー名と頻度の組み合わせであるデフォルト名を受け入れるか、*スケジュール名*をカスタマイズします。
9. スケジュールされたレポートを初めてテストするには、自分自身だけを 受信者 として追加します。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。毎日、毎週、*毎月*を選択できます。
11. **PDF**、**CSV**、***XSLX***のいずれかの形式を選択します。



Excel を使用してコンテンツをカスタマイズしたレポートの場合は、常に **XSLX** を選択します。

12. チェックマーク (✓) をクリックしてレポートスケジュールを保存します。

LIFs - Scheduled Reports [View all Scheduled Reports](#)

[Add Schedule](#)

Schedule Name	View	Recipients	Frequency	Format
Weekly / LIF performar	Performance / LIF pe ▼	test@netapp.com	Weekly ▼ Thursda ▼ 4:30 PM ▼	PDF ▼

✓ ✕

テスト レポートがすぐに送信されます。以降、スケジュール設定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

インポートされた.rptdesignレポートのスケジュール

以前のリリースのUnified Managerで作成およびインポートした既存のレポートをスケジュールできます。

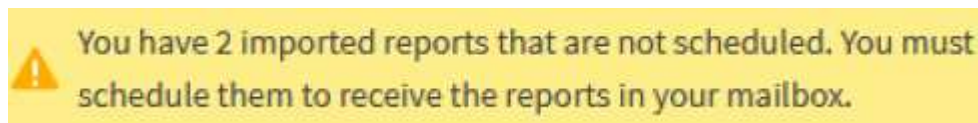
インポートしたレポートをスケジュール設定する場合の要件は次の通りです。

- 以前のUnified Managerリリースで設計し、インポートした.rptdesignファイル レポート
- Unified Manager 9.6 GA以降にアップグレードする場合に該当

Unified Manager 9.6 GA以降にアップグレードすると、[レポート スケジュール]ページにインポートしたレポートが表示されます。これらのレポートのスケジュールを編集して、受信者のEメール アドレス、頻度、形式（PDFまたはCSV）を指定できます。これらの編集をしていないレポートは、Unified Manager UIで編集または表示できません。

手順

1. [レポート スケジュール]ページを開きます。インポートしたレポートがある場合、次のようなメッセージが表示されます。



2. **View** 名をクリックすると、レポートの生成に使用されている SQL クエリが表示されます。



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 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。



不要なレポートは詳細アイコンから削除することもできます 。

レポートスケジュールを管理する

[レポート スケジュール] ページからレポート 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、または削除することができます。



開始する前に

[レポート スケジュール] ページから新しいレポートをスケジュール設定することはできません。スケジュール済みレポートは、オブジェクト インベントリ ページからのみ追加できます。

- アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > レポート スケジュール をクリックします。
2. [レポート スケジュール] ページで、次の手順を実行します。

状況	操作
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	操作
既存のスケジュールを編集する	- 詳細アイコンをクリック  使用したいスケジュールに応じて。 *編集*をクリックします。 - 必要な変更を行います。 - チェック マークをクリックして変更を保存します。
既存のスケジュールを削除する	- 詳細アイコンをクリック  使用したいスケジュールに応じて。 *削除*をクリックします。 - 操作を確定します。

スケジュールされたレポートを編集する

スケジュールを設定したレポートは、[レポート スケジュール]ページで編集できます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > レポート スケジュール をクリックします。

Scheduled Reports

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Search Scheduled Reports					
Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	



適切な権限があれば、システム内のすべてのレポートとそのスケジュールを変更できます。

2. 詳細アイコンをクリック  変更したいスケジュールの。
3. *編集*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、および 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。

スケジュールされたレポートを削除する

スケジュールを設定したレポートは、[レポート スケジュール]ページで削除できます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > レポート スケジュール をクリックします。

Scheduled Reports ?

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Search Scheduled Reports					
Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	⋮
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	⋮
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	⋮



適切な権限があれば、システム内のすべてのレポートとそのスケジュールを削除できます。

2. 詳細アイコンをクリック 削除したいスケジュールの
3. *削除*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、設定され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削除されます。

サンプルのカスタム レポート

以下に記載するサンプルのカスタム レポートを使用して、潜在的な問題を発生前に特定して対処することができます。

レポート リストはすべてのレポートを網羅しているわけではなく、今後も増えていきます。このセクションに追加して欲しいカスタム レポートがあれば、ドキュメントに関するフィードバックの形で提案していただくことができます。



レポートを操作するには、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。

クラスターストレージレポートをカスタマイズする

このセクションのクラスターストレージレポートは、それぞれのストレージシステムリソースの監視に役立つクラスター容量に関するレポートの作成方法を説明するためのサンプルです。

クラスターモデル別に容量を表示するレポートを作成する

クラスターのストレージ容量と利用率をストレージシステムモデルに基づいて分析するためのレポートを作成できます。

開始する前に

- ・アプリケーショ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、クラスター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、ストレージ > クラスター をクリックします。
2. [表示] メニューで、容量 > すべてのクラスター を選択します。
3. レポートに不要な「Cluster FQDN」や「OS Version」などの列を削除するには、「表示/非表示」を選択します。
4. 「Total Raw Capacity」、「Model/Family」、および3つの集計列を「Cluster」列の近くにドラッグします。
5. 「モデル/ファミリー」列の上部をクリックすると、結果をクラスタータイプ別に並べ替えることができます。
6. ビューに表示されている内容を反映する特定の名前 (例: 「Capacity by Cluster Model」) でビューを保存します。
7. インベントリページの*スケジュールされたレポート*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、レポート スケジュール ページに新しい行を追加し、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を入力して、チェックマーク (✓) を行の末尾に追加します。

テストレポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、特定のクラスターに容量を追加したり、古いクラスターモデルをアップグレードしたりすることができます。

未割り当てのLUN容量が最も多いクラスターを識別するレポートを作成します

未割り当てのLUN容量が最も多い (0.5TBを超える) クラスター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。

開始する前に

- ・アプリケーショ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、ストレージ > クラスター をクリックします。
2. [表示] メニューで、容量 > すべてのクラスター 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 LUN 容量」列を「HA ペア」列の近くにドラッグします。
5. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] 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 LUN 容量」列の上部をクリックすると、未割り当て LUN 容量の最大値で結果を並べ替えることができます。
7. ビューに表示されている内容を反映する特定の名前（例：「未割り当てLUN容量の最大値」）でビューを保存し、チェックマーク (✓) 。
8. インベントリページの*スケジュールされたレポート*ボタンをクリックします。
9. 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、「スケジュールの追加」をクリックして「レポート スケジュール」ページに新しい行を追加します。
10. レポートスケジュールの名前を入力し、他のレポートフィールドを入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、クラスタの未割り当てLUN容量を使用できます。

最も利用可能な容量を持つHAペアを表示するレポートを作成します

新しいボリュームやLUNのプロビジョニングに使用できる容量が最も多いハイアベイラビリティ (HA) ペアを検出するレポートを作成できます。

開始する前に

- ・アプリケーショ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、ストレージ > クラスター をクリックします。
2. [表示] メニューで、容量 > すべてのクラスター 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. 「Aggregate Unused Capacity」列を「HA Pair」列の近くにドラッグします。

5. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] 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. 「未使用の総容量」列の上部をクリックすると、未使用の総容量の最大量で結果を並べ替えることができます。
7. ビューに表示されている内容を反映する特定の名前（例：「Least used 集計容量」）でビューを保存し、チェックマーク（✓）。
8. インベントリページの*スケジュールされたレポート*ボタンをクリックします。
9. 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、「スケジュールの追加」をクリックして「レポート スケジュール」ページに新しい行を追加します。
10. レポートスケジュールの名前を入力し、他のレポートフィールドを入力して、チェックマーク（✓）を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、アグリゲートの容量に応じて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を作成します

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。

開始する前に

- アプリケーショ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、ストレージ > ノード 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すると、結果をONTAPの最も古いバージョンで並べ替えることができます。
5. ビューに表示されている内容を反映する特定の名前 (例: 「Nodes by ONTAP version」) でビューを保存します。
6. インベントリページの*スケジュールされたレポート*ボタンをクリックします。
7. 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、「スケジュールの追加」をクリックして「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を入力して、チェックマーク（✓）を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、古いバージョンのONTAPを実行しているノードをアップグレードできます。

総容量レポートをカスタマイズする

以下に記載するサンプルのカスタム レポートを使用して、アグリゲートのストレージ容量に関連する潜在的な問題を特定して対処することができます。

このセクションのレポートは、それぞれのストレージ システム リソースの監視に役立つアグリゲート容量レポートの作成方法を説明するためのサンプルです。

最大容量に達した集計を表示するレポートを作成する

容量がフルに近づいているアグリゲートを検出するレポートを作成して、容量を追加したり、ワークロードを他のアグリゲートに移したりすることができます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、容量がフルに近づいているアグリゲートを表示するカスタム ビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーション ペインで、ストレージ > アグリゲート をクリックします。
2. [表示] メニューで、[容量] > [すべての集計] 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. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] をクリックします。
 - フルまでの日数が45日未満
5. 「満杯までの残り日数」列の上部をクリックすると、満杯になるまでの残り日数が少ない順に結果を並べ替えることができます。
6. ビューに表示されている内容を反映する特定の名前（例：「全集約容量までの日数」）でビューを保存し、チェックマーク (✓)。
7. インベントリページの*スケジュールされたレポート*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、レポート スケジュール ページに新しい行を追加し、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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、容量がフルに近づいているアグリゲートのストレージを拡張できます。また、アグリゲートのスペースが少なくなった場合に早めにイベントを受信して対応できるように、「フルまでの日数」容量しきい値をデフォルトの7日より多い日数に引き上げることができます。

80%以上使用されている集計を表示するレポートを作成します

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。

開始する前に

- アプリケーショ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、ストレージ > アグリゲート をクリックします。
2. [表示] メニューで、[容量] > [すべての集計] 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. 「利用可能なデータ %」列と「使用済みデータ %」列を「集計」列の近くにドラッグします。
5. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] をクリックします。
 - 使用済みデータ (%) が80%を超えている
6. 「使用データ %」列の上部をクリックすると、結果を容量パーセントで並べ替えることができます。
7. ビューに表示されている内容を反映する特定の名前（例：「Aggregates nearing full」）でビューを保存し、チェックマーク (✓)。
8. インベントリページの*スケジュールされたレポート*ボタンをクリックします。
9. 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、「スケジュールの追加」をクリックして「レポート スケジュール」ページに新しい行を追加します。
10. レポートスケジュールの名前を入力し、他のレポートフィールドを入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、一部のアグリゲートからデータを移動できます。

オーバーコミットされている集計を表示するレポートを作成する

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。

開始する前に

- アプリケーショ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、ストレージ > アグリゲート をクリックします。

2. [表示] メニューで、[容量] > [すべての集計] 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「集計」列の近くにドラッグします。
5. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] 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すると、結果を容量パーセントで並べ替えることができます。
7. ビューに表示されている内容を反映する特定の名前（例：Aggregates overcommitted）でビューを保存し、チェックマーク（✓）。
8. インベントリページの*スケジュールされたレポート*ボタンをクリックします。
9. 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、「スケジュールの追加」をクリックして「レポート スケジュール」ページに新しい行を追加します。
10. レポートスケジュールの名前を入力し、他のレポートフィールドを入力して、チェックマーク（✓）を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、アグリゲートに容量を追加したり、特定のアグリゲートからデータを移動したりすることができます。

ボリューム容量レポートをカスタマイズする

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。

スナップショットの自動削除がオフになっている、容量がいっぱいに近づいているボリュームを識別するレポートを作成します。

Snapshotの自動削除機能が無効になっていて容量がフルに近づいているボリュームをリストするレポートを作成できます。このレポートは、Snapshotの自動削除を設定する必要があるボリュームを特定するのに役立ちます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順を実行して、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、ストレージ > ボリューム 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. 「Snapshot Autodelete」列と「Days To Full」列を「Available Data Capacity」列の近く

にドラッグ アンド ドロップします。

5. フィルター アイコンをクリックし、次の2つのフィルターを追加して、[フィルターの適用] 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
6. [フルまでの日数] 列の上部をクリックすると、残り日数が最も少ないボリュームがリストの上部に表示されます。
7. ビューに表示されている内容を反映する特定の名前 (例: 「Vols near capacity」) でビューを保存します。
8. インベントリページの*スケジュールされたレポート*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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、ボリュームでSnapshotの自動削除を有効にしたり、使用可能なスペースを増やす方法を特定したりすることができます。

シンプロビジョニングが無効になっているボリュームで使用されているスペースを識別するレポートを作成します

シンプロビジョニングされていないボリュームは、ボリューム作成時に定義されたスペースの全容量をディスク上で占有します。シンプロビジョニングが無効になっているボリュームを特定することで、特定のボリュームでシンプロビジョニングを有効にする必要があるかどうかを判断できます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順を実行して、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、ストレージ > ボリューム をクリックします。
2. [表示] メニューで、[容量] > [すべてのボリューム] を選択します。
3. レポートに不要な列を削除するには、[表示/非表示] を選択します。
4. 「使用データ %」列と「シン プロビジョニング」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. フィルター アイコンをクリックし、次のフィルター「シン プロビジョニング はいいえ」を追加して、「フィルターの適用」 をクリックします。
6. 「使用データ %」列の上部をクリックすると、最も高いパーセンテージのボリュームがリストの上部に表示されるように結果が並べ替えられます。
7. ビューに表示されている内容を反映する名前 (例: 「Vols no thin provisioning」) を付けてビュー

を保存します。

8. インベントリページの*スケジュールされたレポート*ボタンをクリックします。
9. スケジュールの追加 をクリックして、レポート スケジュール ページに新しい行を追加し、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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、特定のボリュームでシンプロビジョニングを有効にすることができます。

データをクラウド層に移動する必要がある**FabricPool**アグリゲート上のボリュームを識別するレポートを作成します

現在FabricPoolアグリゲートにあってクラウド階層に関する推奨事項があり、さらに大量のコールド データがあるボリュームのリストを記載したレポートを作成できます。このレポートは、より多くのコールド (非アクティブ) データをクラウド層にオフロードするために、特定のボリュームの階層化ポリシーを「自動」または「すべて」に変更する必要があるかどうかを判断するのに役立ちます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- FabricPoolアグリゲートを設定しておく必要があります。また、それらのアグリゲート上にボリュームが必要です。

次の手順を実行して、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、ストレージ > ボリューム 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. 列選択で、「ディスク タイプ」列がビューに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. 「ディスク タイプ」列を「クラウド推奨」列の近くにドラッグ アンド ドロップします。
5. フィルター アイコンをクリックし、次の 3 つのフィルターを追加して、[フィルターの適用] をクリックします。
 - ディスクタイプにFabricPoolが含まれる
 - クラウドに関する推奨事項に階層が含まれる
 - 10 GBを超えるコールドデータ

6. [コールド データ]列の上部をクリックして、コールド データの量が最も多いボリュームがビューの先頭に表示されるようにします。
7. ビューに表示されている内容を反映する名前 (例: 「Vols change tiering policy」) を付けてビューを保存します。

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 ≡ 3

Assign Performance Threshold Policy		Clear Performance Threshold Policy		Schedule Report		
Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_vol4	38 GB ☐	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagnfsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

8. インベントリページの*スケジュールされたレポート*ボタンをクリックします。
9. 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、「スケジュールの追加」をクリックして「レポート スケジュール」ページに新しい行を追加します。
10. レポートスケジュールの名前を入力し、他のレポートフィールドを入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示される結果に基づいて、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する必要がある場合があります。

Qtree容量レポートをカスタマイズする

以下に記載するサンプルのカスタム レポートを使用して、qtree容量に関連する潜在的な問題を特定して対処することができます。

ほぼ満杯のqtreeを表示するレポートを作成する

qtreeのストレージ容量と利用率を分析するために、ほぼフルのqtreeを表示するレポートを作成できます。

開始する前に

- アプリケーショ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、ストレージ > **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. 「Disk Used %」列を「Qtrees」列の近くにドラッグします。
4. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] 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. 「ディスク使用率」列の上部をクリックすると、結果を容量のパーセンテージで並べ替えることができます。
6. ビューに表示されている内容を反映する特定の名前（例：「Qtrees nearing full」）でビューを保存し、チェックマーク (✓)。
7. インベントリページの*スケジュールされたレポート*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、レポート スケジュール ページに新しい行を追加し、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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、ディスクのハード リミットやソフト リミットを調整したり（設定されている場合）、qtree間でデータのバランスを調整したりすることができます。

NFS共有レポートをカスタマイズする

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することができます。たとえば、アクセスできないマウント パスがあるボリュームやデフォルトのエクスポート ポリシーを使用するボリュームを表示するように、レポートをカスタマイズできます。

アクセスできないマウントパスを持つボリュームを表示するレポートを作成します

マウント パスにアクセスできないボリュームを特定するレポートを作成できます。

開始する前に

- アプリケーショ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、ストレージ > **NFS** 共有 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. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] 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. ビューに表示されている内容を反映する特定の名前（例：「アクセスできないマウントパスを持つボリューム」）でビューを保存し、チェックマーク (✓)。
5. インベントリページの*スケジュールされたレポート*ボタンをクリックします。
6. スケジュールの追加 をクリックして、レポート スケジュール ページに新しい行を追加し、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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、アクセスできないマウント パスを修正できます。

デフォルトのエクスポート ポリシーを使用しているボリュームを表示するレポートを作成します。

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検出するレポートを作成できます。

開始する前に

- アプリケーショ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、ストレージ > **NFS** 共有 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. 「エクスポート ポリシー」列を「ボリューム」列の近くにドラッグします。
4. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] 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. ビューに表示されている内容を反映する特定の名前（例：デフォルトのエクスポートポリシーを持つボリューム）でビューを保存し、チェックマーク（✓）。
6. インベントリページの*スケジュールされたレポート*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、レポート スケジュール ページに新しい行を追加し、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を入力して、チェックマーク（✓）を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、カスタムのエクスポート ポリシーを設定できます。

ストレージVMレポートをカスタマイズする

Storage VMレポートを作成して、ボリューム情報を分析したり、全体の健全性とストレージの可用性を確認したりできます。たとえば、レポートを作成して、ボリューム数の上限に達したSVMを表示したり、停止したSVMを分析したりできます。

最大ボリューム制限に達したストレージVMを表示するレポートを作成します

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。

開始する前に

- ・アプリケーショ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、ストレージ > ストレージ 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「ストレージ VM」列の近くにドラッグします。
4. 「最大許容ボリューム」列の上部をクリックすると、結果をボリューム数の多い順に並べ替えることができます。
5. ビューに表示されている内容を反映する特定の名前（例：SVMs reached max volumes）でビューを保存し、チェックマーク（✓）。
6. インベントリページの*スケジュールされたレポート*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、レポート スケジュール ページに新しい行を追加し、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を入力して、チェックマーク（✓）を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、Storage VMに割り当てるボリュームを調整できます。また、可能であれば、ONTAP System Managerを使用して許容される最大ボリューム数を変更することができます。

停止したストレージ**VM**を表示するレポートを作成する

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。

開始する前に

- アプリケーショ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、ストレージ > ストレージ **VM** をクリックします。
2. [表示] メニューで、正常性 > すべてのストレージ **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. 「State」列を「Storage VM」列の近くにドラッグします。
5. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] をクリックします。
 - 状態が停止である
6. ビューに表示されている内容を反映する特定の名前（例：Stopped SVMs）でビューを保存し、チェックマーク (✓)。
7. インベントリページの*スケジュールされたレポート*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、レポート スケジュール ページに新しい行を追加し、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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、SVMが停止した理由を調査して、停止しているSVMの再起動が必要かどうかを確認できます。

