



Ereignis-, Performance- und Zustandsüberwachung

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap/task_cp_monitor_cluster_performance_sm.html on April 24, 2024. Always check docs.netapp.com for the latest.

Inhalt

- Ereignis-, Performance- und Zustandsüberwachung 1
 - Überwachen Sie die Cluster-Performance mit System Manager 1
 - Überwachen und managen Sie die Cluster-Performance über die CLI 12
 - Überwachen Sie die Cluster-Performance mit Unified Manager 49
 - Überwachen Sie die Cluster-Performance mit Cloud Insights 50
- Audit-Protokollierung 51
- AutoSupport 57
- Monitoring des Systemzustands 87
- Filesystem-Analyse 102
- EMS-Konfiguration 116

Ereignis-, Performance- und Zustandsüberwachung

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 Netzwerkobjekten 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.



Ab ONTAP 9.10.1 können Sie die Funktion „Aktivitätsüberwachung“ in Dateisystemanalyse verwenden, um heiße Objekte in einem Volume zu überwachen.


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 bei der Bereitstellung von Storage [Servicequalität \(QoS\)](#) Ist 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. Wählen Sie im System Manager **Storage** und dann **Volumes** aus.
2. Wählen Sie neben dem Volume, für das Sie die QoS ändern möchten, die Option aus  Dann **Bearbeiten**.

Monitoring von Risiken

Ab ONTAP 9.10.0 können Sie mit System Manager die von Active IQ Digital Advisor gemeldeten Risiken überwachen. Ab ONTAP 9.10.1 erkennen Sie mit System Manager auch die Risiken.

NetApp Active IQ Digital Advisor meldet Möglichkeiten zur Risikominimierung und zur Verbesserung der Performance und Effizienz Ihrer Storage-Umgebung. Mit System Manager lernen Kunden die von Active IQ gemeldeten Risiken kennen und erhalten nützliche Informationen. Diese helfen Ihnen bei der Storage-Verwaltung und ermöglichen eine höhere Verfügbarkeit, verbesserte Sicherheit und eine bessere Storage-Performance.

Link zu Ihrem Active IQ Konto

Wenn Sie Informationen zu Risiken von Active IQ erhalten möchten, sollten Sie zuerst einen Link zu Ihrem Active IQ Account vom System Manager erhalten.

Schritte

1. Klicken Sie in System Manager auf **Cluster > Einstellungen**.
2. Klicken Sie unter **Active IQ-Registrierung** auf **Registrieren**.
3. Geben Sie Ihre Zugangsdaten für Active IQ ein.
4. Klicken Sie nach der Authentifizierung auf **Bestätigen, um Active IQ mit dem System Manager zu verknüpfen**.

Zeigen Sie die Anzahl der Risiken an

Ab ONTAP 9.10.0 können Sie sich im Dashboard in System Manager die Anzahl der von Active IQ gemeldeten Risiken anzeigen lassen.

Bevor Sie beginnen

Sie müssen eine Verbindung vom System Manager zu Ihrem Active IQ Konto herstellen. Siehe [Link zu Ihrem Active IQ Konto](#).

Schritte

1. Klicken Sie in System Manager auf **Dashboard**.
2. Zeigen Sie im Abschnitt **Gesundheit** die Anzahl der gemeldeten Risiken an.



Sie können ausführlichere Informationen zu den einzelnen Risiken anzeigen, indem Sie auf die Meldung mit der Anzahl der Risiken klicken. Siehe [Details zu Risiken anzeigen](#).

Details zu Risiken anzeigen

Ab ONTAP 9.10.0 können Sie im System Manager anzeigen, wie die von Active IQ gemeldeten Risiken nach Wirkungsbereichen kategorisiert werden. Sie können außerdem detaillierte Informationen zu jedem gemeldeten Risiko, seinen potenziellen Auswirkungen auf Ihr System und Korrekturmaßnahmen anzeigen.

Bevor Sie beginnen

Sie müssen eine Verbindung vom System Manager zu Ihrem Active IQ Konto herstellen. Siehe [Link zu Ihrem Active IQ Konto](#).

Schritte

1. Klicken Sie Auf **Events > Alle Ereignisse**.
2. Zeigen Sie im Abschnitt **Übersicht** unter **Active IQ-Vorschläge** die Anzahl der Risiken in jeder Kategorie der Wirkungsbereiche an. Die Risikokategorien sind:
 - Performance und Effizienz zu erlangen
 - Verfügbarkeit und Sicherung
 - Kapazität
 - Konfiguration
 - Sicherheit
3. Klicken Sie auf die Registerkarte **Active IQ Suggestions**, um Informationen zu den einzelnen Risiken anzuzeigen, einschließlich der folgenden:
 - Ausmaß der Auswirkungen auf Ihr System
 - Kategorie des Risikos
 - Betroffene Nodes
 - Art der Risikominimierung erforderlich
 - Korrekturmaßnahmen können vorgenommen werden

Erkennen von Risiken

Ab ONTAP 9.10.1 erkennen Sie mit System Manager alle offenen Risiken.

Schritte

1. Zeigen Sie im System Manager die Risikoliste an, indem Sie das Verfahren in durchführen [Details zu Risiken anzeigen](#).
2. Klicken Sie auf den Risikonamen eines offenen Risikos, das Sie bestätigen möchten.
3. Geben Sie Informationen in die folgenden Felder ein:
 - Erinnerung (Datum)
 - Argumentation
 - Kommentare
4. Klicken Sie Auf **Bestätigen**.



Nachdem Sie ein Risiko bestätigt haben, dauert es einige Minuten, bis die Änderung in der Liste der Active IQ-Vorschläge aufgeführt ist.

Risiken nicht anerkennen

Ab ONTAP 9.10.1 können Sie mit System Manager jedes zuvor bestätigte Risiko nicht erkennen.

Schritte

1. Zeigen Sie im System Manager die Risikoliste an, indem Sie das Verfahren in durchführen [Details zu Risiken anzeigen](#).
2. Klicken Sie auf den Risikonamen eines bestätigten Risikos, das Sie nicht bestätigen möchten.
3. Geben Sie Informationen in die folgenden Felder ein:
 - Argumentation
 - Kommentare
4. Klicken Sie Auf **Unquittieren**.



Nachdem Sie ein Risiko nicht bestätigt haben, dauert es einige Minuten, bis die Änderung in der Liste der Active IQ-Vorschläge aufgeführt ist.

Einblicke in System Manager

Ab ONTAP 9.11.1 zeigt System Manager *Insights* an, die Sie bei der Optimierung der Performance und Sicherheit Ihres Systems unterstützen.



Informationen zum Anzeigen, Anpassen und Reagieren auf Erkenntnisse finden Sie unter ["Einblicke zur Optimierung Ihres Systems"](#)

Kapazitätseinblicke

System Manager kann als Reaktion auf die Kapazitätsbedingungen in Ihrem System die folgenden Einblicke anzeigen:

Insight	Schweregrad	Zustand	Korrekturen
---------	-------------	---------	-------------

Lokale Ebenen haben keinen Platz	Risiken beheben	Eine oder mehrere lokale Ebenen sind zu mehr als 95 % voll und wachsen schnell. Bestehende Workloads können sich möglicherweise nicht vergrößern oder in extremen Fällen kann es vorkommen, dass die Menge an Speicherplatz ausbleibt oder ausfällt.	<p>Empfohlener Fix: Führen Sie eine der folgenden Optionen aus.</p> <ul style="list-style-type: none"> • Löschen Sie die Warteschlange für die Volume-Wiederherstellung. • Aktivieren Sie Thin Provisioning auf Thick Provisioning Volumes, um die Freigabe von Storage-Kapazität zu ermöglichen. • Verschieben Sie Volumes auf eine andere lokale Ebene. • Nicht benötigte Snapshot Kopien werden gelöscht. • Löschen Sie nicht benötigte Verzeichnisse oder Dateien in den Volumes. • Aktivieren Sie Fabric Pool für das Tiering der Daten in die Cloud.
Applikationen fehlt Speicherplatz	Erfordert Aufmerksamkeit	Ein oder mehrere Volumes sind zu mehr als 95 % voll, haben aber keine Autogrow aktiviert.	<p>Empfohlen: Aktivieren Sie Autogrow bis zu 150% der aktuellen Kapazität.</p> <p>Andere Optionen:</p> <ul style="list-style-type: none"> • Durch Löschen von Snapshot Kopien wird Speicherplatz zurückgewonnen. • Größe der Volumes ändern. • Verzeichnisse oder Dateien löschen.
Die Kapazität des FlexGroup Volume ist nicht ausgeglichen	Optimieren Sie den Storage	Die Größe der zusammengehörigen Volumes eines oder mehrerer FlexGroup Volumes ist im Laufe der Zeit ungleichmäßig gewachsen, was zu einem Ungleichgewicht bei der Kapazitätsauslastung führte. Wenn die einzelnen Volumes voll werden, können Fehler beim Schreiben auftreten.	<p>Empfohlen: Balancieren Sie die FlexGroup-Volumes aus.</p>

Die Kapazität der Storage-VMs geht zu knapp	Optimieren Sie den Storage	Eine oder mehrere Storage-VMs nähern sich der maximalen Kapazität. Sie können nicht mehr Platz für neue oder bestehende Volumes bereitstellen, wenn die Storage-VMs die maximale Kapazität erreichen.	Empfohlen: Wenn möglich, erhöhen Sie die maximale Kapazitätsgrenze der Speicher-VM.
---	----------------------------	---	--

Sicherheitseinblicke

System Manager kann die folgenden Einblicke als Reaktion auf Umstände anzeigen, die die Sicherheit Ihrer Daten oder Ihres Systems gefährden könnten.

Insight	Schweregrad	Zustand	Korrekturen
Lernmodus für Ransomware noch immer sehr einfach	Erfordert Aufmerksamkeit	Ein oder mehrere Volumes befinden sich seit 90 Tagen im Lernmodus zum Schutz vor Ransomware.	Empfohlen: Aktivieren Sie den Anti-Ransomware-aktiven Modus für diese Volumes.
Das automatische Löschen von Snapshot Kopien ist auf Volumes aktiviert	Erfordert Aufmerksamkeit	Das automatische Löschen von Snapshots ist auf einem oder mehreren Volumes aktiviert.	Empfohlen: Deaktivieren Sie das automatische Löschen von Snapshot Kopien. Andernfalls ist im Fall eines Ransomware-Angriffs möglicherweise keine Datenwiederherstellung für diese Volumes möglich.
Volumes verfügen nicht über Snapshot-Richtlinien	Erfordert Aufmerksamkeit	An ein oder mehrere Volumes ist keine angemessene Snapshot-Richtlinie gebunden.	Empfohlen: Hängen Sie eine Snapshot-Richtlinie an Volumes an, die keine haben. Andernfalls ist im Fall eines Ransomware-Angriffs möglicherweise keine Datenwiederherstellung für diese Volumes möglich.
Native FPolicy ist nicht konfiguriert	Best Practices in sich	Native FPolicy wird nicht auf einer oder mehreren NAS-Storage-VMs konfiguriert.	Empfohlen: WICHTIG: Das Blockieren von Erweiterungen kann zu unerwarteten Ergebnissen führen. Ab 9.11.1 können Sie nativen FPolicy für Storage-VMs aktivieren. Dabei werden mehr als 3000 Dateierweiterungen blockiert, von denen bekannt ist, dass sie für Ransomware-Angriffe verwendet werden. "Konfigurieren Sie nativen FPolicy" In NAS-Speicher-VMs, um die Dateierweiterungen zu steuern, die auf Volumes in Ihrer Umgebung geschrieben werden dürfen oder dürfen.

