



Überwachen und managen Sie die Cluster-Performance über die CLI

ONTAP 9

NetApp
April 24, 2024

Inhalt

- Überwachen und managen Sie die Cluster-Performance über die CLI 1
 - Performance Monitoring und Management – Überblick..... 1
 - Monitoring der Performance..... 1
 - Verwenden Sie Active IQ Digital Advisor, um die Systemleistung anzuzeigen..... 11
 - Managen Sie Performance-Probleme 12

Überwachen und managen Sie die Cluster-Performance über die CLI

Performance Monitoring und Management – Überblick

Sie können grundlegende Aufgaben zur Performance-Überwachung und -Verwaltung einrichten und gängige Performance-Probleme ermitteln und beheben.

Diese Verfahren können Sie zur Überwachung und Verwaltung der Cluster-Performance verwenden, wenn sich folgende Annahmen auf Ihre Situation beziehen:

- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Mit Active IQ Unified Manager (ehemals OnCommand Unified Manager) möchten Sie neben der Befehlszeilenschnittstelle von ONTAP den Systemstatus und die Cluster Performance überwachen und Root-Cause-Analysen durchführen.
- Sie konfigurieren die Storage-Servicequalität (QoS) über die ONTAP Befehlszeilenschnittstelle.

QoS ist auch in System Manager, NSLM, WFA, VSC (VMware Plug-in) und APIs verfügbar.

- Unified Manager soll mithilfe einer virtuellen Appliance installiert werden, anstatt eine Linux- oder Windows-basierte Installation zu verwenden.
- Sie sind bereit, eine statische Konfiguration anstelle von DHCP zu verwenden, um die Software zu installieren.
- Sie können auf der erweiterten Berechtigungsebene auf ONTAP-Befehle zugreifen.
- Sie sind ein Cluster-Administrator mit der Rolle „admin“.

Verwandte Informationen

Wenn diese Annahmen für Ihre Situation nicht richtig sind, sollten Sie die folgenden Ressourcen sehen:

- ["Installation von Active IQ Unified Manager 9.8"](#)
- ["Systemadministration"](#)

Monitoring der Performance

Workflow-Übersicht zur Performance-Überwachung und Wartung

Zur Überwachung und Aufrechterhaltung der Cluster-Performance müssen die Active IQ Unified Manager Software installiert, grundlegende Monitoring-Aufgaben eingerichtet, Performance-Probleme erkannt und nach Bedarf Anpassungen vorgenommen werden.

Stellen Sie sicher, dass Ihre VMware-Umgebung unterstützt wird

Für eine erfolgreiche Installation von Active IQ Unified Manager müssen Sie überprüfen, ob Ihre VMware Umgebung die erforderlichen Anforderungen erfüllt.

Schritte

1. Vergewissern Sie sich, dass Ihre VMware Infrastruktur den Größenanforderungen für die Installation von Unified Manager entspricht.
2. Wechseln Sie zum "[Interoperabilitätsmatrix](#)" Um zu überprüfen, ob Sie eine unterstützte Kombination der folgenden Komponenten haben:
 - ONTAP-Version
 - ESXi-Betriebssystemversion
 - VMware vCenter Server-Version
 - VMware Tools-Version
 - Browsertyp und -Version



Der "[Interoperabilitätsmatrix](#)" Führt die unterstützten Konfigurationen für Unified Manager auf.

3. Klicken Sie auf den Konfigurationsnamen für die ausgewählte Konfiguration.

Details zu dieser Konfiguration werden im Fenster Konfigurationsdetails angezeigt.

4. Überprüfen Sie die Informationen auf den folgenden Registerkarten:

- Hinweise

Listet wichtige Warnmeldungen und Informationen auf, die auf Ihre Konfiguration zugeschnitten sind.

- Richtlinien und Richtlinien

Allgemeine Richtlinien für alle Konfigurationen

Active IQ Unified Manager-Arbeitsblatt

Vor Installation, Konfiguration und Verbindung von Active IQ Unified Manager sollten spezifische Informationen zur Systemumgebung sofort verfügbar sein. Sie können die Informationen im Arbeitsblatt aufzeichnen.

Informationen zur Installation von Unified Manager

Virtual Machine, auf der Software bereitgestellt wird	Ihr Wert
IP-Adresse des ESXi-Servers	
Vollständig qualifizierter Domain-Name des Hosts	
Host-IP-Adresse	
Netzwerkmaske	
Gateway-IP-Adresse	
Primäre DNS-Adresse	

Sekundäre DNS-Adresse	
Domänen durchsuchen	
Wartungs-Benutzername	
Wartungs-Benutzer-Passwort	


Informationen zur Unified Manager-Konfiguration

Einstellung	Ihr Wert
Wartungs-Benutzer-E-Mail-Adresse	
NTP-Server	
Hostname oder IP-Adresse des SMTP-Servers	
SMTP-Benutzername	
SMTP-Passwort	
SMTP-Standardport	25 (Standardwert)
E-Mail, von der aus Benachrichtigungen gesendet werden	
LDAP Bind Distinguished Name	
LDAP-Bindekennwort	
Name des Active Directory-Administrators	
Active Directory-Kennwort	
Authentifizierungsserverbasis mit Distinguished Name	
Hostname oder IP-Adresse des Authentifizierungsservers	

Cluster-Informationen

Erfassen Sie die folgenden Informationen für jedes Cluster auf Unified Manager.

Cluster 1 von N	Ihr Wert
-----------------	----------

Host-Name oder Cluster-Management-IP-Adresse	
Benutzername des ONTAP-Administrators	
 Dem Administrator muss die Rolle „admin“ zugewiesen worden sein.	
ONTAP-Administratorpasswort	
Protokoll (HTTP oder HTTPS)	

Verwandte Informationen

["Administratorauthentifizierung und RBAC"](#)

Installation von Active IQ Unified Manager

Active IQ Unified Manager herunterladen und implementieren

Um die Software zu installieren, müssen Sie die Installationsdatei für die virtuelle Appliance (VA) herunterladen und dann einen VMware vSphere Client verwenden, um die Datei auf einem VMware ESXi-Server bereitzustellen. Die VA ist in einer OVA-Datei verfügbar.

Schritte

1. Gehen Sie auf die Seite **NetApp Support Site zum Software-Download** und suchen Sie nach Active IQ Unified Manager.

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

2. Wählen Sie im Dropdown-Menü **Plattform auswählen** * VMware vSphere* aus und klicken Sie auf **Go!**
3. Speichern Sie die Datei „OVA“ in einem lokalen oder Netzwerkspeicherort, auf den Ihr VMware vSphere Client zugreifen kann.
4. Klicken Sie in VMware vSphere Client auf **Datei > OVF-Vorlage bereitstellen**.
5. Suchen Sie die Datei „OVA“ und stellen Sie die virtuelle Appliance mithilfe des Assistenten auf dem ESXi-Server bereit.

Sie können die Registerkarte **Eigenschaften** im Assistenten verwenden, um Ihre statischen Konfigurationsdaten einzugeben.

6. Schalten Sie die VM ein.
7. Klicken Sie auf die Registerkarte **Konsole**, um den Startvorgang anzuzeigen.
8. Folgen Sie der Eingabeaufforderung, um VMware Tools auf der VM zu installieren.
9. Zeitzone konfigurieren.
10. Geben Sie einen Wartungs-Benutzernamen und ein Passwort ein.
11. Wechseln Sie zur URL, die von der VM-Konsole angezeigt wird.

Konfigurieren Sie die anfänglichen Active IQ Unified Manager-Einstellungen

Das Dialogfeld Active IQ Unified Manager Initial Setup wird angezeigt, wenn Sie zum ersten Mal auf die Web-Benutzeroberfläche zugreifen. Dadurch können Sie einige Anfangseinstellungen konfigurieren und Cluster hinzufügen.

Schritte

1. Akzeptieren Sie die Standardeinstellung AutoSupport Enabled.
2. Geben Sie die NTP-Serverdetails, die E-Mail-Adresse des Wartungsbenedutzers, den SMTP-Servernamen und weitere SMTP-Optionen ein, und klicken Sie dann auf **Speichern**.

Nachdem Sie fertig sind

Nach Abschluss der Ersteinrichtung wird die Seite „Cluster-Datenquellen“ angezeigt, auf der Sie die Cluster-Details hinzufügen können.

Geben Sie die zu überwachenden Cluster an

Sie müssen einem Active IQ Unified Manager-Server ein Cluster hinzufügen, um das Cluster zu überwachen, den Status der Cluster-Erkennung anzuzeigen und die Performance zu überwachen.

Was Sie benötigen

- Sie müssen die folgenden Informationen haben:
 - Host-Name oder Cluster-Management-IP-Adresse

Der Hostname ist der vollständig qualifizierte Domänenname (FQDN) oder der Kurzname, den Unified Manager zur Verbindung mit dem Cluster verwendet. Dieser Hostname muss mit der Cluster-Management-IP-Adresse aufgelöst werden.

Die Cluster-Management-IP-Adresse muss die Cluster-Management-LIF der administrativen Storage Virtual Machine (SVM) sein. Wenn Sie eine Node-Management-LIF verwenden, schlägt der Vorgang fehl.

- Benutzername und Passwort für den ONTAP-Administrator
- Typ des Protokolls (HTTP oder HTTPS), der für das Cluster und die Portnummer des Clusters konfiguriert werden kann
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Der ONTAP-Administrator muss über die ONTAPI- und SSH-Administratorrollen verfügen.
- Der FQDN des Unified Managers muss ONTAP pingen können.

Dies können Sie mit dem ONTAP-Befehl überprüfen `ping -node node_name -destination Unified_Manager_FQDN`.

Über diese Aufgabe

Für eine MetroCluster Konfiguration müssen Sie sowohl die lokalen als auch die Remote-Cluster hinzufügen, und die Cluster müssen korrekt konfiguriert sein.

