



CLIを使用したクラスタパフォーマンスの監視 と管理 ONTAP 9

NetApp
December 20, 2024

目次

CLIを使用したクラスタパフォーマンスの監視と管理	1
パフォーマンスの監視と管理の概要	1
パフォーマンスの監視	1
Digital Advisorを使用してシステムパフォーマンスを表示する	12
パフォーマンスの問題の管理	12

CLIを使用したクラスタパフォーマンスの監視と管理

パフォーマンスの監視と管理の概要

基本的なパフォーマンスの監視と管理タスクを設定し、一般的なパフォーマンスの問題を特定して解決できます。

次の前提条件に該当する場合は、これらの手順を使用してクラスタのパフォーマンスを監視および管理できません。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- ONTAP コマンドラインインターフェイスに加え、Active IQ Unified Manager（旧 OnCommand Unified Manager）を使用して、システムのステータスとアラートを表示し、クラスタのパフォーマンスを監視し、根本原因分析を実施する。
- ONTAPコマンドラインインターフェイスを使用してストレージQuality of Service（QoS；サービス品質）を設定している。また、次の方法でQoSを利用することもできます。
 - System Manager
 - ONTAP REST API
 - ONTAP tools for VMware vSphere
 - NetAppサービスレベルマネージャ（NSLM）
 - OnCommand Workflow Automation（WFA）
- Linux または Windows ベースのインストールではなく、仮想アプライアンスを使用して Unified Manager をインストールする。
- DHCPではなく静的な設定を使用してソフトウェアをインストールします。
- ONTAPコマンドにはadvanced権限レベルでアクセスできます。
- 「admin」ロールを持つクラスタ管理者である。

関連情報

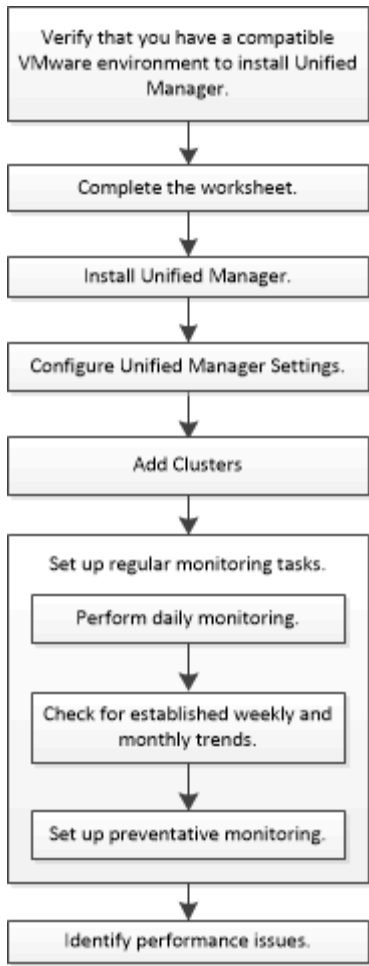
上記の想定条件に該当しない場合は、次の資料を参照してください。

- ["Active IQ Unified Manager 9.8のインストール"](#)
- ["システム管理"](#)

パフォーマンスの監視

パフォーマンスの監視とメンテナンスのワークフローの概要

クラスタパフォーマンスの監視と保守では、Active IQ Unified Manager ソフトウェアをインストールし、基本的な監視タスクを設定し、パフォーマンスの問題を特定し、必要に応じて調整を行います。



VMware環境がサポートされていることの確認

Active IQ Unified Managerをインストールするには、VMware環境が必要な要件を満たしていることを確認する必要があります。

手順

1. VMwareインフラがUnified Managerのインストールに必要なサイジング要件を満たしていることを確認します。
2. に移動し "[Interoperability Matrix](#)"で、次のコンポーネントについて、サポートされている組み合わせであることを確認します。
 - ONTAPのバージョン
 - ESXiオペレーティングシステムのバージョン
 - VMware vCenter Server のバージョン
 - VMware Tools のバージョン
 - ブラウザのタイプとバージョン



Unified Managerでサポートされる構成はInteroperability Matrixで確認できます。

3. 選択した構成の構成名をクリックします。

その構成の詳細が[Configuration Details]ウィンドウに表示されます。

4. 次のタブの情報を確認します。

◦ 脚注

に、構成に固有の重要なアラートと情報を示します。

◦ ポリシーとガイドライン

すべての構成に関する一般的なガイドラインが表示されます。

Active IQ Unified Managerワークシート

Active IQ Unified Managerをインストール、設定、接続する前に、環境に関する特定の情報を確認しておく必要があります。ワークシートに情報を記録できます。

Unified Managerのインストール情報

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

Unified Managerの設定情報

設定	あなたの価値
メンテナンスユーザのEメールアドレス	

NTPサーバ	
SMTPサーバのホスト名またはIPアドレス	
SMTPのユーザ名	
SMTPパスワード	
SMTPのデフォルトポート	25 (デフォルト値)
アラート通知の送信元Eメール	
LDAPのバインド識別名	
LDAPのバインドパスワード	
Active Directory管理者名	
Active Directoryのパスワード	
認証サーバのベース識別名	
認証サーバのホスト名またはIPアドレス	

クラスタ情報

Unified Managerで各クラスタについて次の情報を確認します。

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

関連情報

["カンリシヤニンシヨウトRBAC"](#)

Active IQ Unified Managerのインストール

Active IQ Unified Managerのダウンロードと導入

ソフトウェアをインストールするには、仮想アプライアンス (VA) インストールファイルをダウンロードし、VMware vSphere Clientを使用してVMware ESXiサーバに導入する必要があります。VAはOVAファイルで使用できます。

手順

1. NetApp Support Siteソフトウェアのダウンロード * ページにアクセスし、Active IQ Unified Manager を探します。

<https://mysupport.netapp.com/products/index.html>

2. [Select Platform* (プラットフォームの選択)] ドロップダウンメニューで [* VMware vSphere* (VMware vSphere*)] を選択し、[* Go!* (実行)] をクリックします
3. 「OVA」 ファイルを、VMware vSphere Clientからアクセス可能なローカルまたはネットワーク上の場所に保存します。
4. VMware vSphere Client で、* File * > * Deploy OVF Template * をクリックします。
5. 「OVA」 ファイルを探し、ウィザードを使用してESXiサーバに仮想アプライアンスを導入します。

ウィザードの * Properties * タブを使用して、静的な構成情報を入力できます。

6. VMの電源をオンにします。
7. 最初の起動プロセスを表示するには、* Console * タブをクリックします。
8. プロンプトに従って、VMにVMware Toolsをインストールします。
9. タイムゾーンを設定します。
10. メンテナンスユーザの名前とパスワードを入力します。
11. VMコンソールに表示されるURLに移動します。

Active IQ Unified Managerの初期設定

Web UI への初回アクセス時に Active IQ Unified Manager の初期セットアップ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、いくつかの初期設定を行ったり、クラスタを追加したりできます。

手順

1. デフォルトのAutoSupport Enabled設定をそのまま使用します。
2. NTP サーバの詳細、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、およびその他の SMTP オプションを入力し、* Save * をクリックします。

終了後

初期セットアップが完了すると、クラスタデータソースページが表示され、クラスタの詳細を確認できます。

監視するクラスタを指定

クラスタを監視対象に含め、クラスタの検出ステータスを確認したり、クラスタのパフォーマンスを監視したりするには、クラスタを Active IQ Unified Manager サーバに追加する必要があります。

必要なもの

- 次の情報が必要です。
 - ホスト名またはクラスタ管理IPアドレス
- ホスト名は、Unified Manager がクラスタへの接続に使用する完全修飾ドメイン名（FQDN）または短縮名です。このホスト名は、クラスタ管理IPアドレスに解決される必要があります。

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

- ONTAP管理者のユーザ名とパスワード
- クラスタおよびクラスタのポート番号で設定できるプロトコルのタイプ（HTTP または HTTPS）
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- ONTAP管理者にONTAPIとSSHの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 の FQDN を使用して、ONTAP に ping を実行できる必要があります。

これは、ONTAPコマンドを使用して確認できます `ping -node node_name -destination Unified_Manager_FQDN`。

タスクの内容

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

手順

1. [* Configuration * > * Cluster Data Sources *] をクリックします。
2. [クラスタ] ページで、[* 追加] をクリックします。
3. Add Cluster * （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（IPv4 または IPv6）、ユーザ名、パスワード、通信プロトコル、ポート番号など、必要な値を指定します。

デフォルトでは、HTTPSプロトコルが選択されています。

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

4. [追加]*をクリックします。
5. [HTTPS]が選択されている場合は、次の手順を実行します。
 - a. [* Authorize Host * （ホストの認証 * ）] ダイアログボックスで、[* View Certificate * （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。

