Ereignis- und Performance-Monitoring

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

Ereignis- und Performance-Monitoring

Überwachen Sie die Cluster-Performance mit System Manager

Überwachen Sie die Cluster Performance mit System Manager

Die Themen in diesem Abschnitt zeigen Ihnen, wie Sie den Cluster-Zustand und die Performance mit System Manager in ONTAP 9.7 und neueren Versionen verwalten.

Sie können die Cluster-Performance überwachen, indem Sie im System Manager Dashboard Informationen über das System anzeigen. Das Dashboard zeigt Informationen über wichtige Warnmeldungen und Benachrichtigungen, die Effizienz und Kapazität von Storage-Tiers und Volumes, die in einem Cluster verfügbaren Nodes, den Status der Nodes in einem HA-Paar, die aktivsten Applikationen und Objekte, an. Und die Performance-Kennzahlen eines Clusters oder Node.

Über das Dashboard können Sie die folgenden Informationen bestimmen:

- **Gesundheit**: Wie gesund ist der Cluster?
- **Kapazität**: Welche Kapazität steht auf dem Cluster zur Verfügung?
- **Performance**: Wie gut funktioniert der Cluster, basierend auf Latenz, IOPS und Durchsatz?
- **Netzwerk**: Wie wird das Netzwerk mit Hosts und Speicherobjekten konfiguriert, wie Ports, Schnittstellen und Storage VMs?

Klicken Sie in den Übersichten zu Systemzustand und Kapazität auf → Um zusätzliche Informationen anzuzeigen und Aufgaben auszuführen.

In der Leistungsübersicht können Sie Kennzahlen auf Basis der Stunde, des Tages, der Woche, des Monats oder des Jahres anzeigen.

In der Netzwerkübersicht wird die Anzahl der Objekte im Netzwerk angezeigt (z. B. „8 NVMe/FC-Ports“). Sie können auf die Nummern klicken, um Details zu den einzelnen Netzwerkobjekts anzuzeigen.

Anzeigen der Performance auf dem Cluster-Dashboard

Über das Dashboard können Sie fundierte Entscheidungen zum Hinzufügen oder Verschieben von Workloads treffen. Sie können auch die Spitzenzeiten nutzen, um potenzielle Änderungen zu planen.

Die Leistungswerte werden alle 3 Sekunden aktualisiert, und das Performance-Diagramm wird alle 15 Sekunden aktualisiert.

Schritte

1. Klicken Sie Auf **Dashboard**.
2. Wählen Sie unter **Leistung** das Intervall aus.

Identifizieren von Hot Volumes und anderen Objekten

Beschleunigen Sie die Cluster Performance, indem Sie die Volumes (Hot Volumes) und Daten (Hot Objects) identifizieren, auf die häufig zugegriffen wird.

Schritte

1. Klicken Sie Auf **Storage > Volumes**.
2. Filtern Sie die Spalten IOPS, Latenz und Durchsatz, um die häufig genutzten Volumes und Daten anzuzeigen.

QoS ändern

Ab ONTAP 9.8 ist bei der Bereitstellung von Storage QoS standardmäßig aktiviert. Sie können während des Bereitstellungsprozesses die QoS deaktivieren oder eine individuelle QoS-Richtlinie auswählen. Außerdem können Sie QoS nach der Bereitstellung des Storage ändern.

Schritte

1. Klicken Sie im System Manager auf **Storage** und wählen Sie **Volumes** aus.
2. Klicken Sie neben dem Volume, für das Sie QoS ändern möchten, auf ⋮ Und wählen Sie **Bearbeiten**.

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 Wartungsbenutzers, 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.

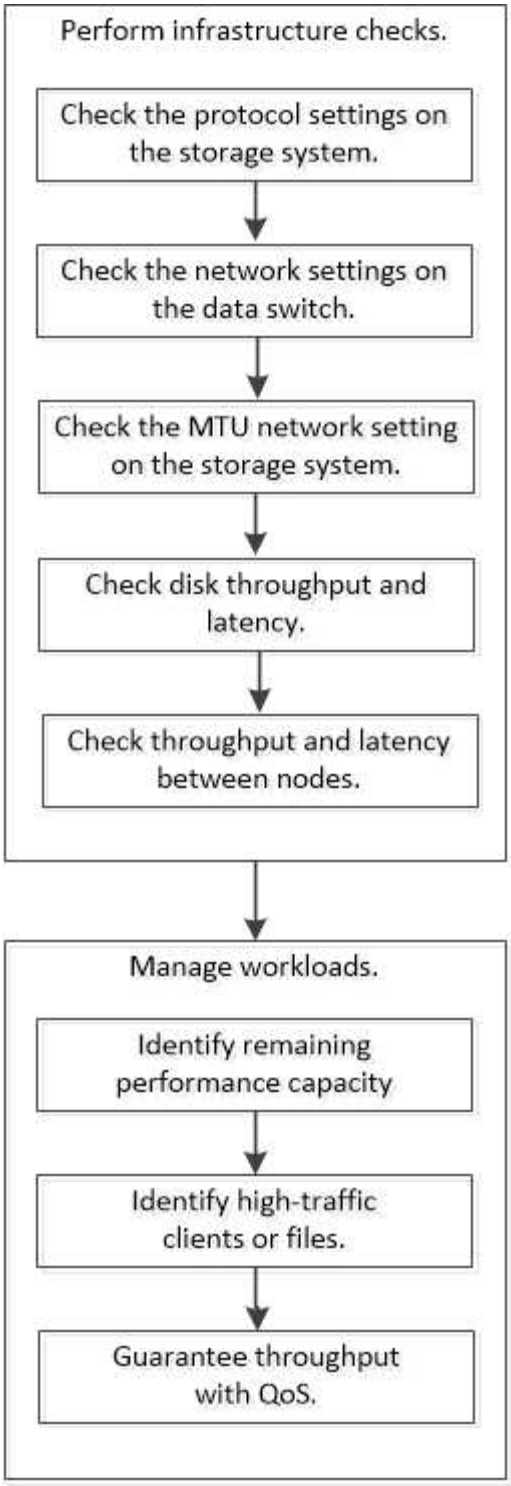
Verwandte Informationen

- "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 -vserv,er 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
                    Busy Total Read  Write  Read    Write   *Latency
  Disk       Node   (%)   Ops   Ops   Ops   (Bps)    (Bps)       (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 subtrahieren `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


                                          *Total
        Client Vserver           Node Protocol    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-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

Garantierter Durchsatz durch QoS

Durchsatz garantieren mit QoS-Übersicht

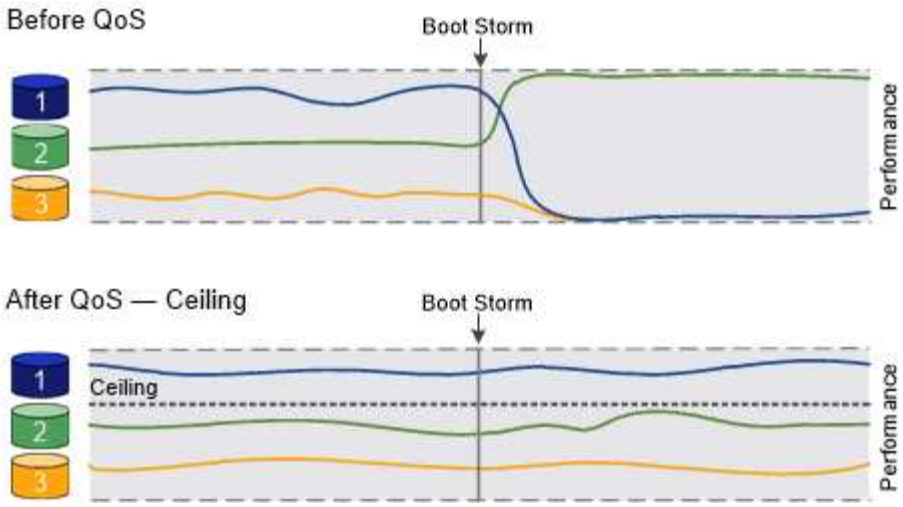
Dank Storage-Servicequalität (QoS) kann die Performance kritischer Workloads nicht durch konkurrierende Workloads beeinträchtigt werden. Sie können für einen konkurrierenden Workload eine Durchsatzbegrenzung festlegen, um die Auswirkungen auf Systemressourcen zu begrenzen oder für einen kritischen Workload 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 Richtliniengruppe 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



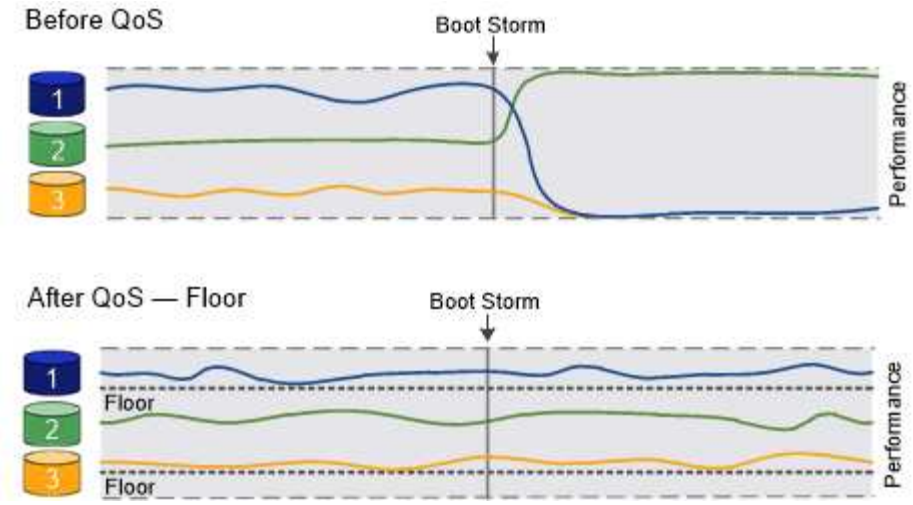
Allgemeines zu Durchsatzböden (QoS Min.)

Eine Durchsatzboden sorgt dafür, dass der Durchsatz für einen Workload nicht unter eine Mindestanzahl von IOPS oder MB/s bzw. IOPS und MB/s fällt. In der nachfolgenden Abbildung stellen die Durchsatzböden für Workload 1 und Workload 3 sicher, dass sie die Mindestanforderungen für den Durchsatz erfüllen, unabhängig vom Bedarf nach Workload 2.

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.

Eine Richtliniengruppe mit Durchsatzboden kann nicht auf eine SVM angewendet werden. Sie können den Boden beim Erstellen der Richtliniengruppe angeben oder warten, bis Sie die Workloads überwachen, um sie anzugeben.

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 Möglichkeit, das neue Verhalten von Floors v2 zu aktivieren/zu deaktivieren, ist in ONTAP 9.7P6 und höher verfügbar.bei kritischen Operationen wie z.B. Kann Eine Arbeitslast unter die angegebene Etage 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, behoben. 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 von ONTAP Select Premium mit SSD unterstützt.

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	• AFF • C190 • ONTAP Select Premium mit SSD *	• 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.	Ja.
SnapMirror Synchronous	Ja.	Nein	Nein	Ja.