ボリューム関係レポートをカスタマイズする

ボリューム関係インベントリ レポートでは、クラスタ内のストレージ インベントリの詳細を分析できるほか、ボリュームに必要な保護レベルを把握したり、障害の原因、パターン、スケジュールに基づいてボリュームの詳細をフィルタリングしたりすることができます。

障害の原因別にボリューム関係をグループ化するレポートを作成する

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。

開始する前に

- ・アプリケーショ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、ストレージ > ボリューム をクリックします。
2. [表示] メニューで、[リレーションシップ] > [すべてのリレーションシップ] を選択します。
3. 表示/非表示 を選択して、ビューに「関係の健全性」列と「不健全な理由」列が表示され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. 「関係の健全性」列と「不健全な理由」列を「状態」列の近くにドラッグします。
5. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] をクリックします。
 - 。関係の健全性に問題あり
6. 「異常な理由」列の上部をクリックして、障害の原因別にボリューム関係をグループ化します。
7. ビューに表示されている内容を反映する特定の名前 (例: 「Vol relationship by failure」) でビューを保存します。
8. インベントリページの*スケジュールされたレポート*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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、障害のタイプごとに原因と影響を調査できます。

問題別にボリューム関係をグループ化するレポートを作成する

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。

開始する前に

- ・アプリケーショ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、ストレージ > ボリューム をクリックします。

2. [表示] メニューで、[リレーションシップ] > [すべてのリレーションシップ] 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. 「Unhealthy Reason」列を「State」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内容を反映する特定の名前 (例: 「Vol relationship by issue」) でビューを保存します。
7. インベントリページの*スケジュールされたレポート*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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、問題のタイプごとに原因と影響を調査できます。

特定の時間間隔でのボリューム転送の傾向を表示するレポートを作成します

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を作成できます。

開始する前に

- ・アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、特定の期間のボリュームを表示するカスタム ビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーション ペインで、ストレージ > ボリューム をクリックします。
2. [表示] メニューで、関係 > 過去 1 か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. 「転送期間」列を「操作結果」列の近くにドラッグします。
5. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] をクリックします。
 - 転送終了時間が過去7日間以内
6. 「転送期間」列の上部をクリックすると、ボリュームを時間間隔で並べ替えることができます。
7. ビューに表示されている内容を反映する特定の名前 (例: 「Volumes by duration」) でビューを保存します。
8. インベントリページの*スケジュールされたレポート*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「毎週」に設定し、他のレポートフィールドに入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、転送期間を調査できます。

ボリューム転送の失敗または成功を表示するレポートを作成します

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。

開始する前に

- アプリケーショ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、ストレージ > ボリューム をクリックします。
2. [表示] メニューで、関係 > 過去 1 か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「状態」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すると、ボリュームをステータス別に並べ替えることができます。
6. ビューに表示されている内容を反映する特定の名前 (例: 「転送ステータス別のボリューム」) でビューを保存します。
7. インベントリページの*スケジュールされたレポート*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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、転送ステータスを調査できます。

転送サイズに基づいてボリューム転送を表示するレポートを作成します

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を作成できます。

開始する前に

- アプリケーショ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、ストレージ > ボリューム をクリックします。
2. [表示] メニューで、関係 > 過去 1 か月の転送率 を選択します。
3. 「合計転送サイズ」列の上部をクリックすると、ボリューム転送をサイズ順に並べ替えることができます。
4. ビューに表示されている内容を反映する特定の名前 (例: 「転送サイズ別のボリューム」) でビューを保存します。

5. インベントリページの*スケジュールされたレポート*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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、ボリューム関係を転送サイズ別に調査できます。

日別にグループ化されたボリューム転送を表示するレポートを作成します

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。

開始する前に

- アプリケーショ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、ストレージ > ボリューム をクリックします。
2. [表示] メニューで、関係 > 過去 1 か月の転送率 を選択します。
3. 「日」列の上部をクリックすると、ボリューム転送が日ごとに並べ替えられます。
4. ビューに表示されている内容を反映する特定の名前 (例: 「Volume transfers by day」) でビューを保存します。
5. インベントリページの*スケジュールされたレポート*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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、ボリューム転送を日付別に調査できます。

ボリュームパフォーマンスレポートをカスタマイズする

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が有効になってい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を作成します。

FabricPool以外のアグリゲート上のコールド データを大量に含むボリュームを表示するレポートを作成できます。このレポートから、FabricPoolアグリゲートに移動する必要があるボリュームを特定できます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。

次の手順に従って、FabricPool対応でないアグリゲート上のコールド データを大量に含むボリュームを表示するカスタム ビューを作成し、そのビューのレポートを生成するようにスケジュール設定します。

手順

1. 左側のナビゲーション ペインで、ストレージ > ボリューム 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. 表示/非表示 を選択して、ビューに「ディスク タイプ」列が表示され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. 「ディスク タイプ」列を「コールド データ」列の近くにドラッグします。
5. フィルター アイコンをクリックし、次のフィルターを追加して、[フィルターの適用] 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) が下部になるようにボリュームをディスク タイプ別に並べ替えます。
7. ビューに表示されている内容を反映する特定の名前 (例: "Cold data vols not FabricPool") でビューを保存します。
8. インベントリページの*スケジュールされたレポート*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を入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、FabricPoolアグリゲートに移動した方がよいボリュームを特定できます。

Microsoft Excelのサンプル レポート

ここでは、Microsoft Excelのサンプル レポートをととして、Excelの高度な機能を使用したレポート オプションを紹介します。

Excelの高度な機能により、ニーズに合わせたさまざまなレポートを作成することができます。Excelの詳細な使用方法については、製品ドキュメントを参照してください。



レポートを操作するには、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。

総容量表とグラフを表示するレポートを作成する

合計および集合縦棒グラフ形式を使用して、容量を分析するためのレポートをExcelファ

イルで作成できます。

開始する前に

- ・アプリケーション管理者またはストレージ管理者のロールが必要です。

以下の手順に従って、「ヘルス: すべての集計」ビューを開き、Excel でビューをダウンロードし、使用可能な容量チャートを作成し、カスタマイズされた Excel ファイルをアップロードして、最終レポートをスケジュールします。

手順

1. 左側のナビゲーション ペインで、ストレージ > アグリゲート 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。



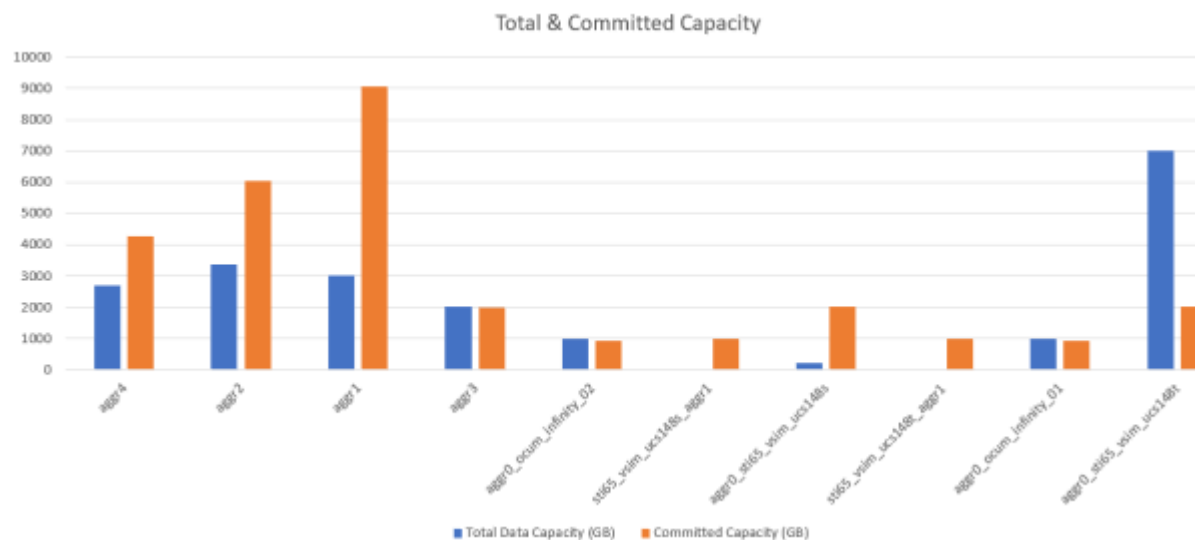
ブラウザによっては、ファイルを保存するために「OK」をクリックする必要がある場合があります。

3. 必要に応じて、[編集を有効にする]をクリックします。
4. ダウンロードしたファイルをExcelで開きます。
5. 新しいシートを作成する（）の後に `data` シートに「**Total Data Capacity**」という名前を付けます。
6. 作成した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。必ず、dataシート（data!）を参照し、キャプチャされたデータの正しい列と行を参照してください（Total Data CapacityはE列の2～20行目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)

この式は、現在のデータに基づいて各列の値を合計します。

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. データシートで、合計データ容量 (GB) 列と コミット容量 (GB) 列を選択します。
2. *挿入*メニューから*推奨グラフ*を選択し、*集合縦棒*グラフを選択します。
3. チャートを右クリックして「チャートを移動」を選択すると、チャートが `Total Data Capacity` シート。
4. グラフを選択すると表示される デザイン メニューと 書式 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。



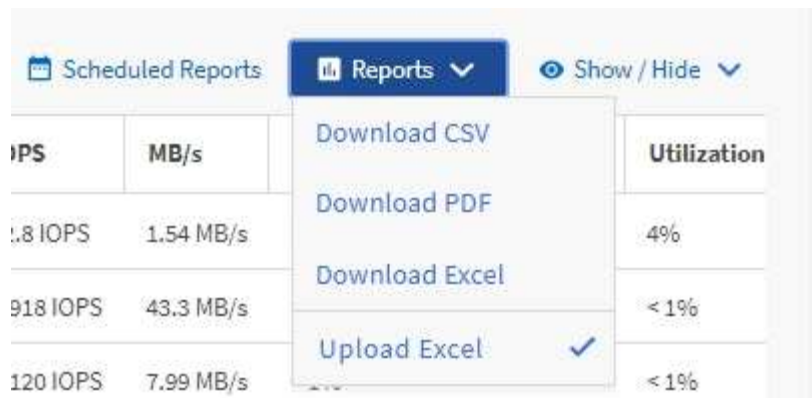
6. Unified Manager で、レポート > **Excel** のアップロード を選択します。



Excelファイルをダウンロードしたときと同じビューが表示されていることを確認してください。

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. *送信*をクリックします。

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。



10. *スケジュールされたレポート*をクリックします。
11. 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、「スケジュールの追加」をクリックして「レポート スケジュール」ページに新しい行を追加します。



レポートの **XLSX** 形式を選択します。

12. レポートスケジュールの名前を入力し、他のレポートフィールドを入力して、チェックマーク (✓) を行の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、どうすればネットワーク全体で使用可能容量を有効に利用できるかを調べることができます。

合計合計と利用可能な容量のグラフを表示するレポートを作成します

ストレージの合計容量とコミット済み容量を分析するためのExcelグラフ形式のレポートを作成できます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。

以下の手順に従って、「ヘルス: すべての集計」ビューを開き、Excel でビューをダウンロードし、合計容量とコミット容量のチャートを作成し、カスタマイズされた Excel ファイルをアップロードして、最終レポートをスケジュールします。

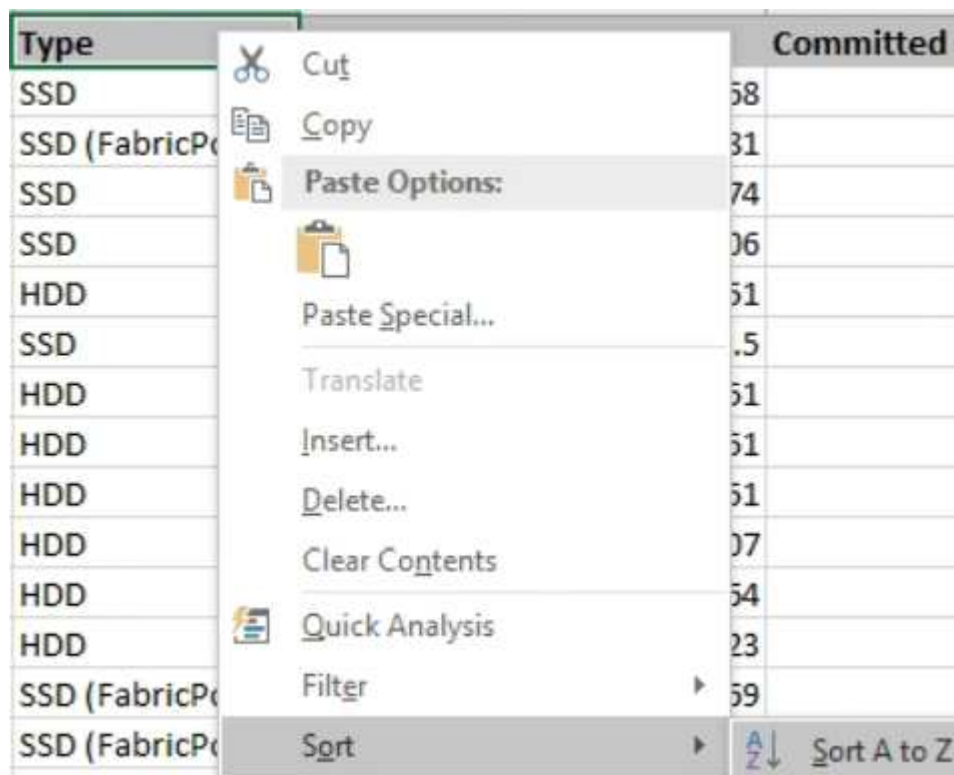
手順

1. 左側のナビゲーション ペインで、ストレージ > アグリゲート 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る場合があります。

3. ダウンロードしたファイルをExcelで開きます。
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]列を右クリックし、[並べ替え]>[AからZの並べ替え]を選択します。



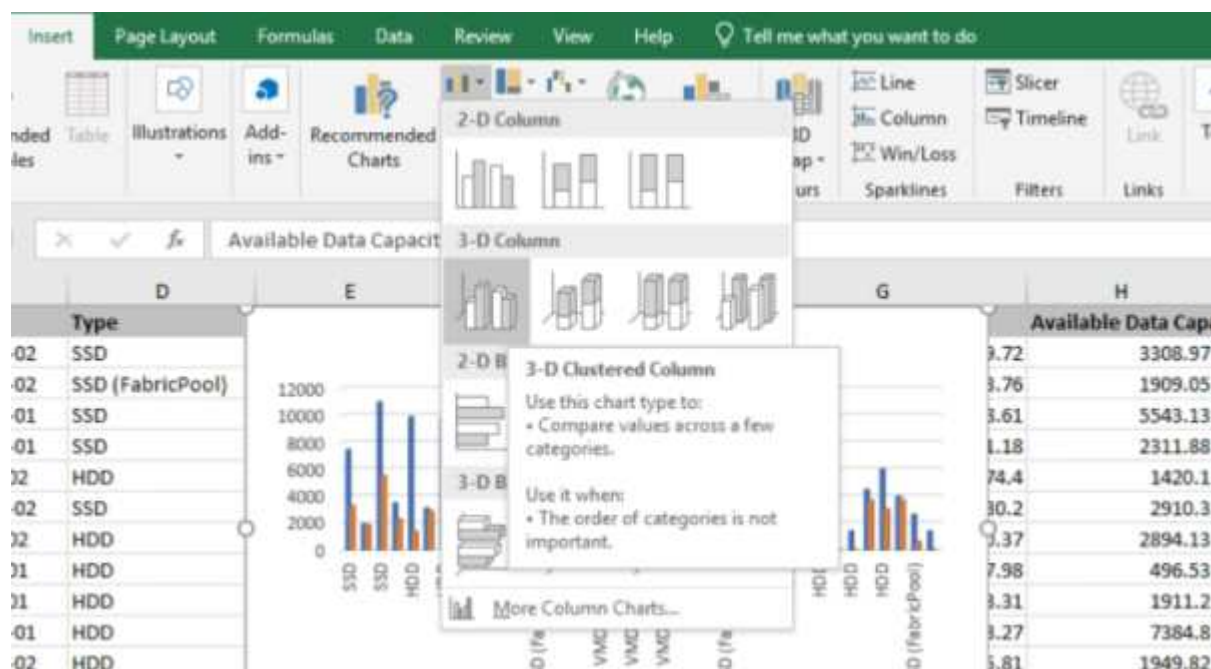
次のようなストレージタイプ別にデータが並べ替えられます。

- HDD
- ハイブリッド
- SSD
- SSD (FabricPool)

6. 選択してください `Type, Total Data Capacity,`そして `Available Data Capacity`列。

7. *挿入*メニューで、`3-D column`チャート。

グラフがdataシートに表示されます。



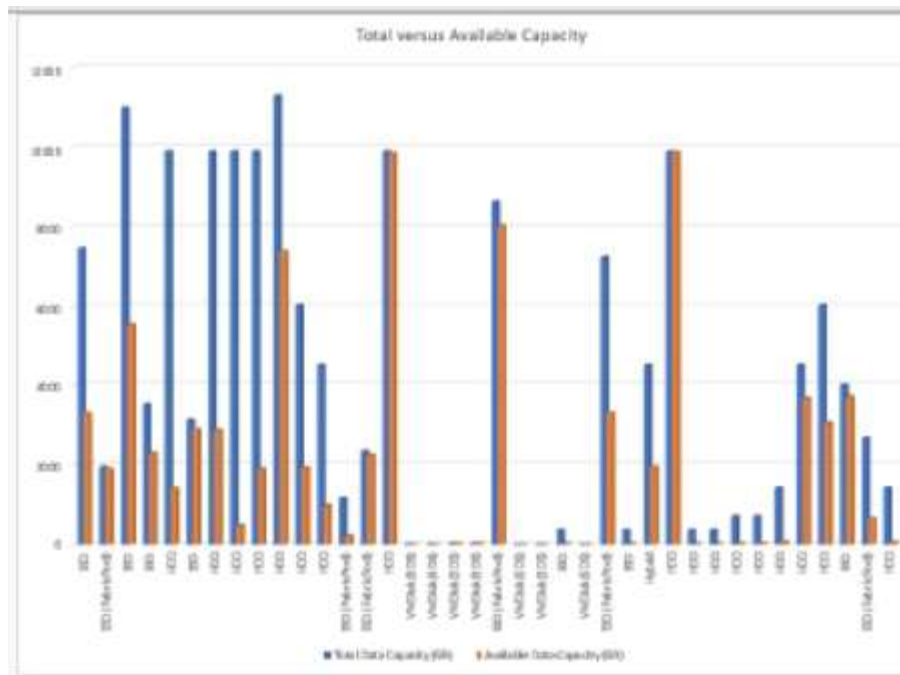
8. グラフを右クリックし、[グラフの移動]を選択します。

9. *新しいシート*を選択し、シートに*Total Storage Charts*という名前を付けます。



infoシートとdataシートのあとに新しいシートが表示されることを確認してください。

10. グラフのタイトルに「合計容量と使用可能な容量」という名前を付けます。
11. グラフを選択すると表示される デザイン メニューと 書式 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是不変しないでください。



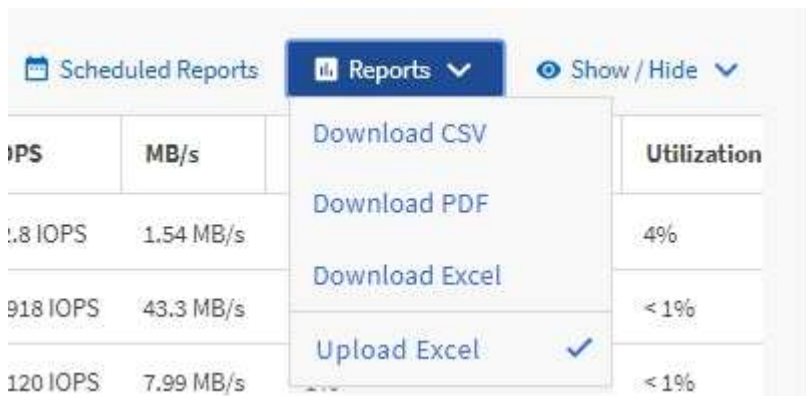
13. Unified Manager で、レポート > **Excel** のアップロードを選択します。



Excelファイルをダウンロードしたときと同じビューが表示されていることを確認してください。

14. 変更したExcelファイルを選択します。
15. *開く*をクリックします。
16. *送信*をクリックします。

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。



17. *スケジュールされたレポート*をクリックします。
18. スケジュールの追加 をクリックして、レポート スケジュール ページに新しい行を追加し、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します。



レポートの **XLSX** 形式を選択します。

19. レポートスケジュールの名前を入力し、他のレポートフィールドを入力して、チェックマーク (✓) を行

の末尾に追加します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、アグリゲートの負荷を分散できます。

利用可能なボリューム容量チャートを表示するレポートを作成します

使用可能なボリューム容量を分析するためのExcelグラフ形式のレポートを作成できます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。

以下の手順に従って、「ヘルス: すべてのボリューム」ビューを開き、Excel でビューをダウンロードし、使用可能な容量チャートを作成し、カスタマイズされた Excel ファイルをアップロードし、最終レポートをスケジュールします。

手順

1. 左側のナビゲーション ペインで、ストレージ > ボリューム 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る場合があります。

3. 必要に応じて、[編集を有効にする]をクリックします。
4. ダウンロードしたファイルをExcelで開きます。
5. オンザ data シートで、使用したいデータを選択します。 `Volume`そして `Available Data` 列。
6. *挿入*メニューで、 3-D piechart.