- b. 「* はい *」をクリックします。

Unified Manager で証明書がチェックされるのはクラスタを最初に追加したときだけです、ONTAP に対する API 呼び出しごとに確認されるわけではありません。

証明書の期限が切れているクラスタは追加できません。SSL証明書を更新してからクラスタを追加する必要があります。

6. * オプション * : クラスタ検出ステータスを表示します。

- a. クラスタセットアップ* ページでクラスタ検出ステータスを確認します。

デフォルトの監視間隔である約 15 分後に、Unified Manager データベースにクラスタが追加されます。

基本的な監視タスクの設定

日々の監視

監視を毎日実行して、注意が必要なパフォーマンスの問題がすぐに発生しないようにすることができます。

手順

1. Active IQ Unified Manager UI から * Event Inventory * ページに移動して、現在のイベントと廃止状態のイベントをすべて表示します。
2. [表示]*オプションからを選択し Active Performance Events、必要な操作を決定します。

週単位と月単位のパフォーマンスの傾向を使用してパフォーマンスの問題を特定

パフォーマンスの傾向を特定すると、ボリュームレイテンシを分析して、クラスタの使用率が高すぎるか低すぎるかを特定するのに役立ちます。同様の手順を使用して、CPU、ネットワーク、またはその他のシステムのボトルネックを特定できます。

手順

1. 使用率が高すぎるか低すぎる疑いがあるボリュームを探します。
2. [ボリュームの詳細] タブで、[*30 d] をクリックして履歴データを表示します。
3. [データのブレイクダウンの条件] ドロップダウンメニューで、[Latency] を選択し、[Submit] をクリックします。
4. クラスタコンポーネント比較グラフで「* Aggregate」を選択解除し、クラスタのレイテンシをボリュームレイテンシグラフと比較します。
5. アグリゲートを選択し、クラスタコンポーネント比較チャート内の他のすべてのコンポーネントの選択を解除して、アグリゲートのレイテンシをボリュームレイテンシチャートと比較します。
6. [読み取り/書き込みレイテンシ] グラフをボリュームレイテンシのグラフと比較します。
7. クライアントアプリケーションの負荷が原因でワークロードの競合が発生していないかどうかを確認し、必要に応じてワークロードをリバランシングします。
8. アグリゲートの使用率が高すぎて競合を引き起こしていないかどうかを確認し、必要に応じてワークロードをリバランシングします。

パフォーマンスしきい値を使用したイベント通知の生成

イベントは、事前に定義された状況が発生したとき、またはパフォーマンスカウンタの値がしきい値を超えたときに、Active IQ Unified Manager で自動的に生成される通知です。イベントによって、監視しているクラスタ内のパフォーマンスの問題を特定できます。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 E メール通知を送信するアラートを設定できます。

パフォーマンスしきい値の設定

パフォーマンスしきい値を設定して、重大なパフォーマンスの問題を監視することができます。ユーザ定義のしきい値は、システムが定義されたしきい値に近づいたとき、または超えたときに警告または重大イベントの通知をトリガーします。

手順

1. 警告イベントと重大イベントのしきい値を作成します。
 - a. [* Configuration * > * Performance Thresholds *] を選択します。
 - b. [作成 (Create)] をクリックします。
 - c. オブジェクトタイプを選択し、ポリシーの名前と説明を指定します。
 - d. オブジェクトカウンタの条件を選択し、警告イベントと重大イベントの制限値を指定します。
 - e. イベントを送信するために制限値に違反する必要がある期間を選択し、[保存] をクリックします。
2. しきい値ポリシーをストレージオブジェクトに割り当てます。
 - a. 以前に選択したクラスタオブジェクトタイプのインベントリページに移動し、View オプションから * Performance * を選択します。
 - b. しきい値ポリシーを割り当てるオブジェクトを選択し、* しきい値ポリシーの割り当て * をクリックします。
 - c. 前の手順で作成したポリシーを選択し、* ポリシーの割り当て * をクリックします。

例

重大なパフォーマンスの問題を特定するためにユーザ定義のしきい値を設定することができます。たとえば、ボリュームのレイテンシが20ミリ秒を超えるとMicrosoft Exchange Serverがクラッシュすることがわかっている場合は、警告しきい値を12ミリ秒、重大しきい値を15ミリ秒のように設定できます。このしきい値の設定を使用して、ボリュームのレイテンシが制限を超えたときに通知を受け取ることができます。

	 Warning	 Critical			
Object Counter Condition*	Average Latency ms/op	12	ms/op	15	ms/op

アラートの追加

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

必要なもの

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

タスクの内容

ここで説明するように、[Alert Setup]ページからアラートを作成するだけでなく、イベントを受信したあとに[Event Details]ページから直接アラートを作成することもできます。

手順

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

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

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

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



複数のイベントを選択するには、Ctrlキーを押しながら選択します。

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



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

SNMPトラップを使用してユーザに通知することもできます。

7. [保存 (Save)] をクリックします。

アラートの追加例

次の例は、次の要件を満たすアラートを作成する方法を示しています。

- アラート名： HealthTest
- リソース：名前に「abc」を含むすべてのボリュームを対象にし、名前に「xyz」を含むすべてのボリュームを除外します。
- イベント：健全性に関するすべての重大イベントを含む
- アクション：「sample@domain.com」、「テスト」スクリプトが含まれており、15分ごとにユーザに通知する必要があります。

[Add Alert]ダイアログボックスで、次の手順を実行します。

1. をクリックし、[アラート名]*フィールドにと入力します HealthTest。
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. [名前に次の文字を含む]フィールドにと入力し abc、名前に「abc」を含むボリュームを表示します。
 - b. [Available Resources]領域で**を選択し[All Volumes whose name contains 'abc']、[Selected Resources]領域に移動します。
 - c. をクリックし、[名前に次の文字を含む]フィールドにと入力し xyz、[追加]*をクリックします。
3. [* イベント] をクリックし、[イベントの重要度] フィールドから [クリティカル*] を選択します。
4. [Matching Events] 領域から [*All Critical Events] を選択し、[Selected Events] 領域に移動します。
5. [Actions]*をクリックし、[Alert These Users]フィールドにと入力します sample@domain.com。
6. 15 分ごとにユーザに通知するには、「* 15 分ごとに通知する」を選択します。

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

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

アラートの設定

アラートについて、アラートをトリガーする Active IQ Unified Manager のイベント、アラートを受け取る E メール受信者、およびアラートの頻度を指定することができます。

必要なもの

アプリケーション管理者のロールが必要です。

タスクの内容

次のタイプのパフォーマンスイベントに対して固有のアラートを設定できます。

- 重大イベント：ユーザ定義のしきい値に違反したときにトリガーされる
- 警告イベント：ユーザ定義のしきい値、システム定義のしきい値、または動的なしきい値に違反したときにトリガーされる

デフォルトでは、すべての新しいイベントについて、Unified Manager の管理者ユーザに E メールアラート

が送信されます。Eメールアラートを他のユーザに送信するには、そのユーザのEメールアドレスを追加します。



特定のタイプのイベントに関するアラートの送信を無効にするには、イベントカテゴリのすべてのチェックボックスをオフにする必要があります。この操作によって、ユーザインターフェイスにイベントが表示されなくな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、 * Storage Management * > * Alert Setup * を選択します。

[Alert Setup]ページが表示されます。

2. [* 追加] をクリックし、各イベントタイプに適切な設定を行います。

Eメールアラートを複数のユーザに送信するには、各Eメールアドレスをカンマで区切って入力します。

3. [保存 (Save)] をクリックします。

Active IQ Unified Managerでのパフォーマンスの問題の特定

パフォーマンスイベントが発生した場合は、Active IQ Unified Manager で問題のソースを特定し、他のツールを使用して修正することができます。イベントのEメール通知を受信したり、日々の監視中にイベントに気付いたりすることがあります。

手順

1. Eメール通知内のリンクをクリックすると、パフォーマンスイベントが発生しているストレージオブジェクトに直接移動できます。

状況	そしたら...
イベントのEメール通知を受信する	リンクをクリックしてイベントの詳細ページに直接移動します。
[Event Inventory]ページを分析中にイベントに注目してください。	イベントを選択してイベントの詳細ページに直接移動します。

2. システム定義のしきい値を超えたイベントの場合は、UIに表示される推奨される対処方法に従って問題をトラブルシューティングします。
3. ユーザ定義のしきい値を超えたイベントの場合は、イベントを分析して対処が必要かどうかを判断します。
4. 問題が解決しない場合は、次の設定を確認します。
 - ストレージシステムのプロトコル設定
 - イーサネットスイッチまたはファブリックスイッチのネットワーク設定
 - ストレージシステムのネットワーク設定
 - ストレージシステムのディスクレイアウトとアグリゲートの指標を表示します
5. 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。