Telnet ist aktiviert	Best Practices in sich	Secure Shell (SSH) sollte für einen sicheren Remote-Zugriff verwendet werden.	Empfohlen: Telnet deaktivieren und SSH für sicheren Remote-Zugriff verwenden.
Es sind zu wenige NTP-Server konfiguriert	Best Practices in sich	Die Anzahl der für NTP konfigurierten Server ist kleiner als 3.	Empfohlen: Mindestens drei NTP-Server mit dem Cluster verknüpfen. Andernfalls können Probleme bei der Synchronisierung der Cluster-Zeit auftreten.
Remote Shell (RSH) ist aktiviert	Best Practices in sich	Secure Shell (SSH) sollte für einen sicheren Remote-Zugriff verwendet werden.	Empfohlen: Deaktivieren Sie RSH und verwenden Sie SSH für sicheren Remote-Zugriff.
Anmeldebanner ist nicht konfiguriert	Best Practices in sich	Anmeldemeldungen sind weder für das Cluster, für die Storage-VM noch für beides konfiguriert.	Empfohlen: Richten Sie die Anmeldebanner für den Cluster und die Speicher-VM ein und aktivieren Sie deren Nutzung.
AutoSupport verwendet ein nicht sicheres Protokoll	Best Practices in sich	AutoSupport ist nicht für die Kommunikation über HTTPS konfiguriert.	Empfohlen: Es wird dringend empfohlen, HTTPS als Standard-Transportprotokoll zu verwenden, um AutoSupport-Nachrichten an den technischen Support zu senden.
Der Standard-Admin-Benutzer ist nicht gesperrt	Best Practices in sich	Niemand hat sich mit einem Standard-Administratorkonto (admin oder diag) angemeldet, und diese Konten sind nicht gesperrt.	Empfohlen: Sperren Sie standardmäßige Administratorkonten, wenn sie nicht verwendet werden.
Secure Shell (SSH) verwendet unsichere Chiffren	Best Practices in sich	Die aktuelle Konfiguration verwendet nicht sichere CBC-Chiffren.	Empfohlen: Sie sollten nur sichere Chiffren auf Ihrem Webserver zulassen, um die sichere Kommunikation mit Ihren Besuchern zu schützen. Entfernen Sie Chiffren mit Namen, die „cbc“ enthalten, z. B. „ais128-cbc“, „aes192-cbc“, „aes256-cbc“ und „3des-cbc“.
Die globale FIPS 140-2-2-Compliance ist deaktiviert	Best Practices in sich	Die globale FIPS 140-2-2-Compliance ist auf dem Cluster deaktiviert.	Empfohlen: Aus Sicherheitsgründen sollten Sie die globale FIPS 140-2-konforme Kryptographie aktivieren, um sicherzustellen, dass ONTAP sicher mit externen Clients oder Server-Clients kommunizieren kann.

Volumes werden nicht auf Ransomware-Angriffe überwacht	Erfordert Aufmerksamkeit	Anti-Ransomware ist auf einem oder mehreren Volumes deaktiviert.	Empfohlen: Aktivieren Sie Anti-Ransomware auf den Volumes. Andernfalls bemerken Sie möglicherweise nicht, wann Volumen bedroht werden oder angegriffen werden.
Storage VMs sind nicht für den Schutz vor Ransomware konfiguriert	Best Practices in sich	Eine oder mehrere Storage-VMs sind nicht für den Schutz vor Ransomware konfiguriert.	Empfohlen: Aktivieren Sie Anti-Ransomware auf den Storage-VMs. Andernfalls werden Sie möglicherweise nicht bemerken, wenn Storage-VMs bedroht sind oder angegriffen werden.

Konfigurationseinblicke

System Manager kann die folgenden Einblicke als Antwort auf Bedenken hinsichtlich der Konfiguration Ihres Systems anzeigen.

Insight	Schweregrad	Zustand	Korrekturen
Das Cluster ist nicht für Benachrichtigungen konfiguriert	Best Practices in sich	E-Mail, Webhooks oder ein SNMP traphost ist nicht so konfiguriert, dass Sie Benachrichtigungen über Probleme mit dem Cluster erhalten.	Empfohlen: Konfigurieren Sie Benachrichtigungen für den Cluster.
Das Cluster ist nicht für automatische Updates konfiguriert.	Best Practices in sich	Das Cluster wurde nicht so konfiguriert, dass es automatische Updates für die neuesten verfügbaren Dateien zur Festplattenqualifizierung, Festplatten-Firmware, Shelf-Firmware und SP/BMC-Firmware empfängt.	Empfohlen: Aktivieren Sie diese Funktion.

Cluster-Firmware ist nicht auf dem neuesten Stand	Best Practices in sich	Ihr System verfügt nicht über das neueste Firmware-Update, das Verbesserungen, Sicherheitspatches oder neue Funktionen zur Sicherung des Clusters für eine bessere Performance bieten könnte.	Empfohlen: Aktualisieren Sie die ONTAP-Firmware.
---	------------------------	---	---

Einblicke zur Optimierung Ihres Systems

Mit System Manager können Sie Einblicke anzeigen, die Ihnen bei der Optimierung Ihres Systems helfen.

Über diese Aufgabe

Ab ONTAP 9.11.0 können Sie sich Einblicke in System Manager anzeigen lassen, mit denen Sie die Kapazitäts- und Sicherheits-Compliance Ihres Systems optimieren können.

Ab ONTAP 9.11.1 können Sie sich zusätzliche Einblicke anzeigen lassen, mit denen Sie Kapazität, Sicherheits-Compliance und Konfiguration Ihres Systems optimieren können.



Das Blockieren von Erweiterungen kann zu unerwarteten Ergebnissen führen. ab ONTAP 9.11.1 können Sie native FPolicy für Storage-VMs mit System Manager aktivieren. Eventuell erhalten Sie eine Empfehlung von System Manager Insight ["Konfigurieren Sie nativen FPolicy"](#) Für eine Storage-VM.

Im FPolicy Native Mode können Sie bestimmte Dateierweiterungen zulassen oder untersagen. System Manager empfiehlt mehr als 3000 unzulässige Dateiendungen, die bei früheren Ransomware-Angriffen verwendet wurden. Einige dieser Erweiterungen können von legitimen Dateien in Ihrer Umgebung verwendet werden und das Blockieren sie kann zu unerwarteten Problemen führen.

Es wird daher dringend empfohlen, die Liste der Erweiterungen an die Anforderungen Ihrer Umgebung anzupassen. Siehe ["So entfernen Sie eine Dateierweiterung aus einer nativen FPolicy-Konfiguration, die von System Manager mithilfe von System Manager erstellt wurde, um die Richtlinie neu zu erstellen"](#).

Weitere Informationen zu nativem FPolicy finden Sie unter ["FPolicy-Konfigurationstypen"](#).

Diese Einblicke werden basierend auf Best Practices auf einer Seite angezeigt, über die Sie sofort Maßnahmen zur Optimierung Ihres Systems einleiten können. Weitere Informationen zu den einzelnen Einblicken finden Sie unter ["Einblicke in System Manager"](#).

Einblicke zur Optimierung





Schritte

1. Klicken Sie in System Manager in der linken Navigationsleiste auf **Einblicke**.

Die Seite **Insights** zeigt Gruppen von Einsichten. Jede Gruppe von Einsichten kann einen oder mehrere Erkenntnisse enthalten. Die folgenden Gruppen werden angezeigt:

- Erfordert Ihre Aufmerksamkeit
- Risiken beheben
- Optimieren Sie Ihren Storage

2. (Optional) Filtern Sie die Informationen, die angezeigt werden, indem Sie oben rechts auf der Seite auf diese Schaltflächen klicken:

-  Zeigt die sicherheitsrelevanten Informationen an.
-  Zeigt die kapazitätsbezogenen Einblicke an.
-  Zeigt die konfigurationsbezogenen Informationen an.
-  Zeigt alle Erkenntnisse an.

Die nötigen Einblicke gewinnen, um das System zu optimieren

In System Manager können Sie auf Erkenntnisse reagieren, indem Sie diese entweder entblenden, verschiedene Wege zur Behebung der Probleme erkunden oder den Prozess zur Behebung der Probleme initiieren.

Schritte

1. Klicken Sie in System Manager in der linken Navigationsleiste auf **Einblicke**.
2. Bewegen Sie den Mauszeiger über einen Einblick, um die Schaltflächen anzuzeigen, mit denen die folgenden Aktionen durchgeführt werden:
 - **Abweisen:** Entferne die Einsicht aus der Sicht. Um „Unabtun“ die Einsichten zu lesen, lesen Sie [\[customize-settings-insights\]](#).
 - **Explore:** Finden Sie verschiedene Wege, um das Problem zu beheben, das in der Einsicht erwähnt wird. Diese Schaltfläche wird nur angezeigt, wenn mehr als eine Methode zur Behebung vorhanden ist.
 - **Fix:** Initiieren Sie den Prozess der Behebung des in der Einsicht genannten Problems. Sie werden aufgefordert zu bestätigen, ob Sie die Aktion ergreifen möchten, die zum Anwenden des Fixes erforderlich ist.




Einige dieser Aktionen können von anderen Seiten im System Manager gestartet werden, aber die Seite **Insights** hilft Ihnen, Ihre täglichen Aufgaben zu optimieren, indem Sie diese Aktion von dieser Seite aus starten können.

Passen Sie die Einstellungen für Erkenntnisse an

Sie können anpassen, über welche Einblicke Sie in System Manager informiert werden.

Schritte


1. Klicken Sie in System Manager in der linken Navigationsleiste auf **Einblicke**.

2. Klicken Sie oben rechts auf der Seite auf  Wählen Sie dann **Einstellungen**.
3. Stellen Sie auf der Seite **Einstellungen** sicher, dass neben den Erkenntnissen, über die Sie benachrichtigt werden möchten, ein Häkchen in die Kontrollkästchen gesetzt wird. Wenn du zuvor eine Einsicht abgewiesen hast, kannst du sie „unabweisen“, indem du dafür gesorgt hast, dass ein Häkchen in seinem Kontrollkästchen ist.
4. Klicken Sie Auf **Speichern**.

Exportieren Sie die Erkenntnisse als PDF-Datei

Sie können alle relevanten Erkenntnisse als PDF-Datei exportieren.

Schritte

1. Klicken Sie in System Manager in der linken Navigationsleiste auf **Einblicke**.
2. Klicken Sie oben rechts auf der Seite auf , Und wählen Sie dann **Export**.

Konfigurieren Sie nativen FPolicy

Wenn Sie ab ONTAP 9.11.1 einen System Manager Insight erhalten, der die Implementierung von nativem FPolicy empfiehlt, können Sie ihn auf Ihren Storage-VMs und -Volumes konfigurieren.

Bevor Sie beginnen

Wenn Sie auf System Manager Insights unter **Best Practices anwenden** zugreifen, erhalten Sie möglicherweise eine Meldung, dass native FPolicy nicht konfiguriert ist.

Weitere Informationen zu FPolicy-Konfigurationstypen finden Sie unter "[FPolicy-Konfigurationstypen](#)".

Schritte

1. Klicken Sie in System Manager in der linken Navigationsleiste auf **Einblicke**.
2. Suchen Sie unter **Best Practices anwenden** nach **Native FPolicy is not configured**.
3. Lesen Sie die folgende Meldung, bevor Sie Maßnahmen ergreifen:



Das Blockieren von Erweiterungen kann zu unerwarteten Ergebnissen führen. ab ONTAP 9.11.1 können Sie native FPolicy für Storage-VMs mit System Manager aktivieren. Im FPolicy Native Mode können Sie bestimmte Dateierweiterungen zulassen oder untersagen. System Manager empfiehlt mehr als 3000 unzulässige Dateierweiterungen, die bei früheren Ransomware-Angriffen verwendet wurden. Einige dieser Erweiterungen können von legitimen Dateien in Ihrer Umgebung verwendet werden und das Blockieren sie kann zu unerwarteten Problemen führen.

Es wird daher dringend empfohlen, die Liste der Erweiterungen an die Anforderungen Ihrer Umgebung anzupassen. Siehe "[So entfernen Sie eine Dateierweiterung aus einer nativen FPolicy-Konfiguration, die von System Manager mithilfe von System Manager erstellt wurde, um die Richtlinie neu zu erstellen](#)".