使用可能なスペースが最も多いボリュームがグラフに表示されます。グラフがdataシートに表示されません。

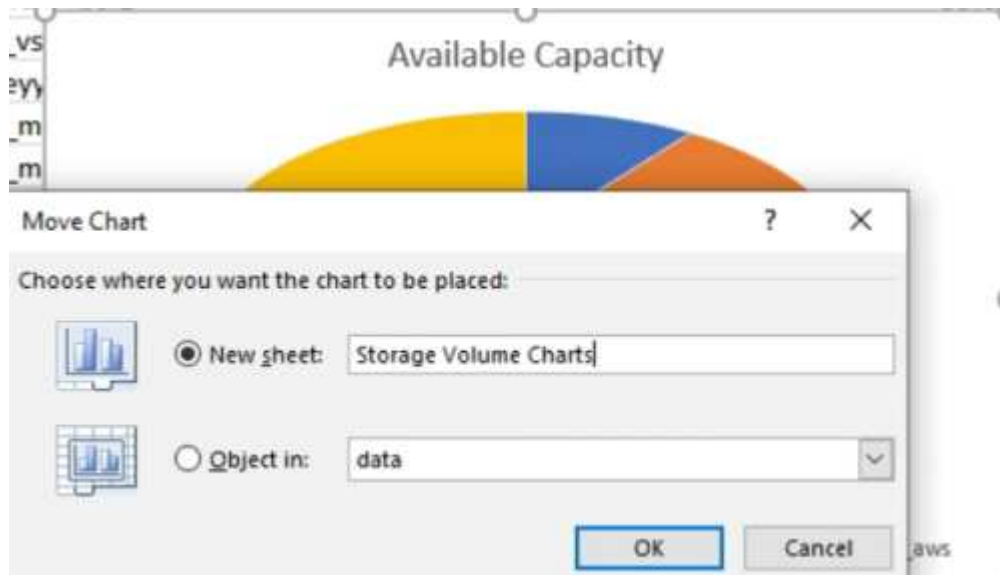


ネットワーク設定によっては、列全体を選択したり、選択したデータ行が多すぎると、円グラフが読めなくなることがあります。このサンプルでは3-D円グラフを使用していますが、任意のグラフタイプを使用できます。キャプチャするデータが適切に表示されるグラフを使用してください。

7. グラフのタイトルに「使用可能な容量」という名前を付けます。
8. グラフを右クリックし、[グラフの移動] を選択します。
9. *新しいシート*を選択し、シートに*ストレージボリュームチャート*という名前を付けます。



infoシートとdataシートのあとに新しいシートが表示されることを確認してください。



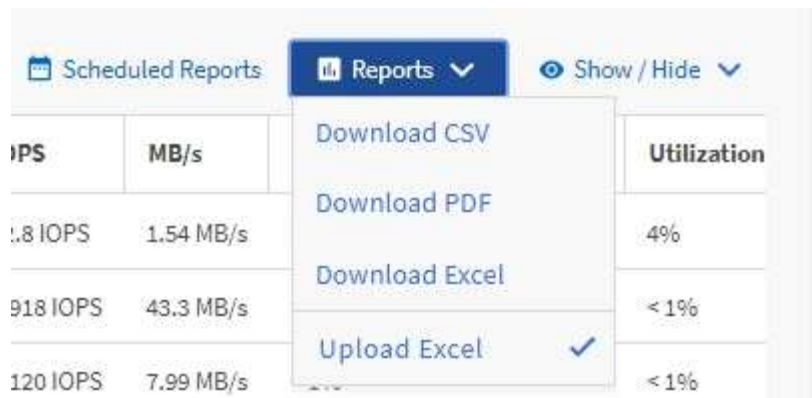
10. グラフを選択すると表示される デザイン メニューと 書式 メニューを使用して、グラフの外観をカスタマイズできます。
11. 問題がなければ、変更したファイルを保存します。
12. Unified Manager で、レポート > **Excel** のアップロード を選択します。



Excelファイルをダウンロードしたときと同じビューが表示されていることを確認してください。

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. *送信*をクリックします。

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。



16. *スケジュールされたレポート*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、レポート スケジュール ページに新しい行を追加し、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を入力して、チェックマーク (✓) を行の末尾に追加します。



レポートの **XLSX** 形式を選択します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、ボリュームの負荷を分散できます。

利用可能なIOPSが最も高いアグリゲートを表示するレポートを作成する

このレポートは、使用可能なIOPSが最も多く、新しいワークロードをプロビジョニング可能なアグリゲートをアグリゲート タイプ別に表示します。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。

以下の手順に従って、「ヘルス: すべてのボリューム」ビューを開き、Excel でビューをダウンロードし、使用可能な容量チャートを作成し、カスタマイズされた Excel ファイルをアップロードし、最終レポートをスケジュールします。

手順

1. 左側のナビゲーション ペインで、ストレージ > アグリゲート をクリックします。
2. *表示*ドロップダウンから*パフォーマンス: すべての集計*を選択します。
3. *表示/非表示*を選択して表示します `Available IOPS`列を非表示にして `Cluster FQDN, Inactive Data Reporting,`そして `Threshold Policy`列。
4. ドラッグアンドドロップ `Available IOPS`そして `Free Capacity`隣の列 `Type`カラム。
5. カスタムビューに名前を付けて保存します Available IOPS Per Aggr.
6. レポート > **Excel** のダウンロード を選択します。



ブラウザによっては、ファイルを保存するために「OK」をクリックする必要がある場合があります。

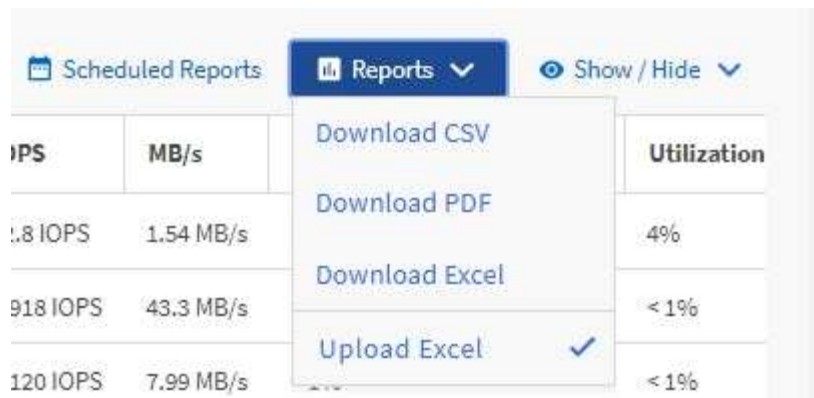
7. 必要に応じて、[編集を有効にする]をクリックします。
8. ダウンロードしたファイルをExcelで開きます。
9. dataシートの左上にある小さい三角形をクリックして、シート全体を選択します。
10. *データ*リボンで、Sort & Filter area.
11. 次の並べ替えレベルを設定します。
 - a. *並べ替え*を次のように指定します Available IOPS (IOPS) 、*ソートオン*として Cell Values, `そして\*順序\*は `Largest to Smallest.
 - b. *レベルの追加*をクリックします。
 - c. 並べ替え*を次のように指定します **Type**、*並べ替えの基準 Cell Values, `そして\*順序\*は `Z to A.
 - d. *レベルの追加*をクリックします。
 - e. *並べ替え*を次のように指定します Free Capacity (GB) , *並べ替え*として Cell Values, `そして\*順序\*は `Largest to Smallest.
 - f. [OK]をクリックします。
12. Excelファイルを保存して、閉じます。
13. Unified Manager で、レポート > **Excel** のアップロード を選択します。



Excelファイルをダウンロードしたときと同じビューが表示されていることを確認してください。

14. 変更したExcelファイルを選択します。この場合は performance-aggregates-<date>.xlsx.
15. *開く*をクリックします。
16. *送信*をクリックします。

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。



17. *スケジュールされたレポート*をクリックします。
18. 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、「スケジュールの追加」をクリックして「レポート スケジュール」ページに新しい行を追加します。
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を入力して、チェックマーク (✓) を行の末尾に追加します。



レポートの **XLSX** 形式を選択します。

テスト レポートがすぐに送信されます。以降、指定した頻度でレポートが生成され、リスト内の受信者にEメールで送信されます。

レポートに表示された結果を基に、使用可能なIOPSが最も多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の使用を開始する

Active IQ Unified Managerには、サポート対象のストレージ システム上のストレージ リソースをRESTful Webサービス インターフェイスを介して管理することにより、あらゆるサードパーティ製品と統合するための一連のAPIが用意されています。

このドキュメントの各トピックでは、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、およびいくつかのサンプル コードを紹介します。この情報を使用して、NetApp Manageabilityソフトウェア ソリューションのRESTfulクライアントを作成し、NetAppシステムを管理することができます。APIは、Representational State Transfer (REST) アーキテクチャ スタイルに基づいています。Create、Read、Update、Delete (CRUDとも呼ばれる) の4つすべてのREST処理がサポートされています。

見る["Active IQ Unified Manager"](#)Active IQ Unified Manager REST API の利点に関する追加リソースと詳細については、こちらをご覧ください。

このドキュメントの対象読者

このドキュメントは、REST APIを使用してActive IQ Unified Managerソフトウェアと連携するアプリケーションを作成する開発者を対象としています。

ストレージ管理者とストレージ設計者は、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ためのクライアント アプリケーションを構築する方法について、この情報を参照して基本的な知識を得ることができます。

ストレージ プロバイダ、ONTAPクラスタ、および管理APIを使用してストレージを管理する場合は、この情報を参照してください。



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必要です。REST API を実行する Unified Manager サーバーの IP アドレスまたは完全修飾ドメイン名を知っておく必要があります。

Active IQ Unified Manager APIアクセスとカテゴリ

Active IQ Unified Manager API を使用すると、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。これらの機能の一部を実行するには、Unified Manager Web UI にアクセスすることもできます。

REST APIに直接アクセスするためのURLを構築する

Python、C#、C++、JavaScript などのプログラミング言語を通じて REST API に直接アクセスできます。以下の形式でホスト名またはIPアドレスとURLを入力して、REST APIにアクセスします。

`https://<ホスト名>/api`



デフォルト 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APIドキュメントページにアクセスする

製品に同梱されている API ドキュメント 参照コンテンツ ページにアクセスして、API ドキュメントを表示したり、手動で API 呼び出し (Swagger などのインターフェース上) を発行したりすることができます。このドキュメントにアクセスするには、メニューバー > ヘルプボタン > *APIドキュメント*をクリックします。

または、以下の形式でホスト名またはIPアドレスとURLを入力して、REST APIページにアクセスします。

`https://<ホスト名>/docs/api/`

カテゴリ

API呼び出しは、分野（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 に付属する REST API は、管理、監視、プロビジョニング機能を実行するのに役立ちます。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。

- 管理サーバー

*manage-server*カテゴリのAPIには、`jobs`、`system`、`そして `events` API。ジョブは、Unified Manager 上のストレージ オブジェクトまたはワークロードの管理に関連して、非同期実行するようにスケジュールされた操作です。その `events` APIはデータセンター内のイベントを返し、`system` API は Unified Manager インスタンスの詳細を返します。

- ストレージプロバイダー

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、これらのAPIを使用してアクセス エンドポイントやActive Directoryを設定したり、ストレージ ワークロードにパフォーマンス サービス レベルとストレージ効率化ポリシーを割り当てたりできます。

- 管理

このカテゴリには、管理タスクを実行するために使用するAPIが含まれています。バックアップ設定を管理したり、信頼ストアにあるUnified Managerデータソースの証明書を確認したり、ONTAPクラスターをUnified Managerのデータソースとして管理したりできます。

- ゲートウェイ

Unified Managerでgateway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。

- 安全

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 サービスと操作について知っておく必要があります。

APIサーバの設定に使用されるプロビジョニングAPIと管理APIでは、読み取り（GET）処理または書き込み（POST、PATCH、DELETE）処理がサポートされます。APIでサポートされるGET、PATCH、POST、およびDELETE処理のいくつかの例を次に示します。

- GETの例: `GET /datacenter/cluster/clusters` データセンター内のクラスターの詳細を取得します。返されるレコードの最大数は、`GET`操作は1000です。



APIでは、サポートされる属性でレコードのフィルタ、ソート、並べ替えが可能です。

- POSTの例: `POST /datacenter/svm/svms` カスタム ストレージ仮想マシン (SVM) を作成します。
- PATCHの例: `PATCH /datacenter/svm/svms/{key}` 一意のキーを使用して SVM のプロパティを変更します。
- DELETEの例: `DELETE /storage-provider/access-endpoints/{key}` 一意のキーを使用して、LUN、SVM、またはファイル共有からアクセス エンドポイントを削除します。

APIを使用して実行できるREST処理は、ユーザ ロール（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）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
オペレーター	データへの読み取り専用アクセス。このロールのユーザは、すべてのGET要求を実行できます。
ストレージ管理者	すべてのデータへの読み取りアクセス。このロールのユーザは、すべてのGET要求を実行できます。 また、管理、ストレージ サービス オブジェクト、ストレージ管理オプションなどの特定のアクティビティを実行するための書き込みアクセス（PATCH、POST、およびDELETE要求を実行するため）が可能です。
アプリケーション管理者	すべてのデータへの読み取りおよび書き込みアクセス。このロールのユーザは、すべての機能に対するGET、PATCH、POST、およびDELETE要求を実行できます。

すべての REST 操作の詳細については、オンライン API ドキュメントを参照してください。

Active IQ Unified ManagerでのAPIのバージョン管理

Active IQ Unified Managerの REST API URI はバージョン番号を指定します。例えば、`/v2/datacenter/svm/svms.`バージョン番号 `v2`で `/v2/datacenter/svm/svms`特定のリリ

ースで使用される API バージョンを示します。バージョン番号を指定することで、クライアントが処理可能な応答が返されるため、APIの変更によるクライアント ソフトウェアへの影響が最小限に抑えられます。

このバージョン番号の数値部分は、リリースごとに増分されます。URIにバージョン番号を指定することにより、将来のリリースでも下位互換性を保持した一貫したインターフェイスが提供されます。バージョンのない同じAPIも見つかります。例えば `/datacenter/svm/svms`、バージョンなしで基本 API を示します。ベースAPIは常に最新バージョンのAPIです。



Swaggerインターフェイスの右上の領域で、使用するAPIのバージョンを選択できます。デフォルトでは、最新バージョンが選択されています。特定のAPIについて、Unified Managerインスタンスで使用可能な（最も大きな数字の）最新バージョンを使用することを推奨します。

すべての要求に対して、使用するAPIバージョンを明示的に指定する必要があります。バージョン番号を指定すると、アプリケーションが処理できない応答要素は返されません。REST要求には、バージョン パラメータを含める必要があります。以前のバージョンのAPIは、数回のリリース後、最終的に廃止されます。このリリースでは、v1 API のバージョンは非推奨です。

ONTAPのストレージ リソース

ONTAPのストレージ リソースは、大きく分けて 物理ストレージ リソース と 論理ストレージ リソース に分類できます。Active Active IQ Unified Managerで提供される API を使用してONTAPシステムを効果的に管理するには、ストレージ リソース モデルとさまざまなストレージ リソース間の関係を理解する必要があります。

- 物理ストレージリソース

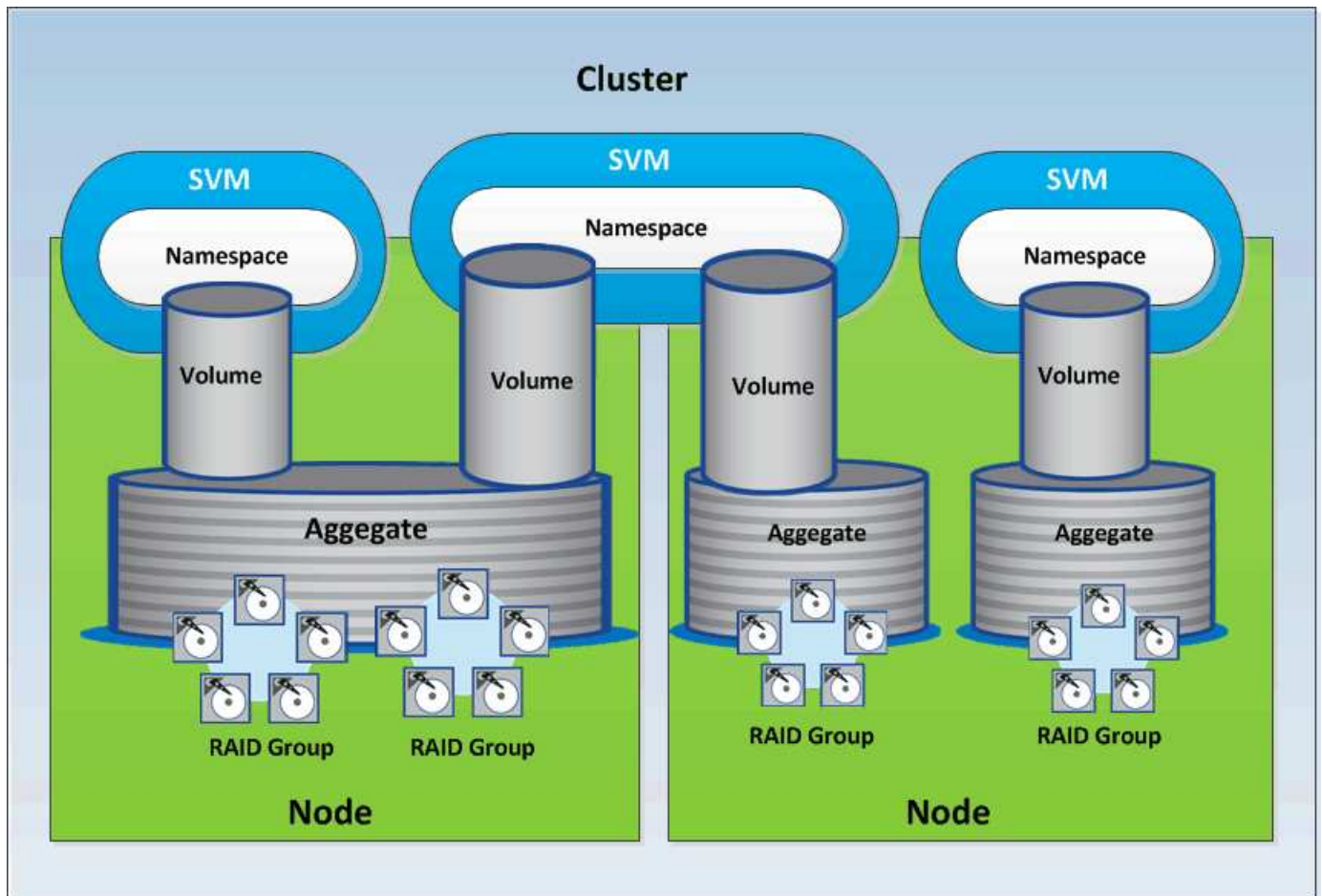
ONTAPが提供する物理ストレージ オブジェクトのことです。物理ストレージ リソースには、ディスク、クラスタ、ストレージ コントローラ、ノード、およびアグリゲートがあります。