Schritte

1. Klicken Sie Auf **Konfiguration > Cluster-Datenquellen**.

2. Klicken Sie auf der Seite Cluster auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Cluster hinzufügen** die erforderlichen Werte an, z. B. den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) des Clusters, Benutzernamen, Passwort, Protokoll zur Kommunikation und Portnummer.

Standardmäßig ist das HTTPS-Protokoll ausgewählt.

Sie können die Cluster-Management-IP-Adresse von IPv6 zu IPv4 oder von IPv4 zu IPv6 ändern. Die neue IP-Adresse wird nach Abschluss des nächsten Überwachungszyklus im Cluster-Raster und die Seite zur Cluster-Konfiguration angezeigt.

4. Klicken Sie Auf **Hinzufügen**.
5. Wenn HTTPS ausgewählt ist, führen Sie die folgenden Schritte aus:
 - a. Klicken Sie im Dialogfeld **Autorisieren Host** auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.
 - b. Klicken Sie Auf **Ja**.

Unified Manager überprüft das Zertifikat nur, wenn das Cluster erstmalig hinzugefügt wird, überprüft es aber nicht für jeden API-Aufruf an ONTAP.

Wenn das Zertifikat abgelaufen ist, können Sie das Cluster nicht hinzufügen. Sie müssen das SSL-Zertifikat erneuern und dann den Cluster hinzufügen.

6. **Optional**: Anzeigen des Clusterermittlungsstatus:
 - a. Überprüfen Sie den Cluster-Erkennungsstatus auf der Seite **Cluster Setup**.

Das Cluster wird der Unified Manager-Datenbank nach dem Standard-Monitoring-Intervall von ca. 15 Minuten hinzugefügt.

Einrichten grundlegender Überwachungsaufgaben

Tägliche Überwachung

Sie können eine tägliche Überwachung durchführen, um sicherzustellen, dass keine unmittelbaren Performance-Probleme auftreten, die Aufmerksamkeit erfordern.

Schritte

1. Rufen Sie in der Active IQ Unified Manager-Benutzeroberfläche die Seite **Ereignisbestand** auf, um alle aktuellen und veralteten Ereignisse anzuzeigen.
2. Wählen Sie aus der Option **Ansicht** die Option `Active Performance Events` Und zu ermitteln, welche Maßnahmen erforderlich sind.

Ermitteln Sie Performance-Probleme anhand von wöchentlichen und monatlichen Performance-Trends

Anhand des Aufspüren von Performance-Trends können Sie erkennen, ob der Cluster überlastet ist oder nicht optimal genutzt wird, indem Sie die Latenz von Volumes analysieren. Anhand ähnlicher Schritte können Sie CPU-, Netzwerk- oder andere Systemengpässe identifizieren.

Schritte

1. Suchen Sie das Volumen, das Sie vermutlich nicht optimal nutzen oder zu wenig nutzen.
2. Klicken Sie auf der Registerkarte **Volume Details** auf **30 d**, um die historischen Daten anzuzeigen.
3. Wählen Sie im Dropdown-Menü „Data by aufbrechen“ die Option **Latenz** aus und klicken Sie dann auf **Senden**.
4. Heben Sie die Auswahl von * Aggregat* im Vergleichstabelle der Cluster-Komponenten auf und vergleichen Sie dann die Cluster-Latenz mit dem Latenzdiagramm für das Volume.
5. Wählen Sie * Aggregat* aus und deaktivieren Sie die Auswahl aller anderen Komponenten im Vergleichstabelle der Cluster-Komponenten, und vergleichen Sie dann die aggregierte Latenz mit dem Latenzdiagramm für das Volume.
6. Vergleichen Sie das Diagramm für die Latenz bei Lese-/Schreibvorgängen mit dem Latenzdiagramm für das Volume.
7. Ermitteln, ob die Client-Applikationslasten einen Workload-Konflikt verursacht haben und Workloads nach Bedarf wieder ausgleichen.
8. Ermitteln Sie, ob das Aggregat zu stark beansprucht ist, und verursachen Sie Konflikte, und gleichen Sie Workloads je nach Bedarf aus.

Verwenden Sie Performance-Schwellenwerte zur Ereignisbenachrichtigung

Ereignisse sind Benachrichtigungen, die die Active IQ Unified Manager automatisch generiert, wenn eine vordefinierte Bedingung eintritt, oder wenn ein Performance-Zählerwert einen Schwellenwert überschreitet. Ereignisse helfen Ihnen bei der Ermittlung von Performance-Problemen in den von Ihnen überwachten Clustern. Sie können Benachrichtigungen so konfigurieren, dass automatisch E-Mail-Benachrichtigungen gesendet werden, wenn Ereignisse bestimmter Schweregrade auftreten.

Festlegen von Performance-Schwellenwerten

Sie können Performance-Schwellenwerte festlegen, um kritische Performance-Probleme zu überwachen. Benutzerdefinierte Schwellenwerte lösen eine Warnung oder eine wichtige Ereignisbenachrichtigung aus, wenn das System den definierten Schwellenwert erreicht oder überschreitet.

Schritte

1. Erstellen der Schwellenwerte für Warnung und kritisches Ereignis:
 - a. Wählen Sie **Konfiguration > Leistungsschwellenwerte**.
 - b. Klicken Sie Auf **Erstellen**.
 - c. Wählen Sie den Objekttyp aus, und geben Sie einen Namen und eine Beschreibung der Richtlinie an.
 - d. Wählen Sie die Zählerbedingung des Objekts aus, und geben Sie die Grenzwerte an, die Warnungs- und kritische Ereignisse definieren.
 - e. Wählen Sie die Dauer aus, für die die Grenzwerte für ein zu sendes Ereignis überschritten werden müssen, und klicken Sie dann auf **Speichern**.
2. Weisen Sie die Schwellenwertrichtlinie dem Storage-Objekt zu.
 - a. Wechseln Sie zur Seite „Inventar“ für denselben Cluster-Objekttyp, den Sie zuvor ausgewählt haben, und wählen Sie aus der Option „Ansicht“ die Option „**Performance**“ aus.

- b. Wählen Sie das Objekt aus, dem Sie die Schwellenwertrichtlinie zuweisen möchten, und klicken Sie dann auf **Grenzwertrichtlinie zuweisen**.
- c. Wählen Sie die zuvor erstellte Richtlinie aus und klicken Sie dann auf **Richtlinie zuweisen**.

Beispiel

Es können benutzerdefinierte Schwellenwerte festgelegt werden, die Informationen zu kritischen Performance-Problemen enthalten. Wenn Sie zum Beispiel einen Microsoft Exchange Server haben und Sie wissen, dass es abstürzt, wenn die Volume-Latenz 20 Millisekunden überschreitet, können Sie einen Warnschwellenwert mit 12 Millisekunden und einen kritischen Schwellenwert mit 15 Millisekunden setzen. Mit dieser Schwellenwerteinstellung können Sie Benachrichtigungen erhalten, wenn die Volume-Latenz die Obergrenze überschreitet.

Warnmeldungen hinzufügen

Sie können Benachrichtigungen konfigurieren, um Sie über die Erzeugung eines bestimmten Ereignisses zu benachrichtigen. Sie können Meldungen für eine einzelne Ressource, für eine Gruppe von Ressourcen oder für Ereignisse mit einem bestimmten Schweregrad konfigurieren. Sie können die Häufigkeit angeben, mit der Sie benachrichtigt werden möchten, und ein Skript der Warnmeldung zuordnen.

Was Sie benötigen

- Sie müssen Benachrichtigungseinstellungen wie die Benutzer-E-Mail-Adresse, den SMTP-Server und den SNMP-Trap-Host konfiguriert haben, damit der Active IQ Unified Manager-Server diese Einstellungen verwenden kann, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Meldung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie ein Skript auf der Grundlage des Ereignisses ausführen möchten, müssen Sie das Skript mithilfe der Seite „Skripte“ zu Unified Manager hinzugefügt haben.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können eine Warnmeldung direkt auf der Seite Ereignisdetails erstellen, nachdem Sie ein Ereignis empfangen haben. Zusätzlich können Sie eine Warnung auf der Seite „Alarmkonfiguration“ erstellen, wie hier beschrieben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management > Alarm-Setup**.
2. Klicken Sie auf der Seite **Alarm-Setup** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
4. Klicken Sie auf **Ressourcen**, und wählen Sie die Ressourcen aus, die in die Warnung aufgenommen oder von ihr ausgeschlossen werden sollen.

Sie können einen Filter festlegen, indem Sie im Feld **Name enthält** eine Textzeichenfolge angeben, um eine Gruppe von Ressourcen auszuwählen. Die Liste der verfügbaren Ressourcen zeigt auf der Grundlage der angegebenen Textzeichenfolge nur die Ressourcen an, die der Filterregel entsprechen. Die von Ihnen angegebene Textzeichenfolge ist die Groß-/Kleinschreibung.

Wenn eine Ressource sowohl den von Ihnen angegebenen Einschl- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschließregel, und die Warnung wird nicht für Ereignisse generiert, die sich auf die ausgeschlossene Ressource beziehen.

5. Klicken Sie auf **Events** und wählen Sie die Ereignisse basierend auf dem Ereignisnamen oder dem Schweregrad aus, für den Sie eine Warnung auslösen möchten.



Um mehrere Ereignisse auszuwählen, drücken Sie die Strg-Taste, während Sie Ihre Auswahl treffen.

6. Klicken Sie auf **Actions**, und wählen Sie die Benutzer aus, die Sie benachrichtigen möchten, wählen Sie die Benachrichtigungshäufigkeit aus, wählen Sie aus, ob ein SNMP-Trap an den Trap-Empfänger gesendet wird, und weisen Sie ein Skript zu, das ausgeführt werden soll, wenn eine Warnung erzeugt wird.