Digital Advisorを使用してシステムパフォーマンスを表示する

AutoSupportの計測データをNetAppに送信するONTAPシステムについて、パフォーマンスと容量に関する広範なデータを表示できます。Digital Advisorでは、System Managerよりも長い期間のシステムパフォーマンスが表示されます。

CPU利用率、レイテンシ、IOPS、プロトコル別のIOPS、およびネットワークスループットのグラフを表示できます。このデータを.csv形式でダウンロードして、他のツールで分析することもできます。

このパフォーマンスデータに加えて、Digital Advisorではワークロード別のストレージ効率を表示し、そのタイプのワークロードで想定される効率と比較できます。容量のトレンドを表示して、特定の期間に追加が必要になる可能性のあるストレージの見積もりを確認できます。



- Storage Efficiencyは、お客様レベル、クラスタレベル、ノードレベルで、メインのダッシュボードの左側に表示されます。
- パフォーマンスは、メインダッシュボードの左側にクラスタレベルおよびノードレベルで表示されます。

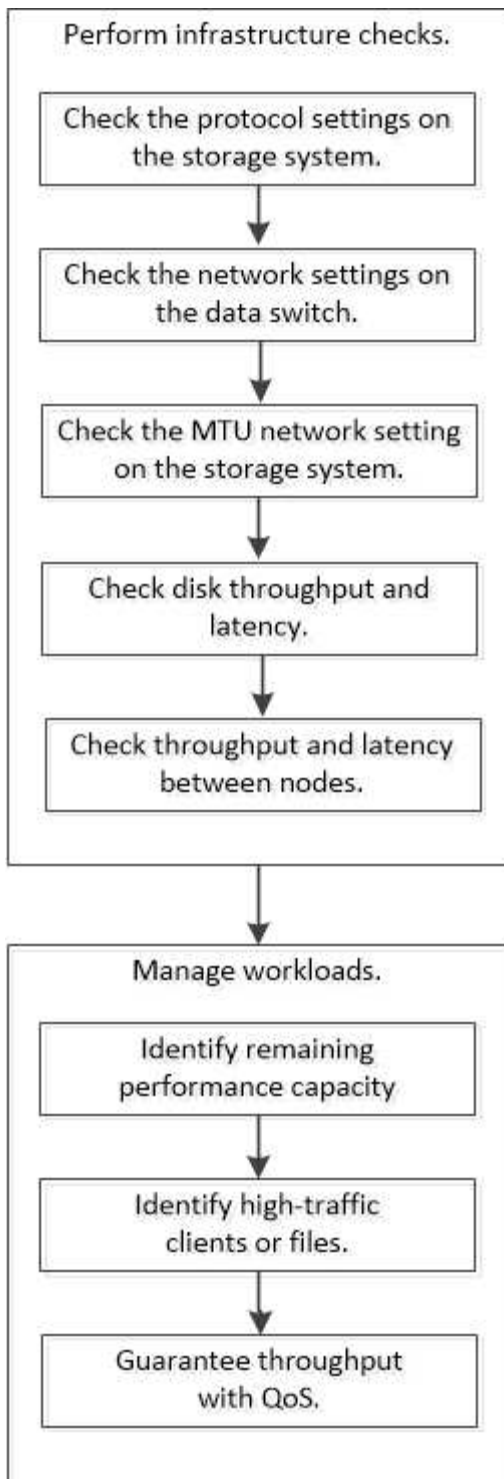
関連情報

- ["Digital Advisorのドキュメント"](#)
- ["Digital Advisorのビデオプレイリスト"](#)
- ["Digital Advisor Webポータル"](#)

パフォーマンスの問題の管理

パフォーマンス管理ワークフロー

パフォーマンスの問題を特定したら、インフラのいくつかの基本的な診断チェックを実行して、明らかな構成エラーを排除できます。問題が特定されない場合は、ワークロード管理の問題に目を向けることができます。



基本的なインフラチェックの実行

ストレージシステムのプロトコル設定を確認

NFS TCP最大転送サイズの確認

NFS の場合、読み取りと書き込みの TCP 最大転送サイズがパフォーマンス問題の原因になっていないかどうかを確認することができます。このサイズが原因でパフォーマンスが低下している可能性がある場合は、サイズを大きくして対処できます。

必要なもの

- このタスクを実行するには、クラスタ管理者の権限が必要です。
- このタスクを実行するには、advanced権限レベルのコマンドを使用する必要があります。

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. TCP 最大転送サイズを確認します。

```
vserver nfs show -vserver vserver_name -instance
```

3. TCP 最大転送サイズが小さすぎる場合は、サイズを大きくします。

```
vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
```

4. 管理者権限レベルに戻ります。

```
set -privilege admin
```

例

次の例は、のTCP最大転送サイズを1048576に変更し`SVM1`ます。

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

iSCSI TCP読み取り/書き込みサイズの確認

iSCSI の場合、TCP 読み取り / 書き込みサイズを確認して、サイズ設定がパフォーマンス問題を作成中であるかどうかを判断できます。サイズが問題のソースである場合は、サイズを変更して対処できます。

必要なもの

このタスクを実行するには、advanced権限レベルのコマンドが必要です。

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. TCP ウィンドウサイズの設定を確認します。

```
vserver iscsi show -vserver vserver_name -instance
```

3. TCP ウィンドウサイズの設定を変更します。

```
vserver iscsi modify -vserver vserver_name -tcp-window-size integer
```


4. admin権限に戻ります。

```
set -privilege admin
```

例

次に、のTCPウィンドウサイズを131、400バイトに変更する例を示し`SVM1`ます。

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

CIFS多重化設定の確認

CIFSネットワークのパフォーマンスが低下してパフォーマンスの問題が発生した場合は、多重化設定を変更して問題を改善および修正できます。

手順

1. CIFS多重化設定を確認します。

```
vserver cifs options show -vserver -vserver_name -instance
```

2. CIFS多重化設定を変更します。

```
vserver cifs options modify -vserver -vserver_name -max-mpx integer
```

例

次に、の最大多重化カウントを255に変更する例を示し`SVM1`ます。

```
cluster1::*> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

FCアダプタのポート速度の確認

パフォーマンスを最適化するには、アダプタのターゲットポートの速度を接続先デバイスの速度と同じにします。ポートに自動ネゴシエーションが設定されている場合、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

必要なもの

このアダプタをホームポートとして使用しているすべてのLIFをオフラインにする必要があります。

手順

1. アダプタをオフラインにします。

```
network fcp adapter modify -node nodename -adapter adapter -state down
```

2. ポートアダプタの最大速度を確認します。

```
fcp adapter show -instance
```

3. 必要に応じてポート速度を変更します。

```
network fcp adapter modify -node nodename -adapter adapter -speed  
{1|2|4|8|10|16|auto}
```

4. アダプタをオンラインにします。

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

5. アダプタのすべてのLIFをオンラインにします。

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }  
-status-admin up
```

例

次に、の `node1` アダプタのポート速度を2Gbpsに変更する例を示し `0d` ます。

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

データスイッチのネットワーク設定を確認する

クライアント、サーバ、およびストレージシステム（ネットワークエンドポイント）では同じMTU設定を維持する必要がありますが、パフォーマンスに影響が及ばないように、NICやスイッチなどの中間ネットワークデバイスは最大MTU値に設定する必要があります。

最高のパフォーマンスを得るには、ネットワーク内のすべてのコンポーネントがジャンボフレーム（IP 9000バイト、イーサネットを含む9022バイト）を転送できる必要があります。データスイッチは少なくとも9022バイトに設定する必要がありますが、ほとんどのスイッチでは標準値9216を使用できます。

手順

データスイッチの場合は、MTUサイズが9022以上に設定されていることを確認します。

詳細については、スイッチベンダーのドキュメントを参照してください。

ストレージシステムのMTUネットワーク設定を確認する

ストレージシステムのネットワーク設定がクライアントまたは他のネットワークエンドポイントと同じでない場合は、設定を変更できます。管理ネットワークのMTU設定は1500に設定されていますが、データネットワークのMTUサイズは9000にする必要があります。

タスクの内容

ブロードキャストドメイン内のポートのMTUサイズはすべて同じですが、管理トラフィックを処理するe0Mポートは例外です。ポートがブロードキャストドメインに属している場合は、コマンドを使用して `broadcast-domain modify`、変更したブロードキャストドメイン内のすべてのポートのMTUを変更します。

NICやデータスイッチなどの中間ネットワークデバイスは、ネットワークエンドポイントよりも大きなMTUサイズに設定できます。詳細については、を参照してください "[データスイッチのネットワーク設定を確認する](#)"。