4. Klicken Sie Auf **Fix**.
5. Wählen Sie die Storage-VMs aus, auf die Sie die native FPolicy anwenden möchten.
6. Wählen Sie für jede Storage-VM die Volumes aus, die die native FPolicy erhalten.

7. Klicken Sie Auf **Konfigurieren**.

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 <div>  Dem Administrator muss die Rolle „admin“ zugewiesen worden sein. </div>	
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 Wartungsbetreibers, den SMTP-Servernamen und weitere SMTP-Optionen ein, und klicken Sie dann auf **Speichern**.

Nachdem Sie fertig sind

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

Geben Sie die zu überwachenden Cluster an

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

Was Sie benötigen

- Sie müssen die folgenden Informationen haben:

- Host-Name oder Cluster-Management-IP-Adresse

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

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

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

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

Über diese Aufgabe

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

Schritte

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

Standardmäßig ist das HTTPS-Protokoll ausgewählt.

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

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

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

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

6. **Optional**: Anzeigen des Clusterermittlungsstatus:
 - a. Überprüfen Sie den Cluster-Erkennungsstatus auf der Seite **Cluster Setup**.Das Cluster wird der Unified Manager-Datenbank nach dem Standard-Monitoring-Intervall von ca. 15 Minuten hinzugefügt.

Einrichten grundlegender Überwachungsaufgaben

Tägliche Überwachung

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

Schritte

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

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

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

Schritte

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

Verwenden Sie Performance-Schwellenwerte zur Ereignisbenachrichtigung

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

Festlegen von Performance-Schwellenwerten

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

Schritte

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

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

Beispiel

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

Warnmeldungen hinzufügen

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

Was Sie benötigen

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

Über diese Aufgabe

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

Schritte

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

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

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

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



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

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



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

Sie können auch Benutzer über SNMP-Traps benachrichtigen.

7. Klicken Sie Auf **Speichern**.

Beispiel für das Hinzufügen einer Meldung

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

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

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

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

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

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

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

8. Klicken Sie Auf **Speichern**.

Konfigurieren Sie die Einstellungen für Warnmeldungen

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

Was Sie benötigen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Über diese Aufgabe

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

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

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



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

Schritte

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

Die Seite „Alarm-Setup“ wird angezeigt.

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

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

3. Klicken Sie Auf **Speichern**.

Performance-Probleme in Active IQ Unified Manager ermitteln

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

Benachrichtigung über ein Ereignis oder eine Benachrichtigung über das Ereignis.

Schritte

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

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

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

Verwenden Sie Active IQ Digital Advisor, um die Systemleistung anzuzeigen

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

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

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



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

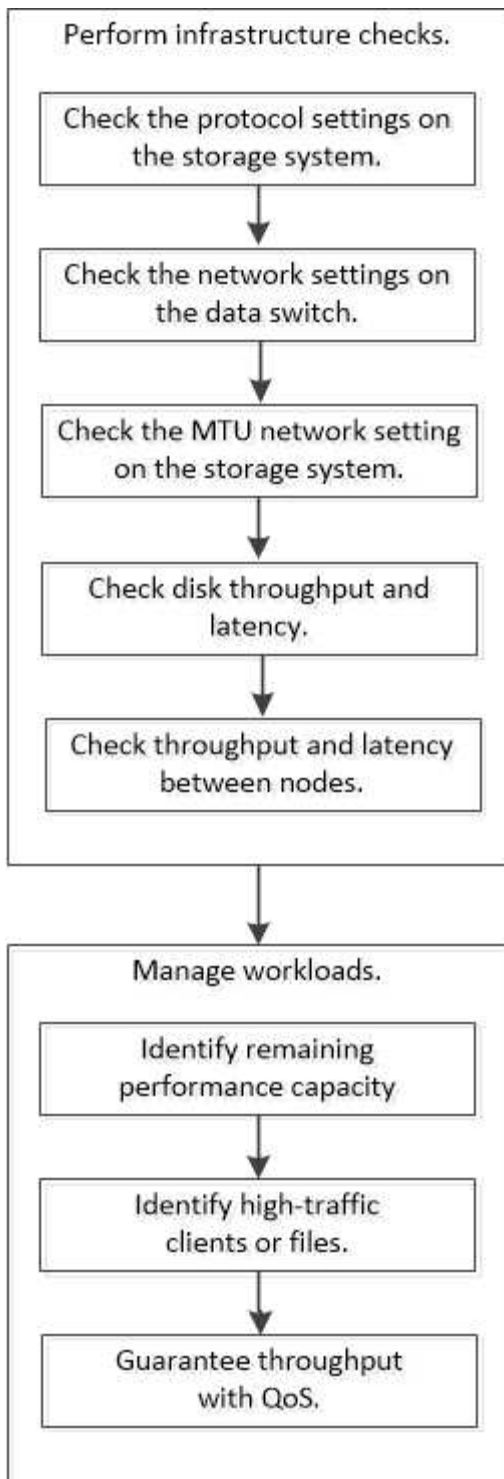
Verwandte Informationen

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

Managen Sie Performance-Probleme

Performance-Management-Workflow

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



Durchführung grundlegender Infrastrukturprüfungen

Prüfen Sie die Protokolleinstellungen auf dem Storage-System

Überprüfen Sie die maximale Übertragungsgröße des NFS TCP

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

Was Sie benötigen

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

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Überprüfen Sie die maximale TCP-Übertragungsgröße:

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

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

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

4. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Beispiel

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

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

Prüfen Sie die iSCSI-TCP-Lese-/Schreibgröße

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

Was Sie benötigen

Für diese Aufgabe sind erweiterte Befehle auf Berechtigungsebene erforderlich.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

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

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

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

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

4. Zurück zur Administratorberechtigung:

```
set -privilege admin
```

Beispiel

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

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

Prüfen Sie die CIFS-Multiplex-Einstellungen

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

Schritte

1. Prüfen Sie die CIFS-Multiplex-Einstellung:

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

2. Ändern Sie die CIFS-Multiplex-Einstellung:

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

Beispiel

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

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

Überprüfen Sie die Geschwindigkeit des FC-Adapter-Ports

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

Was Sie benötigen

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

Schritte

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

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

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

```
fcp adapter show -instance
```

3. Ändern Sie ggf. die Portgeschwindigkeit:

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

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

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

5. Stellen Sie alle LIFs am Adapter online:

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

Beispiel

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

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

Überprüfen Sie die Netzwerkeinstellungen auf den Datenschaltern

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

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

Verfahren

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

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

Überprüfen Sie die MTU-Netzwerkeinstellung auf dem Storage-System

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

Über diese Aufgabe

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

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

Netzwerkeinstellungen auf den Datenschaltern".

Schritte

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

```
network port show -instance
```

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

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

Beispiel

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

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

Überprüfen Sie den Durchsatz und die Latenz der Festplatte

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

Über diese Aufgabe

Für diese Aufgabe sind erweiterte Befehle auf Berechtigungsebene erforderlich.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

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

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

Beispiel

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

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

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

Prüfen Sie Durchsatz und Latenz zwischen Nodes

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

Was Sie benötigen

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

Über diese Aufgabe

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

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



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

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

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

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

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Messung des Durchsatzes und der Latenz zwischen Nodes:

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

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

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

```
cluster1::> network test-path -source-node node1 -destination-cluster cluster2 -destination-node node3 -session-type AsyncMirrorRemote
Test Duration:          10.88 secs
Send Throughput:        18.23 MB/sec
Receive Throughput:     18.23 MB/sec
MB sent:                 198.31
MB received:            198.31
Avg latency in ms:      2301.47
Min latency in ms:      61.14
Max latency in ms:      3056.86
```

3. Zurück zur Administratorberechtigung:

```
set -privilege admin
```

Nachdem Sie fertig sind

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

Management von Workloads

Ermittlung der verbleibenden Performance-Kapazität

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

Was Sie benötigen

Für diese Aufgabe sind erweiterte Befehle auf Berechtigungsebene erforderlich.

Über diese Aufgabe

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

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

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

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Starten Sie die Echtzeitstatistik:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

3. Anzeigen von Informationen zu Reservestatistiken in Echtzeit:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

4. Zurück zur Administratorberechtigung:

```
set -privilege admin
```

Beispiel

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

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

Sie könnten angegeben haben `ewma_daily`, `ewma_weekly`, Oder `ewma_monthly` Um dieselben

Informationen über längere Zeiträume gemittelt zu erhalten.

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

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

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

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

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

2 entries were displayed.

Identifizieren von Clients oder Dateien mit hohem Datenverkehr

Mit der ONTAP Technologie für aktive Objekte können Kunden oder Dateien identifiziert werden, die für unverhältnismäßig hohe Mengen an Cluster-Datenverkehr verantwortlich sind. Sobald Sie die „wichtigsten“ Clients oder Dateien identifiziert haben, können Sie

Cluster-Workloads ausgleichen oder andere Schritte zur Behebung des Problems Unternehmen.

Was Sie benötigen

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

Schritte

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

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

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

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

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

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

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

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

Garantierter Durchsatz durch QoS

Durchsatz garantieren mit QoS-Übersicht

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

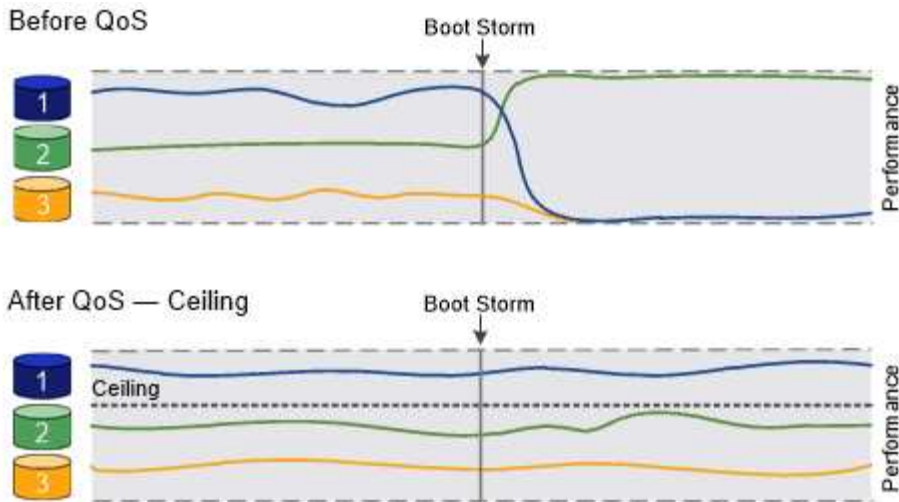
Allgemeines zu Durchsatzbegrenzungen (QoS max.)

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

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



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



Allgemeines zu Durchsatzböden (QoS Min.)

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



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

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

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



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

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

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

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

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

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

Allgemeines zur anpassungsfähigen QoS

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

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

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



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

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

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

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

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

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

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

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

Vorlage für adaptive Richtliniengruppen

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

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

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

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

Allgemeiner Support

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

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

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

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

Unterstützte Workloads bei Durchsatzbegrenzungen

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

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

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

Unterstützte Workloads für Durchsatzböden

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

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

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

Unterstützte Workloads für anpassungsfähige QoS

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

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

Maximale Anzahl an Workloads und Richtliniengruppen

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

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

Aktivieren oder Deaktivieren von Durchsatzböden v2

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

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Geben Sie einen der folgenden Befehle ein:

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



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

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

Befehl auf Quell- und Ziel-Clustern.

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

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.

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

Schritte

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

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

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

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

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

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

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

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

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

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

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

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

4. Überwachung der Richtliniengruppenleistung:

```
qos statistics performance show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.



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

Mit dem folgenden Befehl wird die Performance der Richtliniengruppe angezeigt:

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

Policy Group	IOPS	Throughput	Latency
-total-	12316	47.76MB/s	1264.00us
pg_app2	7216	28.19MB/s	420.00us
_System-Best-Effort	62	13.36KB/s	4.13ms
_System-Background	30	0KB/s	0ms

5. Monitoring der Workload-Performance:

```
qos statistics workload performance show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.