Wenn Sie die für den Benutzer angegebene E-Mail-Adresse ändern und die Warnmeldung zur Bearbeitung erneut öffnen, erscheint das Feld Name leer, da die geänderte E-Mail-Adresse dem zuvor ausgewählten Benutzer nicht mehr zugeordnet ist. Wenn Sie die E-Mail-Adresse des ausgewählten Benutzers auf der Seite Benutzer geändert haben, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

Sie können auch Benutzer über SNMP-Traps benachrichtigen.

7. Klicken Sie Auf **Speichern**.

Beispiel für das Hinzufügen einer Meldung

Dieses Beispiel zeigt, wie eine Warnung erstellt wird, die die folgenden Anforderungen erfüllt:

- Alarmname: HealthTest
- Ressourcen: Enthält alle Volumes, deren Name "abc" enthält und schließt alle Volumes aus, deren Name "xyz" enthält
- Ereignisse: Umfasst alle kritischen Systemzustandsereignisse
- Aktionen: Enthält "sample@domain.com", ein "Test"-Skript, und der Benutzer muss alle 15 Minuten benachrichtigt werden

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

1. Klicken Sie auf **Name** und geben Sie ein HealthTest Im Feld **Alarmname**.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
 - a. Eingabe abc Im Feld **Name enthält** werden die Volumes angezeigt, deren Name "abc" enthält.
 - b. Wählen Sie **<<All Volumes whose name contains 'abc'>>** aus dem Bereich Verfügbare Ressourcen und in den Bereich Ausgewählte Ressourcen verschieben.
 - c. Klicken Sie auf **Ausschließe**, und geben Sie ein xyz Klicken Sie im Feld **Name enthält** auf **Hinzufügen**.
3. Klicken Sie auf **Events** und wählen Sie im Feld Ereignis Severity * die Option **kritisch** aus.
4. Wählen Sie im Bereich passende Ereignisse die Option * Alle kritischen Ereignisse* aus, und verschieben Sie sie in den Bereich Ausgewählte Ereignisse.
5. Klicken Sie auf **Aktionen** und geben Sie ein sample@domain.com Im Feld „Diese Benutzer benachrichtigen“.

6. Wählen Sie **alle 15 Minuten**, um den Benutzer alle 15 Minuten zu benachrichtigen.

Sie können eine Warnung konfigurieren, um wiederholt Benachrichtigungen an die Empfänger für eine bestimmte Zeit zu senden. Legen Sie fest, zu welchem Zeitpunkt die Ereignisbenachrichtigung für die Warnmeldung aktiv ist.

7. Wählen Sie im Menü Skript zum Ausführen auswählen die Option **Test-Skript** aus.

8. Klicken Sie Auf **Speichern**.

Konfigurieren Sie die Einstellungen für Warnmeldungen

Sie können festlegen, welche Ereignisse aus Active IQ Unified Manager-Trigger-Warnmeldungen, die E-Mail-Empfänger für diese Meldungen und die Häufigkeit der Meldungen betreffen.

Was Sie benötigen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Über diese Aufgabe

Sie können eindeutige Alarmeinstellungen für die folgenden Arten von Performance-Ereignissen konfigurieren:

- Kritische Ereignisse, die durch Verstöße gegen benutzerdefinierte Schwellenwerte ausgelöst werden
- Warnereignisse, die durch Verstöße gegen benutzerdefinierte Schwellenwerte, systemdefinierte Schwellenwerte oder dynamische Schwellenwerte ausgelöst werden

Standardmäßig werden E-Mail-Alarme für alle neuen Ereignisse an Unified Manager Admin-Benutzer gesendet. Sie können E-Mail-Benachrichtigungen an andere Benutzer senden, indem Sie die E-Mail-Adressen dieser Benutzer hinzufügen.



Um das Senden von Warnmeldungen für bestimmte Ereignistypen zu deaktivieren, müssen Sie alle Kontrollkästchen in einer Ereigniskategorie löschen. Durch diese Aktion werden Ereignisse nicht in der Benutzeroberfläche angezeigt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Storage-Management > Alarm-Setup** aus.

Die Seite „Alarm-Setup“ wird angezeigt.

2. Klicken Sie auf **Hinzufügen** und konfigurieren Sie die entsprechenden Einstellungen für jeden Ereignistypen.

Um E-Mail-Benachrichtigungen an mehrere Benutzer zu senden, geben Sie ein Komma zwischen den einzelnen E-Mail-Adressen ein.

3. Klicken Sie Auf **Speichern**.

Performance-Probleme in Active IQ Unified Manager ermitteln

Wenn ein Performance-Ereignis eintritt, können Sie die Ursache des Problems in Active IQ Unified Manager lokalisieren und diese mithilfe anderer Tools beheben. Unter Umständen erhalten Sie während der täglichen Überwachung eine E-Mail-

Benachrichtigung über ein Ereignis oder eine Benachrichtigung über das Ereignis.

Schritte

1. Klicken Sie in der E-Mail-Benachrichtigung auf den Link, der Sie mit einem Performance-Ereignis direkt zum Storage-Objekt bringt.

Sie suchen...	Dann...
Sie erhalten eine E-Mail-Benachrichtigung über ein Ereignis	Klicken Sie auf den Link, um direkt zur Seite mit den Veranstaltungsdetails zu gelangen.
Beachten Sie das Ereignis während der Analyse der Seite „Ereignisbestand“	Wählen Sie das Ereignis aus, um direkt zur Seite mit den Veranstaltungsdetails zu gelangen.

2. Wenn das Ereignis einen systemdefinierten Schwellenwert überschritten hat, befolgen Sie die vorgeschlagenen Aktionen in der UI, um das Problem zu beheben.
3. Wenn das Ereignis einen benutzerdefinierten Schwellenwert überschritten hat, analysieren Sie das Ereignis, um zu bestimmen, ob Sie Maßnahmen ergreifen müssen.
4. Wenn das Problem weiterhin besteht, überprüfen Sie die folgenden Einstellungen:
 - Protokolleinstellungen auf dem Storage-System
 - Netzwerkeinstellungen auf jedem Ethernet oder Fabric Switches
 - Netzwerkeinstellungen auf dem Storage-System
 - Das Festplattenlayout und die aggregierte Kennzahlen im Storage-System
5. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support, um Hilfe zu erhalten.

Verwenden Sie Active IQ Digital Advisor, um die Systemleistung anzuzeigen

Bei jedem ONTAP System, das AutoSupport Telemetrie an NetApp sendet, können Sie umfassende Daten zu Performance und Kapazität einsehen. Active IQ zeigt die System-Performance über einen längeren Zeitraum an, als Sie in System Manager sehen können.

Sie können Diagramme der CPU-Auslastung, Latenz, IOPS, IOPS nach Protokoll und Netzwerkdurchsatz anzeigen. Sie können diese Daten auch als .csv-Format für die Analyse in anderen Werkzeugen herunterladen.

Neben diesen Performance-Daten zeigt Active IQ Ihnen Storage-Effizienz je Workload und vergleicht diese Effizienz mit der erwarteten Effizienz für jenen Workload-Typ. Sie können Kapazitätstrends anzeigen und eine Schätzung der Menge an zusätzlichem Storage anzeigen, die Sie möglicherweise zu einem bestimmten Zeitpunkt hinzufügen müssen.



- Storage-Effizienz ist auf der linken Seite des Haupt-Dashboards auf Kunden-, Cluster- und Node-Ebene verfügbar.
- Die Performance ist auf Cluster- und Node-Ebene auf der linken Seite des Haupt-Dashboards verfügbar.

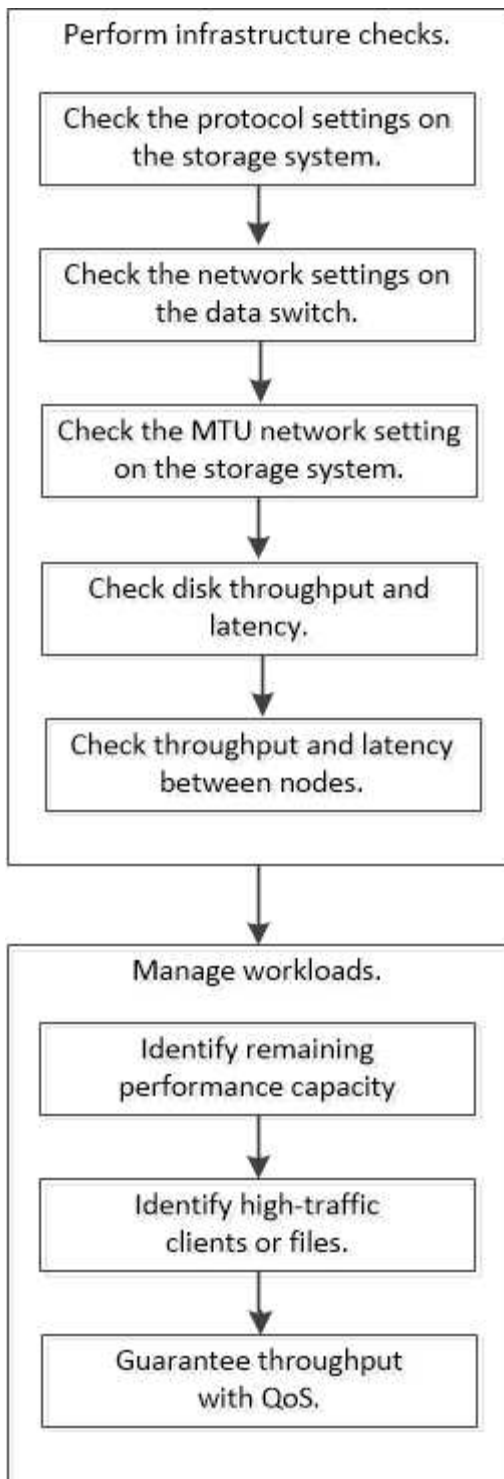
Verwandte Informationen

- ["Active IQ Digital Advisor Dokumentation"](#)
- ["Active IQ Digital Advisor – Video-Playlist"](#)
- ["Active IQ Web Portal"](#)

Managen Sie Performance-Probleme

Performance-Management-Workflow

Sobald Sie ein Performance-Problem erkannt haben, können Sie Ihre Infrastruktur mit einigen grundlegenden Diagnosetprüfungen durchführen, um offensichtliche Konfigurationsfehler auszuschließen. Wenn diese das Problem nicht lokalisieren, können Sie sich mit dem Workload-Management-Problemen in die Lage geben.