手順

1. ストレージシステムのMTUポート設定を確認します。

```
network port show -instance
```

2. ポートで使用するブロードキャストドメインのMTUを変更します。

```
network port broadcast-domain modify -ipspace ipspace -broadcast-domain  
broadcast_domain -mtu new_mtu
```

例

次の例は、MTUポート設定を9000に変更します。

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain  
Cluster -mtu 9000
```

ディスクのスループットとレイテンシを確認する

ディスクのスループットとレイテンシの指標を確認すると、クラスタノードのトラブルシューティングに役立ちます。

タスクの内容

このタスクを実行するには、advanced権限レベルのコマンドが必要です。

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. ディスクのスループットとレイテンシの指標を確認します。

```
statistics disk show -sort-key latency
```

例

次の例は、に対する cluster1`各ユーザの読み取り処理または書き込み処理の合計を表示します `node2。

```

::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15

```

Disk	Node	Busy (%)	Total Ops	Read Ops	Write Ops	Read (Bps)	Write (Bps)	*Latency (us)
1.10.20	node2	4	5	3	2	95232	367616	23806
1.10.8	node2	4	5	3	2	138240	386048	22113
1.10.6	node2	3	4	2	2	48128	371712	19113
1.10.19	node2	4	6	3	2	102400	443392	19106
1.10.11	node2	4	4	2	2	122880	408576	17713

ノード間のスループットとレイテンシを確認

コマンドを使用すると、ネットワークのボトルネックを特定したり、ノード間のネットワークパスを事前に確認したりできます `network test-path`。このコマンドは、クラスタ間ノード間でもクラスタ内ノード間でも実行できます。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するには、advanced権限レベルのコマンドが必要です。
- クラスタ間パスの場合は、ソースクラスタとデスティネーションクラスタのピア関係が確立されている必要があります。

タスクの内容

場合によっては、ノード間のネットワークパフォーマンスがパス構成の想定どおりにならないことがあります。たとえば、SnapMirrorレプリケーション処理で発生する大量のデータ転送では、ソースクラスタとデスティネーションクラスタ間のリンクが10GbEの場合と一致しない場合があります。

コマンドを使用すると、ノード間のスループットとレイテンシを測定できます `network test-path`。このコマンドは、クラスタ間ノード間でもクラスタ内ノード間でも実行できます。



このテストではネットワークパスがデータでいっぱいになるため、システムがビジーでないときやノード間のネットワークトラフィックが過剰でないときにコマンドを実行してください。テストは10秒後にタイムアウトします。このコマンドは、ONTAP 9ノード間でのみ実行できません。

オプションは `session-type`、ネットワークパスで実行する処理のタイプを識別します。たとえば、リモートデスティネーションへのSnapMirrorレプリケーションの場合は「AsyncMirrorRemote」と指定します。タイプによって、テストで使用されるデータの量が決まります。次の表に、セッションタイプを示します。

セッションタイプ (Session Type)	説明
-------------------------	----

AsyncMirrorLocal です	SnapMirrorによって同じクラスタ内のノード間で使用される設定
AsyncMirrorRemote	異なるクラスタのノード間のSnapMirrorで使用される設定（デフォルトタイプ）
RemoteDataTransfer	ONTAP が同じクラスタ内のノード間のリモートデータアクセスに使用する設定（たとえば、別のノードのボリュームに格納されたファイルを取得するためのノードへのNFS要求）

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. ノード間のスループットとレイテンシを測定します。

```
network test-path -source-node source_nodename |local -destination-cluster destination_clustername -destination-node destination_nodename -session-type Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
```

ソースノードはローカルクラスタ内に存在する必要があります。デスティネーションノードは、ローカルクラスタまたはピアクラスタに配置できます。の値が「local」の`-source-node`場合は、コマンドを実行するノードを指定します。

次のコマンドは、ローカルクラスタ上のと`node3`の`cluster2`間のSnapMirrorタイプのレプリケーション処理のスループットとレイテンシを測定し`node1`ます。

```
cluster1::> network test-path -source-node node1 -destination-cluster cluster2 -destination-node node3 -session-type AsyncMirrorRemote
```

出力例は次のとおりです（出力の詳細は、ONTAPのバージョンによって異なります）。

```
Test Duration:      10.88 secs
Send Throughput:    18.23 MB/sec
Receive Throughput: 18.23 MB/sec
MB sent:            198.31
MB received:        198.31
Avg latency in ms: 2301.47
```

3. admin権限に戻ります。

```
set -privilege admin
```

終了後

パス構成に対して期待される値を得られない場合は、ノードのパフォーマンス統計の確認、ツールを使用したネットワークの問題の切り分け、スイッチ設定の確認などを行います。

ワークロードの管理

残りのパフォーマンス容量を特定

パフォーマンス容量（*headroom*）は、リソースのワークロードのパフォーマンスにレイテンシの影響を受ける前にノードまたはアグリゲートに配置できる作業量を測定します。クラスタで利用可能なパフォーマンス容量を把握しておくこと、ワークロードのプロビジョニングと分散に役立ちます。

必要なもの

このタスクを実行するには、advanced権限レベルのコマンドが必要です。

タスクの内容

オプションでは、次の値を使用してヘッドルームの統計を収集および表示できます `-object`。

- CPUの場合は、`resource_headroom_cpu`。
- アグリゲートの場合は、`resource_headroom_aggr`。

このタスクは、System ManagerとActive IQ Unified Managerを使用して実行することもできます。

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. リアルタイムのヘッドルーム統計の収集を開始します。

```
statistics start -object resource_headroom_cpu|aggr
```

コマンド構文全体については、マニュアルページを参照してください。

3. リアルタイムのヘッドルーム統計情報を表示します。

```
statistics show -object resource_headroom_cpu|aggr
```

コマンド構文全体については、マニュアルページを参照してください。

4. admin権限に戻ります。

```
set -privilege admin
```

例

次の例は、クラスタノードの1時間あたりの平均ヘッドルーム統計を表示します。

ノードの使用可能なパフォーマンス容量は、カウンタからカウンタを `optimal_point_utilization`` 引いて計算できます ``current_utilization`。この例では、の利用率 ``CPU_sti2520-213`` は-14%（72%~86%

) であることから、CPUの過去1時間の平均利用率が高すぎるのがわかります。

または `ewma_weekly`` を指定すると ``ewma_monthly``、同じ情報を長期間にわたって平均化できます `ewma_daily``。

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
(statistics show)
```

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213
```

Counter	Value
-----	-----
ewma_hourly	-
current_ops	4376
current_latency	37719
current_utilization	86
optimal_point_ops	2573
optimal_point_latency	3589
optimal_point_utilization	72
optimal_point_confidence_factor	1

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214
```

Counter	Value
-----	-----
ewma_hourly	-
current_ops	0
current_latency	0
current_utilization	0
optimal_point_ops	0
optimal_point_latency	0
optimal_point_utilization	71
optimal_point_confidence_factor	1

```
2 entries were displayed.
```

トラフィックの多いクライアントやファイルを特定

ONTAP の Active Objects テクノロジを使用すると、クラスタのトラフィック量を著しく増大させているクライアントやファイルを特定することができます。これらの「上位」のクライアントまたはファイルを特定したら、クラスタのワークロードをリバランシングするか、その他の手順を実行して問題を解決できます。

必要なもの

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタに最もアクセスする上位のクライアントを表示します。

```
statistics top client show -node node_name -sort-key sort_column -interval
seconds_between_updates -iterations iterations -max number_of_instances
```

コマンド構文全体については、マニュアルページを参照してください。

次のコマンドは、アクセス頻度の高い上位のクライアントを表示し `cluster1` ます。

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10

          Client Vserver                Node Protocol      *Total
-----  -
172.17.180.170    vs4 siderop1-vs4      nfs      668
172.17.180.169    vs3 siderop1-vs3      nfs      337
172.17.180.171    vs3 siderop1-vs3      nfs      142
172.17.180.170    vs3 siderop1-vs3      nfs      137
172.17.180.123    vs3 siderop1-vs3      nfs      137
172.17.180.171    vs4 siderop1-vs4      nfs       95
172.17.180.169    vs4 siderop1-vs4      nfs       92
172.17.180.123    vs4 siderop1-vs4      nfs       92
172.17.180.153    vs3 siderop1-vs3      nfs        0
```

2. クラスタで最も多くアクセスされる上位のファイルを表示します。

```
statistics top file show -node node_name -sort-key sort_column -interval
seconds_between_updates -iterations iterations -max number_of_instances
```

コマンド構文全体については、マニュアルページを参照してください。

次のコマンドは、でアクセスされる上位のファイルを表示し `cluster1` ます。