*C190 und ONTAP Select Support sind ab Version ONTAP 9.6 verfügbar.

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	9.0	9.1	9.2	9.3	9.4 und höher	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	9.2	9.3	9.4 und höher	9.8 und höher
Datenmenge	ja	ja	ja	ja
Datei	Nein	ja	ja	ja

LUN	ja	ja	ja	ja
SVM	Nein	Nein	Nein	Nein
FlexGroup Volume	Nein	Nein	ja	ja
Qtrees *	Nein	Nein	Nein	ja
Mehrere Workloads pro Richtliniengruppe	Nein	Nein	ja	ja
Nicht gemeinsam genutzte Richtliniengruppen	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 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	9.3	9.4 und höher
Datenmenge	ja	ja
Datei	Nein	ja
LUN	Nein	ja
SVM	Nein	Nein
FlexGroup Volume	Nein	ja
Mehrere Workloads pro Richtliniengruppe	ja	ja
Nicht gemeinsam genutzte Richtliniengruppen	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	9.3 und früher	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	`qos settings throughput-floors-v2 -enable false`
Ebenen v2 aktivieren	`qos settings throughput-floors-v2 -enable true`

> 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
```

Storage-QoS-Workflow

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.

Was Sie benötigen

- 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.

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 Knoten oder Aggregat eine ausreichende Performance-Kapazität vorhanden ist, wie in Permalink beschrieben: Identify-remaining-Performance-Capacity-task.HTML[Identify verbleibende Performance Capacity].
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 Mindestdurchsatz 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.

Was Sie benötigen

- Sie müssen ONTAP 9.3 verwenden. 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
   ```

Überwachen Sie die Cluster-Performance mit Unified Manager

Mit Active IQ Unified Manager erhalten Sie maximale Verfügbarkeit und volle Kontrolle über Ihre NetApp AFF und FAS Storage-Infrastruktur. Sie verbessern somit die Skalierbarkeit, Kompatibilität, Performance und Sicherheit.

Active IQ Unified Manager überwacht den Systemzustand fortlaufend und sendet Alarmmeldungen, sodass IT-Mitarbeiter im Unternehmen entlastet werden können. Auf einem zentralen Dashboard können Sie den Storage-Status unmittelbar anzeigen und Probleme mithilfe empfohlener Maßnahmen beheben.

Das Datenmanagement wird dadurch vereinfacht, dass Sie den Storage proaktiv managen und Probleme schnell beheben können, indem Sie Informationen erkennen, überwachen und Benachrichtigungen erhalten.

Sie verbessern die Effizienz Ihrer Administration, da Sie Petabytes von Daten über ein einziges Dashboard überwachen und Ihre Daten bedarfsgerecht managen können.

Mit Active IQ Unified Manager können Sie mit wechselnden Geschäftsanforderungen Schritt halten und die Performance mithilfe von Performance-Daten und erweiterten Analysen optimieren. Die Berichtsfunktionen ermöglichen Ihnen den Zugriff auf Standardberichte oder die Erstellung benutzerdefinierter Betriebsberichte, die den spezifischen Anforderungen Ihres Unternehmens entsprechen.

Überwachen Sie die Cluster-Performance mit Cloud Insights

NetApp Cloud Insights ist ein Monitoring-Tool, mit dem Sie Ihre gesamte Infrastruktur im Blick haben. Es überwacht nicht nur alle Ressourcen, die in Public Clouds und privaten Datacentern liegen, sondern hilft auch dabei, Fehler aufzuspüren und den Ressourceneinsatz zu optimieren. Cloud Insights

Cloud Insights ist in zwei Versionen erhältlich

Die Cloud Insights Basic Edition wurde speziell für die Überwachung und Optimierung Ihrer NetApp Data-Fabric-Ressourcen konzipiert. Er bietet erweiterte Analysen für die Verbindungen zwischen allen NetApp Ressourcen, einschließlich HCI und All Flash FAS (AFF) innerhalb der Umgebung – kostenlos.

Der Schwerpunkt der Cloud Insights Standard Edition liegt nicht nur auf Infrastrukturkomponenten von NetApp Data Fabric, sondern auch auf Umgebungen mit unterschiedlichen Anbietern und Multi-Cloud-Umgebungen. Mit seinen verbesserten Funktionen können Sie auf Support für mehr als 100 Services und Ressourcen zugreifen.

In der heutigen Welt, mit Ressourcen im Spiel von Ihren On-Premises-Rechenzentren bis zu mehreren Public Clouds, ist es von entscheidender Bedeutung, das komplette Bild von der Applikation selbst zu der Backend-Festplatte des Speicher-Array haben. Zusätzliche Unterstützung für das Applikations-Monitoring (wie Kafka, MongoDB und Nginx) gibt Ihnen die nötigen Informationen und Erkenntnisse, um mit optimaler Auslastung und mit einem perfekten Risikopuffer arbeiten zu können.

Beide Versionen (Basic und Standard) lassen sich in NetApp Active IQ Unified Manager integrieren. Kunden, die Active IQ Unified Manager verwenden, können die Join-Informationen innerhalb der Cloud Insights-Benutzeroberfläche anzeigen. Benachrichtigungen, die auf Active IQ Unified Manager gepostet werden, werden nicht übersehen und können jetzt mit Ereignissen in Cloud Insights korreliert werden. Mit anderen Worten, Sie erhalten das Beste aus beiden Welten.

Alle Ressourcen überwachen, optimieren und Fehler beheben

Mit Cloud Insights können Sie erheblich schneller Probleme lösen und verhindern, dass diese sich auf Endbenutzer auswirken. Und die Kosten für die Cloud-Infrastruktur lassen sich senken. Risiken durch Bedrohungen von innen werden reduziert, da sich Daten mithilfe verwertbarer Informationen schützen lassen.

Cloud Insights macht Ihre gesamte Hybrid-Infrastruktur an einem Ort transparent – von der Public Cloud bis hin zum Datacenter. Zudem lassen sich sofort relevante Dashboards erstellen, die an Ihre spezifischen Anforderungen angepasst werden können. Sie können auch gezielte und bedingte Warnmeldungen erstellen, die spezifisch und relevant für die Anforderungen Ihres Unternehmens sind.

Dank erweiterter Anomalieerkennung können Sie Probleme proaktiv vorab beheben. Ressourcenkonflikte und Verschlechterungen können automatisch erkannt werden, sodass die betroffenen Workloads schnell wiederhergestellt werden können. Die Fehlerbehebung wird durch die automatisch erstellte Hierarchie der Beziehungen zwischen den verschiedenen Komponenten im Stack schneller erledigt.

Sie können ungenutzte oder verwaiste Ressourcen in Ihrer Umgebung identifizieren, um Möglichkeiten ausfindig zu machen, wie die Infrastruktur richtig dimensionieren und die gesamten Ausgaben optimieren können.

Cloud Insights visualisiert Ihre Systemtopologie und damit ein Verständnis der Kubernetes Architektur. Kunden können den Zustand der Kubernetes Cluster einschließlich problematischer Nodes überwachen und im Problemfall weitere Details einlesen.

Cloud Insights unterstützt Sie dabei, Unternehmensdaten vor Missbrauch durch böswillige oder kompromittierte Benutzer zu schützen. Dies erfolgt durch erweitertes Machine Learning und Anomalieerkennung, mit dem Sie relevante Informationen zu Bedrohungen von innen erhalten.

Cloud Insights ermöglicht die Visualisierung von Kubernetes-Kennzahlen, damit die Beziehungen zwischen Pods, Nodes und Clustern umfassend verstanden werden können. Sie können den Zustand eines Clusters oder eines Arbeitspodes sowie die aktuell verarbeitete Last beurteilen, sodass Sie den Befehl Ihres K8S-Clusters übernehmen und sowohl den Zustand als auch die Kosten Ihrer Bereitstellung kontrollieren können.

Filesystem-Analyse

File System Analytics – Übersicht

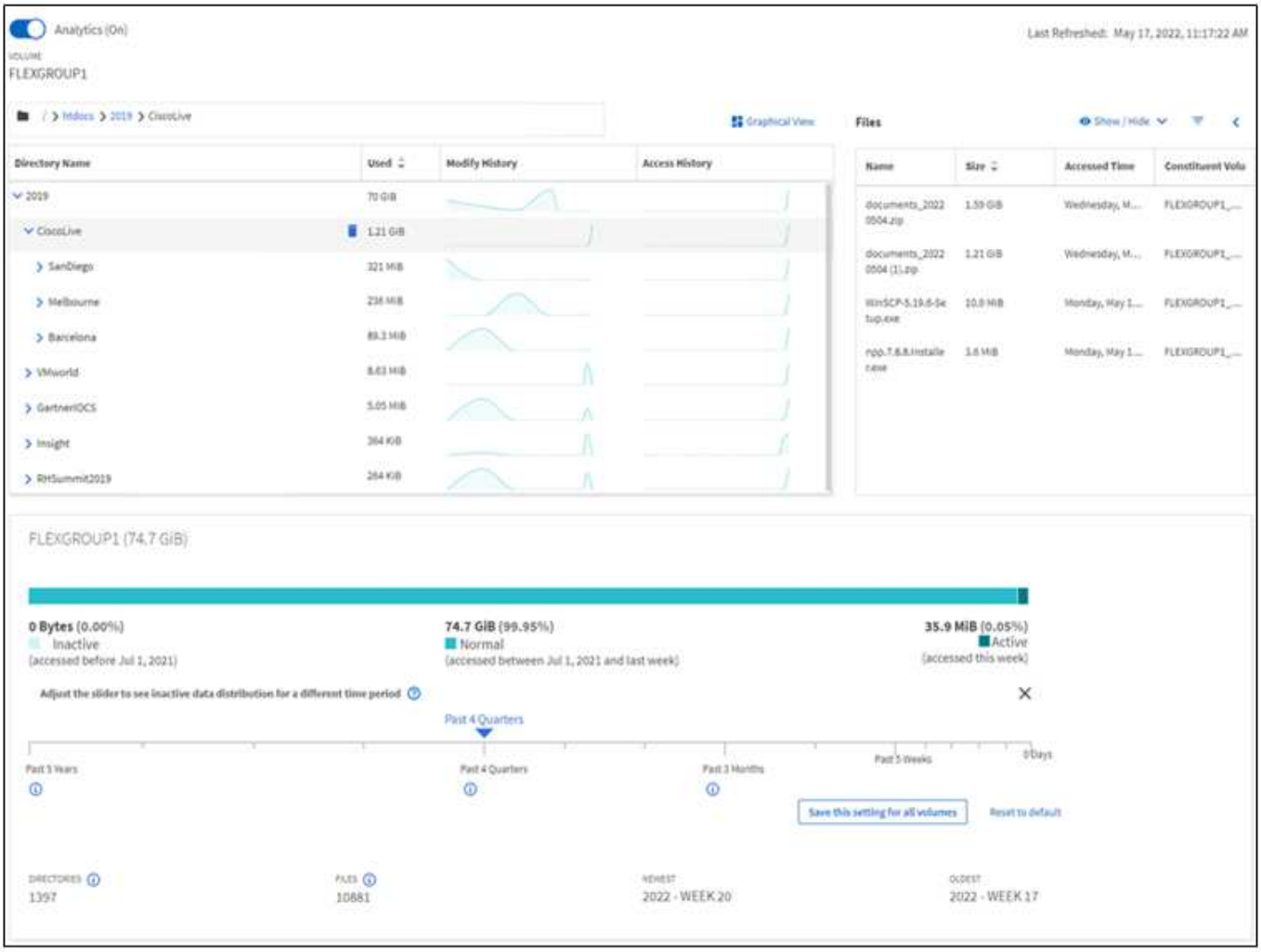
Die File System Analytics (FSA) wurde erstmals in ONTAP 9.8 eingeführt, um Echtzeiteinblick in die Dateinutzung und die Trends in der Storage-Kapazität in ONTAP FlexGroup oder FlexVol Volumes zu bieten. Diese native Funktion macht externe Tools überflüssig und bietet wichtige Einblicke in die Auslastung des Storage und gibt an, ob es Möglichkeiten zur Optimierung des Storage für Ihre geschäftlichen Anforderungen gibt.