Durchführung grundlegender Infrastrukturprüfungen

Prüfen Sie die Protokolleinstellungen auf dem Storage-System

Überprüfen Sie die maximale Übertragungsgröße des NFS TCP

Für NFS können Sie überprüfen, ob die maximale TCP-Übertragungsgröße für die Lese- und Schreibvorgänge zu einem Performance-Problem führen kann. Wenn Sie der Meinung sind, dass die Größe die Performance bremst, können Sie sie erhöhen.

Was Sie benötigen

- Um diese Aufgabe ausführen zu können, müssen Sie über Cluster-Administratorrechte verfügen.
- Sie müssen Befehle der erweiterten Berechtigungsebene für diese Aufgabe verwenden.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Überprüfen Sie die maximale TCP-Übertragungsgröße:

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

3. Wenn die maximale TCP-Übertragungsgröße zu klein ist, vergrößern Sie die Größe:

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

4. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Beispiel

Im folgenden Beispiel wird die maximale TCP-Übertragungsgröße von geändert SVM1 An 1048576:

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

Prüfen Sie die iSCSI-TCP-Lese-/Schreibgröße

Für iSCSI können Sie die TCP-Lese-/Schreibgröße überprüfen, um festzustellen, ob die Größeneinstellung ein Leistungsproblem verursacht. Wenn die Größe die Quelle eines Problems ist, können Sie es korrigieren.

Was Sie benötigen

Für diese Aufgabe sind erweiterte Befehle auf Berechtigungsebene erforderlich.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Überprüfen Sie die Einstellung für die Größe des TCP-Fensters:

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

3. Ändern Sie die Einstellung für die Größe des TCP-Fensters:

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

4. Zurück zur Administratorberechtigung:


```
set -privilege admin
```

Beispiel

Im folgenden Beispiel wird die Größe des TCP-Fensters von geändert SVM1 Bis 131,400 Byte:

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

Prüfen Sie die CIFS-Multiplex-Einstellungen

Wenn eine langsame CIFS-Netzwerkleistung ein Leistungsproblem verursacht, können Sie die Multiplex-Einstellungen ändern, um sie zu verbessern und zu korrigieren.

Schritte

1. Prüfen Sie die CIFS-Multiplex-Einstellung:

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

2. Ändern Sie die CIFS-Multiplex-Einstellung:

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

Beispiel

Im folgenden Beispiel wird die maximale Multiplex-Anzahl geändert SVM1 An 255:

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

Überprüfen Sie die Geschwindigkeit des FC-Adapter-Ports

Die Zielportgeschwindigkeit des Adapters sollte mit der Geschwindigkeit des Geräts übereinstimmen, mit dem es verbunden wird, um die Leistung zu optimieren. Wenn der Port auf Autonegotiation festgelegt ist, kann der erneute Verbindungsaufbau nach einer Übernahme und Rückgabe oder einer anderen Unterbrechung länger dauern.

Was Sie benötigen

Alle LIFs, die diesen Adapter als Home-Port verwenden, müssen offline sein.

Schritte

1. Versetzen Sie den Adapter in den Offline-Modus:

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

2. Überprüfen Sie die maximale Geschwindigkeit des Port-Adapters:

```
fcp adapter show -instance
```

3. Ändern Sie ggf. die Portgeschwindigkeit:

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

4. Versetzen Sie den Adapter in den Online-Modus:

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

5. Stellen Sie alle LIFs am Adapter online:

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

Beispiel

Im folgenden Beispiel wird die Portgeschwindigkeit des Adapters geändert 0d Ein node1 Bis 2 Gbit/s:

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

Überprüfen Sie die Netzwerkeinstellungen auf den Datenschaltern

Obwohl Sie auf Ihren Clients, Servern und Storage-Systemen (d. h. Netzwerkendpunkte) dieselben MTU-Einstellungen vornehmen müssen, sollten zwischengeschaltete Netzwerkgeräte wie NICs und Switches auf ihre maximalen MTU-Werte eingestellt werden, um sicherzustellen, dass die Leistung nicht beeinträchtigt wird.

Um eine optimale Leistung zu erzielen, müssen alle Komponenten im Netzwerk in der Lage sein, Jumbo Frames (9000 Byte IP, 9022 Bytes einschließlich Ethernet) weiterzuleiten. Die Datenschalter sollten auf mindestens 9022 Bytes gesetzt werden, aber bei den meisten Switches ist ein typischer Wert von 9216 möglich.

Verfahren

Überprüfen Sie bei Datenschaltern, ob die MTU-Größe auf 9022 oder höher eingestellt ist.

Weitere Informationen finden Sie in der Dokumentation des Switch-Anbieters.

Überprüfen Sie die MTU-Netzwerkeinstellung auf dem Storage-System

Sie können die Netzwerkeinstellungen im Storage-System ändern, falls diese nicht mit den Einstellungen auf dem Client oder anderen Netzwerkendpunkten übereinstimmen. Während für das Management-Netzwerk die MTU-Einstellung auf 1500 eingestellt ist, sollte die MTU-Größe des Datennetzwerks 9000 sein.

Über diese Aufgabe

Alle Ports innerhalb einer Broadcast-Domäne haben dieselbe MTU-Größe – mit Ausnahme des Port E0M für den Management-Datenverkehr. Wenn der Port Teil einer Broadcast-Domain ist, verwenden Sie das `broadcast-domain modify` Befehl zum Ändern der MTU für alle Ports in der geänderten Broadcast-Domain.

Beachten Sie, dass Zwischennetzgeräte wie NICs und Datenschalter auf höhere MTU-Größen eingestellt werden können als Netzwerkendpunkte. Weitere Informationen finden Sie unter ["Überprüfen Sie die](#)

Netzwerkeinstellungen auf den Datenschaltern".

Schritte

1. Überprüfen Sie die MTU-Porteinstellung auf dem Speichersystem:

```
network port show -instance
```

2. Ändern Sie die MTU in der Broadcast-Domäne, die von den Ports verwendet wird:

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

Beispiel

Im folgenden Beispiel wird die MTU-Porteinstellung auf 9000 geändert:

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

Überprüfen Sie den Durchsatz und die Latenz der Festplatte

Sie können die Metriken zum Festplattendurchsatz und zur Latenz für Cluster-Nodes überprüfen, um Sie bei der Fehlerbehebung zu unterstützen.

Über diese Aufgabe

Für diese Aufgabe sind erweiterte Befehle auf Berechtigungsebene erforderlich.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Überprüfen Sie die Kennzahlen für den Festplattendurchsatz und die Latenz:

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

Beispiel

Im folgenden Beispiel werden die Summen in jedem Benutzer für Lese- oder Schreibvorgänge angezeigt
node2 Ein cluster1:

```

::*> 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

Prüfen Sie Durchsatz und Latenz zwischen Nodes

Sie können das verwenden `network test-path` Befehl zum Identifizieren von Netzwerkengpässen oder zum Vorqualifizieren von Netzwerkpfaden zwischen Nodes. Sie können den Befehl zwischen Cluster Nodes oder Intracluster Nodes ausführen.

Was Sie benötigen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Befehle auf Berechtigungsebene erforderlich.
- Für einen Intercluster-Pfad müssen die Quell- und Ziel-Cluster Peering durchgeführt werden.

Über diese Aufgabe

Gelegentlich erfüllt die Netzwerkleistung zwischen Knoten möglicherweise nicht die Erwartungen an Ihre Pfadkonfiguration. Eine Übertragungsrate von 1 Gbit/s für die Art großer Datentransfers, wie bei SnapMirror Replizierungsvorgängen zu beobachten ist, wäre nicht mit einer 10-GbE-Verbindung zwischen den Quell- und Ziel-Clustern konsistent.

Sie können das verwenden `network test-path` Befehl zum Messen des Durchsatzes und der Latenz zwischen Nodes. Sie können den Befehl zwischen Cluster Nodes oder Intracluster Nodes ausführen.



Der Test sättigt den Netzwerkpfad mit Daten. Wenn also das System nicht ausgelastet ist und der Netzwerk-Traffic zwischen den Nodes nicht zu hoch ist, sollte der Befehl ausgeführt werden. Die Testzeit beträgt nach zehn Sekunden. Der Befehl kann nur zwischen ONTAP 9 Nodes ausgeführt werden.

Der `session-type` Option gibt den Vorgang an, den Sie über den Netzwerkpfad ausführen, z. B. „AsyncMirrorRemote“ für die SnapMirror Replizierung an einem Remote-Ziel. Der Typ gibt die Menge der im Test verwendeten Daten an. Die folgende Tabelle definiert die Sitzungstypen:

Sitzungstyp	Beschreibung
SyncMirrorLocal	Von SnapMirror zwischen den Nodes im selben Cluster verwendete Einstellungen

SyncMirrorRemote	Von SnapMirror verwendete Einstellungen zwischen Nodes in verschiedenen Clustern (Standardtyp)
RemoteDataTransfer	Von ONTAP für Remote-Datenzugriff zwischen Nodes im selben Cluster (z. B. eine NFS-Anforderung an einen Node für eine Datei, die in einem Volume auf einem anderen Node gespeichert ist)

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Messung des Durchsatzes und der Latenz zwischen Nodes:

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

Der Quell-Node muss sich im lokalen Cluster befinden. Der Ziel-Node kann sich im lokalen Cluster oder in einem Peering-Cluster befinden. Ein Wert von "lokal" für `-source-node` Gibt den Node an, auf dem Sie den Befehl ausführen.

Mit dem folgenden Befehl wird der Durchsatz und die Latenz für SnapMirror Replizierungsvorgänge zwischen dem Typ gemessen `node1` Auf dem lokalen Cluster und `node3` Ein `cluster2`:

```
cluster1::> network test-path -source-node node1 -destination-cluster cluster2 -destination-node node3 -session-type AsyncMirrorRemote
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
Min latency in ms:     61.14
Max latency in ms:     3056.86
```

3. Zurück zur Administratorberechtigung:

```
set -privilege admin
```

Nachdem Sie fertig sind

Wenn die Performance die Erwartungen der Pfadkonfiguration nicht erfüllt, sollten Sie die Performance-Statistiken der Nodes überprüfen, die verfügbaren Tools verwenden, um das Problem im Netzwerk zu isolieren, die Switch-Einstellungen zu überprüfen usw.

Management von Workloads

Ermittlung der verbleibenden Performance-Kapazität

Performance-Kapazität (oder *Reserve*) gibt an, wie viel Arbeit auf einem Node oder Aggregat anfallen kann, bevor die Performance der Workloads der Ressource durch die Latenz beeinträchtigt wird. Wenn Sie die verfügbare Performance-Kapazität auf dem Cluster kennen, können Sie Workloads bereitstellen und ausgleichen.

Was Sie benötigen

Für diese Aufgabe sind erweiterte Befehle auf Berechtigungsebene erforderlich.

Über diese Aufgabe

Sie können für das die folgenden Werte verwenden `-object` Option zum Erfassen und Anzeigen von Reservestatistiken:

- Für CPUs, `resource_headroom_cpu`.
- Für Aggregate `resource_headroom_aggr`.

Sie können diese Aufgabe auch mit System Manager und Active IQ Unified Manager ausführen.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Starten Sie die Echtzeitstatistik:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

3. Anzeigen von Informationen zu Reservestatistiken in Echtzeit:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

4. Zurück zur Administratorberechtigung:

```
set -privilege admin
```

Beispiel

Im folgenden Beispiel werden die Statistiken der durchschnittlichen stündlichen Reserve für Cluster-Nodes angezeigt.

Sie können die verfügbare Performance-Kapazität eines Knotens berechnen, indem Sie die `current_utilization` Zähler vom `optimal_point_utilization` Zähler. In diesem Beispiel wird die Auslastungskapazität für `CPU_sti2520-213` liegt -14% (72%-86%), was darauf hindeutet, dass die CPU im Durchschnitt für die letzte Stunde überausgelastet wurde.

Sie könnten angegeben haben ewma_daily, ewma_weekly, Oder ewma_monthly Um dieselben Informationen über längere Zeiträume gemittelt zu erhalten.

```
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.

Identifizieren von Clients oder Dateien mit hohem Datenverkehr

Mit der ONTAP Technologie für aktive Objekte können Kunden oder Dateien identifiziert werden, die für unverhältnismäßig hohe Mengen an Cluster-Datenverkehr verantwortlich

sind. Sobald Sie die „wichtigsten“ Clients oder Dateien identifiziert haben, können Sie Cluster-Workloads ausgleichen oder andere Schritte zur Behebung des Problems Unternehmen.

Was Sie benötigen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Zeigen Sie die wichtigsten Clients an, die auf das Cluster zugreifen:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Mit dem folgenden Befehl werden die wichtigsten Clients angezeigt, auf die zugegriffen wird `cluster1`:

```
cluster1::> statistics top client show
```

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

Client	Vserver	Node	Protocol	*Total Ops
172.17.180.170	vs4	siderop1-vsim4	nfs	668
172.17.180.169	vs3	siderop1-vsim3	nfs	337
172.17.180.171	vs3	siderop1-vsim3	nfs	142
172.17.180.170	vs3	siderop1-vsim3	nfs	137
172.17.180.123	vs3	siderop1-vsim3	nfs	137
172.17.180.171	vs4	siderop1-vsim4	nfs	95
172.17.180.169	vs4	siderop1-vsim4	nfs	92
172.17.180.123	vs4	siderop1-vsim4	nfs	92
172.17.180.153	vs3	siderop1-vsim3	nfs	0