```
cluster1::> statistics top file show
```

```
cluster1 : 3/23/2016 17:59:10
```

```

                                *Total
                                File Volume Vserver Node Ops
-----
/vol/vol1/vm170-read.dat      vol1      vs4 siderop1-vs4 22
/vol/vol1/vm69-write.dat      vol1      vs3 siderop1-vs3 6
/vol/vol2/vm171.dat          vol2      vs3 siderop1-vs3 2
/vol/vol2/vm169.dat          vol2      vs3 siderop1-vs3 2
/vol/vol2/p123.dat           vol2      vs4 siderop1-vs4 2
/vol/vol2/p123.dat           vol2      vs3 siderop1-vs3 2
/vol/vol1/vm171.dat          vol1      vs4 siderop1-vs4 2
/vol/vol1/vm169.dat          vol1      vs4 siderop1-vs4 2
/vol/vol1/vm169.dat          vol1      vs4 siderop1-vs3 2
/vol/vol1/p123.dat           vol1      vs4 siderop1-vs4 2
```

QoSでスループットを保証

QoSの概要によるスループット保証

ストレージQuality of Service (QoS ; サービス品質) を使用して、重要なワークロードのパフォーマンスが競合するワークロードによって低下しないようにすることができます。競合するワークロードに Throughput Ceil_天 を設定して、システムリソースへの影響を制限したり、重要なワークロードに Throughput Floor_下 を設定したりすることで、競合するワークロードによる要求に関係なく最小のスループットターゲットを満たすことができます。同じワークロードに対して上限と下限を設定することもできます。

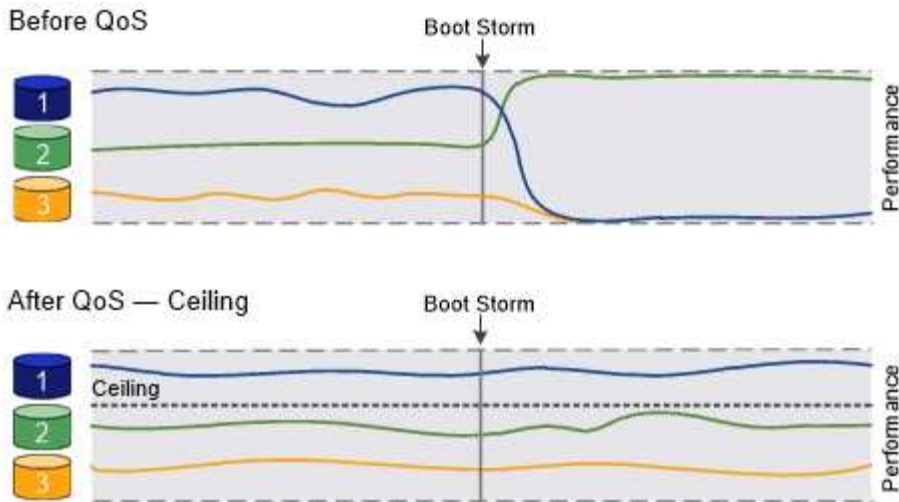
スループットの上限 (最大QoS) について

スループットの上限は、ワークロードのスループットを最大IOPS、最大MBps、またはIOPSとMBpsに制限します。次の図では、ワークロード2のスループットの上限により、ワークロード1と3の「Bully」にならないようになっています。

a_policy group_下 は、1つ以上のワークロードに対するスループットの上限を定義します。ワークロードとは、a_storage オブジェクト: a ボリューム、ファイル、mtree、または LUN、あるいは SVM 内のすべてのボリューム、ファイル、mtree、または LUN の I/O 処理のことです。上限はポリシーグループの作成時に指定することも、ワークロードを監視してから指定することもできます。



ワークロードのスループットは、特にスループットが急激に変化した場合、指定された上限を10%までは超えることができます。バーストに対処するために、上限を50%まで超過することがあります。バーストは、トークンが最大150%蓄積すると、シングルノードで発生します。



スループットの下限（最小QoS）について

スループットの下限は、ワークロードのスループットが最小IOPS、最小MBps、またはIOPSとMBpsを下回らないことを保証します。次の図では、ワークロード1とワークロード3のスループットの下限が設定されているため、ワークロード2からの要求に関係なく、必要な最小スループットが確保されています。



これらの例からわかるように、スループットの上限はスループットを直接調整するのに対し、スループットの下限は下限が設定されたワークロードを優先することでスループットを間接的に調整します。

下限はポリシーグループの作成時に指定できます。また、ワークロードを監視したあとで指定することもできます。

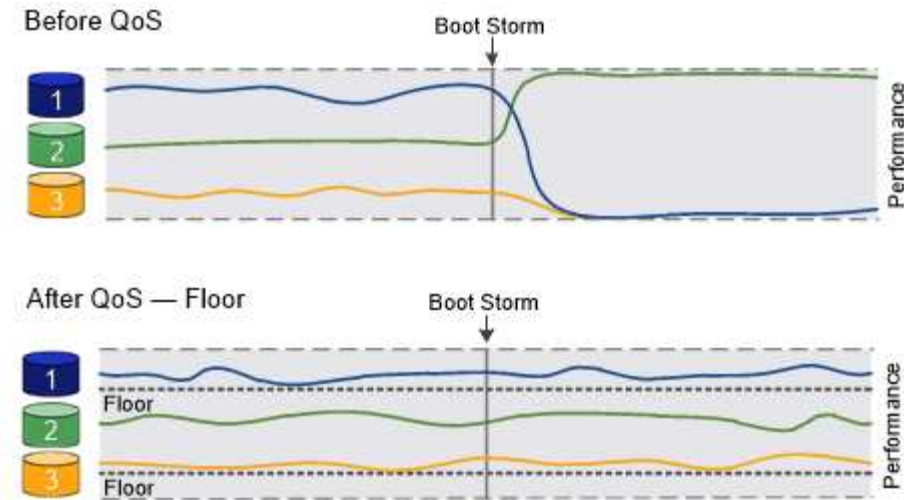
ONTAP 9.13.1以降では、を使用してSVMスコープでスループットの下限を設定でき[\[adaptive-qos-templates\]](#)ます。ONTAP 9.13.1より前のリリースでは、スループットの下限を定義するポリシーグループはSVMに適用できません。



ONTAP 9.7より前のリリースでは、十分なパフォーマンス容量がある場合にスループットの下限が保証されます。

ONTAP 9.7以降では、十分なパフォーマンス容量がない場合でもスループットの下限が保証されます。この新しい下限の動作は、下限v2と呼ばれます。下限v2では、この保証を満たすために、スループットの下限がないワークロードや下限の設定を超える作業でレイテンシが高くなる可能性があります。下限v2は、QoSとアダプティブQoSの両方に適用されます。

ONTAP 9.7P6以降では、下限v2の新しい動作を有効または無効にするオプションを使用できません。などの重要な処理の実行中は、ワークロードが指定された下限を下回ることがあります volume move trigger-cutover。利用可能な容量が十分にあり、重要な処理を実行していない場合でも、ワークロードのスループットが指定された下限を最大5%下回ることがあります。下限がオーバープロビジョニングされていてパフォーマンス容量がない場合、一部のワークロードが指定された下限を下回ることがあります。



共有および非共有のQoSポリシーグループについて

ONTAP 9.4 以降では、`_non-shared_QoS` ポリシーグループを使用して、定義されたスループットの上限または下限の環境を各メンバーのワークロードごとに指定できます。`_shared_policy` グループの動作は 'ポリシー・タイプ' によって異なります

- スループットの上限については、共有ポリシーグループに割り当てられたワークロードの合計スループットが指定した上限を超えることはできません。
- スループットの下限の場合、共有ポリシーグループは単一のワークロードにのみ適用できます。

アダプティブQoSについて

通常、ストレージオブジェクトに割り当てるポリシーグループの値は固定値です。ストレージオブジェクトのサイズが変わった場合は、値を手動で変更する必要があります。たとえば、ボリュームの使用スペースが増えた場合、通常は指定されているスループットの上限も増やす必要があります。

アダプティブ QoS `_ワークロード` のサイズの変更に合わせてポリシーグループの値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。これは、数百、数千のワークロードを管理する大規模な環境では大きなメリットです。

アダプティブQoSは、主にスループットの上限の調整に使用しますが、下限の管理（ワークロードサイズが増加した場合）にも使用できます。ワークロードのサイズは、ストレージオブジェクトに割り当てられたスペースまたはストレージオブジェクトで使用されているスペースのいずれかで表されます。



ONTAP 9.5以降では、使用済みスペースをスループットの下限に使用できます。ONTAP 9.4以前のスループットの下限ではサポートされません。

- 割り当て済みスペースのポリシーでは、ストレージオブジェクトの公称サイズを基準に IOPS と TB / GB の比率が維持されます。比率が100 IOPS/GBの場合、150GBのボリュームのスループットの上限は、ボリュームのサイズが変わらないかぎり15,000 IOPSです。ボリュームのサイズが300GBに変更されると、アダプティブQoSによってスループットの上限が30,000 IOPSに調整されます。
- `a_used space-policy`（デフォルト）は、ストレージ効率化前に格納されている実際のデータの量に基づいて、IOPS/TB|GB の比率を維持します。比率が100 IOPS/GBの場合、100GBのデータが格納されている150GBのボリュームのスループットの上限は10,000 IOPSです。使用済みスペースの量が変わると、アダプティブQoSによって比率に応じてスループットの上限が調整されます。

ONTAP 9.5以降では、アプリケーションのI/Oブロックサイズを指定して、スループット制限をIOPSとMBpsの両方で表すことができます。MBps制限は、ブロックサイズにIOPS制限を掛けて計算されます。たとえば、32KのI/OブロックサイズでIOPSの制限が6144IOPS/TBの場合、MBpsの制限は192MBpsになります。

スループットの上限と下限の両方について、次の動作が想定されます。

- アダプティブQoSポリシーグループにワークロードを割り当てると、上限または下限がただちに更新されます。
- アダプティブQoSポリシーグループに含まれるワークロードのサイズを変更すると、上限または下限が約5分で更新されます。

更新を実行するには、スループットが少なくとも10 IOPS増加する必要があります。

アダプティブQoSポリシーグループは常に非共有です。定義されているスループットの上限または下限は、各メンバーワークロードに個別に適用されます。

ONTAP 9.6以降では、SSDを使用するONTAP Select Premiumでスループットの下限がサポートされます。

アダプティブポリシーグループテンプレート

ONTAP 9.13.1以降では、アダプティブQoSテンプレートをSVMに設定できます。アダプティブポリシーグループテンプレートを使用すると、SVM内のすべてのボリュームにスループットの下限と上限を設定できます。

アダプティブポリシーグループテンプレートは、SVMの作成後にのみ設定できます。`vserver modify` コマンドでパラメータを指定し`-qos-adaptive-policy-group-template`で、ポリシーを設定します。

アダプティブポリシーグループテンプレートを設定すると、ポリシーの設定後に作成または移行されたボリュームには自動的にポリシーが継承されます。ポリシーテンプレートを割り当てても、SVM上の既存のボリュームには影響しません。SVMでポリシーを無効にすると、以降SVMに移行または作成されたボリュームにポリシーは適用されません。アダプティブポリシーグループテンプレートを無効にしても、ポリシーテンプレートが保持されるため、そのポリシーテンプレートを継承したボリュームには影響しません。

詳細については、を参照してください [アダプティブポリシーグループテンプレートの設定](#)。

一般的なサポート

次の表に、スループットの上限、スループットの下限、およびアダプティブQoSのサポートの違いを示します。

リソースまたは機能	スループットの上限	スループットの下限	スループットの下限 v2	アダプティブQoS
ONTAP 9バージョン	すべて	9.2以降	9.7以降	9.3以降
プラットフォーム	すべて	<ul style="list-style-type: none"> • AFF • C190 * • SSDを使用したONTAP Select Premium * 	<ul style="list-style-type: none"> • AFF • C190 • SSDを使用したONTAP Select Premium 	すべて

リソースまたは機能	スループットの上限	スループットの下限	スループットの下限 v2	アダプティブQoS
プロトコル	すべて	すべて	すべて	すべて
FabricPool	○	○ (階層化ポリシーが「none」に設定されていて、ブロックがクラウドにない場合)	○ (階層化ポリシーが「none」に設定されていて、ブロックがクラウドにない場合)	いいえ
SnapMirror Synchronous	○	いいえ	いいえ	○

C190とONTAP Selectのサポートは、ONTAP 9.6リリースから開始されました。

スループットの上限がサポートされるワークロード

次の表に、スループットの上限でサポートされるワークロードをONTAP 9のバージョン別に示します。ルートボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロード - 上限	ONTAP 9.0	ONTAP 9.1	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 ~ 9.7	ONTAP 9.8以降
ボリューム	はい	はい	はい	はい	はい	はい
ファイル	はい	はい	はい	はい	はい	はい
LUN	はい	はい	はい	はい	はい	はい
SVM	はい	はい	はい	はい	はい	はい
FlexGroupボリューム	いいえ	いいえ	いいえ	はい	はい	はい
qtree *	いいえ	いいえ	いいえ	いいえ	いいえ	はい
ポリシーグループごとに複数のワークロード	はい	はい	はい	はい	はい	はい
非共有ポリシーグループ	いいえ	いいえ	いいえ	いいえ	はい	はい

ONTAP 9.8以降では、NFSが有効なFlexVolおよびFlexGroupボリュームのqtreeでNFSアクセスがサポートされます。ONTAP 9.9.1以降では、SMBが有効なFlexVolおよびFlexGroupボリュームのqtreeでもSMBアクセス

がサポートされます。

スループットの下限がサポートされるワークロード

次の表に、スループットの下限がサポートされるワークロードをONTAP 9のバージョン別に示します。ルートボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロード - 下限	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 ~ 9.7	ONTAP 9.8 ~ 9.13.0	ONTAP 9.13.1以降
ボリューム	はい	はい	はい	はい	はい
ファイル	いいえ	はい	はい	はい	はい
LUN	はい	はい	はい	はい	はい
SVM	いいえ	いいえ	いいえ	いいえ	はい
FlexGroupボリューム	いいえ	いいえ	はい	はい	はい
qtree *	いいえ	いいえ	いいえ	はい	はい
ポリシーグループごとに複数のワークロード	いいえ	いいえ	はい	はい	はい
非共有ポリシーグループ	いいえ	いいえ	はい	はい	はい

* ONTAP 9.8以降では、NFSが有効なFlexVol およびFlexGroup のqtreeでNFSアクセスがサポートされます。ONTAP 9.9.1以降では、SMBが有効なFlexVolおよびFlexGroupボリュームのqtreeでもSMBアクセスがサポートされます。

アダプティブQoSがサポートされるワークロード

次の表に、アダプティブQoSがサポートされるワークロードをONTAP 9のバージョン別に示します。ルートボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロード- アダプティブQoS	ONTAP 9.3	ONTAP 9.4 ~ 9.13.0	ONTAP 9.13.1以降
ボリューム	はい	はい	はい
ファイル	いいえ	はい	はい
LUN	いいえ	はい	はい
SVM	いいえ	いいえ	はい
FlexGroupボリューム	いいえ	はい	はい
ポリシーグループごとに複数のワークロード	はい	はい	はい
非共有ポリシーグループ	はい	はい	はい

ワークロードとポリシーグループの最大数

次の表に、ワークロードとポリシーグループの最大数をONTAP 9のバージョン別に示します。

ワークロードのサポート	ONTAP 9.3以前	ONTAP 9.4以降
クラスターあたりの最大ワークロード	12,000	40,000
ノードあたりの最大ワークロード	12,000	40,000
ポリシーグループの最大数	12,000	12,000

スループットの下限v2を有効または無効にする

AFFでスループットの下限v2を有効または無効にすることができます。デフォルトは有効です。下限v2を有効にすると、コントローラの使用率が高く、他のワークロードのレイテンシが高くなることを犠牲にして、スループットの下限を満たすことができます。下限v2は、QoSとアダプティブQoSの両方に適用されます。

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. 次のいずれかのコマンドを入力します。

状況	使用するコマンド
下限v2を無効にする	<pre>qos settings throughput-floors-v2 -enable false</pre>
下限v2を有効にする	<pre>qos settings throughput-floors-v2 -enable true</pre>



MetroClusterクラスターでスループットの下限v2を無効にするには、