Mit FSA haben Sie Sichtbarkeit auf allen Ebenen der Dateisystemhierarchie eines Volumes in NAS. Sie erhalten beispielsweise Einblicke in die Nutzung und Kapazität auf der Ebene der Storage VM (SVM), des Volumes, des Verzeichnisses und der Dateien. Sie können FSA verwenden, um Fragen wie:

- „Wie füllt ich meinen Storage aus? Kann ich große Dateien an einen anderen Speicherort verschieben?“
- Welche Volumes, Verzeichnisse und Dateien sind am aktivsten? Ist meine Storage-Performance für die Bedürfnisse meiner Benutzer optimiert?
- Wie viele Daten wurden im letzten Monat hinzugefügt?
- Wer sind meine aktivsten oder am wenigsten aktiven Storage-Nutzer?
- Wie viele inaktive oder inaktive Daten befinden sich auf meinem Primärspeicher? Kann ich diese Daten auf eine kostengünstigere kalte Tier verschieben?
- Wirken sich meine geplanten Änderungen an der Servicequalität negativ auf den Zugriff auf kritische, häufig genutzte Dateien aus?

Die Dateisystemanalyse ist in ONTAP System Manager integriert. Ansichten in System Manager bieten:

- Echtzeittransparenz für effektives Datenmanagement und Betrieb
- Echtzeit-Datenerfassung und -Aggregation
- Unterverzeichnis-, Dateigrößen und -Zählungen sowie zugehörige Performance-Profile
- Datei Alter Histogramme für ändern und Zugriff auf Historien



Unterstützte Volume-Typen

Die Dateisystemanalyse erlaubt Transparenz auf Volumes mit aktiven NAS-Daten mit Ausnahme von FlexCache Caches und SnapMirror Ziel-Volumes.

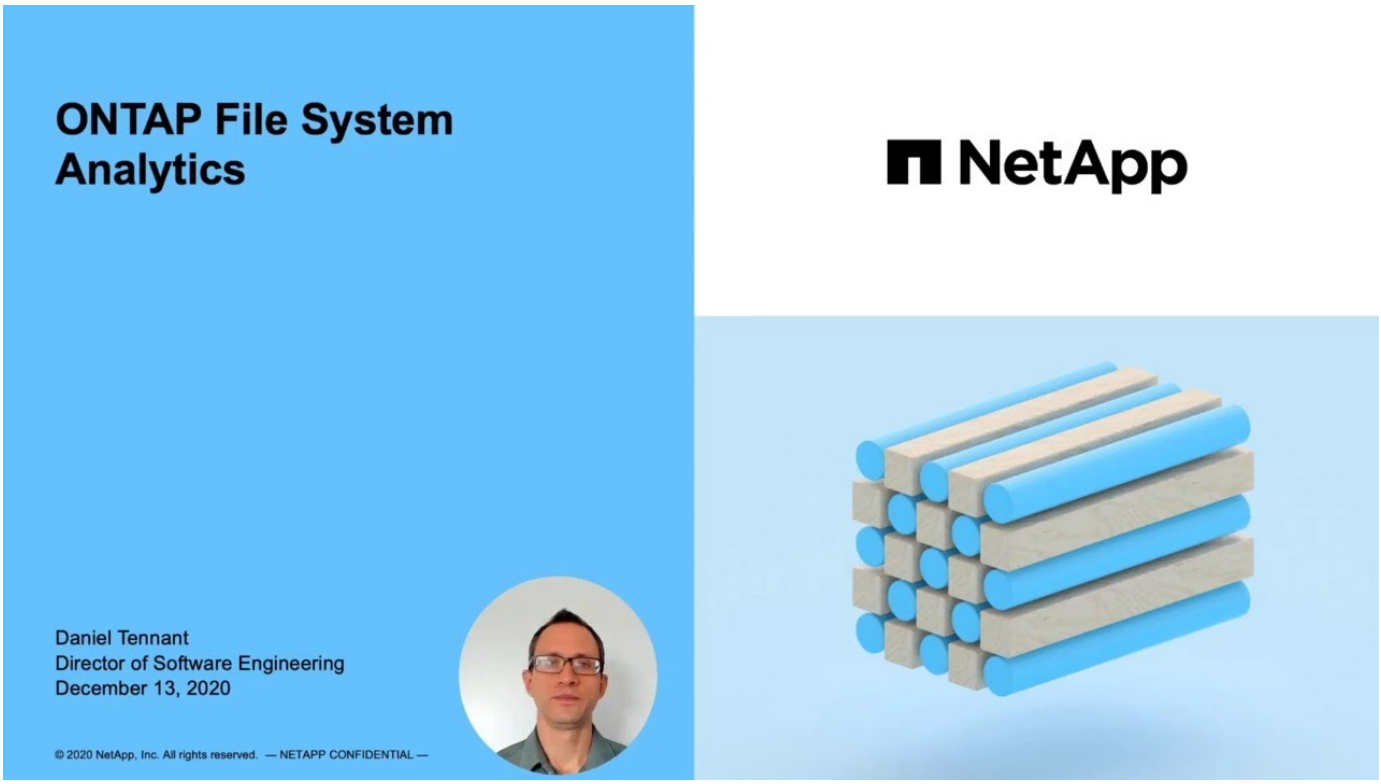
Verfügbarkeit der Filesystem-Analysefunktion

Jede ONTAP Version erweitert den Analysebereich von File System Analytics.

	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
Visualisierung in System Manager	X	X	X	X	X
Kapazitätsanalysen	X	X	X	X	X
Informationen zu inaktiven Daten	X	X	X	X	X
Unterstützung für Volumes, die aus Data ONTAP 7-Mode migriert wurden	X	X	X	X	
Möglichkeit zum Anpassen inaktiver Perioden in System Manager	X	X	X	X	
Aktivitätenverfolgung auf Volume-Ebene	X	X	X		

Vorgangsverfolgungsdaten in CSV herunterladen	X	X	X		
Aktivitätsverfolgung auf SVM-Ebene	X	X			
Zeitachse	X	X			
Nutzungsanalysen	X				

Erfahren Sie mehr über die Dateisystemanalyse



Weitere Informationen

- "TR 4687: Best-Practice Guidelines for ONTAP File System Analytics"
- "Knowledge Base: Hohe oder schwankende Latenz nach der Aktivierung von NetApp ONTAP File System Analytics"

Dateisystemanalyse Aktivieren

Um Nutzungsdaten wie Kapazitätsanalysen zu erfassen und anzuzeigen, müssen Sie die Dateisystemanalyse auf einem Volume aktivieren.

Ab ONTAP 9.8 können Sie die Dateisystemanalyse auf einem neuen oder vorhandenen Volume aktivieren. Wenn Sie ein System auf ONTAP 9.8 oder höher aktualisieren, stellen Sie sicher, dass alle Upgrade-Prozesse abgeschlossen wurden, bevor Sie die Dateisystemanalyse aktivieren.

Schritte

Je nach Größe und Inhalt des Volumes kann die Aktivierung der Analysen etwas Zeit in Anspruch nehmen, während ONTAP vorhandene Daten im Volume verarbeitet. System Manager zeigt den Fortschritt an und zeigt nach Abschluss Analysedaten an. Wenn Sie genauere Informationen über den Initialisierungsfortschritt benötigen, können Sie den CLI-Befehl ONTAP verwenden `volume analytics show`.

Sie können die Dateisystemanalyse mit ONTAP System Manager oder der CLI aktivieren.

System Manager

In ONTAP 9.8 und 9.9.1	Ab ONTAP 9.10.1
1. Wählen Sie **Storage > Volumes**. 2. Wählen Sie das gewünschte Volumen, und wählen Sie dann **Explorer**. 3. Wählen Sie **Analytics aktivieren** oder **Analytics deaktivieren**.	1. Wählen Sie **Storage > Volumes**. 2. Wählen Sie die gewünschte Lautstärke. Wählen Sie im Menü für einzelne Volumes die Option **Dateisystem > Explorer** aus. 3. Wählen Sie **Analytics aktivieren** oder **Analytics deaktivieren**.

CLI

So aktivieren Sie die Dateisystemanalyse mit der CLI:

1. Führen Sie den folgenden Befehl aus:
   `volume analytics on -vserver` *`svm_name`* `-volume` *`volume_name`* `[-foreground {true|false}]`Standardmäßig wird der Befehl im Vordergrund ausgeführt. ONTAP zeigt den Fortschritt an und zeigt nach Abschluss die Analysedaten an. Wenn Sie genauere Informationen benötigen, können Sie den Befehl im Hintergrund über die ausführen `-foreground false` Und dann verwenden Sie die `volume analytics show` Befehl zum Anzeigen des Initialisierungsfortschritts in der CLI.
2. Nach der erfolgreichen Aktivierung der Dateisystemanalyse zeigen Sie die Analysedaten mit ONTAP System Manager an.

Zeigen Sie die Dateisystemaktivität an

Nachdem die Dateisystemanalyse (FSA) aktiviert ist, können Sie den Inhalt des Stammverzeichnisses eines ausgewählten Volumes anzeigen, sortiert nach dem in den einzelnen Unterstrukturen verwendeten Speicherplatz.

Wählen Sie ein beliebiges Dateisystemobjekt aus, um das Dateisystem zu durchsuchen und detaillierte Informationen zu jedem Objekt in einem Verzeichnis anzuzeigen. Informationen zu Verzeichnissen können auch grafisch dargestellt werden. Im Laufe der Zeit werden für jede Unterstruktur historische Daten angezeigt. Der verwendete Platz wird nicht sortiert, wenn mehr als 3000 Verzeichnisse vorhanden sind.

Explorer

Der Bildschirm File System Analytics **Explorer** besteht aus drei Bereichen:

- Strukturansicht von Verzeichnissen und Unterverzeichnissen; erweiterbare Liste mit Namen, Größe, Änderungsverlauf und Zugriffsverlauf.
- Dateien: Name, Größe und Zugriffszeit für das in der Verzeichnisliste ausgewählte Objekt.
- Aktiver und inaktiver Datenvergleich für das in der Verzeichnisliste ausgewählte Objekt.