2. Zeigen Sie die wichtigsten Dateien an, auf die im Cluster zugegriffen wird:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Mit dem folgenden Befehl werden die wichtigsten Dateien angezeigt, auf die zugegriffen wird `cluster1`:


```
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	

Garantierter Durchsatz durch QoS

Durchsatz garantieren mit QoS-Übersicht

Dank Storage-Servicequalität (QoS) kann die Performance kritischer Workloads nicht durch konkurrierende Workloads beeinträchtigt werden. Sie können für einen konkurrierenden Workload eine Durchsatzbegrenzung festlegen, um die Auswirkungen auf Systemressourcen zu begrenzen oder für einen kritischen Workload einen Durchsatz *Floor* festzulegen. So wird sichergestellt, dass er unabhängig von der Nachfrage durch konkurrierende Workloads ein Mindestziel für den Durchsatz erreicht. Sie können sogar eine Decke und einen Boden für die gleiche Arbeitslast einstellen.

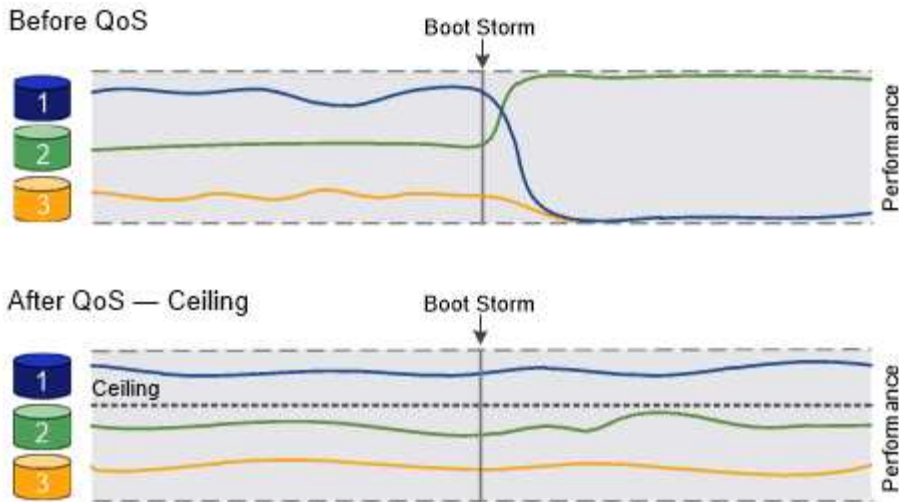
Allgemeines zu Durchsatzbegrenzungen (QoS max.)

Eine Durchsatzbegrenzung beschränkt den Durchsatz für einen Workload auf eine maximale Anzahl an IOPS oder MB/s oder IOPS und MB/Sek.. In der Abbildung unten stellt die Durchsatzobergrenze für Workload 2 sicher, dass die Workloads 1 und 3 nicht „problematische“ Workloads ausgeführt werden.

Eine *Policy Group* definiert die Durchsatzobergrenze für einen oder mehrere Workloads. Ein Workload repräsentiert die I/O-Vorgänge für ein Storage-Objekt: ein Volume, eine Datei, einen qtree oder eine LUN oder alle Volumes, Dateien, qtrees oder LUNs in einer SVM. Sie können beim Erstellen der Richtlinienengruppe die Obergrenze festlegen oder warten, bis Sie die Workloads überwachen und sie angeben.



Der Durchsatz bei Workloads kann den angegebenen Höchstwert um bis zu 10 % überschreiten, insbesondere bei einem Workload, der einen schnellen Durchsatzwechsel aufweist. Die Decke könnte um bis zu 50 % überschritten werden, um mit Ausbrüchen zu umgehen. Stausbrüche erfolgen auf einzelnen Nodes, wenn sich Token bis zu 150 % ansammeln



Allgemeines zu Durchsatzböden (QoS Min.)

Eine Durchsatzmenge stellt sicher, dass der Durchsatz für einen Workload nicht unter eine Mindestanzahl von IOPS oder MB/s bzw. IOPS und MB/s fällt. In der Abbildung unten stellen die Durchsatzböden für Workload 1 und Workload 3 sicher, dass sie unabhängig von der Nachfrage nach Workload 2 ein Mindestdurchsatz erreichen.



Wie die Beispiele zeigen, wird der Durchsatz durch eine Durchsatzbegrenzung direkt gedrosselt. Ein Durchsatzboden drosselt den Durchsatz indirekt, indem den Workloads, für die das Boden festgelegt wurde, Priorität eingeräumt wird.

Sie können den Boden beim Erstellen der Richtliniengruppe angeben oder warten, bis Sie die Workloads überwachen, um sie anzugeben.

Ab ONTAP 9.13.1 lassen sich Durchsatzböden im SVM-Umfang mit festlegen [\[adaptive-qos-templates\]](#). In Versionen von ONTAP vor 9.13.1 kann eine Richtliniengruppe, die eine Durchsatzmenge definiert, nicht auf eine SVM angewendet werden.



In Releases vor ONTAP 9.7 werden Durchsatzböden garantiert, wenn genügend Performance-Kapazität zur Verfügung steht.

In ONTAP 9.7 und höher kann auch bei unzureichender Performance-Kapazität der Durchsatzboden garantiert werden. Dieses neue Bodenverhalten wird Floors v2 genannt. Um die Garantien zu erfüllen, kann Floors v2 zu einer höheren Latenz bei Workloads ohne Durchsatzboden oder Arbeitsleistung führen, die die Bodeneinstellungen überschreitet. Fußböden v2 gelten sowohl für QoS als auch für anpassungsfähige QoS.

Die Option zum Aktivieren/Deaktivieren des neuen Verhaltens von Floors v2 ist ab ONTAP 9.7P6 verfügbar. Ein Workload könnte bei kritischen Prozessen wie beispielsweise unter die angegebene Arbeitslast fallen `volume move trigger-cutover`. Auch wenn genügend Kapazität zur Verfügung steht und geschäftskritische Betriebsabläufe nicht stattfinden, kann der Durchsatz zu einem Workload um bis zu 5 % unter das angegebene Stockwerk fallen. Wenn Böden zu hoch sind und es keine Performance-Kapazität gibt, können einige Workloads unter die angegebene Etage fallen.

Allgemeines zu Shared-QoS-Richtliniengruppen und nicht gemeinsam genutzten QoS-Gruppen

Ab ONTAP 9.4 können Sie mithilfe einer QoS-Richtliniengruppe ohne Shared_ angeben, dass die definierte Durchsatzdecke oder -Etage für jeden Workload der Mitglieder einzeln gilt. Das Verhalten von *shared* -Richtliniengruppen hängt vom Richtlinientyp ab:

- Bei Durchsatzbegrenzungen kann der Gesamtdurchsatz der Workloads, die der gemeinsam genutzten Richtliniengruppe zugewiesen sind, die angegebene Obergrenze nicht überschreiten.
- Bei Durchsatzböden kann die gemeinsame Richtliniengruppe nur auf einen einzelnen Workload angewendet werden.

Allgemeines zur anpassungsfähigen QoS

Normalerweise wird der Wert der Richtliniengruppe, die Sie einem Storage-Objekt zuweisen, beibehalten. Sie müssen den Wert manuell ändern, wenn sich die Größe des Speicherobjekts ändert. Ein Anstieg des Platzansatzes, der z. B. auf einem Volumen genutzt wird, erfordert in der Regel eine entsprechende Erhöhung der für das Volumen angegebenen Durchsatzdecke.

Adaptive QoS skaliert den Richtliniengruppenwert automatisch auf die Workload-Größe und behält das Verhältnis von IOPS zu TBs bei sich änderter Workload-Größe bei. Wenn Sie Hunderte oder Tausende Workloads in einer großen Implementierung managen, bedeutet dies einen enormen Vorteil.

Meist verwenden Kunden anpassungsfähige QoS zur Anpassung der Durchsatzdecken, allerdings können sie auch zum Managen von Durchsatzböden (bei einer Erhöhung der Workload-Größe) eingesetzt werden. Die Workload-Größe wird entweder als zugewiesener Speicherplatz für das Storage-Objekt oder als Speicherplatz angegeben, der vom Storage-Objekt verwendet wird.



Gebrauchte Flächen sind für Durchsatzböden in ONTAP 9.5 und höher verfügbar. Es wird bei Durchsatzböden in ONTAP 9.4 und früher nicht unterstützt.

- Eine Richtlinie „*zugewiesener Speicherplatz*“ behält das IOPS/TB-Verhältnis entsprechend der nominalen Größe des Storage-Objekts bei. Wenn das Verhältnis 100 IOPS/GB ist, wird ein 150 GB großes Volume eine Durchsatzgrenze von 15,000 IOPS aufweisen, solange das Volume diese Größe bleibt. Wenn die Volume-Größe auf 300 GB geändert wird, passt die anpassungsfähige QoS die Durchsatzdecke auf 30,000 IOPS an.
- Eine Richtlinie „*Used space*“ (Standard) behält das Verhältnis von IOPS/TB GB entsprechend der Menge der tatsächlich gespeicherten Daten vor der Storage-Effizienz bei. Wenn das Verhältnis 100 IOPS/GB ist, würde ein 150 GB großes Volumen, das 100 GB gespeicherte Daten hat, eine Durchsatzdecke von 10,000 IOPS haben. Wenn sich die Menge des belegten Speicherplatzes ändert, passt die anpassungsfähige QoS die Durchsatzobergrenze dem Verhältnis an.

Ab ONTAP 9.5 können Sie für Ihre Applikation eine I/O-Blockgröße angeben, die sowohl in IOPS als auch in MB/Sek. ein Durchsatzlimit angegeben. Die Größe des MB/s wird aus der Blockgröße berechnet, die mit dem IOPS-Limit multipliziert wird. Beispielsweise ergibt eine I/O-Blockgröße von 32.000 IOPS bei einem IOPS-Limit von 6144 IOPS/TB einen Grenzwert von 192 MB/s.

Das folgende Verhalten kann sowohl bei Durchsatzdecken als auch bei Böden erwartet werden:

- Wenn ein Workload einer anpassungsfähigen QoS-Richtliniengruppe zugewiesen wird, wird die Decke oder der Boden sofort aktualisiert.
- Wenn die Größe eines Workloads in einer adaptiven QoS-Richtliniengruppe angepasst wird, werden die Decke oder der Boden in etwa fünf Minuten aktualisiert.

Bevor Updates erfolgen, muss der Durchsatz um mindestens 10 IOPS erhöht werden.

Adaptive QoS-Richtliniengruppen werden immer nicht gemeinsam genutzt: Die definierte Durchsatzdecke oder -Etage wird für jeden Workload der Mitglieder einzeln angewendet.

Ab ONTAP 9.6 werden Durchsatzböden auf ONTAP Select Premium mit SSDs unterstützt.

Vorlage für adaptive Richtliniengruppen

Ab ONTAP 9.13.1 können Sie eine anpassungsfähige QoS-Vorlage auf einer SVM festlegen. Mithilfe von Vorlagen für adaptive Richtliniengruppen können Sie Durchsatzraten und -decken für alle Volumes in einer SVM festlegen.

Anpassungsfähige Richtliniengruppen-Vorlagen können erst nach Erstellung der SVM festgelegt werden. Verwenden Sie die `vserver modify` Befehl mit dem `-qos-adaptive-policy-group-template` Parameter zum Festlegen der Richtlinie.

Wenn Sie eine Vorlage für eine Gruppe adaptiver Richtlinien festlegen, übernehmen die nach dem Festlegen der Richtlinie erstellten oder migrierten Volumes automatisch die Richtlinie. Alle Volumes, die auf der SVM vorhanden sind, werden nicht beeinträchtigt, wenn Sie die Richtlinienvorlage zuweisen. Wenn Sie die Richtlinie auf der SVM deaktivieren, erhält jedes später auf die SVM migrierte oder erstellte Volume nicht diese Richtlinie. Die Deaktivierung der Vorlage für adaptive Richtliniengruppen wirkt sich nicht auf Volumes aus, die die Richtlinienvorlage übernommen haben, da sie die Richtlinienvorlage beibehalten.

Weitere Informationen finden Sie unter [Legen Sie eine Vorlage für adaptive Richtliniengruppen fest](#).

Allgemeiner Support

Die folgende Tabelle zeigt die Unterschiede bei der Unterstützung von Durchsatzdecken, Durchsatzböden und anpassungsfähiger QoS.

Ressource oder Funktion	Durchsatzdecke	Durchsatzboden	Durchsatzboden v2	Anpassungsfähige QoS
ONTAP 9-Version	Alle	9.2 und höher	9.7 und höher	9.3 und höher
Plattformen	Alle	<ul style="list-style-type: none">• AFF• C190• ONTAP Select Premium mit SSD *	<ul style="list-style-type: none">• AFF• C190• ONTAP Select Premium mit SSD	Alle
Protokolle	Alle	Alle	Alle	Alle
FabricPool	Ja.	Ja, wenn die Tiering-Richtlinie auf „keine“ eingestellt ist und keine Blöcke in der Cloud liegen.	Ja, wenn die Tiering-Richtlinie auf „keine“ eingestellt ist und keine Blöcke in der Cloud liegen.	Nein

Ressource oder Funktion	Durchsatzdecke	Durchsatzboden	Durchsatzboden v2	Anpassungsfähige QoS
SnapMirror Synchronous	Ja.	Nein	Nein	Ja.

Der Support für C190 und ONTAP Select beginnt mit der Version ONTAP 9.6.

Unterstützte Workloads bei Durchsatzbegrenzungen

Die folgende Tabelle zeigt die Workload-Unterstützung für Durchsatzbegrenzungen mit der Version ONTAP 9. Root-Volumes, Spiegelungen zur Lastverteilung und Datensicherungsspiegelungen werden nicht unterstützt.

Workload Support - Decke	ONTAP 9.0	ONTAP 9.1	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 - 9.7	ONTAP 9.8 und höher
Datenmenge	ja	ja	ja	ja	ja	ja
Datei	ja	ja	ja	ja	ja	ja
LUN	ja	ja	ja	ja	ja	ja
SVM	ja	ja	ja	ja	ja	ja
FlexGroup Volume	Nein	Nein	Nein	ja	ja	ja
Qtrees*	Nein	Nein	Nein	Nein	Nein	ja
Mehrere Workloads pro Richtliniengruppe	ja	ja	ja	ja	ja	ja
Nicht gemeinsam genutzte Richtliniengruppen	Nein	Nein	Nein	Nein	ja	ja

Ab ONTAP 9.8 wird der NFS-Zugriff in qtrees in FlexVol und FlexGroup Volumes mit aktiviertem NFS unterstützt. Ab ONTAP 9.9 wird SMB-Zugriff auch in qtrees in FlexVol und FlexGroup Volumes mit aktiviertem SMB unterstützt.

Unterstützte Workloads für Durchsatzböden

Die folgende Tabelle zeigt Workload-Support für Durchsatzböden mit ONTAP 9 Version. Root-Volumes, Spiegelungen zur Lastverteilung und Datensicherungsspiegelungen werden nicht unterstützt.

Workload Support – Floor	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 - 9.7	ONTAP 9.8 - 9.13.0	ONTAP 9.13.1 und höher
Datenmenge	ja	ja	ja	ja	ja
Datei	Nein	ja	ja	ja	ja
LUN	ja	ja	ja	ja	ja
SVM	Nein	Nein	Nein	Nein	ja
FlexGroup Volume	Nein	Nein	ja	ja	ja
Qtrees *	Nein	Nein	Nein	ja	ja
Mehrere Workloads pro Richtliniengruppe	Nein	Nein	ja	ja	ja
Nicht gemeinsam genutzte Richtliniengruppen	Nein	Nein	ja	ja	ja

*ab ONTAP 9.8 wird der NFS-Zugriff in qtrees in FlexVol- und FlexGroup-Volumes mit aktiviertem NFS unterstützt. Ab ONTAP 9.9 wird SMB-Zugriff auch in qtrees in FlexVol und FlexGroup Volumes mit aktiviertem SMB unterstützt.

Unterstützte Workloads für anpassungsfähige QoS

Die folgende Tabelle zeigt die Workload-Unterstützung für die adaptive QoS von ONTAP 9. Root-Volumes, Spiegelungen zur Lastverteilung und Datensicherungsspiegelungen werden nicht unterstützt.

Workload-Unterstützung: Anpassungsfähige QoS	ONTAP 9.3	ONTAP 9.4 - 9.13.0	ONTAP 9.13.1 und höher
Datenmenge	ja	ja	ja
Datei	Nein	ja	ja
LUN	Nein	ja	ja
SVM	Nein	Nein	ja
FlexGroup Volume	Nein	ja	ja
Mehrere Workloads pro Richtliniengruppe	ja	ja	ja
Nicht gemeinsam genutzte Richtliniengruppen	ja	ja	ja

Maximale Anzahl an Workloads und Richtliniengruppen

In der folgenden Tabelle wird die maximale Anzahl an Workloads und Richtliniengruppen nach Version ONTAP 9 angezeigt.

Workload-Unterstützung	ONTAP 9.3 und frühere Versionen	ONTAP 9.4 und höher
Maximale Workloads pro Cluster	12,000	40,000
Maximale Workloads pro Node	12,000	40,000
Maximale Anzahl von Richtliniengruppen	12,000	12,000

Aktivieren oder Deaktivieren von Durchsatzböden v2

Auf AFF können Sie Durchsatzböden v2 aktivieren oder deaktivieren. Die Standardeinstellung ist aktiviert. Bei aktivierten Etagen v2 können Durchsatzböden eingehalten werden, wenn Controller stark genutzt werden, um Kosten für eine höhere Latenz bei anderen Workloads zu senken. Floors v2 gilt sowohl für QoS als auch für Adaptive QoS.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Geben Sie einen der folgenden Befehle ein:

Ihr Ziel ist	Verwenden Sie den folgenden Befehl:
Deaktivieren Sie die Etagen v2	<code>qos settings throughput-floors-v2 -enable false</code>
Ebenen v2 aktivieren	<code>qos settings throughput-floors-v2 -enable true</code>



Um Durchsatzböden v2 in einem MetroCluster Cluster zu deaktivieren, müssen Sie die ausführen

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

Befehl auf Quell- und Ziel-Clustern.

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

Wenn Sie bereits die Performance-Anforderungen für die Workloads kennen, die Sie mit QoS managen möchten, können Sie beim Erstellen der Richtliniengruppe das Durchsatzlimit angeben. Andernfalls können Sie warten, bis Sie das Limit nach dem Monitoring der Workloads angeben.

Festlegung einer Durchsatzgrenze mit QoS

Sie können das verwenden `max-throughput` Feld für eine Richtliniengruppe zur Definition einer Durchsatzgrenze für Storage-Objekt-Workloads (max. QoS) Sie können die Richtliniengruppe anwenden, wenn Sie das Speicherobjekt erstellen oder ändern.

Was Sie benötigen

- Zum Erstellen einer Richtliniengruppe müssen Sie ein Cluster-Administrator sein.
- Zum Anwenden einer Richtliniengruppe auf eine SVM müssen Sie ein Cluster-Administrator sein.

Über diese Aufgabe

- Ab ONTAP 9.4 können Sie mithilfe einer Richtliniengruppe „*non-shared* QoS“ angeben, dass die definierte Durchsatzobergrenze für jeden einzelnen Mitglied-Workload gilt. Andernfalls wird die Richtliniengruppe „*shared*“: der Gesamtdurchsatz der der Richtliniengruppe zugewiesenen Workloads darf die angegebene Obergrenze nicht überschreiten.

Einstellen `-is-shared=false` Für das `qos policy-group create` Befehl zum Festlegen einer nicht freigegebenen Gruppe.

- Sie können das Durchsatzlimit für IOPS, MB/s oder IOPS, MB/s festlegen Wenn Sie sowohl IOPS als auch MB/s angeben, wird der erste Grenzwert erreicht.



Wenn Sie eine Decke und ein Boden für denselben Workload festlegen, können Sie nur das Durchsatzlimit für den IOPS festlegen.

- Ein Storage-Objekt, das einem QoS-Limit unterliegt, muss von der SVM, der die Richtliniengruppe angehört, enthalten sein. Mehrere Richtliniengruppen können derselben SVM angehören.
- Sie können einer Richtliniengruppe kein Speicherobjekt zuweisen, wenn das zugehörige Objekt oder seine untergeordneten Objekte zur Richtliniengruppe gehören.
- Es handelt sich um eine Best Practice bei QoS, eine Richtliniengruppe auf denselben Storage-Typ anzuwenden.

Schritte

1. Erstellen einer Richtliniengruppe:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page. Sie können das verwenden `qos policy-group modify` Befehl zum Einstellen der Durchsatzdecken.

Mit dem folgenden Befehl wird die gemeinsam genutzte Richtliniengruppe erstellt `pg-vs1` Bei einem maximalen Durchsatz von 5,000 IOPS:


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

Mit dem folgenden Befehl wird die nicht gemeinsam genutzte Richtliniengruppe erstellt `pg-vs3` Bei einem maximalen Durchsatz von 100 IOPS und 400 KB/s:

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

Mit dem folgenden Befehl wird die nicht gemeinsam genutzte Richtliniengruppe erstellt `pg-vs4` Ohne Durchsatzbegrenzung:

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

2. Anwenden einer Richtliniengruppe auf eine SVM, Datei, Volume oder LUN:

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

Eine vollständige Befehlssyntax finden Sie in den man-Pages. Sie können das verwenden `storage_object modify` Befehl zum Anwenden einer anderen Richtliniengruppe auf das Speicherobjekt.

Der folgende Befehl wendet die Richtliniengruppe an `pg-vs1` Zu SVM `vs1`:

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

Die folgenden Befehle wenden eine Richtliniengruppe an `pg-app` Auf die Volumes `app1` Und `app2`:

```
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. Überwachung der Richtliniengruppenleistung:

```
qos statistics performance show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.



Monitoring der Performance über das Cluster Verwenden Sie kein Tool auf dem Host, um die Leistung zu überwachen.

Mit dem folgenden Befehl wird die Performance der Richtliniengruppe angezeigt:

```
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. Monitoring der Workload-Performance:

```
qos statistics workload performance show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.



Monitoring der Performance über das Cluster Verwenden Sie kein Tool auf dem Host, um die Leistung zu überwachen.

Mit dem folgenden Befehl wird die Workload-Performance angezeigt:

```
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



Sie können das verwenden `qos statistics workload latency show` Befehl zum Anzeigen detaillierter Latenzstatistiken für QoS-Workloads

Durchsatzboden festlegen mit QoS

Sie können das verwenden `min-throughput` Feld für eine Richtliniengruppe zur Definition einer Durchsatzfläche für Storage-Objekt-Workloads (QoS Min.) Sie können die Richtliniengruppe anwenden, wenn Sie das Speicherobjekt erstellen oder ändern. Ab ONTAP 9.8 können Sie die Durchsatzfläche in IOPS oder MB/s oder IOPS und MB/s angeben.

Bevor Sie beginnen

- Sie müssen ONTAP 9.2 oder höher ausführen. Durchsatzböden sind ab ONTAP 9.2 verfügbar.
- Zum Erstellen einer Richtliniengruppe müssen Sie ein Cluster-Administrator sein.
- Ab ONTAP 9.13.1 lassen sich Durchsatzraten auf SVM-Ebene mithilfe eines erzwingen [Vorlage für adaptive Richtliniengruppen](#). Sie können keine Vorlage für adaptive Richtliniengruppen auf einer SVM mit einer QoS-Richtliniengruppe festlegen.

Über diese Aufgabe

- Ab ONTAP 9.4 können Sie mithilfe einer Richtliniengruppe ohne Shared_QoS festlegen, dass die definierte Durchsatzfläche auf jeden Workload der Mitglieder einzeln angewendet wird. Dies ist die einzige Bedingung, bei der eine Richtliniengruppe für eine Durchsatzboden auf mehrere Workloads angewendet werden kann.

Einstellen `-is-shared=false` Für das `qos policy-group create` Befehl zum Festlegen einer nicht freigegebenen Richtliniengruppe.

- Der Durchsatz für einen Workload könnte unter die angegebene Etage fallen, wenn auf dem Node oder Aggregat keine Performance-Kapazität (Reserve) vorhanden ist.
- Ein Storage-Objekt, das einem QoS-Limit unterliegt, muss von der SVM, der die Richtliniengruppe angehört, enthalten sein. Mehrere Richtliniengruppen können derselben SVM angehören.
- Es handelt sich um eine Best Practice bei QoS, eine Richtliniengruppe auf denselben Storage-Typ anzuwenden.
- Eine Richtliniengruppe mit Durchsatzboden kann nicht auf eine SVM angewendet werden.

Schritte

1. Prüfen Sie, ob auf dem Node oder Aggregat eine ausreichende Performance-Kapazität verfügbar ist, wie in beschrieben ["Identifizierung der verbleibenden Performance-Kapazität"](#).
2. Erstellen einer Richtliniengruppe:

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

Eine vollständige Befehlssyntax finden Sie in der man Page für Ihr ONTAP Release. Sie können das verwenden `qos policy-group modify` Befehl zum Anpassen der Durchsatzböden.