- 論理ストレージリソース

物理リソースに関連付けられていない、ONTAPが提供するストレージ リソースのことです。これらのリソースはStorage Virtual Machine (SVM、旧Vserver) に関連付けられていて、ディスク、アレイLUN、アグリゲートなどの特定の物理ストレージ リソースには紐づけられていません。

論理ストレージ リソースには、すべてのタイプのボリュームとqtreeだけでなく、Snapshotコピー、重複排除、圧縮、クォータなど、これらのリソースで利用できる機能および設定も含まれます。

次の図は、2ノード クラスタのストレージ リソースを示しています。



Active IQ Unified ManagerでのREST APIへのアクセスおよび認証

Active IQ Unified Manager REST APIには、基本的なHTTP認証メカニズムによるHTTP要求を実行できる任意の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。

要求と応答の例を次に示します。

• 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` API サーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN) です。
- ポート443

443は、デフォルトのHTTPSポートです。必要に応じて、HTTPSポートをカスタマイズできます。

WebブラウザからHTTP要求を実行するには、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ます。情報の流れ（要求と応答）をセキュリティで保護するために、REST APIにはHTTPS経由でのみアクセスできます。APIサーバは、サーバ検証のためにすべてのクライアントに自己署名のSSL証明書を提供します。この証明書は、カスタム証明書（またはCA証明書）で置き換えることができます。

REST APIを呼び出すには、APIサーバへのユーザ アクセスを設定する必要があります。ユーザには、ローカ

ル ユーザ（ローカル データベースに格納されているユーザ プロファイル）またはLDAPユーザ（LDAP経由で認証するようにAPIサーバを設定している場合）を指定できます。Unified Manager Administration Consoleのユーザ インターフェイスにログインして、ユーザ アクセスを管理できます。

Active IQ Unified Managerで使用されるHTTPステータスコード

API を実行したり、問題をトラブルシューティングしたりするときは、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 コードに注意する必要があります。

次の表は、認証に関連するエラー コードを示しています。

HTTPステータス コード	ステータスコードのタイトル	説明
200	OK	同期API呼び出しの実行に成功した場合に返されます。
201	作成	Active Directoryの設定など、同期呼び出しによって新しいリソースが作成されたことを示します。
202	承認済み	LUNやファイル共有の作成など、プロビジョニング機能の非同期呼び出しの実行が成功したときに返されます。
400	Invalid request	入力検証に失敗したことを示します。ユーザは、要求本文に有効なキーを指定するなど、入力を修正する必要があります。
401	Unauthorized request	リソースの表示を許可されていません/権限がありません。
403	Forbidden request	接続しようとしたリソースへのアクセスは禁止されています。
404	Resource not found	アクセスしようとしたリソースが見つかりません。
405	Method Not Allowed	許可されていないメソッドです。
429	Too Many Requests	ユーザから一定の時間内に送信された要求が多すぎる場合に返されます。

HTTPステータス コード	ステータスコードのタイトル	説明
500	Internal server error	内部サーバーエラー。サーバから応答を取得できませんでした。この内部サーバー エラーは永続的である場合もそうでない場合もあります。例えば、`GET`または`GET ALL`操作を実行してこのエラーが発生した場合は、この操作を少なくとも5回再試行することをお勧めします。永続的なエラーの場合、引き続きステータス コード500が返されます。処理が成功した場合、ステータス コード200が返されます。

Active IQ Unified ManagerのAPIの使用に関する推奨事項

Active IQ Unified Managerで API を使用する場合は、特定の推奨プラクティスに従う必要があります。

- 応答のコンテンツ タイプをすべて次の形式にする必要があります。

```
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 バージョンの詳細については、「Active IQ Unified Managerでの REST API のバージョン管理」セクションを参照してください。
- Unified Manager APIを使用して配列値を更新する場合は、値の文字列全体を更新する必要があります。配列に値を付加することはできません。既存の配列のみを置換できます。
- メトリック API の IOPS やパフォーマンスなどの double 値を除くすべてのクエリ パラメータに、パイプ (|) やワイルド カード (++) などのフィルタ演算子を使用できます。
- フィルター演算子ワイルドカード (++) とパイプ (|) の組み合わせを使用してオブジェクトをクエリすることは避けてください。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。
- フィルタの値を使用する場合は、値に次のものが含まれていないことを確認してください。`?` キャラクター。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。
- 注意してください `GET` どの API に対しても、(すべての) リクエストは最大 1000 件のレコードを返します。クエリを次のように設定して実行したとしても、`max\_records` パラメータを 1000 より大きい値に設定すると、1000 件のレコードのみが返されます。
- 管理機能を実行するには、Unified Manager UI を使用することをお勧めします。

トラブルシューティング用のログ

システム ログを使用して、APIの実行中に発生する可能性のある障害の原因を分析し、問題のトラブルシューティングを実行できます。

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	用途
<code>/var/log/ocie/access_log.log</code>	APIを呼び出しているユーザ名、開始時刻、実行時間、ステータス、URLなど、API呼び出しに関するすべての詳細情報が含まれます。 このログ ファイルを使用して、頻繁に使用されるAPIを確認したり、GUIワークフローのトラブルシューティングを行うことができます。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。
<code>/var/log/ocum/ocumserver.log</code>	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。
<code>/var/log/ocie/server.log</code>	すべてのWildflyサーバ構成と、サービスの開始 / 停止に関連するログが含まれています。 このログ ファイルを使用して、Wildflyサーバの開始、停止、または導入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。
<code>/var/log/ocie/au.log</code>	Acquisition Unit関連のログが含まれます。 ONTAPでオブジェクトを作成、変更、または削除したが、Active IQ Unified Manager REST API に反映されない場合に、このログ ファイルを使用できます。

ジョブ オブジェクトの非同期プロセス

Active IQ Unified Managerは、`jobs`他の API の実行中に実行されたジョブに関する情報を取得する API。ジョブ オブジェクトを使用して非同期処理がどのように機能するかを理解する必要があります。

一部のAPI呼び出し、特にリソースの追加や変更を使用されるAPI呼び出しは、他の呼び出しよりも完了に時間がかかることがあります。Unified Manager は、これらの長時間実行要求を非同期的に処理します。

ジョブ オブジェクトを使用して記述された非同期要求

非同期的に実行されるAPI呼び出しを行うと、HTTP応答コード202が返されます。この応答コードは、要求が正常に検証され受け入れられたものの、まだ完了していないことを示します。要求はバックグラウンド タスクとして処理され、クライアントへの最初のHTTP応答後も引き続き実行されます。応答には、要求に対応するジョブ オブジェクトと、その一意の識別子が含まれます。

APIリクエストに関連付けられたジョブオブジェクトをクエリする

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、2つの方法があります。

- 標準ポーリング要求: 現在のジョブの状態がすぐに返されます。
- ロングポーリングリクエスト:ジョブの状態が `NORMAL`, `ERROR`, `または` `PARTIAL_FAILURES`.

非同期要求の手順

以下は、非同期API呼び出しを完了する手順の概要です。

1. 非同期API呼び出しを実行します。
2. 要求が正常に受け取られたことを示すHTTP応答202を受信します。
3. 応答の本文からジョブ オブジェクトの識別子を抽出します。
4. ループ内で、ジョブオブジェクトが終了状態に達するまで待機します。 `NORMAL`, `ERROR`, `または` `PARTIAL_FAILURES`.
5. ジョブの最終状態を確認し、ジョブの結果を取得します。

Hello API server

Hello API サーバー は、単純な 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は、APIサーバーに関する基本的な情報をJSON形式で提供します（サーバーは ``application/json`` 形式）。

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 コードは次の入力パラメータを取ります。

- 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 を呼び出すには、Jersey や RESTEasy などの他のスクリプトを使用して、Active IQ Unified

Manager用の Java REST クライアントを作成することもできます。サンプル コードに関して、次の点に注意する必要があります。

- Active IQ Unified ManagerへのHTTPS接続を使用して、指定されたREST URIを呼び出します。
- Active IQ Unified Managerによって提供された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する
- 用途 `javax.net.ssl.HttpsURLConnection` URI接続の場合
- サードパーティのライブラリを使用する(`org.apache.commons.codec.binary.Base64` HTTP基本認証で使われるBase64エンコードされた文字列を構築するための

サンプル コードをコンパイルして実行するには、バージョン1.8以降のJavaコンパイラを使用する必要があります。

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpsURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import org.apache.commons.codec.binary.Base64;

public class HelloApiServer {

    private static String server;
    private static String user;
    private static String password;
    private static String response_format = "json";
    private static String server_url;
    private static String port = null;

    /*
     * * The main method which takes user inputs and performs the *
    necessary steps
     * to invoke the REST URI and show the response
    */ public static void main(String[] args) {
        if (args.length < 2 || args.length > 3) {
            printUsage();
            System.exit(1);
        }
        setUserArguments(args);
```

```

String serverBaseUrl = "https://" + server;
if (null != port) {
    serverBaseUrl = serverBaseUrl + ":" + port;
}
server_url = serverBaseUrl + "/api/datacenter/svm/svms";
try {
    HttpsURLConnection connection =
getAllTrustingHttpsURLConnection();
    if (connection == null) {
        System.err.println("FATAL: Failed to create HTTPS
connection to URL: " + server_url);
        System.exit(1);
    }
    System.out.println("Invoking API: " + server_url);
    connection.setRequestMethod("GET");
    connection.setRequestProperty("Accept", "application/" +
response_format);
    String authString = getAuthorizationString();
    connection.setRequestProperty("Authorization", "Basic " +
authString);
    if (connection.getResponseCode() != 200) {
        System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
+ connection.getResponseMessage());
        System.exit(1);
    }
    BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
    String response;
    System.out.println("Response:");
    while ((response = br.readLine()) != null) {
        System.out.println(response);
    }
    connection.disconnect();
} catch (Exception e) {
    e.printStackTrace();
}
}

/* Print the usage of this sample code */ private static void
printUsage() {
    System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
    System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
    System.out.println("\tHelloApiServer 10.22.12.34:8320 admin

```

```

password");
    System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
    System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
    System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
}

/* * Set the server, port, username and password * based on user
inputs. */ private static void setUserArguments(
    String[] args) {
    server = args[0];
    user = args[1];
    password = args[2];
    if (server.contains(":")) {
        String[] parts = server.split(":");
        server = parts[0];
        port = parts[1];
    }
}

/*
 * * Create a trust manager which accepts all certificates and * use
this trust
 * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
 * SSL Context and skip * server hostname verification during SSL
handshake. * *
 * Note: Trusting all certificates or skipping hostname verification *
is not
 * required for API Services to work. These are done here to * keep
this sample
 * REST Client code as simple as possible.
 */ private static HttpsURLConnection
getAllTrustingHttpsURLConnection() {
    HttpsURLConnection conn =
null;
    try {
        /* Creating a trust manager that does not
validate certificate chains */
        TrustManager[]
trustAllCertificatesManager = new
TrustManager[]{new
X509TrustManager(){
    public X509Certificate[] getAcceptedIssuers(){return null;}
    public void checkClientTrusted(X509Certificate[]
certs, String authType){}
    public void checkServerTrusted(X509Certificate[]
certs, String authType){}
}};
        /* Initialize the
SSLContext with the all-trusting trust manager */

```

```

        SSLContext sslContext = SSLContext.getInstance("TLS");
sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
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;
}

}

```

統合マネージャー REST API

このセクションでは、Active IQ Unified Managerの REST API がカテゴリ別にリストされています。

すべての REST API 呼び出しの詳細が記載されているオンライン ドキュメント ページを、Unified Manager インスタンスから表示できます。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。ここ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だけが含まれています。特定のAPI呼び出しを検索すると、入力パラメータ、出力形式、HTTPステータス コード、要求処理タイプなど、その呼び出しのすべての詳細を確認できます。

ワークフローで使用している各API呼び出しについて、ドキュメント ページで見つけるのに役立つように次の情報を示します。

- カテゴリ

ドキュメント ページのAPI呼び出しは、機能に関連する分野（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て、該当するAPIカテゴリをクリックします。

- HTTP動詞（呼び出し）

HTTP動詞は、リソースに対して実行する操作を示します。各API呼び出しは、単一のHTTP動詞を使用して実行されます。

- パス

このパスは、呼び出しの実行中に操作が使用する特定のリソースを指定します。コアのURLのあとにパス文字列を追加することで、リソースを識別する完全なURLが形成されます。

APIを使用してデータセンター内のストレージオブジェクトを管理する

REST APIは、`datacenter` カテゴリを使用すると、クラスター、ノード、アグリゲート、ストレージ VM、ボリューム、LUN、ファイル共有、名前空間など、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。オブジェクトの設定を照会するためのAPIや、オブジェクトの追加、削除、変更処理を実行できるAPIがあります。

これらのAPIの大半はクラスタをまたいだ集計値を提供するGET呼び出しで、フィルタ、ソート、およびページ付けをサポートします。これらのAPIを実行すると、データベースからデータが返されます。したがって、新たに作成されたオブジェクトは、次の取得サイクルで検出されるまで応答に表示されません。

特定のオブジェクトの詳細を照会するには、そのオブジェクトの一意のIDを入力する必要があります。たとえば、ストレージオブジェクトのメトリックと分析情報については、以下を参照してください。["パフォーマンス指標の表示"](#)。

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```



cURLコマンド、例、要求、およびAPIへの応答は、Swagger APIインターフェイスで参照できます。Swaggerにも記載されているとおり、結果を特定のパラメータでフィルタおよび順序付けすることができます。これらのAPIを使用すると、クラスター、ボリューム、ストレージ VM などの特定のストレージ オブジェクトの結果をフィルターできます。

データセンター内のストレージ オブジェクト用のAPI

HTTP動詞	パス	説明
GET	 /datacenter/cluster/clusters /datacenter/cluster/clusters/{key}	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。クラスタのIPv4アドレスまたはIPv6アドレスなどの情報、健全性、パフォーマンス容量、ハイアベイラビリティ（HA）ペアなどのノードに関する情報、クラスタがオールSANアレイであるかどうかを示す情報が返されます。

HTTP動詞	パス	説明
GET	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	データセンター内のクラスタにインストールされているライセンスの詳細が返されます。必要な基準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 キーを入力すると特定のライセンスの詳細を取得できます。
GET	/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}	このメソッドを使用して、データセンター内のノードの詳細を表示できます。ノードのクラスタ、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確認できます。
GET	/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}	このメソッドを使用して、データセンター内のCIFS共有の詳細を表示できます。クラスタ、SVM、およびボリュームの詳細のほか、アクセス制御リスト (ACL) に関する情報も返されます。
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	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。 このメソッドを使用して、クラスタまたはStorage VMのエクスポート ポリシーを照会し、NFSファイル共有のプロビジョニングに使用できます。ワークロードへのエクスポート 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。

HTTP動詞	パス	説明
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	このメソッドを使用して、データセンター全体のすべてのアグリゲートまたは特定のアグリゲートを表示し、ワークロードのプロビジョニングや監視を行うことができます。クラスタとノードの詳細、使用済みパフォーマンス容量、使用可能スペースと使用済みスペース、ストレージ効率などの情報が返されます。
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	このメソッドを使用して、データセンター全体のすべてのLUNを表示できます。クラスタとSVMの詳細、QoSポリシー、igroupなど、LUNに関する情報を確認できます。
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	このメソッドを使用して、データセンター内のストレージオブジェクトに適用可能なすべてのQoSポリシーの詳細を表示できます。クラスタとSVMの詳細、固定またはアダプティブのポリシーの詳細、そのポリシーに該当するオブジェクトの数などの情報が返されます。
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	このメソッドを使用して、すべてのFlexVolまたはFlexGroupボリュームについて、データセンター全体のqtreeの詳細を表示できます。クラスタとSVMの詳細、FlexVol、エクスポートポリシーなどの情報が返されます。

HTTP動詞	パス	説明
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	このメソッドを使用して、データセンター内のすべてのボリュームを表示できます。SVMとクラスタの詳細、QoSポリシーとエクスポート ポリシー、ボリュームのタイプ（読み書き可能、データ保護、負荷共有）など、ボリュームに関する情報が返されます。 FlexVolおよびFlexCloneボリュームについては、それぞれのアグリゲートに関する情報を確認できます。FlexGroupボリュームについては、コンスティチュエント アグリゲートのリストが返されます。
GET POST DELETE PATCH	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}	特定のLUNターゲットへのアクセスを許可されたイニシエータ グループ (igroup) を割り当てることができます。既存のigroupがある場合は、そのigroupを割り当てることができます。igroupを作成して、LUNに割り当てすることもできます。 これらのメソッドを使用して、igroupの照会、作成、削除、および変更を実行できます。 注意事項： • `POST:`igroup を作成するときに、アクセスを割り当てるストレージ VM を指定できます。 • `DELETE:`特定の igroup を削除するには、入力パラメータとして igroup キーを指定する必要があります。すでにLUNに割り当てられているigroupは削除できません。 • `PATCH:`特定の igroup を変更するには、入力パラメータとして igroup キーを指定する必要があります。また、更新するプロパティとその値を入力する必要があります。

HTTP動詞	パス	説明
GET	/datacenter/svm/svms	これらのメソッドを使用して、Storage Virtual Machine (Storage VM) を表示、作成、削除、および変更できます。 ・`POST`: 作成するストレージ 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。 ・`DELETE`: 特定のストレージ VM を削除するには、ストレージ VM キーを指定する必要があります。 ・`PATCH`: 特定のストレージ VM を変更するには、ストレージ 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れらの値を入力する必要があります。
POST	/datacenter/svm/svms/{key}	
DELETE		
PATCH		



注意事項：

環境でSLOベースのワークロード プロビジョニングを有効にしている場合、Storage VMを作成する際に、そのStorage VMにLUNおよびファイル共有をプロビジョニングするために必要なすべてのプロトコル（たとえば、CIFSまたはSMB、NFS、FCP、iSCSI）をサポートするようにしてください。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。対応するワークロード タイプのサービスも有効にすることを推奨します。

環境でSLOベースのワークロード プロビジョニングを有効にしている場合、ストレージ ワークロードがプロビジョニングされているStorage VMは削除できません。CIFSまたはSMBサーバが設定されているStorage VMを削除すると、そのCIFS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。

データセンター内のネットワーク要素用の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、具体的にはFCポート、FCインターフェイス、イーサネット ポート、およびIPインターフェイスに関する情報を取得します。