  Ab ONTAP 9.9 können Sie den Bereich für die Meldung anpassen. Der Standardwert ist ein Jahr. Auf der Grundlage dieser Anpassungen können Sie Korrekturmaßnahmen vornehmen, z. B. Volumes verschieben und die Tiering-Richtlinie ändern.

Die Zugriffszeit wird standardmäßig angezeigt. Wenn jedoch der Datenträger-Standard aus der CLI geändert wurde (durch Einstellen der `-atime-update` Option auf `false` Mit dem `volume modify` Befehl), dann wird

nur die letzte geänderte Zeit angezeigt. Beispiel:

- Die Baumansicht zeigt nicht die **Zugriffshistorie** an.
- Die Ansicht der Dateien wird geändert.
- Die aktive/inaktive Datenansicht basiert auf der geänderten Zeit (`mtime`).

Mithilfe dieser Anzeigen können Sie Folgendes überprüfen:

- Speicherorte von Dateisystemen, die den meisten Speicherplatz belegen
- Detaillierte Informationen zu einer Verzeichnisstruktur, einschließlich der Anzahl von Dateien und Unterverzeichnissen innerhalb von Verzeichnissen und Unterverzeichnissen
- Dateisystemstandorte, die alte Daten enthalten (z. B. Scratch-, Temp- oder Log-Bäume)

Beachten Sie bei der Interpretation der FSA-Ausgabe folgende Punkte:

- FSA zeigt an, wo und wann Ihre Daten in Gebrauch sind, nicht wie viele Daten verarbeitet werden. Ein großer Speicherverbrauch von kürzlich aufgerufenen oder geänderten Dateien bedeutet beispielsweise nicht unbedingt, dass die Verarbeitungslasten des Systems sehr hoch sind.
- Die Art und Weise, wie die Registerkarte **Volume Explorer** den Platzbedarf für FSA berechnet, kann von anderen Tools abweichen. Insbesondere könnten erhebliche Unterschiede zum Verbrauch im **Volume Overview** bestehen, wenn für das Volume Storage-Effizienzfunktionen aktiviert sind. Dies liegt daran, dass die Registerkarte **Volume Explorer** keine Effizienzeinsparungen enthält.
- Aufgrund von Platzbeschränkungen in der Verzeichnisanzeige ist es nicht möglich, eine Verzeichnistiefe von mehr als 8 Ebenen in der *Listenansicht* anzuzeigen. Um Verzeichnisse anzuzeigen, die mehr als 8 Ebenen tief sind, müssen Sie zu *Graphical View* wechseln, das gewünschte Verzeichnis suchen und dann zurück zu *List View* wechseln. Dadurch wird zusätzlicher Bildschirmbereich im Display angezeigt.

Schritte

1. Anzeigen des Root-Verzeichnis-Inhalts eines ausgewählten Volumes:

In ONTAP 9.8 und 9.9.1	Ab ONTAP 9.10.1
Klicken Sie auf **Storage > Volumes**, wählen Sie das gewünschte Volumen aus und klicken Sie dann auf **Explorer**.	Wählen Sie **Storage > Volumes**, wählen Sie das gewünschte Volumen aus. Wählen Sie im Menü für einzelne Volumes die Option **Dateisystem > Explorer** aus.

Aktivitäts-Tracking Aktivieren

Seit ONTAP 9.10.1 umfasst die Dateisystemanalyse eine Funktion zur Verfolgung von Aktivitäten, mit der Sie Hot Objects identifizieren und als CSV-Datei herunterladen können. Ab ONTAP 9.11.1 ist das Activity Tracking auf den SVM-Umfang erweitert. Seit ONTAP 9.11.1 verfügt der System Manager über eine Zeitleiste zur Verfolgung von Aktivitäten, mit der Sie bis zu fünf Minuten Daten zur Aktivitätsverfolgung durchschauen können.

Die Verfolgung von Aktivitäten ermöglicht die Überwachung in vier Kategorien:

- Verzeichnisse

- Dateien
- Clients
- Benutzer

Für jede überwachte Kategorie werden Lese-IOPS, Schreib-IOPS, Lese-Durchsätze und Schreibdurchsätze angezeigt. Abfragen zum Aktualisieren der Aktivität alle 10 bis 15 Sekunden, die sich auf Hotspots beziehen, die im System im vorherigen Intervall von fünf Sekunden angezeigt werden.

Informationen zur Vorgangsverfolgung sind ungefähre Angaben, und die Genauigkeit der Daten hängt von der Verteilung des eingehenden I/O-Datenverkehrs ab.

Wenn Sie in System Manager die Aktivitäts-Tracking-Funktion auf Volume-Ebene anzeigen, wird nur das Menü des erweiterten Volumes aktiv aktualisiert. Wenn die Ansicht von Volumes ausgeblendet ist, werden sie erst aktualisiert, wenn die Volume-Anzeige erweitert wird. Sie können die Aktualisierungen mit der Schaltfläche **Aktualisieren anhalten** anhalten. Vorgangsdaten können in einem CSV-Format heruntergeladen werden, das alle für das ausgewählte Volume erfassten Point-in-Time-Daten anzeigt.

Mit der ab ONTAP 9.11.1 verfügbaren Zeitachsenfunktion können Sie eine Aufzeichnung der Hotspot-Aktivitäten auf einem Volume oder einer SVM aufbewahren. Sie aktualisieren kontinuierlich ungefähr alle fünf Sekunden und behalten die Daten der letzten fünf Minuten. Zeitachsendaten werden nur für Felder gespeichert, die auf der Seite sichtbar sind. Wenn Sie eine Tracking-Kategorie ausblenden oder scrollen, damit die Zeitleiste nicht mehr angezeigt wird, wird die Datenerfassung durch die Zeitleiste unterbrochen. Standardmäßig sind die Zeitleisten deaktiviert und werden automatisch deaktiviert, wenn Sie von der Registerkarte „Vorgang“ wegnavigieren.

Aktivitäts-Tracking für ein einzelnes Volume aktivieren

Sie können die Aktivitätsverfolgung mit ONTAP System Manager oder der ONTAP-CLI aktivieren.

Über diese Aufgabe

Wenn Sie RBAC mit der ONTAP REST API oder System Manager verwenden, müssen Sie benutzerdefinierte Rollen erstellen, um den Zugriff auf die Verfolgung von Aktivitäten zu managen. Siehe Rollenbasierte Zugriffssteuerung Für diesen Prozess.

System Manager

Schritte

1. Wählen Sie **Storage > Volumes**. Wählen Sie das gewünschte Volumen aus. Wählen Sie im Menü für einzelne Volumes die Option Dateisystem und anschließend die Registerkarte Aktivität aus.
2. Stellen Sie sicher, dass **Activity Tracking** aktiviert ist, um einzelne Berichte auf Top-Verzeichnissen, Dateien, Clients und Benutzern anzuzeigen.
3. Um Daten ohne Aktualisierungen in größerer Tiefe zu analysieren, wählen Sie **Aktualisieren anhalten**. Sie können die Daten auch herunterladen, um einen CSV-Datensatz des Berichts zu erhalten.

CLI

Schritte

1. Verfolgung Von Aktivitäten Aktivieren:

   ```
   volume activity-tracking on -vsverver svm_name -volume volume_name
   ```

2. Sie können mit dem Befehl überprüfen, ob der Status der Aktivitätsüberwachung für ein Volume ein- oder ausgeschaltet ist:

   ```
   volume activity-tracking show -vsverver svm_name -volume volume_name -state
   ```

3. Wenn die Option aktiviert ist, können Sie die Daten zur Aktivitätsverfolgung mithilfe von ONTAP System Manager oder der ONTAP REST API anzeigen.

Aktivitäts-Tracking für mehrere Volumes aktivieren

Sie können mit System Manager die Activity Tracking für mehrere Volumes gleichzeitig aktivieren.

Über diese Aufgabe

Wenn Sie RBAC mit der ONTAP REST API oder System Manager verwenden, müssen Sie benutzerdefinierte Rollen erstellen, um den Zugriff auf die Verfolgung von Aktivitäten zu managen. Siehe Rollenbasierte Zugriffssteuerung Für diesen Prozess.

Für bestimmte Volumes

Schritte

1. Wählen Sie **Storage > Volumes**. Wählen Sie das gewünschte Volumen aus. Wählen Sie im Menü für einzelne Volumes die Option Dateisystem und anschließend die Registerkarte Aktivität aus.
2. Wählen Sie die Volumes aus, auf denen die Vorgangsverfolgung aktiviert werden soll. Wählen Sie oben in der Lautstärkeliste die Schaltfläche **Weitere Optionen**. Wählen Sie **Activity Tracking Aktivieren**.
3. Um die Vorgangsverfolgung auf SVM-Ebene anzuzeigen, wählen Sie die spezifische SVM aus, die Sie in **Storage > Volumes** anzeigen möchten. Navigieren Sie zur Registerkarte Dateisystem, dann zu „Vorgang“, und Sie sehen Daten für die Volumes, auf denen die Aktivitätsverfolgung aktiviert ist.

Für alle Volumes einer SVM

Schritte

1. Wählen Sie **Storage > Volumes**. Wählen Sie eine SVM aus dem Menü aus.
2. Navigieren Sie zur Registerkarte **Dateisystem** und wählen Sie die Registerkarte **Mehr**, um die Vorgangsverfolgung auf allen Volumes in der SVM zu aktivieren.

Analysen von der Nutzung ermöglichen

Durch das Tracking von Verzeichnissen nach Größe können Sie wichtige Daten über die Verzeichnisse in einem Volume unter Verwendung des größten Speicherplatzes erfassen. Das Tracking von Verzeichnissen nach Größe ist ab ONTAP 9.12.1 verfügbar und bietet:

- Die Gesamtzahl der Verzeichnisse im Volume
- Die Gesamtzahl der Dateien im Volume
- Ein Balkendiagramm, das die größten Verzeichnisse im Volumen nach Größe in absteigender Reihenfolge identifiziert

Das Tracking für große Verzeichnisse aktualisiert sich alle 15 Minuten. File System Analytics beschränkt die Berichterstellung von großen Verzeichnissen auf die 25 Verzeichnisse, die den meisten Speicherplatz verbrauchen.

Sie können die aktuellste Aktualisierung überwachen, indem Sie oben auf der Seite den Zeitstempel **Letzte Aktualisierung** auswählen. Zusätzlich können Sie die Tracking-Daten mit der **Download**-Schaltfläche in ein Excel-Arbeitsbuch herunterladen. Der Download-Vorgang wird im Hintergrund ausgeführt und enthält die zuletzt gemeldeten Informationen für das ausgewählte Volume.

Wenn der Scan ohne Ergebnisse zurückkehrt, stellen Sie sicher, dass das Volumen online ist. Ereignisse wie SnapRestore führen dazu, dass die Dateisystemanalyse die Liste der großen Verzeichnisse neu erstellt.