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

Mit dem folgenden Befehl wird die Workload-Performance angezeigt:

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

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



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

Verwendung von adaptiven QoS-Richtliniengruppen

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

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



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

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

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



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

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

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

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

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

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

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

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

Schritte

1. Erstellung einer anpassungsfähigen QoS-Richtliniengruppe:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.



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

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

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

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

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

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

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

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

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

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

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

Legen Sie eine Vorlage für adaptive Richtliniengruppen fest

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

Über diese Aufgabe

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

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

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

Schritte

1. SVM so ändern, dass sie die Vorlage für die Gruppe der anpassbaren Richtlinien anwendet:
`vserver modify -qos-adaptive-policy-group-template apg1`

2. Bestätigen Sie, dass die Richtlinie festgelegt wurde:
`vserver show -fields qos-adaptive-policy-group`

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.

Verwandte Links:

- ["Erfahren Sie mehr über Active IQ Unified Manager"](#)
- ["Erste Schritte mit Active IQ Unified Manager für VMware"](#)
- ["Erste Schritte mit Active IQ Unified Manager für Linux"](#)
- ["Erste Schritte mit Active IQ Unified Manager für Windows"](#)

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 sich über die Cloud Insights Benutzeroberfläche Join-Informationen anzeigen lassen. Benachrichtigungen, die auf Active IQ Unified Manager gepostet werden, werden nicht übersehen und können 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.

Weiterführende Links

- ["Erfahren Sie mehr über Cloud Insights"](#)
- ["Legen Sie los – mit Cloud Insights"](#)

Audit-Protokollierung

So implementiert ONTAP Audit-Protokollierung

Die im Audit-Protokoll aufgezeichneten Managementaktivitäten sind Teil der AutoSupport-Standardberichte und bestimmte Protokollierungsaktivitäten werden in EMS-Nachrichten erfasst. Sie können das Auditprotokoll auch an die von Ihnen angegebenen Ziele weiterleiten und Audit-Log-Dateien über die CLI oder einen Webbrowser anzeigen.

Ab ONTAP 9.11.1 können Sie den Inhalt des Revisionsprotokolls mithilfe von System Manager anzeigen.

Ab ONTAP 9.12.1 bietet ONTAP Manipulationswarnungen für Prüfprotokolle. ONTAP führt einen täglichen Hintergrundjob aus, um auf Manipulation von audit.log Dateien zu überprüfen und sendet eine EMS-Warnung, wenn Protokolldateien gefunden werden, die geändert oder manipuliert wurden.

ONTAP protokolliert Managementaktivitäten, die auf dem Cluster ausgeführt werden, beispielsweise eine Anfrage, den Benutzer, der die Anforderung ausgelöst hat, die Zugriffsmethode des Benutzers und die Zeit der Anfrage.

Die Management-Aktivitäten können eine der folgenden Arten sein:

- LEGEN Sie Anforderungen FEST, die in der Regel für Befehle oder Vorgänge ohne Anzeige gelten
 - Diese Anfragen werden ausgegeben, wenn Sie ein ausführen `create`, `modify`, Oder `delete` Befehl zum Beispiel.
 - Festgelegte Anforderungen werden standardmäßig protokolliert.

- ABRUFEN von Anforderungen, die Informationen abrufen und in der Managementoberfläche anzeigen
 - Diese Anfragen werden ausgegeben, wenn Sie ein ausführen `show` Befehl zum Beispiel.
 - GET Requests werden nicht standardmäßig protokolliert, Sie können jedoch kontrollieren, ob GET Requests from the ONTAP CLI gesendet WERDEN (`-cliget`), aus der ONTAP API (`-ontapiget`), oder von der REST API (`-httpget`) Sind in der Datei protokolliert.

ONTAP zeichnet die Managementaktivitäten in auf `/mroot/etc/log/mlog/audit.log` Datei eines Node. Befehle aus den drei Shells für CLI-Befehle - die clustershell, die nodeshell, und die nicht-interaktive Systemshell (interaktive Systemshell-Befehle werden nicht protokolliert)- sowie API-Befehle werden hier protokolliert. In den Audit-Protokollen werden Zeitstempel verwendet, um anzuzeigen, ob alle Nodes in einem Cluster Zeit synchronisiert sind.

Der `audit.log` Die Datei wird vom AutoSupport-Tool an die angegebenen Empfänger gesendet. Sie können den Inhalt auch sicher an angegebene externe Ziele weiterleiten, z. B. an einen Splunk oder Syslog-Server.

Der `audit.log` Die Datei wird täglich gedreht. Die Rotation tritt auch auf, wenn sie 100 MB groß erreicht, und die vorherigen 48 Kopien erhalten bleiben (mit maximal 49 Dateien). Wenn die Audit-Datei ihre tägliche Rotation durchführt, wird keine EMS-Nachricht erzeugt. Wenn die Überwachungsdatei sich dreht, weil ihre Dateigröße überschritten wird, wird eine EMS-Nachricht generiert.

Änderungen an der Auditprotokollierung in ONTAP 9

Ab ONTAP 9 beginnt der `command-history.log` Datei wird durch ersetzt `audit.log`, Und das `mgwd.log` Die Datei enthält keine Audit-Informationen mehr. Wenn Sie ein Upgrade auf ONTAP 9 durchführen, sollten Sie alle Skripte oder Tools lesen, die sich auf die vorhandenen Dateien und deren Inhalte beziehen.

Nach dem Upgrade auf ONTAP 9 ist vorhanden `command-history.log` Dateien bleiben erhalten. Sie werden als neu ausgedreht (gelöscht) `audit.log` Dateien werden in gedreht (erstellt).

Tools und Skripte, die den prüfen `command-history.log` Die Datei wird möglicherweise weiterhin verwendet, da ein Soft-Link von verwendet wird `command-history.log` Bis `audit.log` Wird beim Upgrade erstellt. Jedoch Tools und Skripte, die prüfen, die `mgwd.log` Die Datei schlägt fehl, da diese Datei keine Audit-Informationen mehr enthält.

Darüber hinaus enthalten Audit-Protokolle in ONTAP 9 und höher nicht mehr die folgenden Einträge, da sie nicht als nützlich betrachtet werden und unnötige Protokollierungsaktivitäten verursachen:

- Interne Befehle, die von ONTAP ausgeführt werden (d. h., Benutzername=Root)
- Befehlsaliasen (getrennt vom Befehl, auf den sie verweisen)

Ab ONTAP 9 können Sie die Prüfprotokolle sicher mit den Protokollen TCP und TLS an externe Ziele übertragen.

Zeigt den Inhalt des Prüfprotokolls an

Sie können den Inhalt des Clusters anzeigen `/mroot/etc/log/mlog/audit.log` Dateien mithilfe der ONTAP-CLI, System Manager oder eines Webbrowsers.

Die Protokolldateieinträge des Clusters umfassen Folgendes:

Zeit

Zeitstempel der Protokolleingabe.

Applikation

Die Anwendung, die zum Herstellen einer Verbindung zum Cluster verwendet wird. Beispiele für mögliche Werte sind `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, Und `service-processor`.

Benutzer

Der Benutzername des Remote-Benutzers.

Bundesland

Der aktuelle Status des Audit-Antrags. Dies kann der Fall sein `success`, `pending`, Oder `error`.

Nachricht

Ein optionales Feld, das Fehler oder zusätzliche Informationen zum Status eines Befehls enthalten kann.

Sitzungs-ID

Die Sitzungs-ID, für die die Anforderung eingeht. Jeder `SSH_Session_` wird eine Session-ID zugewiesen, während jedem HTTP, ONTAPI oder SNMP *Request* eine eindeutige Session-ID zugewiesen wird.

Storage VM

Der SVM, über die der Benutzer verbunden ist.

Umfang

Anzeigen `svm` Wenn sich die Anforderung auf einer Storage-VM befindet, wird anderenfalls angezeigt `cluster`.

Command ID

Die ID für jeden Befehl, der in einer CLI-Sitzung empfangen wurde. So können Sie Anfragen und Antworten korrelieren. ZAPI-, HTTP- und SNMP-Anforderungen verfügen nicht über Befehl-IDs.

Sie können die Protokolleinträge des Clusters aus der ONTAP CLI, aus einem Webbrowser und beginnend mit ONTAP 9.11.1, von System Manager anzeigen.

System Manager

- Um den Bestand anzuzeigen, wählen Sie **Events & Jobs > Audit Logs**. + jede Spalte verfügt über Steuerelemente zum Filtern, Sortieren, Suchen, Anzeigen und Inventar Kategorien. Die Bestandsdetails können als Excel-Arbeitsmappe heruntergeladen werden.
- Um Filter einzustellen, klicken Sie oben rechts auf die Schaltfläche **Filter** und wählen Sie dann die gewünschten Felder aus. + Sie können auch alle Befehle anzeigen, die in der Sitzung ausgeführt wurden, in der ein Fehler aufgetreten ist, indem Sie auf den Link Session-ID klicken.

CLI

Um die von mehreren Knoten im Cluster zusammengeführten Auditeinträge anzuzeigen, geben Sie: + ein `security audit log show [parameters]`

Sie können das verwenden `security audit log show` Befehl zum Anzeigen von Auditeinträgen für einzelne Nodes oder, die von mehreren Nodes im Cluster zusammengeführt wurden. Sie können auch den Inhalt des anzeigen `/mroot/etc/log/mlog` Verzeichnis auf einem einzelnen Knoten mit einem Webbrowser. Details finden Sie auf der man-Seite.

Webbrowser


Sie können den Inhalt des anzeigen `/mroot/etc/log/mlog` Verzeichnis auf einem einzelnen Knoten mit einem Webbrowser. ["Erfahren Sie, wie Sie auf einen Knoten Protokoll zugreifen, Core Dump, und MIB-Dateien mit einem Web-Browser"](#).

Verwalten DER Einstellungen für AUDITANFRAGE

Während FESTGELEGTE Anforderungen standardmäßig protokolliert werden, sind GET-Anforderungen nicht. Sie können jedoch kontrollieren, ob Anfragen von ONTAP HTML gesendet WERDEN (`-httpget`), die ONTAP CLI (`-cliget`) Oder von den ONTAP APIs (`-ontapiget`) Sind in der Datei protokolliert.

Sie können die Einstellungen für die Protokollierung von Audits über die ONTAP-CLI ändern, und beginnend mit ONTAP 9.11.1, in System Manager.

System Manager

1. Wählen Sie **Events & Jobs > Audit Logs** Aus.
2. Klicken Sie Auf  Wählen Sie in der rechten oberen Ecke die Anforderungen aus, die hinzugefügt oder entfernt werden sollen.

CLI

- Um festzulegen, dass GET-Anforderungen aus der ONTAP-CLI oder APIs im Audit-Protokoll (die Datei audit.log) aufgezeichnet werden sollen, geben Sie zusätzlich zu den Standard-Set-Anforderungen: + ein
`security audit modify [-cliget {on|off}][--httpget {on|off}][--ontapiget {on|off}]`
- Um die aktuellen Einstellungen anzuzeigen, geben Sie: + ein
`security audit show`

Weitere Informationen finden Sie auf den man-Pages.

Verwalten von Zielen für Überwachungsprotokolle

Sie können das Audit-Protokoll an maximal 10 Ziele weiterleiten. Sie können das Protokoll beispielsweise an einen Splunk oder Syslog-Server für Monitoring-, Analyse- und Backup-Zwecke weiterleiten.

Über diese Aufgabe

Für die Konfiguration der Weiterleitung müssen Sie die IP-Adresse des Syslog- oder Splunk-Hosts, seine Portnummer, ein Übertragungsprotokoll sowie die Syslog-Einrichtung für die weitergeleiteten Protokolle angeben. ["Hier erfahren Sie mehr über Syslog-Funktionen"](#).