HTTP動詞	パス	説明
GET	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	データセンター環境内のすべてのイーサネット ポートに関する情報を取得します。入力パラメータとしてポート キーを使用すると、そのポートの情報を確認できます。クラスタの詳細、ブロードキャスト ドメイン、ポートの状態、速度、タイプなどの詳細、ポートが有効になっているかどうかなどの情報が返されます。
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	このメソッドを使用して、データセンター環境内のFCインターフェイスの詳細を表示できます。入力パラメータとしてインターフェイス キーを使用すると、そのインターフェイスの情報を確認できます。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返されます。
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	データセンター環境内のノードで使用されているすべてのFCポートに関する情報を取得します。入力パラメータとしてポート キーを使用すると、そのポートの情報を確認できます。クラスタの詳細、ポートの説明、サポートされているプロトコル、ポートの状態などの情報が返されます。
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	このメソッドを使用して、データセンター環境内のIPインターフェイスの詳細を表示できます。入力パラメータとしてインターフェイス キーを使用すると、そのインターフェイスの情報を確認できます。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になっているかどうかなどの情報が返されます。

プロキシアクセスを介して**ONTAP API**にアクセスする

ゲートウェイAPIを使用すると、Active IQ Unified Managerのクレデンシャルを使用してONTAP REST APIを実行し、ストレージ オブジェクトを管理することができます。これらのAPIは、Unified Manager Web UIからAPIゲートウェイ機能を有効にすると使用できるようになります。

Unified Manager REST APIでUnified Managerのデータソース（ONTAPクラスタ）に対して実行できるのは、一部の処理のみです。それ以外の処理はONTAP APIを使用して実行できます。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、各データセンター クラスタに個別にログインせずに直接管理対象のONTAPクラスタに対してすべてのAPI要求を実行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、そのUnified Managerインスタンスが管理するONTAPクラスタ全体に対してAPIを実行することができます。APIゲートウェイ機能を使用すると、それぞれのONTAPクラスタに個別にログインすることなく、単一のコントロール プレーンであるUnified Managerから複数のONTAPクラスタを一元的に管理できます。Unified Managerにログインしたままで、ONTAP REST API処理を実行して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すべてのONTAP REST処理を実行できます。

ゲートウェイは、ヘッダーと本文の形式をONTAP APIと同じにすることで、API要求をトンネリングするプロキシとして機能します。個々のクラスタのクレデンシャルを渡すことなく、Unified Managerのクレデンシャルを使用して特定の処理を実行し、ONTAPクラスタにアクセスして管理することができます。クラスタ認証とクラスタ管理は引き続き管理されますが、API要求は特定のクラスタにリダイレクトされて直接実行されます。APIから返される応答は、対応するONTAP REST APIをONTAPから直接実行した場合と同じです。

HTTP動詞	パス (URL)	説明
GET	/gateways	このGETメソッドは、Unified Managerで管理されているクラスタのうち、ONTAP REST呼び出しをサポートするすべてのクラスタのリストを取得します。クラスタのUniversal Unique Identifier (UUID) に基づいてクラスタの詳細を確認し、他のメソッドを実行することができます。  ゲートウェイAPIは、ONTAP 9.5以降でサポートされていて、HTTPSを使用してUnified Managerに追加されたクラスタのみを取得します。

HTTP動詞	パス (URL)	説明
GET POST DELETE PATCH OPTIONS(Swagger では利用できません) HEAD(Swagger では利用できません)	/gateways/{uuid}/{path}  {uuid} の値は、REST 操作が行われるクラスター 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て、HTTPSを使用してUnified Managerに追加されたクラスターのUUIDを指定してください。{path} はONTAP REST URL に置き換える必要があります。削除する必要があります。'/api/' URLから。	これは単一ポイントのプロキシAPIで、POST、DELETE、PATCHの処理に加え、すべてのONTAP REST APIのGETをサポートしています。ONTAPでサポートされているかぎり、どのAPIにも制限はありません。トンネリングまたはプロキシ機能を無効にすることはできません。 その `OPTIONS` メソッドは、ONTAP REST API でサポートされているすべての操作を返します。たとえば、ONTAP APIが `GET` 操作、実行 `OPTIONS` このゲートウェイAPIを使用してメソッドを返す `GET` 応答として。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ツールでは実行できます。 その `OPTIONS` メソッドは、リソースが利用可能かどうかを判断します。この処理を使用して、リソースに関するメタデータをHTTP応答ヘッダーに表示できます。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ツールでは実行できます。

APIゲートウェイトンネリングを理解する

ゲートウェイAPIを使用すると、Unified ManagerからONTAPオブジェクトを管理できます。Unified Managerはクラスターと認証の詳細を管理し、ONTAP RESTエンドポイントに要求をリダイレクトします。ゲートウェイAPIは、ヘッダーおよび応答本文のURLとHypermedia as the Engine of Application State (HATEOAS) リンクをAPIゲートウェイのベースURLで変換します。ゲートウェイAPIはプロキシのベースURLとして機能し、これにONTAP REST URLを追加して必要なONTAP RESTエンドポイントを実行します。



ONTAP APIがAPIゲートウェイ経由で実行されるためには、APIを実行するONTAPクラスターのバージョンでAPIがサポートされている必要があります。ONTAPクラスターでサポートされていないAPIを実行した場合、結果は何も返されません。

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}/

取得したONTAP API は次のとおりです。 /storage/volumes。このONTAP API REST URLをpathパラメータの値として追加する必要があります。



パスを追加する際は、「」を削除したことを確認してください。/`" symbol at the beginning of the URL. For the API `/storage/volumes,`追加`storage/volumes.

追加された URL は次のとおりです。 /gateways/{uuid}/storage/volumes

実行時に GET`この操作により、生成される URL は次のようになります。

`GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes

その `api`追加された URL ではONTAP REST URL の タグが削除され、ゲートウェイ API のタグは保持されます。

サンプルcURLコマンド

```
curl -X GET "https://<hostname>/api/gateways/lcd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

このAPIは、指定した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、同じAPIをONTAPから実行した場合と同じです。返されるステータス コードは、ONTAP RESTのステータス コードです。

APIスコープを設定する

すべてのAPIは、コンテキストがクラスタのスコープ内に設定されています。Storage VMを対象とするAPIのスコープもクラスタです。つまり、管理対象クラスタ内の特定のStorage VMでAPI処理が実行されます。実行すると `/gateways/{uuid}/{path}`API を使用する場合は、操作を実行するクラスターのクラスター UUID (Unified Manager データ ソース UUID) を必ず入力してください。そのクラスタ内の特定のStorage VMにコンテキストを設定する場合は、Storage VMのキーをX-Dot-SVM-UUIDパラメータとして入力するか、Storage VMの名前をX-Dot-SVM-Nameパラメータとして入力します。指定した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、クラスタ内のそのStorage VMのスコープ内で処理が実行されます。

サンプルcURLコマンド

```
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、以下を参照してください。<https://docs.netapp.com/us-en/ontap-automation/index.html>["ONTAP REST APIの自動化のドキュメントを参照してください。"]

API を使用して管理タスクを実行する

以下のAPIを使用することができます。`administration`このカテゴリでは、バックアップ設定を変更したり、バックアップ ファイル情報とクラスタ証明書を確認したり、ONTAPクラスタをActive IQ Unified Managerデータ ソースとして管理したりできます。



これらの処理を実行するには、アプリケーション管理者のロールが必要です。これらの設定は、Unified Manager Web UIでも実行できます。

HTTP動詞	パス	説明
GET PATCH	/admin/backup-settings /admin/backup-settings	使用することができます `GET` 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する方法。次の情報を確認できます。 • スケジュールが有効か無効か • スケジュールされたバックアップの頻度（毎日または毎週） • バックアップの時刻 • アプリケーションに保持するバックアップ ファイルの最大数 バックアップの時刻はサーバのタイムゾーンに基づきます。 データベース バックアップ設定はUnified Managerでデフォルトで使用可能で、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、`PATCH`デフォルト設定を変更する方法。
GET	/admin/backup-file-info	Unified Managerのバックアップ スケジュールが変更されると、そのたびにバックアップ ダンプ ファイルが生成されます。このメソッドを使用すると、変更されたバックアップ設定に従ってバックアップ ファイルが生成されているかどうか、およびファイルの情報が変更された設定と一致してい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、信頼ストアにあるデータソース（クラスタ）の証明書を表示できます。ONTAPクラスタをUnified Managerの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。

HTTP動詞	パス	説明
GET	/admin/datasources/clusters	使用することができます `GET` Unified Manager によって管理されるデータ ソース (ONTAP クラスタ) の詳細を取得する方法。
POST	/admin/datasources/clusters/{key}	新しいクラスタを Unified Manager にデータソースとして追加することもできます。クラスタを追加するには、ホスト名、ユーザ名、パスワードが必要です。
PATCH		
DELETE		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を使用してユーザーを管理する

APIは、`security` Active IQ Unified Manager内の選択されたクラスター オブジェクトへのユーザー アクセスを制御するカテゴリ。ローカル ユーザまたはデータベース ユーザを追加できます。また、認証サーバに属するリモート ユーザやリモート グループを追加することもできます。ユーザは、それぞれに割り当てられたロールの権限に基づいて、Unified Managerでストレージ オブジェクトを管理したり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のロールが必要です。これらの設定は、Unified Manager Web UIでも実行できます。

APIは ``security`` カテゴリは、ユーザー 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、ユーザー名であるユーザー パラメータを使用します。

HTTP動詞	パス	説明
GET	/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。
POST	/security/users	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。

HTTP動詞	パス	説明
GET	/security/users/{name}	GETメソッドで、名前、Eメールアドレス、ロール、認証タイプなど、ユーザのすべての詳細を取得できます。PATCHメソッドで詳細を更新できます。DELETEメソッドでユーザを削除できます。
PATCH		
DELETE		

API を使用してパフォーマンス メトリックを表示する

Active IQ Unified Managerは、以下のAPIセットを提供します。`/datacenter` データセンター内のクラスターとストレージ オブジェクトのパフォーマンス データを表示できるカテゴリです。これらのAPIは、クラスター、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。

その `/metrics` そして `/analytics` API はパフォーマンス メトリックのさまざまなビューを提供し、それを使用して、データセンター内の次のストレージ オブジェクトの詳細をさまざまなレベルにドリルダウンできます。

- クラスター
- 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

次の表は、`/metrics` そして `/analytics` 取得されたパフォーマンス データの詳細に関する API。

メトリクス	Analytics
単一のオブジェクトについてのパフォーマンスの詳細。例えば、 /datacenter/cluster/clusters/{key}/metrics API では、特定のクラスターのメトリックを取得するためのパス パラメータとしてクラスター 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についてのパフォーマンスの詳細。例えば、 /datacenter/cluster/clusters/analytics API は、データセンター内のすべてのクラスターの集会的なメトリックを取得します。

メトリクス	Analytics
取得間隔パラメータに基づく、あるストレージ オブジェクトについてのパフォーマンス指標サンプル。	特定のタイプのストレージ オブジェクトについての特定の期間（72時間以上）におけるパフォーマンス集計値。
ノードやクラスタの詳細など、オブジェクトの基本的な詳細が取得される。	個別の詳細は取得されない。
単一のオブジェクトについて、読み取り、書き込み、合計などの分類で、一定期間におけるパフォーマンスの最小値、最大値、95パーセンタイル値、平均値の累積カウンタが取得される。	同じタイプのすべてのオブジェクトについて、集計された値が1つ表示される。

メトリクス	Analytics
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。1h、12h、1d、2d、3d、15d、1w、1m、2m、3m、6mがあります。期間が3日（72時間）を超える場合は1時間ごとのサンプル、それ以外の期間は5分ごとのサンプルが取得されます。各期間ごとの詳細は次のとおりです。 • 1 時間: 5 分間にサンプリングされた、直近 1 時間のメトリック。 • 12 時間: 5 分ごとにサンプリングされた、過去 12 時間のメトリック。 • 1d: 5 分間にサンプリングされた最新 1 日間のメトリック。 • 2d: 5 分間にサンプリングされた過去 2 日間のメトリック。 • 3d: 5 分間にサンプリングされた過去 3 日間のメトリック。 • 15d: 1 時間にわたってサンプリングされた、過去 15 日間のメトリック。 • 1w: 1 時間にわたってサンプリングされた、直近 1 週間のメトリック。 • 1m: 1 時間にわたってサンプリングされた、直近 1 か月間のメトリック。 • 2m: 1 時間にわたってサンプリングされた、過去 2 か月間のメトリック。 • 3m: 1 時間にわたってサンプリングされた、過去 3 か月間のメトリック。 • 6m: 1 時間にわたってサンプリングされた、過去 6 か月間のメトリック。 使用可能な値: 1h、12h、1d、2d、3d、15d、1w、1m、2m、3m、6m デフォルト値: 1時間	72時間超。サンプルの計算期間はISO-8601標準形式で表されます。

metrics APIの出力例

例えば、`/datacenter/cluster/nodes/{key}/metrics` API は、ノードについて次のような詳細 (とりわけ) を取得します。



サマリに表示される95パーセンタイルの値は、その期間に収集されたサンプルの95%のカウンタ値がその値を下回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
}
},
```

analytics APIの出力例

例えば、`/datacenter/cluster/nodes/analytics` API は、すべてのノードに対して次の値 (およびその他の値) を取得します。

```
{
  "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の一覧

次の表は、`/metrics`そして`/analytics`APIの詳細。



これらのAPIによって返されるIOPSとパフォーマンスメトリックはdouble値です。たとえば、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サポートされていません。

HTTP動詞	パス	説明
GET	/datacenter/cluster/clusters/{key}/metrics	クラスター キーの入力パラメータで指定したクラスターについて、パフォーマンス データ（サンプルとサマリ）を取得します。クラスター キーやUUID、期間、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ーについて、パフォーマンス指標の概要を取得します。必要な基準に基づいて結果をフィルタリングできます。IOPSやスループットの集計値、収集期間（時間数）などの情報が返されます。
GET	/datacenter/cluster/nodes/{key}/metrics	ノード キーの入力パラメータで指定したノードについて、パフォーマンス データ（サンプルとサマリ）を取得します。ノードのUUID、期間、IOPS、スループット、レイテンシ、パフォーマンスのサマリ、収集されたサンプル数、利用率などの情報が返されます。
GET	/datacenter/cluster/nodes/analytics	データセンター内のすべてのノードについて、パフォーマンス指標の概要を取得します。必要な基準に基づいて結果をフィルタリングできます。ノードとクラスターのキー、IOPSやスループットの集計値、収集期間（時間数）などの情報が返されます。
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したアグリゲートについて、パフォーマンス データ（サンプルとサマリ）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サマリ、各カウンタについて収集されたサンプル数、利用率などの情報が返されます。

HTTP動詞	パス	説明
GET	/datacenter/storage/aggregates/analytics	データセンター内のすべてのアグリゲートについて、パフォーマンス指標の概要を取得します。必要な基準に基づいて結果をフィルタリングできます。アグリゲートとクラスタのキー、IOPSやスループットの集計値、収集期間（時間数）などの情報が返されます。
GET	/datacenter/storage/luns/{key}/metrics /datacenter/storage/volumes/{key}/metrics	LUNキーまたはボリューム（ファイル共有）キーの入力パラメータで指定したLUNまたはボリュームについて、パフォーマンス データ（サンプルとサマリ）を取得します。読み取り、書き込み、合計のIOPS、レイテンシ、スループットのサマリ（最小値、最大値、平均値）、各カウンタについて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/analytics /datacenter/storage/volumes/analytics	データセンター内のすべてのLUNまたはボリュームについて、パフォーマンス指標の概要を取得します。必要な基準に基づいて結果をフィルタリングできます。Storage VMとクラスタのキー、IOPSやスループットの集計値、収集期間（時間数）などの情報が返されます。
GET	/datacenter/svm/svms/{key}/metrics	Storage VMキーの入力パラメータで指定したStorage VMについて、パフォーマンス データ（サンプルとサマリ）を取得します。サポートされている各プロトコルに基づくIOPSの概要、例：nvmf, fcp, iscsi、そして `nfs、スループット、レイテンシ、および収集されたサンプル数が返されます。

HTTP動詞	パス	説明
GET	/datacenter/svm/svms/analytics	データセンター内のすべてのStorage VMについて、パフォーマンス指標の概要を取得します。必要な基準に基づいて結果をフィルタリングできます。Storage VMのUUID、IOPS、レイテンシ、スループットの集計値、収集期間（時間数）などの情報が返されます。
GET	/datacenter/network/ethernet/ports/{key}/metrics	ポート キーの入力パラメータで指定したイーサネット ポートについて、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の間隔（期間）を指定すると、その期間におけるパフォーマンス値の最小値、最大値、平均値などの累積カウンタが返されます。
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や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やUUIDなど、使用可能なパラメータで結果をフィルタリングできます。
GET	/datacenter/network/fc/interfaces/{key}/metrics	インターフェイス キーの入力パラメータで指定したネットワークFC インターフェイスについて、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の間隔（期間）を指定すると、その期間におけるパフォーマンス値の最小値、最大値、平均値などの累積カウンタが返されます。

HTTP動詞	パス	説明
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インターフェイスのキーや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や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。
GET	/datacenter/network/fc/ports/{key}/metrics	ポート キーの入力パラメータで指定したFCポートについて、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の間隔（期間）を指定すると、その期間におけるパフォーマンス値の最小値、最大値、平均値などの累積カウンタが返されます。
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や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や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インターフェイスについて、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の間隔（期間）を指定すると、サンプル数、累積カウンタ、スループット、送受信パケット数などの情報が返されます。

HTTP動詞	パス	説明
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インターフェイスのキーや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や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。

ジョブとシステムの詳細を表示する

使用することができます `jobs` APIの `management-server` 非同期操作の実行の詳細を表示するためのカテゴリ。その `system` APIの `management-server` カテゴリを使用すると、Active IQ Unified Manager環境内のインスタンスの詳細を表示できます。

ジョブを表示

Active IQ Unified Managerでは、リソースの追加や変更などの処理は、同期および非同期のAPI呼び出しによって実行されます。非同期で実行予定の呼び出しは、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、このURIを使用してジョブの進行状況を表示して追跡できます。このAPIを使用して、それぞれの実行の詳細情報を取得できます。

このAPIを使用すると、データセンターのすべてのジョブ オブジェクトを履歴データも含めて照会できます。デフォルトではすべてのジョブが照会され、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の20件のジョブの詳細が返されます。特定のジョブを表示するには組み込みのフィルタを使用してください。ジョブ キーを使用して特定のジョブの詳細を照会し、リソースに対して後続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	説明
management-server	GET	/management-server/jobs	すべてのジョブの詳細を返します。ソート順序が指定されていない場合、最後に送信されたジョブ オブジェクトが最初に返されます。

カテゴリ	HTTP動詞	パス	説明
management-server	GET	/management-server/jobs/{key} ジョブ オブジェクトのジョブ キーを入力すると、そのジョブの詳細が表示されます。	特定のジョブ オブジェクトの詳細を返します。

システムの詳細を表示

を使用することで `/management-server/system` API を使用すると、Unified Manager 環境のインスタンス固有の詳細を照会できます。システムにインストールされている Unified Manager のバージョン、UUID、ベンダー名、ホスト OS、名前、説明、Unified Manager インスタンスで実行されているサービスのステータスなど、製品やサービスに関する情報が返されます。

カテゴリ	HTTP動詞	パス	説明
management-server	GET	/management-server/system	このAPIの実行に必要な入力パラメータはありません。デフォルトで、現在の Unified Manager インスタンスのシステムの詳細が返されます。