Schritte

1. Wählen Sie **Storage > Volumes**. Wählen Sie das gewünschte Volumen aus.
2. Wählen Sie im Menü für einzelne Volumes die Option **Dateisystem** aus. Wählen Sie dann die Registerkarte **Verwendung** aus.
3. Schalten Sie den Schalter **Analytics** ein, um die Nutzungsanalyse zu aktivieren.
4. System Manager zeigt ein Balkendiagramm an, in dem die Verzeichnisse mit der größten Größe in absteigender Reihenfolge identifiziert werden.

ONTAP zeigt möglicherweise teilweise oder gar keine Daten an, während die Liste der Top-Verzeichnisse erfasst wird. Der Fortschritt des Scans kann auf der Registerkarte **Verwendung** angezeigt werden, die während des Scans angezeigt wird.

Weitere Informationen zu einem beliebigen Verzeichnis erhalten Sie, indem Sie das Verzeichnis auswählen, um zur Registerkarte Explorer zu gelangen. Weitere Informationen über die Registerkarte **Explorer** finden Sie unter Zeigen Sie die Aktivität auf einem Dateisystem an.

Durchführung von Korrekturmaßnahmen basierend auf Analysen

Ab ONTAP 9.9 können Sie Korrekturmaßnahmen auf Basis aktueller Daten und gewünschter Ergebnisse direkt aus den Dateisystemanalysen-Anzeigen durchführen.

Wenn die Analyse aktiviert ist, können Sie die folgenden Aktionen durchführen:

- Löschen von Verzeichnissen und Dateien

  In der Explorer-Anzeige können Sie Verzeichnisse oder einzelne Dateien zum Löschen auswählen. Verzeichnisse werden mit der Funktion zum Löschen von Schnellverzeichnissen mit geringer Latenz gelöscht. (Schnelles Löschen von Verzeichnissen ist ab ONTAP 9.9.1 auch verfügbar, ohne dass die Analyse aktiviert ist.)

- Weisen Sie Medienkosten auf Storage-Tiers zu, um die Kosten inaktiver Storage-Standorte zu vergleichen

  Medienkosten sind ein Wert, den Sie basierend auf der Evaluierung der Storage-Kosten zuweisen. Diese Werte werden als Währung pro GB angegeben. Wenn die Einstellung festgelegt ist, verwendet System Manager die zugewiesenen Medienkosten, um die geschätzten Einsparungen beim Verschieben von Volumes zu projizieren.

  Die von Ihnen festgelegten Medienkosten sind nicht dauerhaft; sie können nur für eine einzelne Browsersitzung festgelegt werden.

- Verschieben Sie Volumes, um die Storage-Kosten auf Basis von Analysen und Kostenvergleichen für Medien zu senken. Verschieben Sie Volumes auf kostengünstigeren Storage in lokalen Tiers.

  Es kann jeweils nur ein Volume verglichen und verschoben werden.

Um diese Aktion auszuführen…	Schritte Unternehmen…
Verzeichnisse oder Dateien löschen	1. Klicken Sie auf **Storage > Volumes** und dann auf **Explorer**. Wenn Sie den Mauszeiger über eine Datei oder einen Ordner bewegen, wird die Option zum Löschen angezeigt. Sie können jeweils nur ein Objekt löschen. Wenn Verzeichnisse und Dateien gelöscht werden, werden die neuen Speicherkapazitätswerte nicht sofort angezeigt.

Kostenvergleich durch Medien aktivieren	1. Klicken Sie auf **Storage > Tiers** und dann auf **Media Cost** in den gewünschten Kacheln der lokalen Ebene (Aggregate). Achten Sie darauf, aktive und inaktive Ebenen auszuwählen, um den Vergleich zu ermöglichen. 2. Geben Sie eine Währungstyp und einen Betrag ein. Wenn Sie die Medienkosten eingeben oder ändern, wird die Änderung in allen Medientypen vorgenommen.
Verschieben Sie Volumes in eine kostengünstigere Tier	1. Klicken Sie nach der Aktivierung der Medienkostenanzeige auf **Storage > Tiers** und dann auf **Volumes**. 2. Klicken Sie auf, um die Zieloptionen für ein Volume zu vergleichen ⋮ Klicken Sie für den Volume dann auf **Move**. 3. Wählen Sie in der Anzeige **Lokales Tier auswählen** Zielebenen aus, um die geschätzte Kostendifferenz anzuzeigen. 4. Wählen Sie nach dem Vergleich der Optionen die gewünschte Ebene aus und klicken Sie auf **Verschieben**.

Rollenbasierte Zugriffssteuerung mit Filesystem-Analyse

Ab ONTAP 9.12.1 enthält ONTAP eine vordefinierte Rolle zur rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) `admin-no-fsa`. Der `admin-no-fsa` Rolle gewährt Berechtigungen auf Administratorebene, verhindert jedoch, dass der Benutzer Vorgänge im Zusammenhang mit dem ausführt `files` endpunkt (d. h. Dateisystemanalyse) ist in der ONTAP CLI, DER REST-API und in System Manager enthalten.

Weitere Informationen zum `admin-no-fsa` Rolle, siehe Vordefinierte Rollen für Cluster-Administratoren.

Wenn Sie eine Version von ONTAP verwenden, die vor ONTAP 9.12.1 veröffentlicht wurde, müssen Sie eine dedizierte Rolle erstellen, um den Zugriff auf Dateisystemanalysen zu steuern. Vor ONTAP Versionen von ONTAP 9.12.1 müssen Sie RBAC-Berechtigungen über die ONTAP CLI oder die ONTAP REST API konfigurieren.

System Manager

Ab ONTAP 9.12.1 können Sie RBAC-Berechtigungen für die Dateisystemanalyse mit System Manager konfigurieren.

Schritte

1. Wählen Sie **Cluster > Einstellungen**. Navigieren Sie unter **Sicherheit** zu **Benutzer und Rollen** und wählen Sie →.
2. Wählen Sie unter **Rollen** die Option + Add .
3. Geben Sie einen Namen für die Rolle ein. Konfigurieren Sie unter Rollenattribute den Zugriff oder die Einschränkungen für die Benutzerrolle, indem Sie das entsprechende festlegen "API-Endpunkte". In der folgenden Tabelle finden Sie primäre Pfade und sekundäre Pfade zum Konfigurieren von Zugriff oder Einschränkungen bei der Dateisystemanalyse.

Einschränkung	Primärer Pfad	Sekundärer Pfad
Verfolgung von Aktivitäten auf Volumes	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
Verfolgung von Aktivitäten auf SVMs	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
Alle Dateisystemanalysen	`/api/storage/volumes`	`/:uuid/files`

   Verwenden Sie können `/*/` Statt einer UUID zur Festlegung der Richtlinie für alle Volumes oder SVMs am Endpunkt.

   Wählen Sie die Zugriffsberechtigungen für jeden Endpunkt aus.

4. Wählen Sie **Speichern**.
5. Informationen zum Zuweisen der Rolle zu einem Benutzer oder Benutzer finden Sie unter Kontrolle des Administratorzugriffs.

CLI

Wenn Sie eine vor ONTAP 9.12.1 veröffentlichte ONTAP Version verwenden, erstellen Sie eine

benutzerdefinierte Rolle mithilfe der CLI von ONTAP.

Schritte

1. Erstellen Sie eine Standardrolle, um Zugriff auf alle Funktionen zu haben.

   Dies muss vor der Erstellung der restriktiven Rolle erfolgen, um sicherzustellen, dass die Rolle nur auf der Verfolgung von Aktivitäten beschränkt ist:

   ```
   security login role create -cmddirname DEFAULT -access all -role
   storageAdmin
   ```

2. Erstellen Sie die restriktive Rolle:

   ```
   security login role create -cmddirname "volume file show-disk-usage"
   -access none -role storageAdmin
   ```

3. Autorisieren Sie Rollen für den Zugriff auf die Web-Services der SVM:

   - `rest` Für REST-API-Aufrufe
   - `security` Für den Kennwortschutz
   - `sysmgr` Für System Manager Zugriff

     ```
     vserver services web access create -vserver svm-name -name_ -name rest
     -role storageAdmin

     vserver services web access create -vserver svm-name -name security
     -role storageAdmin
     ```

   ```
   vserver services web access create -vserver svm-name -name sysmgr -role
   storageAdmin
   ```

4. Erstellen Sie einen Benutzer.

   Sie müssen für jede Anwendung, die Sie auf den Benutzer anwenden möchten, einen eindeutigen Erstellungsbefehl ausgeben. Beim Aufruf Erstellen mehrfach auf demselben Benutzer werden einfach alle Anwendungen auf einen Benutzer angewendet und nicht jedes Mal ein neuer Benutzer erstellt. Der `http` Parameter für Applikationstyp gilt für die ONTAP REST API und System Manager.

   ```
   security login create -user-or-group-name storageUser -authentication
   -method password -application http -role storageAdmin
   ```

5. Mit den neuen Benutzeranmeldeinformationen können Sie sich jetzt bei System Manager anmelden oder über die ONTAP REST-API auf Daten zur Analyse von Dateisystemen zugreifen.

Weitere Informationen

- Vordefinierte Rollen für Cluster-Administratoren
- Steuern Sie den Administratorzugriff mit System Manager
- "Erfahren Sie mehr über RBAC-Rollen und die ONTAP REST API"

Überlegungen zur Dateisystemanalyse

Sie sollten bestimmte Nutzungsbeschränkungen und potenzielle Performance-Auswirkungen im Zusammenhang mit der Implementierung von File System Analytics kennen.

SVM-geschützte Beziehungen

Wenn Sie die Dateisystemanalyse auf Volumes aktiviert haben, deren SVM sich in einer Sicherungsbeziehung befindet, werden die Analysedaten nicht auf der Ziel-SVM repliziert. Wenn die Quell-SVM in einem Recovery-Vorgang erneut synchronisiert werden muss, müssen Sie die Analysen auf gewünschten Volumes nach der Recovery manuell erneut aktivieren.

Überlegungen zur Performance

In einigen Fällen kann die Aktivierung von Filesystem-Analysen die Performance während der ersten Metadatensammlung beeinträchtigen. Dies wird meist auf Systemen mit maximaler Auslastung beobachtet. Um Analysen auf solchen Systemen zu vermeiden, können Sie Tools zum Performance-Monitoring von ONTAP System Manager verwenden.

Wenn die Latenz deutlich erhöht wird, lesen Sie den Artikel in der Knowledge Base "Hohe oder schwankende Latenz nach Aktivierung von NetApp ONTAP File System Analytics".

EMS-Konfiguration

EMS-Konfigurationsübersicht

Sie können ONTAP 9 schnell konfigurieren, um wichtige EMS-Ereignisbenachrichtigungen (Event Management System) direkt an eine E-Mail-Adresse, einen Syslog-Server, ein Simple Management Network Protocol (SNMP) traphost oder EINEN REST-API-Server zu senden, sodass Sie sofort über Systemprobleme informiert werden, bei denen eine sofortige Aufmerksamkeit erforderlich ist.

Um die wichtigsten Aktivitäten in Ihrem System zu überwachen, müssen Sie die wichtigen EMS-Ereignisse überwachen.

Da wichtige Ereignisbenachrichtigungen standardmäßig nicht aktiviert sind, müssen Sie das EMS so konfigurieren, dass Benachrichtigungen entweder an eine E-Mail-Adresse, einen Syslog-Server, einen SNMP traphost oder REST API-Server gesendet werden.