Sie können einen der folgenden Übertragungswerte auswählen:

UDP unverschlüsselt

User Datagram Protocol ohne Sicherheit (Standard)

TCP unverschlüsselt

Übertragungsprotokoll ohne Sicherheit

TCP verschlüsselt

Transmission Control Protocol mit Transport Layer Security (TLS) + A **Verify Server** Option ist verfügbar, wenn das TCP verschlüsselte Protokoll ausgewählt ist.

Sie können die Prüfprotokolle von der ONTAP CLI, und beginnend mit ONTAP 9.11.1, von System Manager weiterleiten.

System Manager

- Um die Ziele des Prüfprotokolls anzuzeigen, wählen Sie **Cluster >Einstellungen**. + die Anzahl der Protokollziele wird in der Kachel **Benachrichtigungsmanagement** angezeigt. Klicken Sie Auf **:** Um Details anzuzeigen.
- Um Ziele für das Auditprotokoll hinzuzufügen, zu ändern oder zu löschen, wählen Sie **Events & Jobs > Audit Logs** und klicken Sie dann rechts oben auf dem Bildschirm auf **Audit-Ziele verwalten**. + Klicken **+ Add**, Oder klicken Sie auf **:** In der Spalte **Host Address** können Sie Einträge bearbeiten oder löschen.

CLI

1. Geben Sie für jedes Ziel, an das Sie das Prüfprotokoll weiterleiten möchten, die Ziel-IP-Adresse oder den Host-Namen und alle Sicherheitsoptionen an.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

- Wenn der `cluster log-forwarding create` Der Befehl kann den Ziel-Host nicht pingen, um die Verbindung zu überprüfen. Der Befehl schlägt mit einem Fehler fehl. Obwohl nicht empfohlen, verwenden Sie die `-force` Parameter mit dem Befehl umgeht die Konnektivitätsprüfung.
 - Wenn Sie die einstellen `-verify-server` Parameter an `true`, Die Identität des Protokollweiterleitungsziels wird durch die Validierung seines Zertifikats überprüft. Sie können den Wert auf einstellen `true` Nur wenn Sie das auswählen `tcp-encrypted` Wert im `-protocol` Feld.
2. Überprüfen Sie, ob die Zieldatensätze korrekt sind, indem Sie die verwenden `cluster log-forwarding show` Befehl.

```
cluster1::> cluster log-forwarding show
```

Destination Host	Port	Protocol	Verify Server	Syslog Facility
192.168.123.96	514	udp-unencrypted	false	user
192.168.123.98	514	tcp-encrypted	true	user

2 entries were displayed.

Weitere Informationen finden Sie auf den man-Pages.

AutoSupport

Managen Sie AutoSupport-Einstellungen mit System Manager

Sie können mit System Manager die Einstellungen für Ihr AutoSupport Konto verwalten.

Sie können folgende Aktionen durchführen:

Zeigen Sie AutoSupport-Einstellungen an

Mit System Manager können Sie die Einstellungen für Ihr AutoSupport Konto anzeigen.

Schritte

1. Klicken Sie in System Manager auf **Cluster > Einstellungen**.

Im Abschnitt **AutoSupport** werden folgende Informationen angezeigt:

- Status
- Transportprotokoll
- Proxy-Server
- Von E-Mail-Adresse


2. Wählen Sie im Abschnitt **AutoSupport** die Option aus  Wählen Sie dann **Weitere Optionen**.

Weitere Informationen zu den AutoSupport-Verbindungs- und E-Mail-Einstellungen werden angezeigt. Außerdem wird der Übertragungsverlauf von Nachrichten aufgelistet.

AutoSupport Daten generieren und senden

In System Manager können Sie die Generierung von AutoSupport Meldungen initiieren und aus welchem Cluster-Node oder welchen Nodes die Daten erfasst werden.


Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **AutoSupport** die Option aus  Wählen Sie dann **Generieren und Senden**.
3. Geben Sie einen Betreff ein.
4. Aktivieren Sie das Kontrollkästchen unter **Collect Data From**, um die Knoten anzugeben, von denen die Daten erfasst werden sollen.

Verbindung zu AutoSupport testen

Von System Manager können Sie eine Testmeldung senden, um die Verbindung zu AutoSupport zu überprüfen.

Schritte

1. Klicken Sie in System Manager auf **Cluster > Einstellungen**.
2. Wählen Sie im Abschnitt **AutoSupport** die Option aus  Wählen Sie dann **Verbindung testen**.
3. Geben Sie einen Betreff für die Nachricht ein.

Aktivieren oder deaktivieren Sie AutoSupport



AutoSupport bietet NetApp Kunden bewährte geschäftliche Vorteile. Dazu zählt die proaktive Erkennung möglicher Konfigurationsprobleme und die schnellere Behebung von Support-Fällen. AutoSupport ist in neuen Systemen standardmäßig aktiviert. Bei Bedarf können Sie mit System Manager die Fähigkeit von AutoSupport zum Überwachen des Zustands des Storage-Systems und zum Senden von Benachrichtigungen deaktivieren. Sie können AutoSupport erneut aktivieren, nachdem sie deaktiviert wurde.

Über diese Aufgabe

Bevor Sie AutoSupport deaktivieren, sollten Sie beachten, dass Sie das NetApp Call-Home-System ausschalten, und Sie verlieren die folgenden Vorteile:

- **Systemüberwachung:** AutoSupport überwacht den Zustand Ihres Speichersystems und sendet Benachrichtigungen an den technischen Support und Ihre interne Supportorganisation.
- **Automatisierung:** AutoSupport automatisiert das Reporting von Support Cases. Die meisten Support-Fälle werden automatisch geöffnet, bevor Kunden ein Problem erkennen.
- **Schnellere Lösung:** Systeme, die AutoSupport-Daten senden, haben ihre Support-Fälle in der Hälfte der Zeit gelöst, im Vergleich zu Fällen, bei denen keine AutoSupport-Daten gesendet werden.
- **Schnellere Upgrades:** AutoSupport unterstützt Self-Service-Workflows von Kunden wie Versionsupgrades, Add-ons, Verlängerungen und die Automatisierung von Firmware-Updates in System Manager.
- **Weitere Funktionen:** Bestimmte Funktionen in anderen Tools funktionieren nur, wenn AutoSupport aktiviert ist, zum Beispiel einige Workflows in BlueXP.

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie im Abschnitt **AutoSupport** die Option aus  Wählen Sie dann **Deaktivieren**.
3. Wenn Sie AutoSupport wieder aktivieren möchten, wählen Sie im Abschnitt **AutoSupport** die Option aus  Wählen Sie dann **enable**.

Generierung von Support-Fällen unterdrücken


Ab ONTAP 9.10.1 können Sie mit System Manager eine Anfrage an AutoSupport senden, um die Erstellung von Support-Fällen zu unterdrücken.

Über diese Aufgabe

Um die Generierung von Supportfällen zu unterdrücken, geben Sie die Knoten und die Anzahl der Stunden an, für die die Unterdrückung stattfinden soll.

Das Unterdrücken von Support-Cases ist besonders hilfreich, wenn AutoSupport während der Wartungsarbeiten an Ihren Systemen keine automatisierten Cases erstellt.


Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie im Abschnitt **AutoSupport** die Option aus  Wählen Sie dann **Support Case Generation unterdrücken**.
3. Geben Sie die Anzahl der Stunden ein, die die Unterdrückung stattfinden soll.
4. Wählen Sie die Knoten aus, für die die Unterdrückung stattfinden soll.

Wiederaufnahme der Erstellung von Support-Cases

Ab ONTAP 9.10.1 können Sie mit System Manager die Generierung von Support-Cases von AutoSupport fortsetzen, wenn diese unterdrückt wurde.



Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie im Abschnitt **AutoSupport** die Option aus  Wählen Sie dann **Support Case Generation fortsetzen**.
3. Wählen Sie die Knoten aus, für die die Erzeugung fortgesetzt werden soll.

AutoSupport-Einstellungen bearbeiten

Mit System Manager können Sie die Verbindungs- und E-Mail-Einstellungen für Ihr AutoSupport Konto ändern.

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie im Abschnitt **AutoSupport** die Option aus  Wählen Sie dann **Weitere Optionen**.
3. Wählen Sie im Abschnitt **Verbindungen** oder im Abschnitt **E-Mail** die Option aus  **Edit** Um die Einstellungen für einen der Abschnitte zu ändern.

Verwalten Sie AutoSupport mit der CLI

AutoSupport managen – Übersicht

AutoSupport ist ein Mechanismus, der proaktiv den Zustand Ihres Systems überwacht und automatisch Meldungen an den technischen Support von NetApp, Ihre interne Support-Abteilung und einen Support-Partner sendet. Obwohl AutoSupport Meldungen an den technischen Support standardmäßig aktiviert sind, müssen Sie die richtigen Optionen festlegen und einen gültigen Mail-Host besitzen, der Meldungen an Ihre interne Support-Abteilung gesendet hat.

Nur der Cluster-Administrator kann AutoSupport-Management durchführen. Der SVM-Administrator (Storage Virtual Machine) hat keinen Zugriff auf AutoSupport.

AutoSupport ist standardmäßig aktiviert, wenn Sie das Storage-System zum ersten Mal konfigurieren. AutoSupport beginnt 24 Stunden nach Aktivierung von AutoSupport mit dem Senden von Meldungen an den technischen Support. Sie können die Dauer von 24 Stunden verkürzen, indem Sie das System aktualisieren oder zurücksetzen, die AutoSupport Konfiguration ändern oder die Systemzeit auf eine andere als 24 Stunden verkürzen.



Sie können AutoSupport jederzeit deaktivieren, aber Sie sollten sie aktiviert lassen. Wenn auf dem Storage-System ein Problem auftritt, kann die Problembestimmung und -Behebung durch das Aktivieren von AutoSupport erheblich beschleunigt werden. Standardmäßig erfasst das System AutoSupport Informationen und speichert sie lokal, selbst wenn Sie AutoSupport deaktivieren.

Weitere Informationen zu AutoSupport finden Sie auf der NetApp Support Site.

Verwandte Informationen

- ["NetApp Support"](#)
- ["Weitere Informationen zu den AutoSupport-Befehlen finden Sie in der ONTAP-CLI"](#)

Nutzen Sie AutoSupport und Active IQ Digital Advisor

Die AutoSupport-Komponente von ONTAP erfasst Telemetrie und sendet diese zur Analyse. Active IQ Digital Advisor analysiert die Daten von AutoSupport und bietet proaktive Betreuung und Optimierung. Mithilfe künstlicher Intelligenz erkennt Active IQ potenzielle Probleme und löst sie, bevor sie sich auf das Geschäft auswirken.

Mit Active IQ optimieren Kunden ihre Dateninfrastruktur in der gesamten globalen Hybrid Cloud. Dazu bieten sie konkrete prädiktive Analysen und proaktiven Support über ein Cloud-basiertes Portal und eine mobile App. NetApp Kunden mit aktivem SupportEdge-Vertrag profitieren von Daten-fokussierten Einblicken und Empfehlungen von Active IQ (Funktionen variieren je nach Produkt- und Support-Tier).

Folgende Möglichkeiten bietet Active IQ:

- Planung von Upgrades: Active IQ erkennt Probleme in Ihrer Umgebung, die durch ein Upgrade auf eine neuere Version von ONTAP behoben werden können, und die Upgrade Advisor Komponente unterstützt Sie bei der Planung eines erfolgreichen Upgrades.
- Sehen Sie sich das Wellness-System an. Ihr Active IQ Dashboard meldet alle Probleme im Zusammenhang mit dem Wellness-Bereich und hilft Ihnen, diese Probleme zu beheben. Überwachen Sie die Systemkapazität, um sicherzugehen, dass nie mehr Speicherplatz belegt wird. Zeigen Sie Support-Cases für Ihr System an.
- Performance-Management: Active IQ zeigt die System-Performance über einen längeren Zeitraum an, als Sie in System Manager sehen können. Identifizieren Sie Konfigurations- und Systemprobleme, die Ihre Performance beeinträchtigen.
- Maximale Effizienz Anzeige von Storage-Effizienz-Metriken und Identifizierung von Möglichkeiten, mehr Daten auf weniger Speicherplatz zu speichern
- Anzeige von Inventar und Konfiguration Active IQ zeigt vollständige Informationen zur Bestands- und Software- und Hardwarekonfiguration an. Prüfen Sie, wann die Serviceverträge ablaufen und verlängern Sie sie, um sicherzustellen, dass der Support weiterhin gewährleistet ist.