APIを使用してイベントとアラートを管理する

その `events`、`alerts`、そして `scripts` API は `management-server` カテゴリを使用すると、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た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、監視 / 管理対象のクラスタに対して ONTAP で生成されたイベントを受信します。これらの API を使用して、クラスタに対して生成されたイベントを確認し、解決および更新することができます。

実行することで `GET` 方法 `/management-server/events` API を使用すると、履歴データを含むデータセンター内のイベントをクエリできます。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 タイプなどの組み込みフィルタを使用して、特定のイベントを表示できます。リソース タイプと領域のパラメータを指定すると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が返され、影響領域を指定すると可用性、容量、構成、セキュリティ、保護、パフォーマンスなど、イベントが発生した問題に関する情報が返されます。

このAPIのPATCH処理を実行すると、イベントの解決ワークフローを有効にすることができます。イベントを自分または別のユーザに割り当てたり、イベントの受信確認を行ったりできます。リソースに対して手順を実行してイベントの原因となった問題を解決したら、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、["イベントを管理する"](#)。

カテゴリ	HTTP動詞	パス	説明
management-server	GET	/management-server/events /management-server/events/{key}	Get ALLメソッドを実行すると、データセンター内のすべてのイベントの詳細が返されます。特定のキーを使用してイベントの詳細を取得すると、特定のイベントの詳細を表示し、リソースに対して後続の一連の処理を実行できます。応答にはそのイベントの詳細のみが含まれます。
management-server	PATCH	management-server/events/{key}	このAPIを使用して、イベントを割り当てたり、状態を確認済みや解決済みに変更したりできます。このメソッドを使用して、自分または別のユーザーにイベントを割り当てることもできます。これは同期処理です。

アラートを管理する

イベントは自動かつ継続的に生成されます。Unified Manager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を生成します。アラートを生成するイベントは選択することができます。を使用することで `/management-server/alerts` API を使用すると、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通知を自動的に送信するようにアラートを構成できます。

アラートの詳細については、以下を参照してください。"[アラートを管理する](#)"。

カテゴリ	HTTP動詞	パス	説明
management-server	GET	/management-server/alerts /management-server/alerts/{key}	環境内の既存のアラートをすべて照会するか、アラート キーを使用して特定のアラートを照会します。環境内で生成されたアラートについて、その説明、対処法、通知の送信先EメールID、イベント、重大度などの情報を確認できます。

カテゴリ	HTTP動詞	パス	説明
management-server	POST	/management-server/alerts	このメソッドを使用して、特定のイベントに対するアラートを追加できます。アラートの名前、物理または論理リソース、アラートの対象となるイベント、アラートを有効にするかどうか、およびSNMPトラップを発行するかどうかを指定する必要があります。そのほかにも、対処法、通知先の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）などを追加できます。
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、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。



アラートの追加でリソースを選択する際、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を対象とするアラートを作成した場合、受信するのはクラスタの重大イベントに対するアラートのみです。ノードやアグリゲートなどの重大イベントに対するアラートは受信しません。

スクリプトを管理する

を使用することで `/management-server/scripts` API では、アラートがトリガーされたときに実行されるスクリプトにアラートを関連付けることもできます。スクリプトを使用して、Unified Manager 内の複数のストレージ 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。イベントでアラートがトリガーされるとスクリプトが実行されます。カスタム スクリプトをアップロードし、アラートが生成されたときの動作をテストできます。Unified Managerでイベントに対するアラートが発生したときにスクリプトが実行されるように、アラートにスクリプトを関連付けることができます。

スクリプトの詳細については、"[スクリプトを管理する](#)"。

カテゴリ	HTTP動詞	パス	説明
management-server	GET	/management-server/scripts	このAPIを使用して、環境内の既存のスクリプトをすべて照会できます。特定のスクリプトのみを表示するには、標準のフィルタを使用して処理順に並べ替えてください。
management-server	POST	/management-server/scripts	このAPIを使用して、スクリプトの説明を追加したり、アラートに関連付けられたスクリプト ファイルをアップロードしたりできます。

APIを使用してワークロードを管理する

ここで説明するAPIは、ストレージ ワークロードの表示、LUNとファイル共有の作成、パフォーマンス サービス レベルとストレージ効率化ポリシーの管理、ストレージ ワークロードに対するポリシーの割り当てなど、ストレージ管理のさまざまな機能に対応しています。

API を使用してストレージ ワークロードを表示する

ここに記載されているAPIを使用すると、データセンター内のすべてのONTAPクラスタのストレージ ワークロードをまとめて表示できます。API は、Active IQ Unified Manager環境でプロビジョニングされたストレージ ワークロードの数と、それらの容量およびパフォーマンス (IOPS) 統計の概要ビューも提供します。

ストレージ ワークロードの表示

データセンター内の全クラスタの全ストレージ 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。特定の列に基づいて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 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
storage-provider	GET	/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、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。API は、ストレージ ワークロードの概要、Unified Manager によって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、割り当てられたパフォーマンス サービス レベルの観点からのデータ センターの合計、使用済み、使

用可能なスペースと IOPS の概要を提供します。この API への応答として受信された情報は、Unified Manager UI のダッシュボードに入力するために使用されます。

カテゴリ	HTTP動詞	パス
storage-provider	GET	/storage-provider/workloads-summary

API を使用してアクセス エンドポイントを管理する

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

次の方法を使用して、Unified Manager 環境内のアクセス エンドポイントのリストを表示できます。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
storage-provider	GET	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

アクセス エンドポイントの追加

カスタムのアクセス エンドポイントを作成して、必要なプロパティを割り当てることができます。作成するアクセス エンドポイントの詳細を、入力パラメータとして指定する必要があります。この API、System Manager、またはONTAP CLI を使用して、各ノードにアクセス エンドポイントを作成できます。アクセス エンドポイントの作成では、IPv4アドレスとIPv6アドレスの両方がサポートされます。



LUNとファイル共有をプロビジョニングするためには、SVMにノードあたりの最小アクセス エンドポイント数を設定する必要があります。SVMには、ノードごとに少なくとも2つのアクセス エンドポイントを設定する必要があります。1つはCIFSプロトコルおよび/またはNFSプロトコルをサポートし、もう1つはiSCSIプロトコルまたはFCPプロトコルをサポートします。

カテゴリ	HTTP動詞	パス
storage-provider	POST	/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
storage-provider	DELETE	/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
storage-provider	PATCH	/storage-provider/access-endpoints/{key}

API を使用して **Active Directory** マッピングを管理する

ここに記載されたAPIを使用して、SVM上のCIFS共有のプロビジョニングに必要なSVMのActive Directoryマッピングを管理できます。ONTAPで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
storage-provider	GET	/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
storage-provider	POST	/storage-provider/active-directories-mappings

APIを使用してファイル共有を管理する

使用することができます。`/storage-provider/file-shares` データ センター環境内の CIFS および NFS ファイル共有ボリュームを表示、追加、変更、削除するための API。

ファイル共有ボリュームをプロビジョニングする前に、SVMが作成済みで、サポートされるプロトコルでプロビジョニングされていることを確認してください。プロビジョニング時にパフォーマンス サービス レベル (PSL) またはストレージ効率化ポリシー (SEP) を割り当てる場合は、ファイル共有を作成する前にPSLまたはSEPを作成する必要があります。

ファイル共有の表示

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にONTAPクラスタをデータソースとして追加すると、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
storage-provider	GET	/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
storage-provider	POST	/storage-provider/file-shares



アクセス制御リスト (ACL) パラメータまたはエクスポート ポリシー パラメータのどちらを指定するかに応じて、CIFS共有またはNFSファイル共有が作成されます。ACLパラメータの値を指定しない場合、CIFS共有は作成されず、デフォルトでNFS共有が作成され、すべてのアクセスが提供されます。

データ保護ボリュームの作成: SVMにファイル共有を追加すると、マウントされるボリュームのタイプはデフォルトで `rw` (読み書き可能)。データ保護 (DP) ボリュームを作成するには、`dp` の値として `type` パラメータ

タ。

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指定する必要があります。

カテゴリ	HTTP動詞	パス
storage-provider	DELETE	/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。複数更新する場合は、このAPIを繰り返し実行する必要があります。

カテゴリ	HTTP動詞	パス
storage-provider	PATCH	/storage-provider/file-shares/{key}

APIを使用してLUNを管理する

使用することができます。`/storage-provider/luns` データ センター環境内の LUN を表示、追加、変更、削除するための API。

LUNをプロビジョニングする前に、SVMが作成され、サポートされるプロトコルでプロビジョニングされていることを確認してください。プロビジョニング時にパフォーマンス サービス レベル（PSL）またはストレージ効率化ポリシー（SEP）を割り当てる場合は、LUNを作成する前にPSLまたはSEPを作成する必要があります。

LUNの表示

Unified Manager環境のLUNを表示するには、次のメソッドを使用します。Active IQ Unified Manager にONTAPクラスタをデータソースとして追加すると、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
storage-provider	GET	/storage-provider/luns /storage-provider/luns/{key}

LUNを追加する

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
storage-provider	POST	/storage-provider/luns



cURL要求で、入力にオプションのパラメータvolume_name_tagの値を指定すると、LUNの作成でボリュームの名前を指定する際にその値が使用されます。このタグにより、ボリュームを簡単に検索できるようになります。要求にボリューム キーを指定した場合、このタギングは省略されます。

LUNを削除する

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、そのボリューム上で Unified Manager を通じて 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、そのボリュームもONTAPクラスタから削除されます。

カテゴリ	HTTP動詞	パス
storage-provider	DELETE	/storage-provider/luns/{key}

LUNの変更

LUNを変更してそのプロパティを更新するには、次のメソッドを使用します。特定のLUNを変更するには、LUNキーを指定する必要があります。また、更新するLUNプロパティとその値を入力する必要があります。この API を使用して LUN アレイを更新する場合は、「API の使用に関する推奨事項」の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。複数更新する場合は、このAPIを繰り返し実行する必要があります。

カテゴリ	HTTP動詞	パス

storage-provider	PATCH	/storage-provider/luns/{key}

APIを使用してパフォーマンス サービス レベルを管理する

Active IQ Unified Managerのストレージ 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パフォーマンス サービス レベルをすべて表示し、すべてのパフォーマンス サービス レベルの属性を取得します。特定のパフォーマンス サービス レベルを照会する場合は、パフォーマンス サービス レベルの一意のIDを入力して詳細を取得する必要があります。

カテゴリ	HTTP動詞	パス
storage-provider	GET	/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、次のメソッドでカスタム パフォーマンス サービス レベルを作成し、ストレージ ワークロードに割り当てることができます。作成するパフォーマンス サービス レベルの詳細を入力します。IOPSプロパティには、有効な値の範囲を入力してください。

カテゴリ	HTTP動詞	パス
storage-provider	POST	/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、または他に使用可能なパフォーマンス サービス レベルがない場合、そのパフォーマンス サービス レベルは削除できません。特定のパフォーマンス サービス レベルを削除するには、パフォーマンス サービス レベルの一意のIDを入力パラメータとして指定する必要があります。

カテゴリ	HTTP動詞	パス
storage-provider	DELETE	/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、その一意のIDを指定する必要があります。また、更新するIOPSプロパティと有効な値も入力する必要があります。

カテゴリ	HTTP動詞	パス
storage-provider	PATCH	/storage-provider/performance-service-levels/{key}

パフォーマンス サービス レベルに基づいて集計機能を表示する

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できる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
storage-provider	GET	/storage-provider/aggregate-capabilities /storage-provider/aggregate-capabilities/{key}

APIを使用してストレージ効率ポリシーを管理する

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ときに、ストレージ効率ポリシーを割り当てること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。
- ワークロードに重複排除や圧縮などのONTAPボリュームで指定されたストレージ設定がある場合、それらの設定は、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ポリシーで指定された設定によって上書きされる可能性があります。

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には、ポリシーの一意のIDを入力して詳細を取得する必要があります。

カテゴリ	HTTP動詞	パス
storage-provider	GET	/storage-provider/storage-efficiency-policies /storage-provider/storage-efficiency-policies/{key}

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、次のメソッドでカスタムのストレージ効率化ポリシーを作成し、ストレージ ワークロードに割り当てることができます。作成するストレージ効率化ポリシーの詳細を入力パラメータとして指定します。

カテゴリ	HTTP動詞	パス
storage-provider	POST	/storage-provider/storage-efficiency-policies

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
storage-provider	DELETE	/storage-provider/storage-efficiency-policies/{key}

ストレージ効率化ポリシーを変更し、そのプロパティを更新するには、次のメソッドを使用します。システム定義のストレージ効率化ポリシー、またはワークロードに割り当てられているストレージ効率化ポリシーは変更できません。特定のストレージ効率化ポリシーを変更するには、ストレージ効率化ポリシーの一意のIDを指定する必要があります。また、更新するプロパティとその値を指定する必要があります。

カテゴリ	HTTP動詞	パス
storage-provider	PATCH	/storage-provider/storage-efficiency-policies/{key}

ストレージ管理の一般的なAPIワークフロー

ここでは、クライアント アプリケーション開発者向けに、クライアント アプリケーションからActive IQ Unified Manager APIを呼び出して一般的なストレージ管理機能を実行する一般的なワークフローを紹介します。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。

ワークフローごとに、代表的なストレージ管理のユースケースと、使用するサンプル コードを記載します。各タスクは、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記述されます。

ワークフローで使用されるAPI呼び出しを理解する

すべての REST API 呼び出しの詳細が記載されているオンライン ドキュメント ページを、Unified Manager インスタンスから表示できます。このドキュメントでは、オンライン ドキュメントの詳細については説明しません。このドキュメントのワークフロー サンプルで使用されている各API呼び出しには、ドキュメント ページで呼び出しを検索するために必要な情報だけが含まれています。特定のAPI呼び出しを見つけたら、入力パラメータ、出力形式、HTTPステータス コード、要求処理のタイプなど、呼び出しの詳細を確認できます。

ワークフローで使用している各API呼び出しについて、ドキュメント ページで見つけるのに役立つように次の情報を示します。

- カテゴリ: API 呼び出しは、ドキュメント ページ上で機能的に関連する領域またはカテゴリに整理されています。特定のAPI呼び出しを見つけるには、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識別します。各API呼び出しは、単一のHTTP動詞を使用して実行されます。
- パス: パスは、呼び出しの実行の一環としてアクションが適用される特定のリソースを決定します。コアのURLのあとにパス文字列を追加することで、リソースを識別する完全なURLが形成されます。

API を使用して集計のスペースの問題を特定する

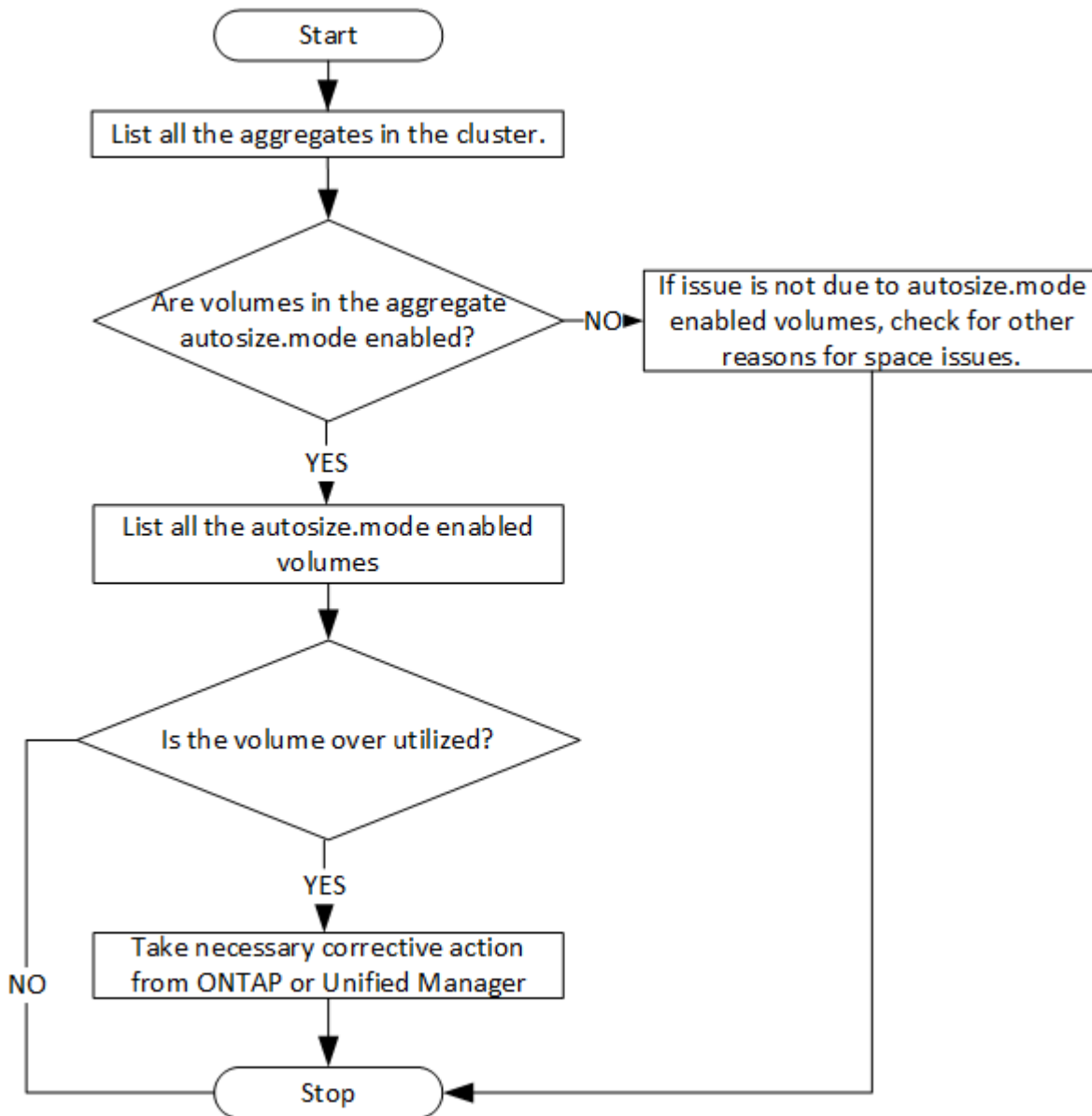
Active IQ Unified ManagerのデータセンターAPIを使用して、ボリューム内のスペースの可用性と使用率を監視できます。ボリューム内のスペースの問題を特定し、使用率が高すぎる、または十分に活用されていないストレージ リソースを特定できます。

アグリゲート用のデータセンターAPIは、使用可能スペースや使用済みスペース、スペース削減のための効率

化設定などの関連情報を取得します。また、指定した属性に基づいて取得した情報をフィルタすることもできます。

アグリゲートにスペースが不足しているかどうかを確認する方法の1つとして、環境内にオートサイズ モードが有効なボリュームがあるかを確認する方法があります。次に、使用率が高すぎるボリュームを特定し、対処策を実行する必要があります。

次のフローチャートは、オートサイズ モードが有効な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ですでに作成され、Unified Managerに追加されていることを前提としています。

1. クラスタ キーの値がわからない場合は取得します。

カテゴリ	HTTP動詞	パス
datacenter	GET	/datacenter/cluster/clusters

2. クラスター キーをフィルタ パラメータとして使用して、そのクラスターのアグリゲートを照会します。

カテゴリ	HTTP動詞	パス
datacenter	GET	/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. 各集計キーを使用して、autosize.modeパラメータの値が次の値であるすべてのボリュームをフィルタリングします。 grow.