Konfigurieren Sie EMS-Ereignisbenachrichtigungen für wichtige Ereignisse, wenn Folgendes zutrifft:

- Sie implementieren eines der folgenden Szenarien:
  - Sie einrichten ein neues System mit ONTAP 9, das nicht über EMS konfiguriert ist.
  - Sie haben ein System, auf dem ONTAP 9 ausgeführt wird und das über kein EMS konfiguriert ist.
  - Sie aktualisieren gerade auf ONTAP 9, das nicht über EMS konfiguriert ist.
  - Sie haben gerade den Übergang von Data ONTAP im 7-Mode zu ONTAP 9 abgeschlossen.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie wollen nicht viel konzeptuellen Hintergrund lesen.

Den EMS-Veranstaltungskatalog finden Sie unter Weitere Ressourcen auf dieser Seite: "ONTAP 9 Produktbibliothek". Siehe Konvertieren Sie das Routing für ältere Ereignisse in Ereignisbenachrichtigungen Weitere Informationen zur Durchführung der Benachrichtigungsbasierten Modellkonvertierung. Sie können auch auf die verweisen "EMS-Referenz".

Konfigurieren Sie EMS-Ereignisbenachrichtigungen und -Filter mit System Manager

Mit System Manager können Sie konfigurieren, wie das Event Management System (EMS) Ereignisbenachrichtigungen bereitstellt, sodass Sie über Systemprobleme informiert werden können, bei denen Ihre Eingabeaufforderung angezeigt wird.

ONTAP-Version	Die Vorzüge von System Manager:
ONTAP 9.12.1 und höher	Geben Sie das TLS-Protokoll (Transport Layer Security) an, wenn Ereignisse an Remote-Syslog-Server gesendet werden.
ONTAP 9.10.1 und höher	Konfigurieren Sie E-Mail-Adressen, Syslog-Server und Webhook-Anwendungen sowie SNMP-Traphosts.
ONTAP 9.7 auf 9.10.0	Konfigurieren Sie nur SNMP-Trap-Hosts. Sie können ein anderes EMS-Ziel mit der ONTAP CLI konfigurieren. Siehe "EMS-Konfigurationsübersicht".

Sie können folgende Aktionen durchführen:

- [add-ems-destination]
- [create-ems-filter]
- [edit-ems-destination]
- [edit-ems-filter]
- [delete-ems-destination]
- [delete-ems-filter]

Verwandte Informationen

- "EMS-Ereigniskatalog"
- "Mit der CLI können Sie SNMP-Traphosts für den Empfang von Ereignisbenachrichtigungen konfigurieren"

Fügen Sie ein EMS-Ereignisbenachrichtigungs-Ziel hinzu

Sie können mit System Manager angeben, an welche Empfänger von EMS-Nachrichten gesendet werden sollen.

Ab ONTAP 9.12.1 können EMS-Ereignisse über das TLS-Protokoll (Transport Layer Security) an einen bestimmten Port auf einem Remote-Syslog-Server gesendet werden. Weitere Informationen finden Sie im `event notification destination create` Man-Page.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.

2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisziele** aus.
4. Klicken Sie Auf + Add .
5. Geben Sie einen Namen, einen EMS-Zieltyp und Filter an.

   ⓘ Bei Bedarf können Sie einen neuen Filter hinzufügen. Klicken Sie auf **Neuen Ereignisfilter hinzufügen**.

6. Geben Sie je nach gewähltem EMS-Zieltyp Folgendes an:

So konfigurieren Sie…	… angeben oder auswählen
SNMP traphost	• TrapHost-Name
E-Mail (Ab 9.10.1)	• E-Mail-Adresse des Zielorts • Mailserver • Von E-Mail-Adresse
Syslog-Server (Ab 9.10.1)	• Hostname oder IP-Adresse des Servers • Syslog-Port (beginnend mit 9.12.1) • Syslog-Transport (ab 9.12.1) Durch die Auswahl von **TCP Encrypted** wird das TLS-Protokoll (Transport Layer Security) aktiviert. Wenn für **Syslog-Port** kein Wert eingegeben wird, wird ein Standard basierend auf der Auswahl **Syslog Transport** verwendet.
Webhook (Ab 9.10.1)	• Webhook-URL • Clientauthentifizierung (wählen Sie diese Option, um ein Clientzertifikat anzugeben)

Erstellen Sie einen neuen EMS-Ereignisbenachrichtigungs-Filter

Ab ONTAP 9.10.1 können Sie mit System Manager neue benutzerdefinierte Filter definieren, die die Regeln für den Umgang mit EMS-Benachrichtigungen festlegen.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisfilter** aus.
4. Klicken Sie Auf + Add .
5. Geben Sie einen Namen an, und wählen Sie aus, ob Regeln aus einem vorhandenen Ereignisfilter kopiert oder neue Regeln hinzugefügt werden sollen.

6. Führen Sie je nach Ihrer Wahl die folgenden Schritte aus:

Wenn Sie… auswählen.	Führen Sie dann diese Schritte… aus
Regeln aus vorhandenem Ereignisfilter kopieren	1. Wählen Sie einen vorhandenen Ereignisfilter aus. 2. Ändern Sie die vorhandenen Regeln. 3. Fügen Sie bei Bedarf weitere Regeln hinzu, indem Sie auf klicken + Add .
Neue Regeln hinzufügen	Geben Sie für jede neue Regel Typ, Namensmuster, Schweregrade und SNMP-Trap-Typ an.

Bearbeiten Sie ein EMS-Ereignisbenachrichtigungs-Ziel

Ab ONTAP 9.10.1 können Sie mit System Manager die Zielinformationen für die Ereignisbenachrichtigung ändern.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisziele** aus.
4. Klicken Sie neben dem Namen des Ereignisziels auf ⋮Klicken Sie dann auf **Bearbeiten**.
5. Ändern Sie die Informationen zum Event-Ziel und klicken Sie dann auf **Speichern**.

Bearbeiten Sie einen EMS-Ereignisbenachrichtigungs-Filter

Ab ONTAP 9.10.1 können Sie mit System Manager benutzerdefinierte Filter ändern, um die Handhabung von Ereignisbenachrichtigungen zu ändern.

ⓘ Sie können keine systemdefinierten Filter ändern.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisfilter** aus.
4. Klicken Sie neben dem Namen des Ereignisfilters auf ⋮Klicken Sie dann auf **Bearbeiten**.
5. Ändern Sie die Informationen zum Ereignisfilter und klicken Sie dann auf **Speichern**.

Löschen Sie ein EMS-Ereignisbenachrichtigungs-Ziel

Ab ONTAP 9.10.1 können Sie mit System Manager ein EMS-Ereignisbenachrichtigungs-Ziel löschen.

ⓘ SNMP-Ziele können nicht gelöscht werden.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮ Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisziele** aus.
4. Klicken Sie neben dem Namen des Ereignisziels auf ⋮ Klicken Sie dann auf **Löschen**.

Löschen Sie einen EMS-Ereignisbenachrichtigungs-Filter

Ab ONTAP 9.10.1 können Sie mit System Manager benutzerdefinierte Filter löschen.

ⓘ Sie können keine systemdefinierten Filter löschen.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮ Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisfilter** aus.
4. Klicken Sie neben dem Namen des Ereignisfilters auf ⋮ Klicken Sie dann auf **Löschen**.

Konfigurieren Sie EMS-Ereignisbenachrichtigungen mit der CLI

EMS-Konfigurationsworkflow

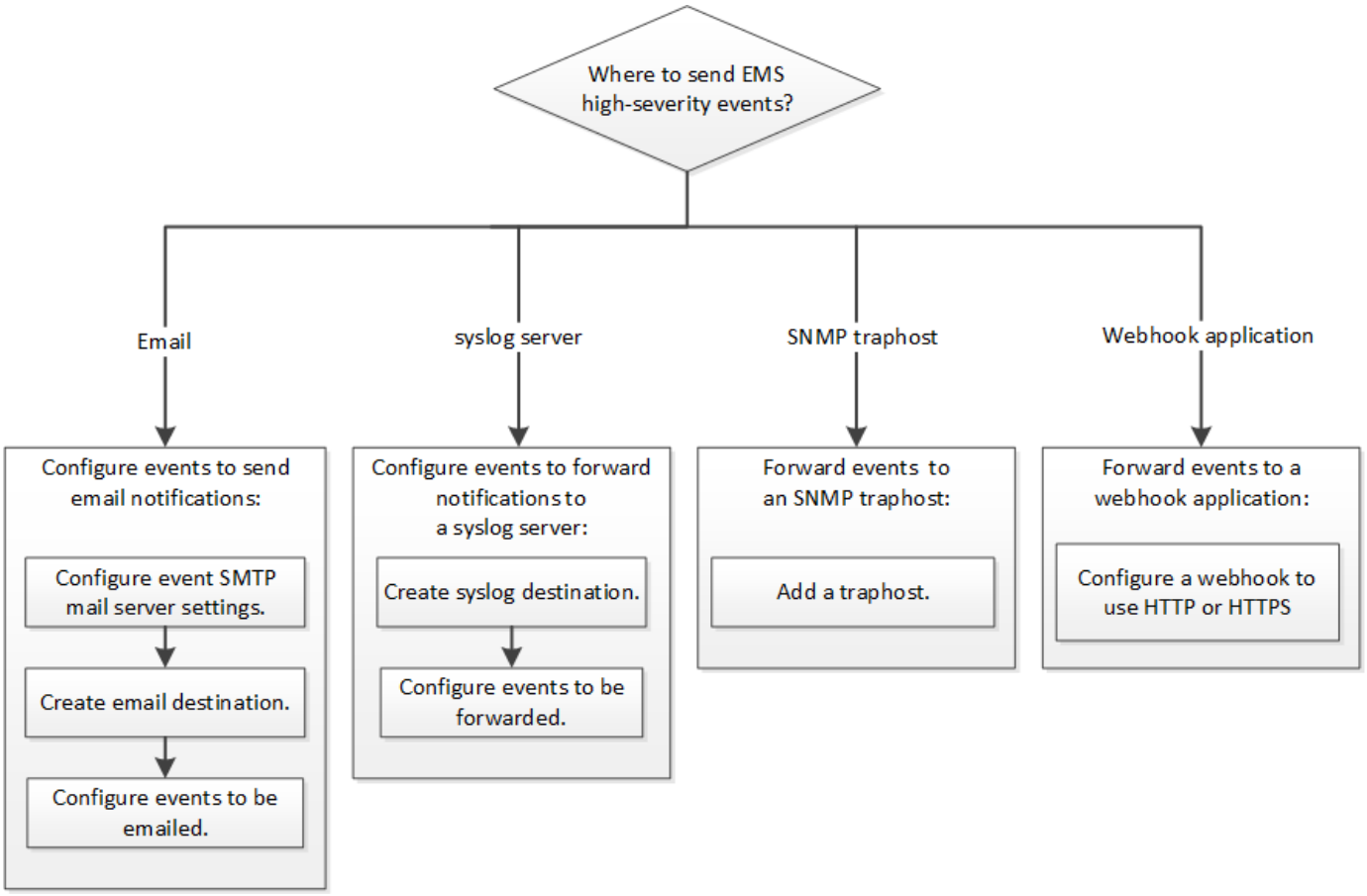
Sie müssen wichtige EMS-Ereignisbenachrichtigungen so konfigurieren, dass sie entweder als E-Mail gesendet, an einen Syslog-Server weitergeleitet, an einen SNMP traphost weitergeleitet oder an eine Webhook-Anwendung weitergeleitet werden. Auf diese Weise können Sie Systemstörungen vermeiden, indem Sie Korrekturmaßnahmen rechtzeitig ergreifen.