Verwandte Informationen

["NetApp Dokumentation: Active IQ Digital Advisor"](#)

["Starten Sie Active IQ"](#)

["SupportEdge Services"](#)

Wann und wo AutoSupport Meldungen gesendet werden

AutoSupport sendet je nach Nachrichtentyp Meldungen an verschiedene Empfänger. Wann und wo AutoSupport Nachrichten sendet, können Ihnen dabei helfen, Mitteilungen zu verstehen, die Sie per E-Mail oder auf der Active IQ-Website (ehemals My AutoSupport) erhalten.

Sofern nicht anders angegeben, handelt es sich bei den Einstellungen in den folgenden Tabellen um Parameter des `system node autosupport modify` Befehl.

Ereignisgesteuerte Meldungen

Wenn auf dem System Ereignisse auftreten, die Korrekturmaßnahmen erfordern, sendet AutoSupport automatisch eine Meldung, bei der ein Ereignis ausgelöst wurde.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
AutoSupport antwortet auf ein Trigger-Ereignis im EMS	Adressen angegeben in <code>-to</code> Und <code>-noteto</code> . (Es werden nur kritische Ereignisse gesendet, die sich auf den Service auswirken.) Adressen angegeben in <code>-partner-address</code> Technische Unterstützung, wenn <code>-support</code> Ist auf festgelegt <code>enable</code>

Geplante Nachrichten

AutoSupport sendet automatisch mehrere Meldungen zu einem regelmäßigen Zeitplan.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
Täglich (standardmäßig wird zwischen 12:00 Uhr gesendet Und 1:00 Uhr Als Protokollmeldung)	Adressen angegeben in <code>-partner-address</code> Technische Unterstützung, wenn <code>-support</code> Ist auf festgelegt <code>enable</code>
Täglich (standardmäßig wird zwischen 12:00 Uhr gesendet Und 1:00 Uhr Als Leistungsmeldung), wenn der <code>-perf</code> Parameter ist auf festgelegt <code>true</code>	Adressen angegeben in <code>-Partner-address`</code> Technische Unterstützung, wenn <code>-support</code> Ist auf festgelegt <code>enable</code>
Wöchentlich (standardmäßig gesendet Sonntag zwischen 12:00 Uhr Und 1:00 Uhr)	Adressen angegeben in <code>-partner-address</code> Technische Unterstützung, wenn <code>-support</code> Ist auf festgelegt <code>enable</code>

Manuell ausgelöste Nachrichten

Sie können eine AutoSupport Meldung manuell initiieren oder erneut senden.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
<p>Sie initiieren eine Meldung manuell über das <code>system node autosupport invoke</code> Befehl</p>	<p>Wenn ein URI mit angegeben wird <code>-uri</code> Parameter in <code>system node autosupport invoke</code> Befehl, die Meldung wird an diesen URI gesendet.</p> <p>Wenn <code>-uri</code> Wird nicht angegeben, wird die Meldung an die in angegebenen Adressen gesendet <code>-to</code> Und <code>-partner-address</code>. Die Meldung wird auch an den technischen Support gesendet, wenn <code>-support</code> Ist auf festgelegt <code>enable</code>.</p>
<p>Sie initiieren eine Meldung manuell über das <code>system node autosupport invoke-core-upload</code> Befehl</p>	<p>Wenn ein URI mit angegeben wird <code>-uri</code> Parameter in <code>system node autosupport invoke-core-upload</code> Befehl, die Meldung wird an diesen URI gesendet und die Core Dump-Datei wird auf den URI hochgeladen.</p> <p>Wenn <code>-uri</code> Wird im nicht angegeben <code>system node autosupport invoke-core-upload</code> Befehl, die Meldung wird an den technischen Support gesendet und die Core Dump-Datei wird auf die Website des technischen Supports hochgeladen.</p> <p>Beide Szenarien erfordern das <code>-support</code> Ist auf festgelegt <code>enable</code> Und <code>-transport</code> Ist auf festgelegt <code>https</code> Oder <code>http</code>.</p> <p>Aufgrund der großen Größe von Core Dump-Dateien wird die Meldung nicht an die Adressen gesendet, die in angegeben sind <code>-to</code> Und <code>-partner-addresses</code> Parameter.</p>

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
Sie initiieren eine Meldung manuell über das <code>system node autosupport invoke-performance-archive</code> Befehl	<p>Wenn ein URI mit angegeben wird <code>-uri</code> Parameter in <code>system node autosupport invoke-performance-archive</code> Befehl, die Meldung wird an diesen URI gesendet und die Performance-Archivdatei wird auf den URI hochgeladen.</p> <p>Wenn <code>-uri</code> Wird im nicht angegeben <code>system node autosupport invoke-performance-archive</code>, Die Nachricht wird an den technischen Support gesendet, und die Archiv-Datei für die Performance wird auf die Website des technischen Supports hochgeladen.</p> <p>Beide Szenarien erfordern das <code>-support</code> Ist auf festgelegt <code>enable</code> Und <code>-transport</code> Ist auf festgelegt <code>https</code> Oder <code>http</code>.</p> <p>Aufgrund der großen Größe von Performance-Archivdateien wird die Meldung nicht an die Adressen gesendet, die in angegeben sind <code>-to</code> Und <code>-partner-addresses</code> Parameter.</p>
Sie senden eine frühere Nachricht manuell mit dem erneut <code>system node autosupport history retransmit</code> Befehl	Nur für den URI, den Sie im angeben <code>-uri</code> Parameter von <code>system node autosupport history retransmit</code> Befehl

Meldungen, die durch den technischen Support ausgelöst werden

Der technische Support kann Meldungen von AutoSupport über die AutoSupport OnDemand Funktion anfordern.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
Wenn das AutoSupport Lieferanweisungen erhält, um neue AutoSupport Meldungen zu generieren	<p>Adressen angegeben in <code>-partner-address</code></p> <p>Technische Unterstützung, wenn <code>-support</code> Ist auf festgelegt <code>enable</code> Und <code>-transport</code> Ist auf festgelegt <code>https</code></p>
Wenn AutoSupport Lieferanweisungen erhält, um frühere AutoSupport Meldungen erneut zu senden	Technische Unterstützung, wenn <code>-support</code> Ist auf festgelegt <code>enable</code> Und <code>-transport</code> Ist auf festgelegt <code>https</code>
Wenn AutoSupport Anweisungen zur Bereitstellung erhält, um neue AutoSupport Meldungen zu generieren, die Core Dump- oder Performance-Archivdateien hochladen	Technische Unterstützung, wenn <code>-support</code> Ist auf festgelegt <code>enable</code> Und <code>-transport</code> Ist auf festgelegt <code>https</code> . Die Core Dump- oder Performance-Archivdatei wird auf die technische Support-Website hochgeladen.

Wie AutoSupport ereignisgesteuerte Meldungen erstellt und sendet

AutoSupport erstellt ereignisgesteuerte AutoSupport-Meldungen, wenn das EMS ein Trigger-Ereignis verarbeitet. Eine ereignisgesteuerte AutoSupport-Meldung benachrichtigt Empfänger von Problemen, die Korrekturmaßnahmen erfordern und enthält nur für das Problem relevante Informationen. Sie können anpassen, welche Inhalte enthalten werden sollen und wer die Nachrichten erhält.

AutoSupport verwendet den folgenden Prozess, um ereignisgesteuerte AutoSupport-Meldungen zu erstellen und zu senden:

1. Wenn das EMS ein Triggerereignis verarbeitet, sendet EMS eine Anfrage an AutoSupport.

Ein Auslöser ist ein EMS-Ereignis mit einem AutoSupport Ziel und einem Namen, der mit einem beginnt `callhome.` Präfix.

2. AutoSupport erstellt eine ereignisgesteuerte AutoSupport-Meldung.

AutoSupport sammelt grundlegende und Fehlerbehebungsinformationen von Subsystemen, die mit dem Auslöser verbunden sind, um eine Meldung zu erstellen, die nur relevante Informationen für das Trigger-Ereignis enthalten.

Jedem Trigger ist ein Standardsatz von Untersystemen zugeordnet. Sie können jedoch wählen, ob Sie zusätzliche Untersysteme mit einem Trigger verknüpfen möchten, indem Sie das verwenden `system node autosupport trigger modify` Befehl.

3. AutoSupport sendet die ereignisgesteuerte AutoSupport-Nachricht an die vom definierten Empfänger `system node autosupport modify` Befehl mit dem `-to`, `-noteto`, `-partner-address`, und `-support` Parameter.

Sie können die Übermittlung von AutoSupport Meldungen für bestimmte Auslöser aktivieren und deaktivieren, indem Sie das verwenden `system node autosupport trigger modify` Befehl mit dem `-to` Und `-noteto` Parameter.

Beispiel für Daten, die für ein bestimmtes Ereignis gesendet werden

Der `storage shelf PSU failed` EMS-Ereignis löst eine Nachricht aus, die Basisdaten aus obligatorischen, Log-Dateien, Speicher, RAID, HA, enthält. Plattform- und Netzwerk-Subsysteme sowie Daten zur Fehlerbehebung von obligatorischen, Log-Dateien und Storage-Subsystemen.