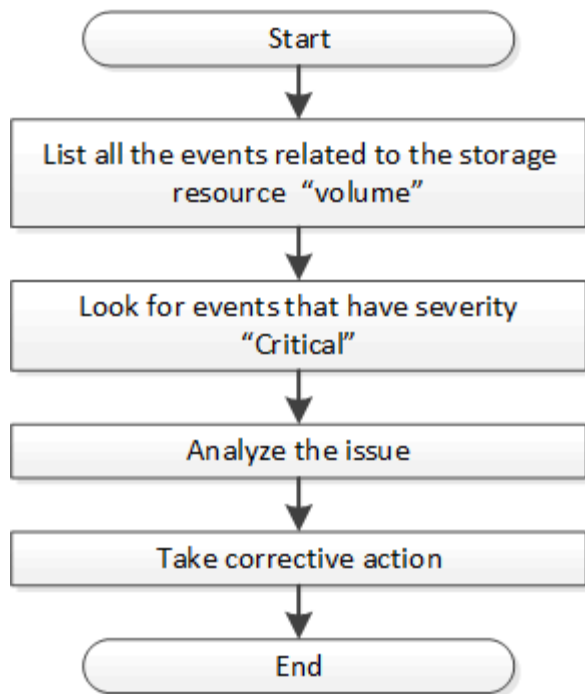
カテゴリ	HTTP動詞	パス
datacenter	GET	/datacenter/storage/volumes

5. 使用率が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を解決するために、ボリュームをアグリゲート間で移動するなどの必要な対処策を実行します。これらの処理は、ONTAPまたはUnified Manager Web UIから実行できます。

イベント **API** を使用してストレージ オブジェクトの問題を特定する

データセンター内のストレージ 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を受け取ります。この通知を使用して、問題を分析し、 events API。

このワークフローでは、リソース オブジェクトがボリュームの場合を例に取り上げます。使用することができます `events` 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修正アクションを実行する API。



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対する重大なActive IQ Unified Manager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、ボリュームの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	GET	/management-server/events

3. 出力を確認し、特定のボリュームの問題を分析します。
4. Unified Manager REST APIまたはWeb UIを使用して必要な措置を講じ、問題を解決します。

ゲートウェイ **API** を使用して**ONTAP**ボリュームのトラブルシューティングを行う

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、修正策を実施して報告された問題に対処するためのゲートウェイとして機能します。

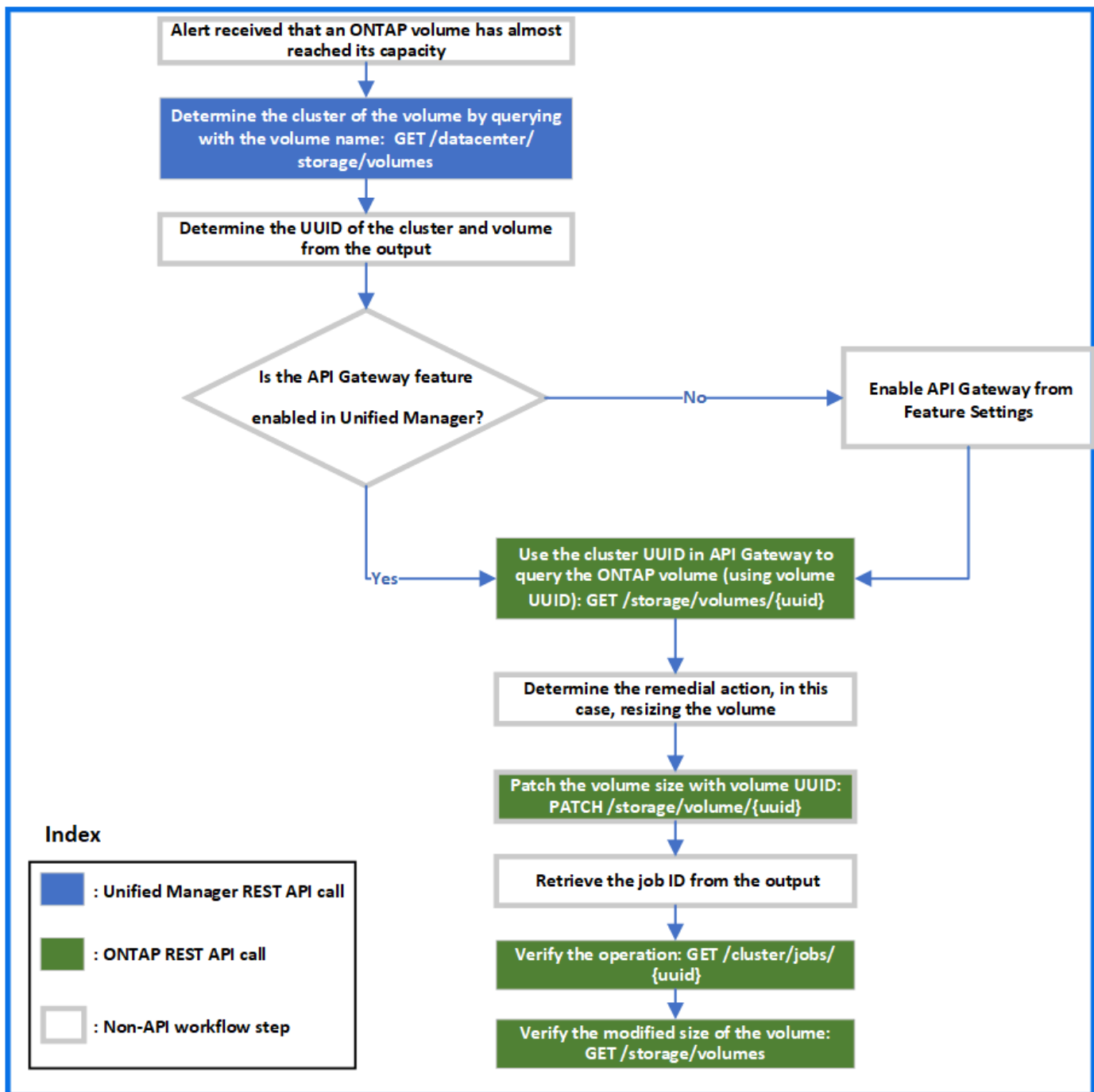
このワークフローでは、ONTAPボリュームの容量がほぼフルに達したときにイベントが生成されるユースケースを例に取り上げます。ワークフローには、Active IQ Unified ManagerとONTAPそれぞれのREST APIを呼び出してこの問題に対処する手順も含まれています。

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とその使用方法を理解している。詳細については、"[プロキシ アクセスによるONTAP APIへのアクセス](#)"。
- ONTAP REST APIの使用方法を理解している。ONTAP REST APIの使用については、以下を参照してください。 <https://docs.netapp.com/us-en/ontap-automation/index.html>["ONTAP Automation ドキュメント"]。
- アプリケーション管理者である。
- REST API処理を実行するクラスタがONTAP 9.5以降でサポートされており、HTTPSを使用してUnified Managerに追加されている。

次の図は、ONTAPボリュームの使用容量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たものです。



このワークフローには、Unified ManagerとONTAP両方のREST APIの呼び出しポイントが含まれています。

1. ボリュームの使用容量を通知するイベントからボリューム名をメモします。
2. ボリューム名をnameパラメータに指定し、次のUnified Manager APIを実行してボリュームを照会します。

カテゴリ	HTTP動詞	パス
datacenter	GET	/datacenter/storage/volumes

3. 出力からクラスタのUUIDとボリュームの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 に移動して、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。この機能が有効になっていないと、gateway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有効にします。
- クラスタUUIDを使用してONTAP APIを実行します`/storage/volumes/{uuid}`APIゲートウェイ経由で。APIパラメータとしてボリュームのUUIDを渡した場合は、ボリュームの詳細が返されます。

APIゲートウェイを使用してONTAP APIを実行する場合、Unified Managerのクレデンシャルが内部で渡されて認証されます。このため、クラスタ アクセスのたびに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 : gateway	GET	ゲートウェイ API: /gateways/{uuid}/{path}
ONTAP : storage		ONTAP API: /storage/volumes/{uuid}



/gateways/{uuid}/{path} では、{uuid} の値を、REST 操作を実行するクラスター UUID に置き換える必要があります。{path} は、ONTAP REST URL /storage/volumes/{uuid} に置き換える必要があります。

追加された URL は次のとおりです。

/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}

GET 操作を実行すると、生成される URL は次のようになります。

GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes/{volume_uuid}

サンプルcURLコマンド

```
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>"
```

- サイズ、使用量、および実施する修正策を出力から確認します。このワークフローでは、ボリュームのサイズを変更します。
- クラスタのUUIDを使用し、APIゲートウェイを使用して次のONTAP APIを実行し、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 : gateway	PATCH	ゲートウェイ API: /gateways/{uuid}/{path}
ONTAP : storage		ONTAP API: /storage/volumes/{uuid}



ボリュームのサイズを変更するには、クラスタのUUIDとボリュームのUUIDに加え、sizeパラメータの値を入力する必要があります。必ず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 100 GB から 120 GB に増やしたい場合は、クエリの最後にパラメータ size の値を入力します。-d {"size": 128849018880}"

サンプルcURLコマンド

```
curl -X PATCH "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>" -d {"size": 128849018880}"
```

JSON出力でジョブのUUIDが返されます。

- ジョブの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。クラスタのUUIDとジョブのUUIDを使用し、APIゲートウェイを使用して次の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 : gateway	GET	ゲートウェイ API: /gateways/{uuid}/{path}
ONTAP : cluster		ONTAP API: /cluster/jobs/{uuid}

返されるHTTPコードは、ONTAP REST APIのHTTPステータス コードと同じです。

- 次のONTAP APIを実行して、サイズ変更後の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 : gateway	GET	ゲートウェイ API: /gateways/{uuid}/{path}
ONTAP : storage		ONTAP API: /storage/volumes/{uuid}

出力には拡張後のボリューム サイズとして120GBと表示されます。

APIによるワークロード管理のワークフロー

Active IQ Unified Managerを使用すると、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

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 でストレージ仮想マシン (SVM) をプロビジョニングするためのワークフロー。



このワークフローは、Unified Manager で LUN またはファイル共有をプロビジョニングする前に実行する必要があります。

- ファイル共有のプロビジョニング
- LUNのプロビジョニング
- LUNとファイル共有の変更（ストレージ ワークロードのパフォーマンス サービス レベル パラメータの更新例を使用）
- CIFSプロトコルをサポートするためのNFSファイル共有の変更
- QoSをAQoSにアップグレードするためのワークロードの変更



各プロビジョニング ワークフロー（LUNおよびファイル共有）では、クラスタのSVMを確認するワークフローを完了しておく必要があります。

また、ワークフローで各APIを使用する前に、推奨事項と制限事項を確認しておく必要があります。APIの詳細については、関連する概念および資料に記載されている個々のセクションを参照してください。

API を使用してクラスタ上の **SVM** を検証する

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 Machines (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。



このワークフローでは、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付与されている必要があります。

- クラスタにSVMが作成されているかどうかを確認します。

カテゴリ	HTTP動詞	パス
datacenter	GET	/datacenter/svm/svms /datacenter/svm/svms/{key }

サンプル **cURL**

```
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ーキーが必要です。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
datacenter	GET	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}

クラスターキーを取得します。

サンプル cURL

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H  
"accept: application/json" -H "Authorization: Basic  
<Base64EncodedCredentials>"
```

3. 出力からクラスターキーを取得し、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、そのSVMにLUNとファイル共有をプロビジョニングするため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
datacenter	POST	/datacenter/svm/svms

サンプル cURL

SVMオブジェクトの詳細を入力パラメータとして指定します。

```
curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Content-Type: application/json" -H "Authorization:
Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": {},
\"key\": \"1cd8a442-86d1,type=objecttype,uid=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,uid=1cd8a442-86d1-11e0-ae1c-
9876567890123\" },
\"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ],
\"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] },
\"fcg\": { \"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。

- ジョブ オブジェクト キーを使用して照会し、SVMの作成を確認します。SVMが正常に作成されている場合、SVMキーが応答に返されます。

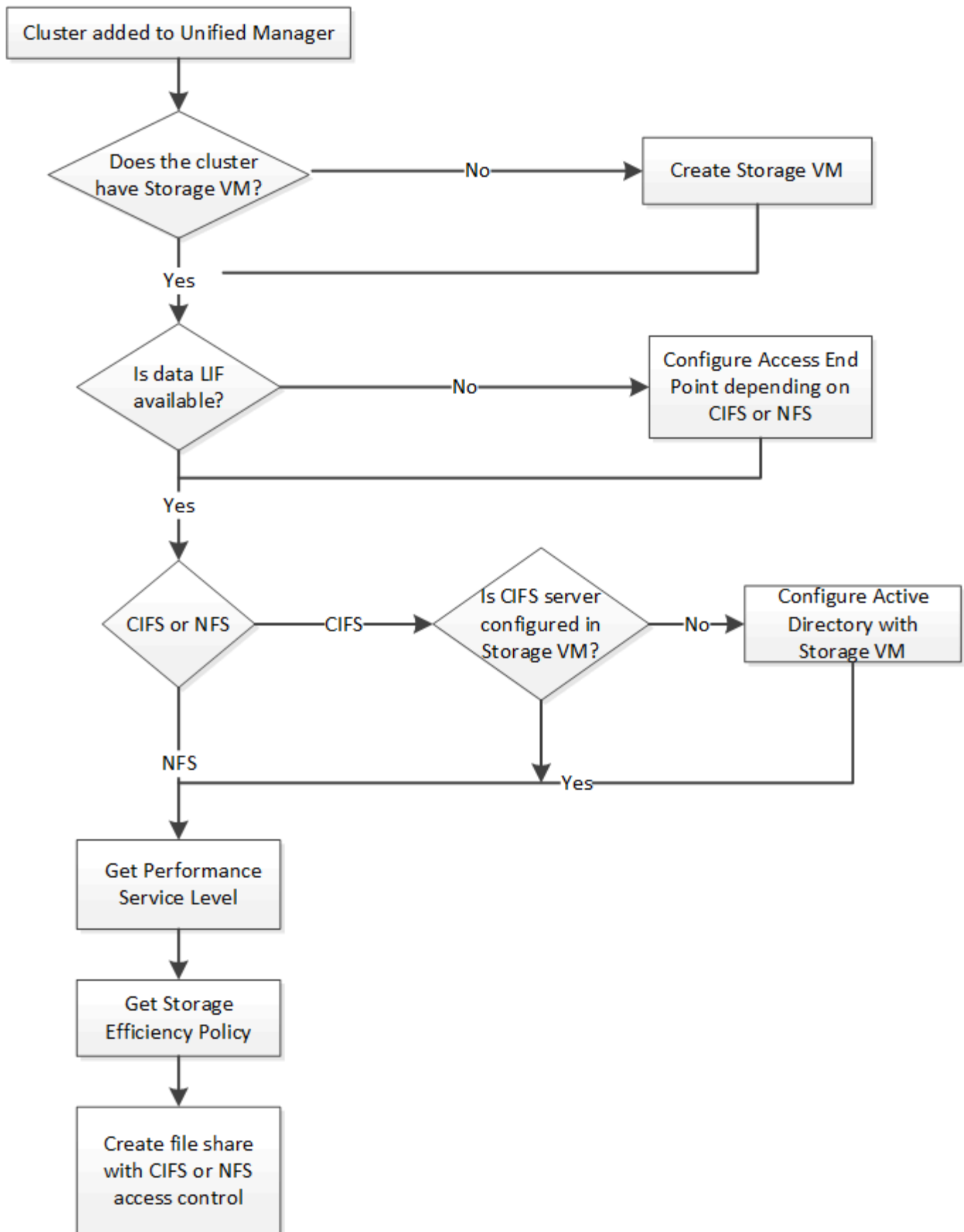
カテゴリ	HTTP動詞	パス
management-server	GET	/management-server/jobs/{key}

API を使用して **CIFS** および **NFS** ファイル共有をプロビジョニングする

Active IQ Unified Managerの一部として提供されるプロビジョニング API を使用して、Storage Virtual Machines (SVM) 上で CIFS 共有および NFS ファイル共有をプロビ

ジョニングできます。このプロビジョニング ワークフローでは、ファイル共有を作成する前にSVM、パフォーマンス サービス レベル、およびストレージ効率化ポリシーのキーを取得する手順について詳しく説明します。

次の図は、ファイル共有のプロビジョニング ワークフローの各手順を示しています。ワークフローには、CIFS共有とNFSファイル共有の両方のプロビジョニングが含まれています。



以下を確認してください。



- ONTAPクラスタが Unified Manager に追加され、クラスタ キーが取得されました。
- クラスタにSVMが作成されている必要があります。
- SVMでCIFSサービスとNFSサービスがサポートされている必要があります。SVMで必要なサービスがサポートされていない場合、ファイル共有のプロビジョニングに失敗することがあります。
- FCPポートがポート プロビジョニング用にオンラインになっている必要があります。

1. CIFS共有を作成するSVMで、データLIFまたはアクセス エンドポイントを使用できるかどうかを確認します。SVMで使用可能なアクセス エンドポイントのリストを取得します。

カテゴリ	HTTP動詞	パス
storage-provider	GET	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

サンプル cURL

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. 使用するアクセス エンドポイントがリストに表示されている場合は、アクセス エンドポイント キーを取得します。表示されていない場合は、アクセス エンドポイントを作成します。



CIFSプロトコルを有効にしてアクセス エンドポイントを作成してください。CIFS プロトコルが有効になっているアクセス エンドポイントを作成していない場合、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
storage-provider	POST	/storage-provider/access-endpoints

サンプル cURL

作成するアクセス エンドポイントの詳細を、入力パラメータとして指定する必要があります。

```
curl -X POST "https://<hostname>/api/storage-provider/access-endpoints"
-H "accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
{ \"data_protocols\": \"nfs\",
  \"fileshare\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=volume,uuid=f3063d27-2c71-44e5-9a69-a3927c19c8fc\" },
  \"gateway\": \"10.132.72.12\",
  \"ip\": { \"address\": \"10.162.83.26\",
  \"ha_address\": \"10.142.83.26\",
  \"netmask\": \"255.255.0.0\" },
  \"lun\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=lun,uuid=d208cc7d-80a3-4755-93d4-5db2c38f55a6\" },
  \"mtu\": 15000, \"name\": \"aep1\",
  \"svm\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a178d39e12:type=vserver,uuid=1d1c3198-fc57-11e8-99ca-00a098d38e12\" },
  \"vlan\": 10}
```

JSON出力にジョブ オブジェクト キーが表示され、作成したアクセス エンドポイントの検証に使用できます。

3. アクセス エンドポイントを検証します。

カテゴリ	HTTP動詞	パス
management-server	GET	/management-server/jobs/{key}

4. CIFS共有とNFSファイル共有のどちらを作成する必要があるかを判断します。CIFS共有を作成するには、次の手順を実行します。

- a. SVMにCIFSサーバが設定されているかどうかを確認します。そのためには、SVMにActive Directoryマッピングが作成されているかどうかを特定します。

カテゴリ	HTTP動詞	パス
storage-provider	GET	/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
storage-provider	POST	/storage-provider/active-directories-mappings

サンプル cURL

Active Directoryマッピングを作成するための詳細を、入力パラメータとして指定する必要があります。