Über diese Aufgabe

Wenn in Ihrer Umgebung bereits ein Syslog-Server zur Aggregation der protokollierten Ereignisse von anderen Systemen, wie z. B. Servern und Anwendungen, vorhanden ist, ist es einfacher, diesen Syslog-Server auch für wichtige Ereignisbenachrichtigungen von Speichersystemen zu verwenden.

Wenn in Ihrer Umgebung noch kein Syslog-Server vorhanden ist, ist es einfacher, E-Mails für wichtige Ereignisbenachrichtigungen zu verwenden.

Wenn Sie Ereignisbenachrichtigungen bereits an einen SNMP traphost weiterleiten, können Sie diesen traphost bei wichtigen Ereignissen überwachen.



Wahlmöglichkeiten

- Setzen Sie EMS ein, um Ereignisbenachrichtigungen zu senden.

Ihre Situation	Lesen Sie dazu…
Das EMS sendet wichtige Ereignisbenachrichtigungen an eine E-Mail-Adresse	Konfigurieren Sie wichtige EMS-Ereignisse zum Senden von E-Mail-Benachrichtigungen
Das EMS sendet wichtige Ereignisbenachrichtigungen an einen Syslog-Server	Konfigurieren Sie wichtige EMS-Ereignisse, um Benachrichtigungen an einen Syslog-Server weiterzuleiten
Wenn Sie möchten, dass der EMS Ereignisbenachrichtigungen an einen SNMP traphost weitergibt	Konfigurieren Sie SNMP-Trap-Hosts für den Empfang von Ereignisbenachrichtigungen
Wenn Sie möchten, dass das EMS Ereignisbenachrichtigungen an eine Webhook-Anwendung weitergibt	Konfigurieren Sie wichtige EMS-Ereignisse, um Benachrichtigungen an eine Webhook-Anwendung weiterzuleiten

Konfigurieren Sie wichtige EMS-Ereignisse zum Senden von E-Mail-Benachrichtigungen

Um E-Mail-Benachrichtigungen über die wichtigsten Ereignisse zu erhalten, müssen Sie das EMS so konfigurieren, dass E-Mail-Nachrichten für Ereignisse gesendet werden, die

wichtige Aktivitäten signalisieren.

Was Sie benötigen

DNS muss auf dem Cluster konfiguriert sein, um die E-Mail-Adressen zu lösen.

Über diese Aufgabe

Sie können diese Aufgabe jederzeit ausführen, wenn das Cluster ausgeführt wird, indem Sie die Befehle in die ONTAP-Befehlszeile eingeben.

Schritte

1. Konfigurieren Sie die Einstellungen des SMTP-E-Mail-Servers für den Event:

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

2. E-Mail-Ziel für Ereignisbenachrichtigungen erstellen:

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

3. Konfigurieren Sie die wichtigen Ereignisse zum Senden von E-Mail-Benachrichtigungen:

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

Konfigurieren wichtiger EMS-Ereignisse zur Weiterleitung von Benachrichtigungen an einen Syslog-Server

Um Benachrichtigungen über die schwersten Ereignisse auf einem Syslog-Server zu protokollieren, müssen Sie das EMS so konfigurieren, dass Benachrichtigungen für Ereignisse, die wichtige Aktivitäten signalisieren, weitergesendet werden.

Was Sie benötigen

DNS muss auf dem Cluster konfiguriert werden, um den syslog-Servernamen aufzulösen.

Über diese Aufgabe

Wenn in Ihrer Umgebung kein Syslog-Server für Ereignisbenachrichtigungen vorhanden ist, müssen Sie zuerst einen erstellen. Falls Ihre Umgebung bereits einen Syslog-Server zum Protokollieren von Ereignissen aus anderen Systemen enthält, sollten Sie diesen Server möglicherweise für wichtige Ereignisbenachrichtigungen verwenden.

Sie können diese Aufgabe jederzeit ausführen, wenn das Cluster ausgeführt wird, indem Sie die Befehle in der ONTAP-CLI eingeben.

Ab ONTAP 9.12.1 können EMS-Ereignisse über das TLS-Protokoll (Transport Layer Security) an einen bestimmten Port auf einem Remote-Syslog-Server gesendet werden. Es sind zwei neue Parameter verfügbar:

`tcp-encrypted`

Wenn `tcp-encrypted` Wird für das angegeben `syslog-transport`, ONTAP überprüft die Identität des Ziel-Host durch die Validierung seines Zertifikats. Der Standardwert ist `udp-unencrypted`.

`syslog-port`

Der Standardwert `syslog-port` Parameter hängt von der Einstellung für das ab `syslog-transport` Parameter. Wenn `syslog-transport` Ist auf festgelegt `tcp-encrypted`, `syslog-port` Hat den Standardwert 6514.

Weitere Informationen finden Sie im `event notification destination create` Man-Page.

Schritte

1. Erstellen eines Syslog-Serverziels für wichtige Ereignisse:

   `event notification destination create -name` *`syslog-ems`* `-syslog` *`syslog-server-address`* `-syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}`

   Ab ONTAP 9.12.1 können für folgende Werte angegeben werden `syslog-transport`:

   - `udp-unencrypted` - User Datagram Protocol ohne Sicherheit
   - `tcp-unencrypted` - Transmission Control Protocol ohne Sicherheit
   - `tcp-encrypted` - Transmission Control Protocol mit Transport Layer Security (TLS)

   Das Standardprotokoll ist `udp-unencrypted`.

2. Konfigurieren Sie die wichtigen Ereignisse, um Benachrichtigungen an den Syslog-Server weiterzuleiten:

   `event notification create -filter-name` *`important-events`* `-destinations` *`syslog-ems`*

Konfigurieren Sie SNMP-Trap-Hosts für den Empfang von Ereignisbenachrichtigungen

Um Ereignisbenachrichtigungen auf einem SNMP traphost zu erhalten, müssen Sie einen traphost konfigurieren.

Was Sie benötigen

- SNMP- und SNMP-Traps müssen auf dem Cluster aktiviert sein.

  SNMP- und SNMP-Traps sind standardmäßig aktiviert.

- DNS muss auf dem Cluster konfiguriert werden, um die traphost-Namen zu lösen.

Über diese Aufgabe

Wenn Sie noch keinen SNMP traphost für den Empfang von Ereignisbenachrichtigungen (SNMP Traps) konfiguriert haben, müssen Sie einen hinzufügen.

Sie können diese Aufgabe jederzeit ausführen, wenn das Cluster ausgeführt wird, indem Sie die Befehle in die ONTAP-Befehlszeile eingeben.

Schritt

1. Wenn in Ihrer Umgebung noch kein SNMP traphost für den Empfang von Ereignisbenachrichtigungen konfiguriert ist, fügen Sie eine hinzu:

   `system snmp traphost add -peer-address` *`snmp_traphost_name`*

Alle Ereignisbenachrichtigungen, die standardmäßig von SNMP unterstützt werden, werden an den SNMP traphost weitergeleitet.

Konfigurieren Sie wichtige EMS-Ereignisse, um Benachrichtigungen an eine Webhook-Anwendung weiterzuleiten

Sie können ONTAP so konfigurieren, dass wichtige Ereignisbenachrichtigungen an eine Webhook-Anwendung weitergesendet werden. Die erforderlichen Konfigurationsschritte hängen vom gewählten Sicherheitsniveau ab.

Bereiten Sie sich auf die Konfiguration der EMS-Ereignisweiterleitung vor

Es gibt verschiedene Konzepte und Anforderungen, die Sie berücksichtigen sollten, bevor Sie ONTAP konfigurieren, um Ereignisbenachrichtigungen an eine Webhook-Anwendung weiterzuleiten.

Webhook-Anwendung

Sie benötigen eine Webhook-Anwendung, die die ONTAP-Ereignisbenachrichtigungen erhalten kann. Ein Webhook ist eine benutzerdefinierte Callback-Routine, die die Fähigkeit der Remote-Anwendung oder des Servers erweitert, auf dem sie ausgeführt wird. Webhooks werden vom Client (in diesem Fall ONTAP) aufgerufen oder aktiviert, indem eine HTTP-Anfrage an die Ziel-URL gesendet wird. Insbesondere sendet ONTAP eine HTTP-POST-Anfrage an den Server, der die Webhook-Anwendung hostet, sowie die in XML formatierten Ereignisbenachrichtigungen.

Sicherheitsoptionen

Je nach Verwendung des TLS-Protokolls (Transport Layer Security) stehen verschiedene Sicherheitsoptionen zur Verfügung. Die von Ihnen gewählte Option bestimmt die erforderliche ONTAP-Konfiguration.

ⓘ TLS ist ein kryptografisches Protokoll, das im Internet weit verbreitet ist. Sie bietet Datenschutz sowie Datenintegrität und Authentifizierung unter Verwendung eines oder mehrerer Public-Key-Zertifikate. Die Zertifikate werden von vertrauenswürdigen Zertifizierungsstellen ausgestellt.

HTTP

Sie können HTTP für die Übertragung von Ereignisbenachrichtigungen verwenden. Bei dieser Konfiguration ist die Verbindung nicht sicher. Die Identitäten des ONTAP-Clients und der Webhook-Anwendung werden nicht überprüft. Darüber hinaus ist der Netzwerkverkehr weder verschlüsselt noch geschützt. Siehe "Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTP" Für die Konfigurationsdetails.

HTTPS

Für zusätzliche Sicherheit können Sie ein Zertifikat auf dem Server installieren, der die Webhook-Routine hostet. Das HTTPS-Protokoll wird von ONTAP verwendet, um die Identität des Webhook-Anwendungsservers sowie von beiden Parteien zu überprüfen, um die Privatsphäre und Integrität des Netzwerkdatenverkehrs zu gewährleisten. Siehe "Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS" Für die Konfigurationsdetails.

HTTPS mit gegenseitiger Authentifizierung

Sie können die HTTPS-Sicherheit weiter erhöhen, indem Sie ein Clientzertifikat beim ONTAP-System installieren, das die Webbook-Anfragen ausgibt. Zusätzlich zur ONTAP, die die Identität des Webhook-Anwendungsservers überprüft und den Netzwerkverkehr schützt, überprüft die Webhook-Anwendung die Identität des ONTAP-Clients. Diese Zweiwege-Peer-Authentifizierung wird als *Mutual TLS* bezeichnet. Siehe "Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS mit gegenseitiger

Authentifizierung" Für die Konfigurationsdetails.