```
qos settings throughput-floors-v2 -enable false
```

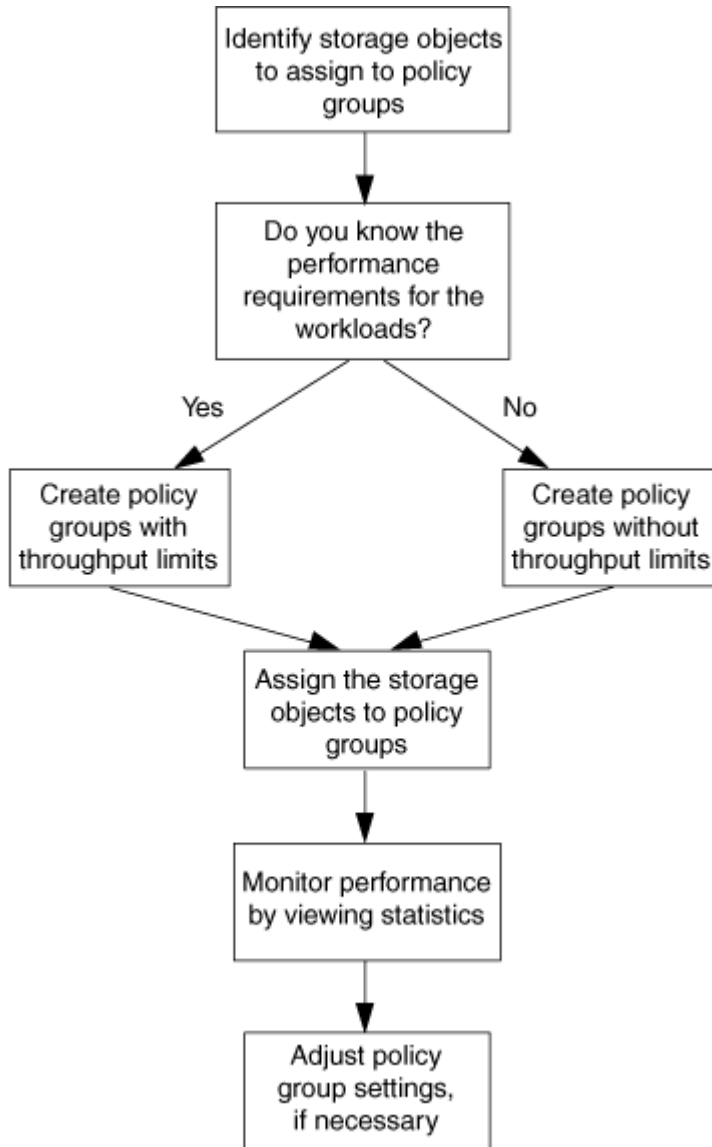
ソースクラスターとデスティネーションクラスターの両方でコマンドを実行します。

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

ストレージQoSのワークフロー

QoSで管理するワークロードのパフォーマンス要件がすでにわかっている場合は、ポリ

シーグループを作成するときにスループットの制限を指定できます。それ以外の場合は、ワークロードを監視したうえで指定することができます。



QoSによるスループットの上限の設定

ポリシーグループのフィールドを使用して、ストレージオブジェクトのワークロードのスループットの上限（最大QoS）を定義できます `max-throughput`。ポリシーグループは、ストレージオブジェクトを作成または変更するときに適用できます。

必要なもの

- ポリシーグループを作成するには、クラスタ管理者である必要があります。
- ポリシーグループをSVMに適用するには、クラスタ管理者である必要があります。

タスクの内容

- ONTAP 9.4 以降では、`_non-shared_QoS` ポリシーグループを使用して、定義されたスループットの上限環境を各メンバーのワークロードごとに指定できます。ポリシーグループが `_shared` : 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合計スループットが指定した上限を超えることはできません。

非共有ポリシーグループを指定するには、コマンドに `qos policy-group create`` を設定します `-is-shared=false`。

- スループットの上限は、IOPS、MB/秒、またはIOPS、MB/秒で指定できます。IOPSとMBpsの両方を指定した場合は、先に上限に達した方が適用されます。



同じワークロードに対して上限と下限を設定する場合は、スループット制限はIOPS単位でのみ指定できます。

- QoS制限の対象となるストレージオブジェクトは、ポリシーグループが属するSVMに含める必要があります。同じSVMに複数のポリシーグループを含めることができます。
- そのストレージオブジェクトまたは子オブジェクトがポリシーグループに属している場合、そのストレージオブジェクトをポリシーグループに割り当てることはできません。
- QoSのベストプラクティスとして、同じタイプのストレージオブジェクトにポリシーグループを適用することを推奨します。

手順

1. ポリシーグループを作成します。