```
curl -X POST "https://<hostname>/api/storage-provider/active-directories-mappings" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
{ \["_links\": {},
\"dns\": \"10.000.000.000\",
\"domain\": \"example.com\",
\"password\": \"string\",
\"svm\": { \"key\": \"9f4ddea-e395-11e9-b660-005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },
\"username\": \"string\"}"
```

+

これは同期呼び出しであり、Active Directoryマッピングの作成を出力で確認できます。エラーが発生した場合はエラー メッセージが表示されるため、トラブルシューティングして要求を再実行します。

5. 「クラスタ上の SVM の検証」ワークフロー トピックの説明に従って、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。
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
storage-provider	GET	/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は、`system_defined``入力パラメータ ``true`。出力から、ファイル共有に適用するパフォーマンス サービス レベルのキーを取得します。

7. 必要に応じて、次のAPIを実行し、応答からファイル共有に適用するストレージ効率化ポリシーのキーを取得します。

カテゴリ	HTTP動詞	パス
storage-provider	GET	/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 ポリシーを指定と、CIFSとNFSの両方をサポートするファイル共有を作成できます。次の手順は、ボリュームのどちらか一方のプロトコルのみをサポートするファイル共有を作成する場合の情報を示しています。作成後にNFSファイル共有を更新し、アクセス制御リストを追加することもできます。詳細については、「ストレージ ワークロードの変更」トピックを参照してください。

- a. CIFS共有のみを作成する場合は、アクセス制御リスト（ACL）に関する情報を収集します。CIFS共有を作成するには、次の入力パラメータに有効な値を指定します。割り当てたユーザ グループごとに、CIFS共有またはSMB共有のプロビジョニング時にACLが作成されます。ACLおよびActive Directoryマッピングに入力した値に基づいて、CIFS共有の作成時にアクセス制御とマッピングが決定されます。

サンプル値を含む **cURL** コマンド

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
  },
}
```

- b. NFSファイル共有のみを作成する場合は、エクスポート ポリシーに関する情報を収集します。NFSファイル共有を作成するには、次の入力パラメータに有効な値を指定します。この値に基づいて、NFSファイル共有の作成時にエクスポート ポリシーが適用されます。



NFS 共有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 キーを指定する必要があります。キーがわからない場合は、/datacenter/protocols/nfs/export-policies API。新しいポリシーを作成する場合は、次の例に示すようにルールを入力する必要があります。入力されたルールに対して、APIはホスト、Storage VM、およびルールを照合して既存のエクスポート ポリシーを検索します。既存のエクスポート ポリシーがある場合は、そのポリシーが使用されます。ない場合は、新しいエクスポート ポリシーが作成されます。

サンプル値を含む **cURL** コマンド

```
"export_policy": {
  "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
  "name_tag": "ExportPolicyNameTag",
  "rules": [
    {
      "clients": [
        {
          "match": "0.0.0.0/0"
        }
      ]
    }
  ]
}
```

アクセス制御リストとエクスポート ポリシーを設定したら、CIFSとNFSファイル共有の両方に必須のパラメータに有効な値を入力します。



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
storage-provider	POST	/storage-provider/file-shares

JSON出力にジョブ オブジェクト キーが表示され、作成したファイル共有の検証に使用できます。。ジョブの照会で返されたジョブ オブジェクト キーを使用して、ファイル共有の作成を確認します。

カテゴリ	HTTP動詞	パス
management-server	GET	/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
storage-provider	GET	/storage-provider/file-shares/{key}

サンプルJSON出力

POSTメソッドの `/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。例えば、`/storage-provider/performance-service-levels/` ファイル共有にパフォーマンス サービス レベルを割り当てるための API。

```

{
  "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
  "name": "FileShare_377",
  "cluster": {
    "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
    "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
    "name": "AFFA300-206-68-70-72-74",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959"
      }
    }
  }
}

```

```

    },
    "svm": {
      "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
      "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
      "name": "RRT_ritu_vs1",
      "_links": {
        "self": {
          "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959"
        }
      }
    },
    "assigned_performance_service_level": {
      "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
      "name": "Value",
      "peak_iops": 75,
      "expected_iops": 75,
      "_links": {
        "self": {
          "href": "/api/storage-provider/performance-service-levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
        }
      }
    },
    "recommended_performance_service_level": {
      "key": null,
      "name": "Idle",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
    "space": {
      "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
      "key": null,
      "name": "Unassigned",
      "_links": {}
    },
    "access_control": {
      "acl": [
        {
          "user_or_group": "everyone",
          "permission": "read"
        }
      ]
    }
  }
}

```

```

    }
  ],
  "export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
      {
        "anonymous_user": "65534",
        "clients": [
          {
            "match": "0.0.0.0/0"
          }
        ],
        "index": 1,
        "protocols": [
          "nfs3",
          "nfs4"
        ],
        "ro_rule": [
          "sys"
        ],
        "rw_rule": [
          "sys"
        ],
        "superuser": [
          "none"
        ]
      },
      {
        "anonymous_user": "65534",
        "clients": [
          {
            "match": "0.0.0.0/0"
          }
        ],
        "index": 2,
        "protocols": [
          "cifs"
        ],
        "ro_rule": [
          "ntlm"
        ],
        "rw_rule": [
          "ntlm"
        ]
      }
    ]
  }
}

```

```

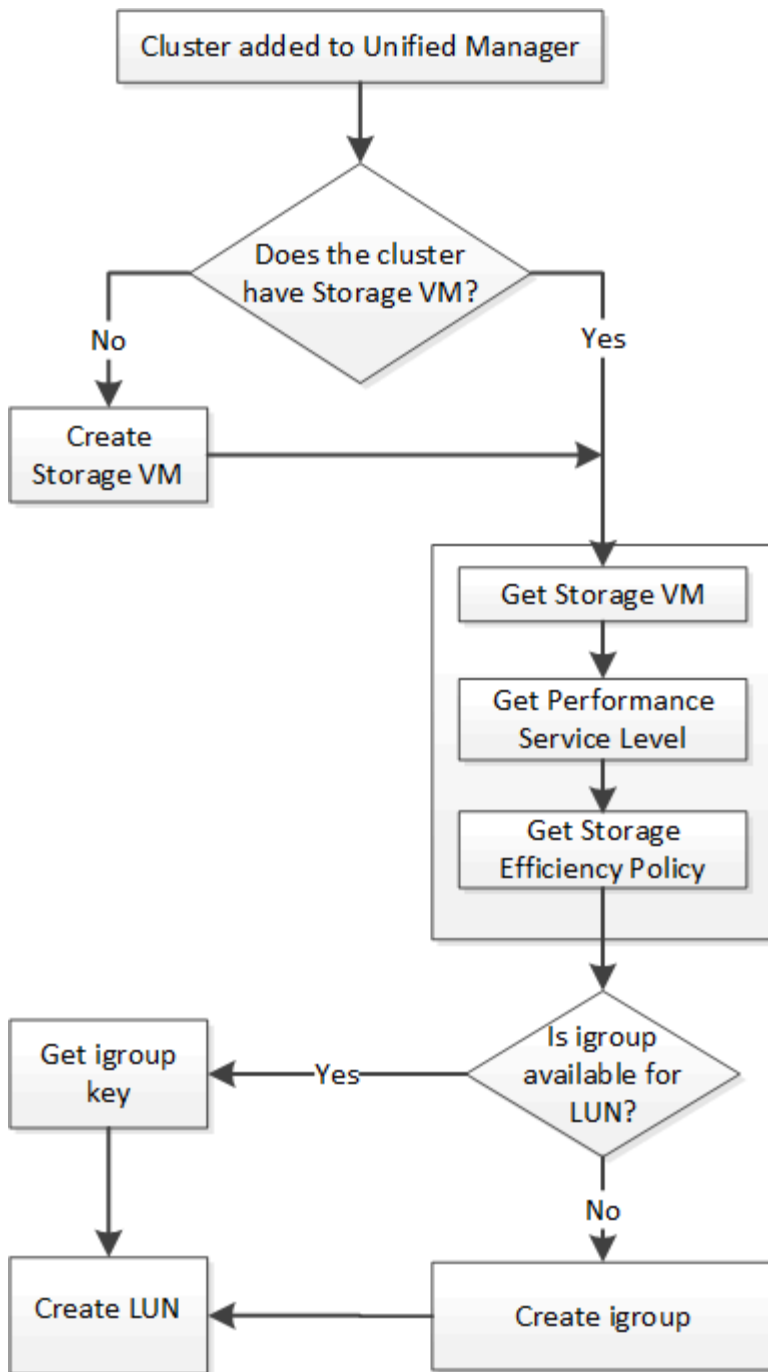
        ],
        "superuser": [
            "none"
        ]
    },
    ],
    "_links": {
        "self": {
            "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
        }
    }
},
"_links": {
    "self": {
        "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
    }
}
}
}

```

API を使用して LUN をプロビジョニングする

Active IQ Unified Managerの一部として提供されるプロビジョニング API を使用して、Storage Virtual Machines (SVM) 上で LUN をプロビジョニングできます。このプロビジョニング ワークフローでは、LUNを作成する前にSVM、パフォーマンス サービスレベル、およびストレージ効率化ポリシーのキーを取得する手順について詳しく説明します。

次の図は、LUNのプロビジョニング ワークフローの手順を示しています。



このワークフローでは、ONTAPクラスタが Unified Manager に追加され、クラスタ キーが取得されていることを前提としています。また、SVMがすでにクラスタに作成されていることも前提としています。

1. 「クラスタ上の SVM の検証」ワークフロー トピックの説明に従って、LUN を作成する SVM の SVM キーを取得します。
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
storage-provider	GET	/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は、`system_defined``入力パラメータ ``true`。出力から、LUNに適用するパフォーマンス サービス レベルのキーを取得します。

- 必要に応じて、次のAPIを実行し、応答からLUNに適用するストレージ効率化ポリシーのキーを取得します。

カテゴリ	HTTP動詞	パス
storage-provider	GET	/storage-provider/storage-efficiency-policies

- 作成するLUNターゲットへのアクセスを付与するイニシエータ 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
datacenter	GET	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}

igroupがアクセス権を有するSVMをパラメータ値として入力する必要があります。また、特定のigroupを照会する場合は、入力パラメータとしてigroup名（キー）を指定します。

- アクセスを付与するigroupが出力に見つかった場合は、そのキーを取得します。見つからない場合はigroupを作成します。

カテゴリ	HTTP動詞	パス
datacenter	POST	/datacenter/protocols/san/igroups

作成するigroupの詳細を入力パラメータとして指定する必要があります。これは同期呼び出しであり、igroupの作成を出力で確認できます。エラーが発生した場合はエラー メッセージが表示されるため、トラブルシューティングしてAPIを再実行します。

- LUNを作成

カテゴリ	HTTP動詞	パス
storage-provider	POST	/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指定する必要があります。



ストレージ効率化ポリシーは、LUNの作成ではオプションのパラメータです。

サンプル cURL

作成するLUNのすべての詳細を入力パラメータとして指定する必要があります。

JSON出力にジョブ オブジェクト キーが表示され、作成したLUNの検証に使用できます。

7. ジョブの照会で返されたジョブ オブジェクト キーを使用して、LUNの作成を確認します。

カテゴリ	HTTP動詞	パス
management-server	GET	/management-server/jobs/{key}

応答の末尾に、作成されたLUNのキーが表示されます。

8. 返されたキーを指定して次のAPIを実行し、LUNの作成を確認します。

カテゴリ	HTTP動詞	パス
storage-provider	GET	/storage-provider/luns/{key}

サンプルJSON出力

POSTメソッドの /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。例えば、`/storage-provider/performance-service-levels/ LUN にパフォーマンス サービス レベルを割り当てるための API。

== LUNの作成またはマッピングの失敗に関する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たあとも引き続きLUNの作成に失敗することがあります。LUNの作成に成功しても、LUNを作成したノードにSAN LIFまたはアクセス エンドポイントがないためにigroupとのLUNマッピングが失敗することがあります。エラーが発生した場合は、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.
```

このエラーを回避するには、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
storage-provider	POST	/storage-provider/access-endpoints

サンプル cURL

作成するアクセス エンドポイントの詳細を、入力パラメータとして指定する必要があります。



入力パラメータに、LUNのホーム ノードを示すaddressと、ホーム ノードのパートナー ノードを示すha_addressを追加したことを確認します。この処理を実行すると、ホーム ノードとパートナー ノードの両方にアクセス エンドポイントが作成されます。

2. JSON出力で返されたジョブ オブジェクト キーを使用してジョブを照会し、SVMにアクセス エンドポイントを追加するジョブが正常に実行されたこと、およびSVMでiSCSI/FCPサービスが有効になっていることを確認します。

カテゴリ	HTTP動詞	パス
management-server	GET	/management-server/jobs/{key}

サンプルJSON出力

出力の末尾に、作成されたアクセス エンドポイントのキーが表示されます。次の出力では、「name': "accessEndpointKey" の値は、キーが 9c964258-14ef-11ea-95e2-00a098e32c28 である 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ています。"name': "accessEndpointHAKey" 値は、ホーム ノードのパートナー ノード上に作成されたアクセス エンドポイントを示します。そのキーは 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
storage-provider	PATCH	/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。

サンプル cURL

JSON出力にジョブ オブジェクト キーが表示され、マッピングが成功したかどうかの検証に使用できます。

4. LUNキーを指定して照会することで、LUNマッピングを確認します。

カテゴリ	HTTP動詞	パス
storage-provider	GET	/storage-provider/luns/{key}

サンプルJSON出力

出力から、LUNのプロビジョニング時に使用されたigroup（キー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 を使用してストレージ ワークロードを変更する

ストレージ ワークロードを変更するには、パラメータが不足しているLUNまたはファイル共有を更新するか、既存のパラメータを変更します。

このワークフローは、LUNとファイル共有のパフォーマンス サービス レベルを更新する例を示しています。



ワークフローは、LUNまたはファイル共有がパフォーマンス サービス レベルでプロビジョニングされていることを前提としています。

ファイル共有の変更

ファイル共有の変更では、次のパラメータを更新できます。

- 容量またはサイズ
- オンラインまたはオフラインの設定
- ストレージ効率化ポリシー
- パフォーマンス サービス レベル
- アクセス制御リスト（ACL）の設定
- エクスポート ポリシーの設定。エクスポート ポリシー パラメータを削除して、ファイル共有のデフォルト（空）のエクスポート ポリシー ルールに戻すこともできます。



1回のAPIの実行で更新できるパラメータは1つだけです。

この手順では、パフォーマンス サービス レベルをファイル共有に追加する方法について説明します。その他のファイル共有プロパティを更新する場合にも、同じ手順を使用できます。

1. 更新するファイル共有のCIFS共有キーまたはNFSファイル共有キーを取得します。このAPIは、データセンター上のすべてのファイル共有を照会します。ファイル共有キーがすでにわかっている場合は、この手順を省略してください。

カテゴリ	HTTP動詞	パス
storage-provider	GET	/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
storage-provider	GET	/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	GET	/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は、`system_defined``入力パラメータ `true`。出力から、ファイル共有に適用するパフォーマンス サービス レベルのキーを取得します。

4. ファイル共有にパフォーマンス サービス レベルを適用します。

カテゴリ	HTTP動詞	パス
storage-provider	PATCH	/storage-provider/file-shares/{key}

入力では、更新するパラメータのみをファイル共有キーとともに指定する必要があります。ここでは、パフォーマンス サービス レベルのキーを指定します。

サンプル **cURL**

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{
  \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" },
}"
```

JSON出力にジョブ オブジェクトが表示されます。このジョブ オブジェクトを使用して、ホーム ノードとパートナー ノードのアクセス エンドポイントが作成されたかどうかを確認することができます。

- 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
管理サーバー	GET	/management-server/jobs/{key}

ジョブ オブジェクトのIDで照会すると、ファイル共有が更新されたかどうかを確認できます。正しく処理されていなかった場合は、問題を解決してからAPIを再度実行します。作成に成功したら、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
storage-provider	GET	/storage-provider/file-shares/{key}

出力内のファイル共有の詳細を確認します。

```
"assigned_performance_service_level": {
  "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
  "name": "Value",
  "peak_iops": 75,
  "expected_iops": 75,
  "_links": {
    "self": {
      "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
    }
  }
}
```

LUNを更新する

LUNの更新では、次のパラメータを変更できます。

- 容量またはサイズ
- オンラインまたはオフラインの設定
- ストレージ効率ポリシー
- パフォーマンス サービス レベル
- LUNマップ



1回のAPIの実行で更新できるパラメータは1つだけです。

この手順では、パフォーマンス サービス レベルをLUNに追加する方法について説明します。その他のLUNプロパティを更新する場合にも、同じ手順を使用できます。

1. 更新するLUNのLUNキーを取得します。このAPIは、データセンター内のすべてのLUNの詳細を返します。LUNキーがすでにわかっている場合は、この手順を省略してください。

カテゴリ	HTTP動詞	パス
storage-provider	GET	/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
storage-provider	GET	/storage-provider/luns/{key}

出力内のLUNの詳細を確認します。このLUNにはパフォーマンス サービス レベルが割り当てられていないことがわかります。

サンプルJSON出力

```
"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	GET	/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は、`system_defined``入力パラメータ ``true`。出力から、LUNに適用するパフォーマンス サービス レベルのキーを取得します。

4. LUNにパフォーマンス サービス レベルを適用します。

カテゴリ	HTTP動詞	パス
storage-provider	PATCH	/storage-provider/lun/{key}

入力では、更新するパラメータのみをLUNキーとともに指定する必要があります。ここでは、パフォーマンス サービス レベルのキーを指定します。

サンプル cURL

```
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
storage-provider	GET	/storage-provider/luns/{key}

出力内のLUNの詳細を確認します。このLUNにパフォーマンス サービス レベルが割り当てられていることがわかります。

サンプルJSON出力

```

"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**API**を使用して**NFS**ファイル共有を変更する

CIFSプロトコルをサポートするようにNFSファイル共有を変更できます。ファイル共有を作成する際には、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 ルールの両方を指定できます。ただし、NFSファイル共有を作成したボリュームでCIFSを有効にする場合は、CIFSをサポートするようにファイル共有のACLパラメータを更新できます。

開始する前に

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を表示し、ジョブ ID を使用してファイル共有キーを取得する方法については、「CIFS および NFS ファイル共有のプロビジョニング」を参照してください。

この処理は、ACLパラメータは指定せずに、エクスポート ポリシー ルールのみを指定して作成したNFSファイル共有が対象です。NFSファイル共有を変更してACLパラメータを追加します。

手順

1. NFSファイル共有で、 PATCH CIFS アクセスを許可するための ACL 詳細を使用した操作。

カテゴリ	HTTP動詞	パス
storage-provider	PATCH	/storage-provider/file-shares

サンプル **cURL**

次の例に示すように、ユーザ グループに割り当てたアクセス権限に基づいてACLが作成され、ファイル共有に割り当てられます。


```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
  }
}
```

サンプルJSON出力

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
storage-provider	GET	/storage-provider/file-shares/{key}

サンプルJSON出力

```
"access_control": {
  "acl": [
    {
      "user_or_group": "everyone",
      "permission": "read"
    }
  ],
  "export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
      {
        "anonymous_user": "65534",
        "clients": [
          {
            "match": "0.0.0.0/0"
          }
        ]
      }
    ]
  }
}
```

```

        "index": 1,
        "protocols": [
            "nfs3",
            "nfs4"
        ],
        "ro_rule": [
            "sys"
        ],
        "rw_rule": [
            "sys"
        ],
        "superuser": [
            "none"
        ]
    },
    {
        "anonymous_user": "65534",
        "clients": [
            {
                "match": "0.0.0.0/0"
            }
        ],
        "index": 2,
        "protocols": [
            "cifs"
        ],
        "ro_rule": [
            "ntlm"
        ],
        "rw_rule": [
            "ntlm"
        ],
        "superuser": [
            "none"
        ]
    }
],
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
}
},

```

```
    "_links": {  
      "self": {  
        "href": "/api/storage-provider/file-shares/7d5a59b3-953a-  
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-  
00a098dcc6b6"  
      }  
    }  
  }
```

同じファイル共有に対して、エクスポート ポリシーに加えてACLが割り当てられていることがわかります。

法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲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

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

<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

この製品で使用されているサードパーティの著作権とライセンスに関する情報。

["Active IQ Unified Manager 9.16 に関するお知らせ"](#)

著作権に関する情報

Copyright © 2025 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。