Mit dem folgenden Befehl wird die gemeinsam genutzte Richtliniengruppe erstellt `pg-vs2` Bei einem Minstdurchsatz von 1,000 IOPS:

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

Mit dem folgenden Befehl wird die nicht gemeinsam genutzte Richtliniengruppe erstellt `pg-vs4` Ohne Durchsatzbegrenzung:

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

3. Anwenden einer Richtliniengruppe auf ein Volume oder eine LUN:

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

Eine vollständige Befehlssyntax finden Sie in den man-Pages. Sie können das verwenden `_storage_object_modify` Befehl zum Anwenden einer anderen Richtliniengruppe auf das Speicherobjekt.

Der folgende Befehl wendet die Richtliniengruppe an `pg-app2` Auf das Volume `app2`:

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

4. Überwachung der Richtliniengruppenleistung:

```
qos statistics performance show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.



Monitoring der Performance über das Cluster Verwenden Sie kein Tool auf dem Host, um die Leistung zu überwachen.

Mit dem folgenden Befehl wird die Performance der Richtliniengruppe angezeigt:

```
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. Monitoring der Workload-Performance:

```
qos statistics workload performance show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.



Monitoring der Performance über das Cluster Verwenden Sie kein Tool auf dem Host, um die Leistung zu überwachen.

Mit dem folgenden Befehl wird die Workload-Performance angezeigt:

```
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



Sie können das verwenden `qos statistics workload latency show` Befehl zum Anzeigen detaillierter Latenzstatistiken für QoS-Workloads

Verwendung von adaptiven QoS-Richtliniengruppen

Mithilfe einer Richtliniengruppe „*Adaptive QoS*“ können Sie eine Durchsatzobergrenze oder -Stellfläche automatisch skalieren und bei sich änderungsem Volume das Verhältnis von IOPS zu GB/s. Wenn Sie Hunderte oder Tausende Workloads in einer großen Implementierung managen, bedeutet dies einen enormen Vorteil.

Bevor Sie beginnen

- Sie müssen ONTAP 9.3 oder höher ausführen. Adaptive QoS-Richtliniengruppen sind ab ONTAP 9.3 verfügbar.
- Zum Erstellen einer Richtliniengruppe müssen Sie ein Cluster-Administrator sein.

Über diese Aufgabe

Ein Storage-Objekt kann Mitglied einer adaptiven Richtliniengruppe oder einer nicht-adaptiven Richtliniengruppe sein, jedoch nicht beides. Die SVM des Storage-Objekts und die Richtlinie müssen identisch sein. Das Storage-Objekt muss online sein.

Adaptive QoS-Richtliniengruppen werden immer nicht gemeinsam genutzt: Die definierte Durchsatzdecke oder -Etage wird für jeden Workload der Mitglieder einzeln angewendet.

Das Verhältnis der Durchsatzbegrenzungen zum Storage-Objektgröße wird durch die Interaktion der folgenden Felder bestimmt:

- `expected-iops` Ist der erwartete Mindestwert für IOPS pro zugewiesenem TB GB.



``expected-iops`` Wird nur auf AFF Plattformen garantiert.
``expected-iops`` Wird für FabricPool nur garantiert, wenn die Tiering-Richtlinie auf „keine“ eingestellt ist und keine Blöcke in der Cloud liegen. ``expected-iops`` Ist garantiert für Volumes die nicht in einer SnapMirror synchronen Beziehung sind.

- `peak-iops` Ist die maximal mögliche IOPS pro zugewiesenem oder belegtem TB.

- `expected-iops-allocation` Gibt an, ob der zugewiesene Speicherplatz (Standard) bzw. der genutzte Speicherplatz für erwartete iops verwendet wird.



`expected-iops-allocation` ist in ONTAP 9.5 und höher verfügbar. Es wird nicht unterstützt in ONTAP 9.4 und früher.

- `peak-iops-allocation` Gibt an, ob der zugewiesene Speicherplatz oder der genutzte Speicherplatz (der Standard) für verwendet werden `peak-iops`.
- `absolute-min-iops` Ist die absolute Mindestanzahl an IOPS. Sie können dieses Feld mit sehr kleinen Speicherobjekten verwenden. Es überschreibt beide `peak-iops` Und/oder `expected-iops` Wenn `absolute-min-iops` Ist größer als der berechnete `expected-iops`.

Beispiel: Wenn Sie einstellen `expected-iops` Bis zu 1,000 IOPS/TB, und die Volume-Größe beträgt weniger als 1 GB, wird der berechnet `expected-iops` Wird ein fraktionaler IOP sein. Der berechnet `peak-iops` Wird ein noch kleiner Bruchteil. Sie können dies durch die Einstellung vermeiden `absolute-min-iops` Auf einen realistischen Wert.

- `block-size` Gibt die I/O-Blockgröße der Anwendung an. Der Standardwert ist 32K. Gültige Werte sind 8K, 16K, 32K, 64K, BELIEBIG. IRGENDWELCHE bedeutet, dass die Blockgröße nicht durchgesetzt wird.

In der folgenden Tabelle sind drei Adaptive QoS-Richtliniengruppen verfügbar. Sie können diese Richtliniengruppen direkt auf ein Volume anwenden.

Standardrichtliniengruppe	Erwartete IOPS/TB	Max. IOPS/TB	Absolute IOPS-Minimum
extreme	6,144	12,288	1000
performance	2,048	4,096	500
value	128	512	75

Sie können einer Richtliniengruppe kein Speicherobjekt zuweisen, wenn das zugehörige Objekt oder seine untergeordneten Objekte einer Richtliniengruppe angehören. In der folgenden Tabelle sind die Einschränkungen aufgeführt.

Wenn Sie die folgende Zuordnung zuweisen:	Dann kann nicht zugewiesen werden...
SVM zu einer Richtliniengruppe	Alle Storage-Objekte, die der SVM in einer Richtliniengruppe enthalten sind
Volume zu einer Richtliniengruppe	Das Volume enthält SVM oder untergeordnete LUNs einer Richtliniengruppe
LUN einer Richtliniengruppe	Die LUN enthält Volume oder SVM zu einer Richtliniengruppe
Datei zu einer Richtliniengruppe	Die Datei mit Volume oder SVM in einer Richtliniengruppe

Schritte

1. Erstellung einer anpassungsfähigen QoS-Richtliniengruppe:

```
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
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.



-expected-iops-allocation Und -block-size Ist in ONTAP 9.5 und höher verfügbar. Diese Optionen werden in ONTAP 9.4 und früher nicht unterstützt.

Mit dem folgenden Befehl wird die adaptive QoS-Richtliniengruppe erstellt `adpg-app1` Mit `-expected-iops` Festlegen auf 300 IOPS/TB `-peak-iops` Festlegen auf 1,000 IOPS/TB `-peak-iops-allocation` Auf einstellen `used-space`, und `-absolute-min-iops` Auf 50 IOPS einstellen:

```
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. Anwenden einer anpassungsfähigen QoS-Richtliniengruppe auf ein Volume:

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

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

Mit dem folgenden Befehl wird die adaptive QoS Policy Group angewendet `adpg-app1` Auf Volumen `app1`:

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

Mit den folgenden Befehlen wird die standardmäßige adaptive QoS-Richtliniengruppe angewendet `extreme` Zum neuen Volume `app4` Und zum vorhandenen Volume `app5`. Die für die Richtliniengruppe definierte Durchsatzobergrenze gilt für Volumes `app4` Und `app5` Individuell:

```
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
```

Legen Sie eine Vorlage für adaptive Richtliniengruppen fest

Ab ONTAP 9.13.1 lassen sich Durchsatzraten und -decken auf SVM-Ebene mithilfe einer Vorlage für adaptive Richtliniengruppen durchsetzen.

Über diese Aufgabe

- Die Vorlage für die adaptive Richtliniengruppe ist eine Standardrichtlinie `apg1`. Die Richtlinie kann jederzeit geändert werden. Sie kann nur mit der CLI oder der ONTAP-REST-API festgelegt werden und kann nur auf vorhandene SVMs angewendet werden.
- Die Vorlage für die adaptive Richtliniengruppe wirkt sich nach Festlegen der Richtlinie nur auf Volumes aus, die auf der SVM erstellt oder auf sie migriert wurden. Vorhandene Volumes auf der SVM behalten ihren vorhandenen Status bei.

Wenn Sie die Vorlage für die adaptive Policy-Gruppe deaktivieren, behalten Volumes auf der SVM ihre vorhandenen Richtlinien. Nur Volumes, die anschließend auf der SVM erstellt oder zu dieser migriert wurden, werden von der Deaktivierung beeinträchtigt.

- Sie können keine Vorlage für adaptive Richtliniengruppen auf einer SVM mit einer QoS-Richtliniengruppe festlegen.
- Vorlagen für adaptive Richtliniengruppen wurden für AFF-Plattformen entwickelt. Eine Vorlage für adaptive Richtliniengruppen kann auf anderen Plattformen festgelegt werden, die Richtlinie kann jedoch keinen minimalen Durchsatz erzwingen. Auf ähnliche Weise können Sie einer SVM eine Vorlage für anpassungsfähige Richtliniengruppen in einem FabricPool Aggregat oder einem Aggregat hinzufügen, das keinen minimalen Durchsatz unterstützt, jedoch wird die Durchsatzmenge nicht durchgesetzt.
- Wenn sich die SVM in einer MetroCluster Konfiguration oder SnapMirror Beziehung befindet, wird die Vorlage für die adaptive Richtliniengruppe auf der gespiegelten SVM erzwungen.

Schritte

1. SVM so ändern, dass sie die Vorlage für die Gruppe der anpassbaren Richtlinien anwendet: `vserver modify -qos-adaptive-policy-group-template apg1`
2. Bestätigen Sie, dass die Richtlinie festgelegt wurde: `vserver show -fields qos-adaptive-policy-group`

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.