Verwandte Informationen

- "Das TLS-Protokoll (Transport Layer Security) Version 1.3"

Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTP

Sie können ONTAP so konfigurieren, dass Ereignisbenachrichtigungen mithilfe von HTTP an eine Webhook-Anwendung weitergesendet werden. Dies ist die am wenigsten sichere Option, aber die einfachste Einrichtung.

Schritte

1. Erstellen Sie ein neues Ziel `restapi-ems` So erhalten Sie die Ereignisse:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   Im obigen Befehl müssen Sie das **HTTP**-Schema für das Ziel verwenden.

2. Erstellen Sie eine Benachrichtigung, die den verknüpft `important-events` Mit dem filtern `restapi-ems` Ziel:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS

Sie können ONTAP so konfigurieren, dass Ereignisbenachrichtigungen mithilfe von HTTPS an eine Webhook-Anwendung weitergesendet werden. ONTAP verwendet das Serverzertifikat, um die Identität der Webhook-Anwendung zu bestätigen und den Netzwerkverkehr zu sichern.

Bevor Sie beginnen

- Generieren Sie einen privaten Schlüssel und ein Zertifikat für den Webhook-Anwendungsserver
- Lassen Sie das Root-Zertifikat zur Installation in ONTAP zur Verfügung

Schritte

1. Installieren Sie den entsprechenden Server-privaten Schlüssel und die entsprechenden Zertifikate auf dem Server, der Ihre Webhook-Anwendung hostet. Die spezifischen Konfigurationsschritte hängen vom Server ab.
2. Installieren Sie das Server-Root-Zertifikat in ONTAP:

   ```
   security certificate install -type server-ca
   ```

   Der Befehl fragt nach dem Zertifikat.

3. Erstellen Sie die `restapi-ems` Ziel für den Empfang der Ereignisse:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   Im obigen Befehl müssen Sie das Schema **HTTPS** für das Ziel verwenden.

4. Erstellen Sie die Benachrichtigung, die den verbindet `important-events` Mit dem neuen Filter filtern

`restapi-ems` Ziel:

```
event notification create -filter-name important-events -destinations restapi-ems
```

Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS mit gegenseitiger Authentifizierung

Sie können ONTAP so konfigurieren, dass Ereignisbenachrichtigungen mithilfe von HTTPS mit gegenseitiger Authentifizierung an eine Webhook-Anwendung weitergesendet werden. Mit dieser Konfiguration gibt es zwei Zertifikate. ONTAP verwendet das Serverzertifikat, um die Identität der Webhook-Anwendung zu bestätigen und den Netzwerkverkehr zu sichern. Darüber hinaus verwendet die Anwendung, die den Webhook hostet, das Clientzertifikat, um die Identität des ONTAP-Clients zu bestätigen.

Bevor Sie beginnen

Vor dem Konfigurieren von ONTAP müssen Sie Folgendes ausführen:

- Generieren Sie einen privaten Schlüssel und ein Zertifikat für den Webhook-Anwendungsserver
- Lassen Sie das Root-Zertifikat zur Installation in ONTAP zur Verfügung
- Generieren Sie einen privaten Schlüssel und ein Zertifikat für den ONTAP-Client

Schritte

1. Führen Sie die ersten beiden Schritte in der Aufgabe aus "Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS" So installieren Sie das Serverzertifikat, damit ONTAP die Identität des Servers überprüfen kann.
2. Installieren Sie die entsprechenden Root- und Zwischenzertifikate in der Webhook-Anwendung, um das Clientzertifikat zu validieren.
3. Installieren Sie das Client-Zertifikat in ONTAP:

   ```
   security certificate install -type client
   ```

   Der Befehl fragt nach dem privaten Schlüssel und dem Zertifikat.

4. Erstellen Sie die `restapi-ems` Ziel für den Empfang der Ereignisse:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application> -certificate-authority <issuer of the client
   certificate> -certificate-serial <serial of the client certificate>
   ```

   Im obigen Befehl müssen Sie das Schema **HTTPS** für das Ziel verwenden.

5. Erstellen Sie die Benachrichtigung, die den verbindet `important-events` Mit dem neuen Filter filtern `restapi-ems` Ziel:

   ```
   event notification create -filter-name important-events -destinations restapi-ems
   ```

Aktualisieren der veralteten EMS-Ereigniszuordnung

EMS-Modelle für die Ereigniszuordnung

Vor ONTAP 9.0 konnten EMS-Ereignisse basierend auf dem Abgleich von Ereignisnamen nur Ereigniszielen zugeordnet werden. Die ONTAP-Befehle werden eingestellt (`event destination`, `event route`), die dieses Modell verwenden, ist weiterhin in den neuesten Versionen von ONTAP verfügbar, aber sie sind seit ONTAP 9.0 veraltet.

Seit ONTAP 9.0 empfiehlt sich die Verwendung des skalierbareren Ereignisfiltermodells für ONTAP EMS, in dem die Musteranpassung für mehrere Felder mit dem durchgeführt wird `event filter`, `event notification`, und `event notification destination` Befehlssätze.

Wenn Ihre EMS-Zuordnung mit den veralteten Befehlen konfiguriert ist, sollten Sie Ihre Zuordnung aktualisieren, um die zu verwenden `event filter`, `event notification`, und `event notification destination` Befehlssätze.

Es gibt zwei Arten von Ereigniszielen:

1. **Systemgenerierte Ziele**: Es gibt fünf vom System generierte Ereignisziele (standardmäßig erstellt)
    - `allevents`
    - `asup`
    - `criticals`
    - `pager`
    - `traphost`

      Einige der vom System generierten Ziele sind für besondere Zwecke. Zum Beispiel leitet das Asup-Zielgerät Callhome.* Ereignisse an das AutoSupport-Modul in ONTAP weiter, um AutoSupport-Nachrichten zu generieren.
2. **Vom Benutzer erstellte Ziele**: Diese werden manuell mit dem erstellt `event destination create` Befehl.

```
cluster-1::event*> destination show
                                                                    Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
traphost          -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
test              test@xyz.com      -                  -
false
traphost          -                 -                  -
false
6 entries were displayed.
```

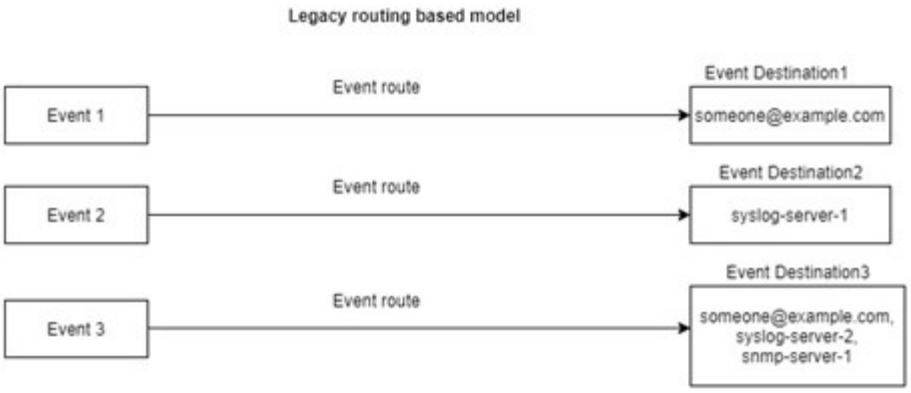
Im veralteten Modell werden EMS-Ereignisse individuell einem Ziel über zugeordnet `event route add-destinations` Befehl.

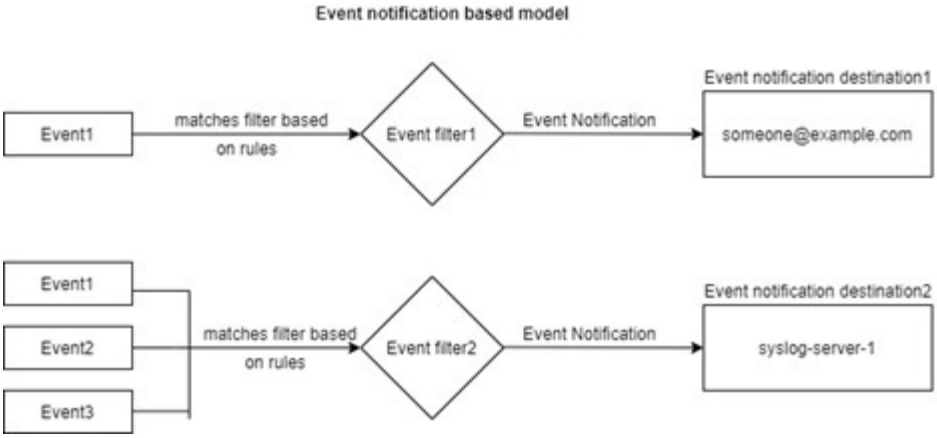
```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

Der neue, besser skalierbare EMS-Mechanismus für Ereignisbenachrichtigungen basiert auf Ereignisfiltern und Zielorten für Ereignisbenachrichtigungen. Detaillierte Informationen zum neuen Benachrichtigungsmechanismus für Ereignisse finden Sie in dem folgenden KB-Artikel:

- "Übersicht über das Event Management System für ONTAP 9"





Aktualisieren der EMS-Ereigniszuordnung aus veralteten ONTAP Befehlen

Wenn Ihre EMS-Ereigniszuordnung derzeit mit den veraltet ONTAP-Befehlssätzen konfiguriert ist (`event destination`, `event route`Sie sollten dieses Verfahren befolgen, um Ihr Mapping zu aktualisieren, um das zu verwenden `event filter`, `event notification`, und `event notification destination` Befehlssätze.

Schritte

1. Listen Sie alle Event-Ziele im System mithilfe von auf `event destination show` Befehl.

```
cluster-1::event*> destination show

Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

2. Führen Sie für jedes Ziel die Ereignisse auf, die ihm mithilfe des zugeordnet sind `event route show -destinations <destination name>` Befehl.

```
cluster-1::event*> route show -destinations test
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

3. Erstellen Sie eine entsprechende `event filter` Welches all diese Teilmengen von Ereignissen enthält. Beispiel: Wenn Sie nur die einschließen möchten `raid.aggr.*` Ereignisse, verwenden Sie einen Platzhalter für die `message-name` Parameter beim Erstellen des Filters. Sie können auch Filter für einzelne Ereignisse erstellen.

> Sie können bis zu 50 Ereignisfilter erstellen.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. Erstellen Sie ein `event notification destination` Für jede der `event destination` Endpunkte (z. B. SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  --------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

5. Erstellen Sie eine Ereignisbenachrichtigung, indem Sie den Ereignisfilter dem Ziel der Ereignisbenachrichtigung zuordnen.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                    Destinations
---- ------------------------------ -----------------
1    default-trap-events            snmp-traphost
2    asup_events                    dest1
2 entries were displayed.
```

6. Wiederholen Sie die Schritte 1-5 für jede einzelne `event destination` Das ist ein `event route` Zuordnung:

> An SNMP-Ziele weitergeleitete Ereignisse sollten dem zugeordnet werden `snmp-traphost` Ziel der Ereignisbenachrichtigung Das SNMP traphost-Ziel verwendet das System konfigurierte SNMP traphost.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

                Destination Name: snmp-traphost
            Type of Destination: snmp
                    Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```