```
qos policy-group create -policy-group policy_group -vserver SVM -max-throughput number_of_iops|Mb/S|iops,Mb/S -is-shared true|false
```

コマンド構文全体については、マニュアルページを参照してください。スループットの上限は、コマンドを使用して調整できます `qos policy-group modify`。

次のコマンドは、最大スループットが5,000 IOPSの共有ポリシーグループを作成し `pg-vs1`` ます。

```
cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1 -max-throughput 5000iops -is-shared true
```

次のコマンドは、最大スループットが100 IOPS、400KB/秒の非共有ポリシーグループを作成し `pg-vs3`` ます。

```
cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3 -max-throughput 100iops,400KB/s -is-shared false
```

次のコマンドは、スループットの制限がない非共有ポリシーグループを作成し `pg-vs4`` ます。

```
cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4 -is-shared false
```

2. ポリシーグループをSVM、ファイル、ボリューム、またはLUNに適用します。

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

コマンド構文全体については、マニュアルページを参照してください。コマンドを使用すると、ストレージオブジェクトに別のポリシーグループを適用できます `storage_object modify`。

次のコマンドは、ポリシーグループをSVM `vs1` に適用し `pg-vs1` ます。

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

次のコマンドは、ボリューム `app1` および `app2` ポリシーグループを適用し `pg-app` ます。

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1  
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1  
-qos-policy-group pg-app
```

3. ポリシーグループのパフォーマンスを監視します。

```
qos statistics performance show
```

コマンド構文全体については、マニュアルページを参照してください。



パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

次のコマンドは、ポリシーグループのパフォーマンスを表示します。

```
cluster1::> qos statistics performance show
```

Policy Group	IOPS	Throughput	Latency
-total-	12316	47.76MB/s	1264.00us
pg_vs1	5008	19.56MB/s	2.45ms
_System-Best-Effort	62	13.36KB/s	4.13ms
_System-Background	30	0KB/s	0ms

4. ワークロードのパフォーマンスを監視します。

```
qos statistics workload performance show
```

コマンド構文全体については、マニュアルページを参照してください。



パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

次のコマンドは、ワークロードのパフォーマンスを表示します。

```
cluster1::> qos statistics workload performance show
Workload          ID      IOPS      Throughput      Latency
-----
-total-          -      12320      47.84MB/s      1215.00us
app1-wid7967     7967      7219      28.20MB/s      319.00us
vs1-wid12279    12279      5026      19.63MB/s       2.52ms
_USERSPACE_APPS    14         55      10.92KB/s      236.00us
_Scan_Backgro... 5688         20         0KB/s          0ms
```



QoSワークロードの詳細なレイテンシ統計を表示するには、コマンドを使用し `qos statistics workload latency show` ます。

QoSでスループットの下限を設定

ポリシーグループのフィールドを使用して、ストレージオブジェクトのワークロードのスループットの下限（最小QoS）を定義できます `min-throughput`。ポリシーグループは、ストレージオブジェクトを作成または変更するときに適用できます。ONTAP 9.8以降では、スループットの下限をIOPS、MBps、またはIOPS/MBpsで指定できます。

開始する前に

- ONTAP 9.2以降が実行されている必要があります。スループットの下限はONTAP 9以降で使用できます。2.
- ポリシーグループを作成するには、クラスタ管理者である必要があります。
- ONTAP 9.13.1以降では、を使用してSVMレベルでスループットの下限を適用できます [アダプティブポリシーグループテンプレート](#)。QoSポリシーグループを含むSVMにアダプティブポリシーグループテンプレートを設定することはできません。

タスクの内容

- ONTAP 9.4 以降では、`_non-shared_qos` ポリシーグループを使用して、定義したスループットの下限を各メンバーワークロードに個別に適用するように指定できます。これは、スループットの下限が設定されたポリシーグループを複数のワークロードに適用できる唯一の条件です。

共有されていないポリシーグループを指定するには、コマンドに `qos policy-group create` を設定します -is-shared=false。`

- ノードまたはアグリゲートに十分なパフォーマンス容量（ヘッドルーム）がない場合、ワークロードのスループットが指定された下限を下回ることがあります。
- QoS制限の対象となるストレージオブジェクトは、ポリシーグループが属するSVMに含める必要があります。同じSVMに複数のポリシーグループを含めることができます。
- QoSのベストプラクティスとして、同じタイプのストレージオブジェクトにポリシーグループを適用することを推奨します。
- スループットの下限が定義されたポリシーグループは、SVMには適用できません。

手順

1. の説明に従って、ノードまたはアグリゲートに十分なパフォーマンス容量があることを確認します。
2. ポリシーグループを作成します。

```
qos policy-group create -policy group policy_group -vserver SVM -min  
-throughput qos_target -is-shared true|false
```

完全なコマンド構文については、ONTAPリリースのマニュアルページを参照してください。スループットの下限を調整するには、コマンドを使用し `qos policy-group modify` ます。

次のコマンドは、最小スループットが1,000 IOPSの共有ポリシーグループを作成し `pg-vs2` ます。

```
cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2  
-min-throughput 1000iops -is-shared true
```

次のコマンドは、スループットの制限がない非共有ポリシーグループを作成し `pg-vs4` ます。

```
cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4  
-is-shared false
```

3. ポリシーグループをボリュームまたはLUNに適用します。

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

コマンド構文全体については、マニュアルページを参照してください。コマンドを使用すると、ストレージオブジェクトに別のポリシーグループを適用できます `_storage_object_modify`。

次のコマンドは、ポリシーグループをボリューム `app2` に適用し `pg-app2` ます。

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1  
-qos-policy-group pg-app2
```

4. ポリシーグループのパフォーマンスを監視します。

```
qos statistics performance show
```

コマンド構文全体については、マニュアルページを参照してください。



パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

次のコマンドは、ポリシーグループのパフォーマンスを表示します。

```
cluster1::> qos statistics performance show
Policy Group          IOPS          Throughput    Latency
-----
-total-              12316         47.76MB/s    1264.00us
pg_app2              7216          28.19MB/s    420.00us
_System-Best-Effort   62            13.36KB/s     4.13ms
_System-Background   30            0KB/s         0ms
```

5. ワークロードのパフォーマンスを監視します。

```
qos statistics workload performance show
```

コマンド構文全体については、マニュアルページを参照してください。



パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

次のコマンドは、ワークロードのパフォーマンスを表示します。

```
cluster1::> qos statistics workload performance show
Workload             ID           IOPS          Throughput    Latency
-----
-total-              -            12320         47.84MB/s    1215.00us
app2-wid7967         7967         7219          28.20MB/s    319.00us
vs1-wid12279         12279        5026          19.63MB/s    2.52ms
_USERSPACE_APPS      14           55            10.92KB/s    236.00us
_Scan_Backgro...    5688         20            0KB/s         0ms
```



QoSワークロードの詳細なレイテンシ統計を表示するには、コマンドを使用し `qos statistics workload latency show` ます。

アダプティブQoSポリシーグループを使用する

アダプティブ QoS ポリシーグループを使用すると、ボリュームサイズの変更に合わせてスループットの上限や下限を自動的に調整し、TB または GB あたりの IOPS を一定に保つことができます。これは、数百、数千のワークロードを管理する大規模な環境では大きなメリットです。

開始する前に

- ONTAP 9.3以降が実行されている必要があります。アダプティブQoSポリシーグループは、ONTAP 9以降で使用できます。3.
- ポリシーグループを作成するには、クラスタ管理者である必要があります。

タスクの内容

ストレージオブジェクトはアダプティブポリシーグループまたは非アダプティブポリシーグループのメンバーにすることはできますが、両方のメンバーにすることはできません。SVMはストレージオブジェクトとポリシーで同じである必要があります。ストレージオブジェクトはオンラインである必要があります。

アダプティブQoSポリシーグループは常に非共有です。定義されているスループットの上限または下限は、各メンバーワークロードに個別に適用されます。

ストレージオブジェクトサイズに対するスループット制限の比率は、次のフィールドの組み合わせによって決まります。

- ``expected-iops``は、割り当て済み (TB / GB) あたりの最小想定IOPSです。



``expected-iops``は、AFFプラットフォームでのみ保証されます。
``expected-iops`FabricPool`については、階層化ポリシーが「none」に設定されていて、ブロックがクラウドにない場合にのみ保証されます。
``expected-iops``は、SnapMirror同期関係にないボリュームに対して保証されます。

- ``peak-iops``は、割り当て済みまたは使用済み (TB / GB) あたりの最大IOPSです。
- ``expected-iops-allocation````expected-iops``に割り当てスペース (デフォルト) と使用スペースのどちらを使用するかを示します。



``expected-iops-allocation``ONTAP 9 .5以降で使用できます。ONTAP 9 .4以前ではサポートされていません。

- `peak-iops-allocation``に割り当てスペースと使用済みスペース (デフォルト) のどちらを使用するかを示します ``peak-iops``。
- `absolute-min-iops``は、絶対最小IOPSです。このフィールドは、非常に小さいストレージオブジェクトで使用できます。が計算値より大きい場合は ``absolute-min-iops``、および/または ``expected-iops`` の両方が ``expected-iops`` 上書きされ ``peak-iops`` ます。

たとえば、TBあたり1,000 IOPS/TBに設定した場合、ボリュームサイズが1GB未満の場合は `expected-iops``、フラクショナルIOPが計算され ``expected-iops`` ます。計算された割合は ``peak-iops`` 以上に小さい割合になります。これを回避するには、を現実的な値に設定し ``absolute-min-iops`` ます。

- ``block-size``アプリケーションI/Oブロックサイズを指定します。デフォルトは32Kです。有効な値は、8K、16K、32K、64K、ANYです。anyは、ブロックサイズが適用されないことを意味します。

次の表に示す3つのデフォルトのアダプティブQoSポリシーグループがあります。これらのポリシーグループはボリュームに直接適用できます。

デフォルトのポリシーグループ	想定IOPS/TB	最大IOPS/TB	絶対最小 IOPS
extreme	6,144	12,288	1000
performance	2,048	4,096	500

value	128	512	75
-------	-----	-----	----

そのストレージオブジェクトまたは子オブジェクトがポリシーグループに属している場合、そのストレージオブジェクトをポリシーグループに割り当てることはできません。次の表に、制限事項を示します。

割り当て内容	割り当てることができない項目
SVM	SVMに含まれているストレージオブジェクトのポリシーグループへの割り当て
ボリューム	そのボリュームを含むSVMまたは子LUN
LUN	そのLUNを含むボリュームまたはSVM
ファイル	そのファイルを含むボリュームまたはSVM

手順

1. アダプティブQoSポリシーグループを作成します。

```
qos adaptive-policy-group create -policy group policy_group -vserver SVM
-expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
-iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
```

コマンド構文全体については、マニュアルページを参照してください。



`-expected-iops-allocation`および`-block-size`は、ONTAP 9.5以降で使用できます。これらのオプションは、ONTAP 9.4以前ではサポートされていません。

次のコマンドは、300 IOPS/TB `-peak-iops`、1,000 IOPS/TB、`-used-space`および`-absolute-min-iops` 50 IOPSに設定され`-peak-iops-allocation`と`-expected-iops`アダプティブQoSポリシーグループを作成し`adpg-app1`ます。

```
cluster1::> qos adaptive-policy-group create -policy group adpg-app1
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

2. アダプティブQoSポリシーグループをボリュームに適用します。

```
volume create -vserver SVM -volume volume -aggregate aggregate -size number_of
TB|GB -qos-adaptive-policy-group policy_group
```

コマンド構文全体については、マニュアルページを参照してください。

次のコマンドは、アダプティブQoSポリシーグループをボリューム`app1`に適用し`adpg-app1`ます。

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

次のコマンドは、デフォルトのアダプティブQoSポリシーグループを新しい`app4`ボリュームと既存のボリューム`app5`に適用し`extreme`ます。ポリシーグループに対して定義されたスループットの上限は、ボリュームに`app5`個別に適用され`app4`ます。

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

アダプティブポリシーグループテンプレートの設定

ONTAP 9.13.1以降では、アダプティブポリシーグループテンプレートを使用し、SVMレベルでスループットの下限と上限を適用できます。

タスクの内容

- アダプティブポリシーグループテンプレートはデフォルトポリシーです `apg1`。ポリシーはいつでも変更できます。CLIまたはONTAP REST APIでのみ設定でき、既存のSVMにのみ適用できます。
- アダプティブポリシーグループテンプレートは、ポリシーの設定後にSVMで作成またはSVMに移行されるボリュームにのみ影響します。SVM上の既存のボリュームのステータスは維持されます。

アダプティブポリシーグループテンプレートを無効にした場合、SVM上のボリュームの既存のポリシーは保持されます。無効化の影響を受けるのは、あとでSVMに作成または移行されたボリュームだけです。

- QoSポリシーグループを含むSVMにアダプティブポリシーグループテンプレートを設定することはできません。
- アダプティブポリシーグループテンプレートは、AFFプラットフォーム向けに設計されています。アダプティブポリシーグループテンプレートは他のプラットフォームでも設定できますが、ポリシーによって最小スループットが適用されない場合があります。同様に、FabricPoolアグリゲートまたは最小スループットをサポートしないアグリゲート内のSVMにアダプティブポリシーグループテンプレートを追加することもできますが、スループットの下限は適用されません。
- SVMがMetroCluster構成またはSnapMirror関係に含まれている場合は、ミラーされたSVMにアダプティブポリシーグループテンプレートが適用されます。

手順

1. SVMを変更してアダプティブポリシーグループテンプレートを適用します。 `vserver modify -qos -adaptive-policy-group-template apg1`
2. ポリシーが設定されたことを確認します。 `vserver show -fields qos-adaptive-policy-group`

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。