Sie möchten künftig Daten zu NFS in alle AutoSupport-Meldungen aufnehmen, die als Antwort gesendet werden `storage shelf PSU failed` Ereignis: Sie geben den folgenden Befehl ein, um die Fehlerbehebung von Daten für NFS für die zu aktivieren `callhome.shlf.ps.fault` Ereignis:

```
cluster1::\>
system node autosupport trigger modify -node nodel -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Beachten Sie, dass die `callhome.` Das Präfix wird vom gelöscht `callhome.shlf.ps.fault` Ereignis, wenn Sie das verwenden `system node autosupport trigger` Befehle, oder bei Verwendung von AutoSupport- und EMS-Ereignissen in der CLI.

Arten von AutoSupport Nachrichten und deren Inhalt

AutoSupport-Meldungen enthalten Statusinformationen zu unterstützten Subsystemen. Erfahren Sie, welche AutoSupport-Nachrichten enthalten, können Sie dabei unterstützen, Nachrichten zu interpretieren oder auf sie zu reagieren, die Sie per E-Mail oder auf der Active IQ-Website (früher unter dem Namen „My AutoSupport“ bekannt) erhalten.

Nachrichtentyp	Typ der Daten, die die Nachricht enthält
Ereignis ausgelöst	Dateien, die kontextsensitive Daten über das spezifische Subsystem enthalten, in dem das Ereignis aufgetreten ist
Täglich	Log-Dateien
Leistung	Performance-Daten, die in den letzten 24 Stunden erfasst wurden
Wöchentlich	Konfigurations- und Statusdaten
Ausgelöst durch das <code>system node autosupport invoke</code> Befehl	<p>Hängt von dem im angegebenen Wert ab <code>-type</code> Parameter:</p> <ul style="list-style-type: none">• <code>test</code> Sendet eine vom Benutzer ausgelöste Nachricht mit einigen Basisdaten. <p>Bei dieser Meldung wird außerdem eine automatische E-Mail-Antwort vom technischen Support auf alle angegebenen E-Mail-Adressen über das <code>ausgelöst -to</code> Option, damit Sie bestätigen können, dass die AutoSupport Meldungen empfangen werden.</p> <ul style="list-style-type: none">• <code>performance</code> Sendet Performance-Daten.• <code>all</code> Sendet eine vom Benutzer ausgelöste Nachricht mit einem vollständigen Satz von Daten, die der wöchentlichen Nachricht ähnlich sind, einschließlich der Fehlerbehebungsdaten von jedem Subsystem. <p>Technischer Support fordert diese Meldung in der Regel an.</p>
Ausgelöst durch das <code>system node autosupport invoke-core-upload</code> Befehl	Core Dump-Dateien für einen Node
Ausgelöst durch das <code>system node autosupport invoke-performance-archive</code> Befehl	Performance-Archivdateien für einen bestimmten Zeitraum

Nachrichtentyp	Typ der Daten, die die Nachricht enthält
Wird von AutoSupport OnDemand ausgelöst	<p>AutoSupport OnDemand kann neue Nachrichten oder frühere Nachrichten anfordern:</p> <ul style="list-style-type: none"> • Je nach Typ der AutoSupport-Sammlung können neue Meldungen lauten <code>test</code>, <code>all</code>, Oder <code>performance</code>. • Frühere Nachrichten hängen von der Art der Nachricht ab, die neu gesendet wird. <p>AutoSupport OnDemand kann neue Meldungen anfordern, die die folgenden Dateien auf die NetApp Support Site unter hochladen "mysupport.netapp.com":</p> <ul style="list-style-type: none"> • Core Dump • Performance-Archivierung

Was sind AutoSupport-Subsysteme

Jedes Subsystem enthält grundlegende und Fehlerbehebungsinformationen, die AutoSupport für seine Meldungen verwendet. Jedes Subsystem wird auch mit Triggerereignissen verbunden, sodass AutoSupport nur Informationen aus Subsystemen sammeln können, die für das Triggerereignis relevant sind.

AutoSupport erfasst kontextabhängige Inhalte. Sie können Informationen zu Subsystemen und Ereignissen über das `anzeigen system node autosupport trigger show` Befehl.

Budgets für die Größe und Zeit von AutoSupport

AutoSupport sammelt Informationen, organisiert nach Subsystem und erzwingt ein Volumen- und Zeitbudget für die Inhalte jedes Subsystems. Bei wachsendem Storage-System bieten AutoSupport-Budgets die Kontrolle über die AutoSupport-Nutzlast, wodurch wiederum die skalierbare Bereitstellung von AutoSupport Daten ermöglicht wird.

AutoSupport erfasst Informationen nicht mehr und schneidet den AutoSupport-Inhalt ab, wenn der Subsysteminhalt seine Größe oder ihr Budget überschreitet. Wenn der Inhalt nicht leicht gekürzt werden kann (z. B. Binärdateien), macht AutoSupport den Inhalt aus.

Sie sollten die Standardgröße und -Zeit nur ändern, wenn Sie dazu vom NetApp Support aufgefordert werden. Sie können auch die Standardgröße und das Zeitbudget der Subsysteme überprüfen, indem Sie die verwenden `autosupport manifest show` Befehl.

In ereignis ausgelösten AutoSupport Meldungen gesendete Dateien

Ereignisgesteuerte AutoSupport Meldungen enthalten nur grundlegende und Fehlerbehebungsinformationen aus Subsystemen, die mit dem Ereignis verknüpft sind, die zum Generieren der Meldung durch AutoSupport geführt haben. Diese Daten helfen NetApp Support und Support Partnern bei der Problemlösung.

AutoSupport verwendet die folgenden Kriterien, um Inhalte in ereignisausgelösten AutoSupport Meldungen zu kontrollieren:

- Welche Subsysteme sind im Lieferumfang enthalten

Daten werden zu Subsystemen wie allgemeinen Subsystemen wie z. B. Log-Dateien und speziellen Subsystemen wie z. B. RAID gruppiert. Jedes Ereignis löst eine Meldung aus, die nur die Daten aus spezifischen Subsystemen enthält.

- Die Detailebene jedes enthaltenen Subsystems

Die Daten für jedes enthaltene Subsystem werden auf Basis- oder Fehlerbehebungsebene bereitgestellt.

Sie können über das alle möglichen Ereignisse anzeigen und bestimmen, welche Subsysteme in Meldungen zu jedem Ereignis enthalten sind `system node autosupport trigger show` Befehl mit dem `-instance` Parameter.

Zusätzlich zu den standardmäßig für jedes Ereignis enthaltenen Subsystemen können Sie über das zusätzliche Subsysteme auf Basis- oder Fehlerbehebungsebene hinzufügen `system node autosupport trigger modify` Befehl.

In AutoSupport-Meldungen gesendete Protokolldateien

AutoSupport Meldungen können mehrere wichtige Protokolldateien enthalten, mit denen Mitarbeiter des technischen Supports die letzten Systemaktivitäten überprüfen können.

Alle Arten von AutoSupport-Meldungen können die folgenden Protokolldateien enthalten, wenn das Subsystem Log-Dateien aktiviert ist:

Protokolldatei	Menge der Daten aus der Datei enthalten
<ul style="list-style-type: none">• Log-Dateien aus dem <code>/mroot/etc/log/mlog/</code> Verzeichnis• DIE MELDUNGSPROTOKOLLDATTEI	<p>Es werden nur neue Zeilen hinzugefügt, die den Protokollen seit der letzten AutoSupport Meldung bis zu einem angegebenen Maximum hinzugefügt wurden. Dadurch wird sichergestellt, dass AutoSupport-Nachrichten über eindeutige, relevante und nicht überlappende Daten verfügen.</p> <p>(Log-Dateien von Partnern sind ausgenommen, für Partner sind maximal zulässige Daten enthalten.)</p>
<ul style="list-style-type: none">• Log-Dateien aus dem <code>/mroot/etc/log/shelflog/</code> Verzeichnis• Log-Dateien aus dem <code>/mroot/etc/log/acp/</code> Verzeichnis• Ereignismanagementsystem (EMS) Protokolldaten	<p>Die letzten Datenzeilen bis zu einem festgelegten Maximum.</p>

Der Inhalt von AutoSupport-Meldungen kann zwischen Versionen von ONTAP ändern.

In wöchentlichen AutoSupport Meldungen gesendete Dateien

Wöchentliche AutoSupport-Meldungen enthalten zusätzliche Konfigurations- und Statusdaten, die dazu dienen, Änderungen im System im Laufe der Zeit nachzuverfolgen.

Die folgenden Informationen werden in wöchentlichen AutoSupport Meldungen gesendet:

- Grundlegende Informationen über jedes Subsystem
- Inhalt der ausgewählten `/mroot/etc` Verzeichnisdateien
- Log-Dateien
- Ausgabe von Befehlen zur Angabe von Systemdaten
- Weitere Informationen, darunter Informationen zu replizierten Datenbanken (RDB), Service-Statistiken und mehr

Wie AutoSupport OnDemand Anweisungen zur Bereitstellung durch den technischen Support erhält

AutoSupport OnDemand kommuniziert regelmäßig mit dem technischen Support, um Lieferanweisungen für das Senden, erneute Senden und Ablehnen von AutoSupport Meldungen zu erhalten sowie große Dateien auf die NetApp Support Website hochzuladen. AutoSupport OnDemand ermöglicht das bedarfsgerechte Senden von AutoSupport Meldungen anstatt auf die Ausführung des wöchentlichen AutoSupport Jobs zu warten.

AutoSupport OnDemand besteht aus den folgenden Komponenten:

- AutoSupport OnDemand-Client, der auf jedem Node ausgeführt wird
- AutoSupport OnDemand Service im technischen Support

Der AutoSupport OnDemand Client fragt regelmäßig den AutoSupport OnDemand Service ab, um Anweisungen zum technischen Support zu erhalten. Beispielsweise kann der technische Support den AutoSupport OnDemand Service verwenden, um eine neue AutoSupport Meldung zu erstellen. Wenn der AutoSupport OnDemand-Client den AutoSupport OnDemand-Service abfragt, erhält der Client die Lieferanweisungen und sendet die neue AutoSupport Meldung nach Bedarf.

AutoSupport OnDemand ist standardmäßig aktiviert. AutoSupport OnDemand verlässt sich jedoch auf einige AutoSupport-Einstellungen, um die Kommunikation mit dem technischen Support fortzusetzen. AutoSupport OnDemand kommuniziert automatisch mit dem technischen Support, wenn die folgenden Anforderungen erfüllt sind:

- AutoSupport ist aktiviert.
- AutoSupport wurde konfiguriert, um Meldungen an den technischen Support zu senden.
- AutoSupport ist für die Verwendung des HTTPS-Transportprotokolls konfiguriert.

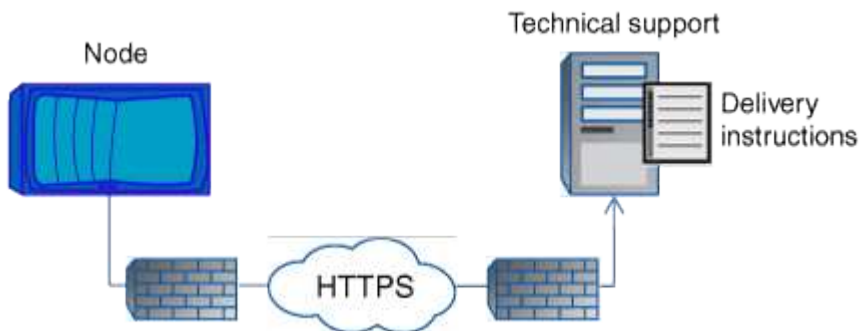
Der AutoSupport OnDemand-Client sendet HTTPS-Anforderungen an denselben technischen Support-Standort, an den AutoSupport Meldungen gesendet werden. Der AutoSupport OnDemand-Client akzeptiert keine eingehenden Verbindungen.



AutoSupport OnDemand kommuniziert über das „AutoSupport“ Benutzerkonto mit dem technischen Support. ONTAP verhindert, dass Sie dieses Konto löschen.

Wenn Sie AutoSupport OnDemand deaktivieren, AutoSupport jedoch aktiviert lassen möchten, verwenden Sie den Befehl `Link:https://docs.netapp.com/us-en/ontap-cli-9121/system-node-autosupport-modify.html#parameters[system node autosupport modify -ondemand-state disable]`.

Die folgende Abbildung zeigt, wie AutoSupport OnDemand HTTPS-Anfragen an den technischen Support sendet, um Lieferanweisungen zu erhalten.



Die Lieferanweisungen können auch Anfragen von AutoSupport zu folgenden Aufgaben enthalten:

- Generieren neuer AutoSupport Meldungen.

Der technische Support fordert möglicherweise neue AutoSupport Meldungen zur Unterstützung der Problembehebung an.

- Generieren neuer AutoSupport Meldungen, die Core Dump-Dateien oder Performance-Archivdateien auf die NetApp Support Site hochladen.

Der technische Support fordert möglicherweise Core Dump- oder Performance-Archivdateien an, um Probleme frühzeitig zu erkennen.

- Zuvor erzeugte AutoSupport Meldungen erneut übertragen.

Diese Anforderung tritt automatisch ein, wenn aufgrund eines Lieferfehlers keine Meldung empfangen wurde.

- Deaktivieren der Bereitstellung von AutoSupport Meldungen für bestimmte Trigger-Ereignisse.

Der technische Support deaktiviert möglicherweise die Bereitstellung von Daten, die nicht verwendet werden.

Struktur der per E-Mail gesendeten AutoSupport Nachrichten

Wenn eine AutoSupport-Nachricht per E-Mail gesendet wird, hat die Nachricht einen Standard-Betreff, einen kurzen Text und einen großen Anhang im 7z-Dateiformat, der die Daten enthält.



Wenn AutoSupport so konfiguriert ist, dass private Daten ausgeblendet werden, werden bestimmte Informationen, z. B. der Hostname, in der Kopfzeile, dem Betreff, dem Körper und den Anhängen weggelassen oder maskiert.

Betreff

Die vom AutoSupport-Mechanismus gesendete Betreffzeile von Nachrichten enthält eine Textzeichenfolge, die den Grund für die Benachrichtigung identifiziert. Das Format der Betreffzeile:

HA Group Notification from *System_Name* (*Message*) *Severity*

- *System_Name* ist je nach AutoSupport-Konfiguration entweder der Hostname oder die System-ID

Text

Der Text der AutoSupport-Meldung enthält die folgenden Informationen:

- Datum und Zeitstempel der Nachricht
- Die Version von ONTAP auf dem Node, der die Meldung generiert hat
- System-ID, Seriennummer und Hostname des Node, der die Meldung generiert hat
- AutoSupport-Sequenznummer
- Name und Standort des SNMP-Kontakts, falls angegeben
- System-ID und Hostname des HA Partner Node

Angehängte Dateien

Die Schlüsselinformationen in einer AutoSupport-Nachricht sind in Dateien enthalten, die in eine 7z-Datei mit dem Namen komprimiert werden `body.7z` und an die Nachricht angehängt.

Die Dateien in dem Anhang sind spezifisch für den Typ der AutoSupport-Nachricht.

AutoSupport-Schweregrade

AutoSupport-Meldungen enthalten Typen von Schweregraden, mit denen Sie den Zweck jeder Meldung verstehen – beispielsweise das sofortige Aufzeichnen eines Notfallproblems oder nur das Bereitstellen von Informationen.

Die Nachrichten haben eine der folgenden Schweregrade:

- **Alarm:** Warnhinweise zeigen an, dass ein Ereignis der nächsten höheren Ebene auftreten kann, wenn Sie keine Aktion ergreifen.

Sie müssen innerhalb von 24 Stunden eine Aktion für Warnmeldungen durchführen.

- **Notfall:** Notmeldungen werden angezeigt, wenn eine Störung aufgetreten ist.

Sie müssen sofort Maßnahmen gegen Notmeldungen ergreifen.

- **Fehler:** Fehlerbedingungen geben an, was passieren könnte, wenn Sie ignorieren.
- **Hinweis:** Normaler, aber bedeutender Zustand.
- **Info:** Informationsmeldung enthält Details zum Problem, das Sie ignorieren können.
- **Debug:** Debug-Level-Meldungen enthalten Anweisungen, die Sie durchführen sollten.

Wenn Ihre interne Support-Abteilung AutoSupport-Meldungen über E-Mail erhält, wird der Schweregrad in der Betreffzeile der E-Mail-Nachricht angezeigt.

Anforderungen für die Verwendung von AutoSupport

Sie müssen HTTPS mit TLSv1.2 oder sicheren SMTP für die Bereitstellung von AutoSupport-Nachrichten verwenden, um die beste Sicherheit zu gewährleisten und alle neuesten AutoSupport-Funktionen zu unterstützen. AutoSupport-Nachrichten, die mit einem anderen Protokoll geliefert wurden, werden abgelehnt.

Unterstützte Protokolle

Alle diese Protokolle werden auf IPv4 oder IPv6 ausgeführt, basierend auf der Adressfamilie, in die der Name auflöst.

Protokoll und Port	Beschreibung
HTTPS an Port 443	<p>Dies ist das Standardprotokoll. Sie sollten dies wann immer möglich verwenden.</p> <p>Dieses Protokoll unterstützt AutoSupport OnDemand und Uploads großer Dateien.</p> <p>Das Zertifikat des Remote-Servers wird mit dem Stammzertifikat validiert, es sei denn, Sie deaktivieren die Validierung.</p> <p>Die Lieferung verwendet eine HTTPS PUT-Anforderung. Bei PUT wird die Anforderung bei der Übertragung neu gestartet, wo sie angehalten wurde. Wenn der Server, der die Anforderung empfängt, PUT nicht unterstützt, verwendet die Zustellung eine HTTPS-POST-Anforderung.</p>
HTTP an Port 80	<p>Dieses Protokoll ist über SMTP bevorzugt.</p> <p>Dieses Protokoll unterstützt Uploads großer Dateien, jedoch nicht AutoSupport OnDemand.</p> <p>Die Lieferung verwendet eine HTTPS PUT-Anforderung. Bei PUT wird die Anforderung bei der Übertragung neu gestartet, wo sie angehalten wurde. Wenn der Server, der die Anforderung empfängt, PUT nicht unterstützt, verwendet die Zustellung eine HTTPS-POST-Anforderung.</p>

Protokoll und Port	Beschreibung
SMTP an Port 25 oder an einem anderen Port	<p>Dieses Protokoll sollten Sie nur verwenden, wenn HTTPS über die Netzwerkverbindung nicht zulässig ist.</p> <p>Der standardmäßige Port-Wert ist 25, Sie können jedoch AutoSupport für einen anderen Port konfigurieren.</p> <p>Beachten Sie bei der Verwendung von SMTP die folgenden Einschränkungen:</p> <ul style="list-style-type: none"> • AutoSupport OnDemand und Uploads großer Dateien werden nicht unterstützt. • Die Daten sind nicht verschlüsselt. <p>SMTP sendet Daten im Klartext, sodass Text in der AutoSupport-Nachricht einfach abgefangen und gelesen werden kann.</p> <ul style="list-style-type: none"> • Einschränkungen hinsichtlich der Nachrichtenlänge und der Linienlänge können eingeführt werden.

Wenn Sie AutoSupport mit bestimmten E-Mail-Adressen für Ihre interne Support-Abteilung oder eine Support-Partnerorganisation konfigurieren, werden diese Meldungen immer über SMTP gesendet.

Wenn Sie beispielsweise das empfohlene Protokoll zum Senden von Meldungen an den technischen Support verwenden und auch Meldungen an Ihre interne Support-Organisation senden möchten, werden Ihre Nachrichten sowohl über HTTPS als auch SMTP übertragen.

AutoSupport begrenzt die maximale Dateigröße für jedes Protokoll. Die Standardeinstellung für HTTP- und HTTPS-Transfers ist 25 MB. Die Standardeinstellung für SMTP-Transfers ist 5 MB. Wenn die Größe der AutoSupport-Meldung das konfigurierte Limit übersteigt, liefert AutoSupport so viel wie möglich. Sie können die maximale Größe bearbeiten, indem Sie die AutoSupport-Konfiguration ändern. Siehe `system node autosupport modify` Man-Page für weitere Informationen.



AutoSupport überschreibt automatisch die maximale Dateigröße für die HTTPS- und HTTP-Protokolle, wenn Sie AutoSupport Meldungen generieren und senden, die Core Dump- oder Performance-Archivdateien auf die NetApp Support-Website oder einen angegebenen URI hochladen. Die automatische Überschreibung gilt nur, wenn Sie Dateien mit dem hochladen `system node autosupport invoke-core-upload` Oder im `system node autosupport invoke-performance-archive` Befehle.

Konfigurationsanforderungen

Abhängig von Ihrer Netzwerkkonfiguration erfordert das HTTPS-Protokoll möglicherweise eine zusätzliche Konfiguration einer Proxy-URL. Wenn HTTPS AutoSupport-Nachrichten an den technischen Support senden soll und Sie über einen Proxy verfügen, müssen Sie die URL für diesen Proxy angeben. Wenn der Proxy einen anderen Port als den Standardport verwendet, der 3128 ist, können Sie den Port für diesen Proxy angeben. Sie können auch einen Benutzernamen und ein Kennwort für die Proxy-Authentifizierung angeben.

Wenn Sie SMTP zum Senden von AutoSupport-Meldungen an Ihre interne Supportorganisation oder an den technischen Support verwenden, müssen Sie einen externen E-Mail-Server konfigurieren. Das Speichersystem kann nicht als E-Mail-Server verwendet werden. Es ist ein externer Mail-Server an Ihrem Standort erforderlich, um E-Mails zu senden. Der Mail-Server muss ein Host sein, der den SMTP-Port (25) oder einen anderen Port abhört und für das Senden und Empfangen von 8-Bit-MIME-Kodierungen (MultiPurpose Internet Mail Extensions) konfiguriert sein muss. Zu den Beispiel-Mail-Hosts gehört ein UNIX-Host, auf dem ein SMTP-Server ausgeführt wird, z. B. das sendmail-Programm, und ein Windows-Server, auf dem der Microsoft Exchange-Server ausgeführt wird. Sie können einen oder mehrere E-Mail-Hosts haben.

AutoSupport einrichten

Sie haben die Möglichkeit, zu steuern, ob und wie AutoSupport Informationen an den technischen Support und Ihre interne Support-Abteilung gesendet werden, und können anschließend testen, ob die Konfiguration richtig ist.

Über diese Aufgabe

In ONTAP 9.5 und höher können Sie AutoSupport aktivieren und seine Konfiguration auf allen Nodes des Clusters gleichzeitig ändern. Wenn ein neuer Node dem Cluster hinzugefügt wird, übernimmt der Node die AutoSupport-Cluster-Konfiguration automatisch. Sie müssen die Konfiguration auf jedem Knoten nicht separat aktualisieren.



Ab ONTAP 9.5 wird der Umfang von `system node autosupport modify` Befehl gilt für das gesamte Cluster. Die AutoSupport-Konfiguration wird auf allen Nodes im Cluster geändert, auch wenn der `-node` Option ist angegeben. Die Option wird ignoriert, wurde aber für die Rückwärtskompatibilität mit CLI beibehalten.

In ONTAP 9.4 und älteren Versionen ist der Umfang des `system node autosupport modify` Der Befehl ist für den Node spezifisch. Die AutoSupport-Konfiguration sollte auf jedem Node im Cluster geändert werden.

Standardmäßig ist AutoSupport auf jedem Node aktiviert, um Meldungen mithilfe des HTTPS-Transportprotokolls an den technischen Support zu senden.

Sie müssen HTTPS mit TLSv1.2 oder sicheren SMTP für die Bereitstellung von AutoSupport-Nachrichten verwenden, um die beste Sicherheit zu gewährleisten und alle neuesten AutoSupport-Funktionen zu unterstützen.

Schritte

1. Vergewissern Sie sich, dass AutoSupport aktiviert ist:

```
system node autosupport modify -state enable
```

2. Wenn Sie technischen Support AutoSupport Meldungen erhalten möchten, verwenden Sie den folgenden Befehl:

```
system node autosupport modify -support enable
```

Sie müssen diese Option aktivieren, wenn Sie AutoSupport aktivieren möchten, um mit AutoSupport OnDemand zu arbeiten, oder wenn Sie große Dateien wie Core Dump- und Performance-Archivdateien

auf technischen Support oder eine angegebene URL hochladen möchten.

3. Wenn der technische Support für den Empfang von AutoSupport Meldungen aktiviert ist, geben Sie an, welches Transportprotokoll für die Meldungen verwendet werden soll.

Sie können aus folgenden Optionen wählen:

Ihr Ziel ist	Stellen Sie dann die folgenden Parameter des ein <code>system node autosupport modify</code> Befehl...
Verwenden Sie das HTTPS-Standardprotokoll	<p>a. Einstellen <code>-transport</code> Bis <code>https</code>.</p> <p>b. Wenn Sie einen Proxy verwenden, legen Sie fest <code>-proxy-url</code> An die URL Ihres Proxy. Diese Konfiguration unterstützt die Kommunikation mit AutoSupport OnDemand und das Hochladen großer Dateien.</p>
Verwenden Sie SMTP	<p>Einstellen <code>-transport</code> Bis <code>smtp</code>.</p> <p>Diese Konfiguration unterstützt weder AutoSupport OnDemand noch Uploads großer Dateien.</p>

4. Wenn Sie möchten, dass Ihre interne Support-Abteilung oder ein Support-Partner AutoSupport-Meldungen erhalten, führen Sie die folgenden Aktionen durch:

- a. Identifizieren Sie die Empfänger in Ihrem Unternehmen, indem Sie die folgenden Parameter des festlegen `system node autosupport modify` Befehl:

Diesen Parameter festlegen...	Künftige Situation
<code>-to</code>	Bis zu fünf kommagetrennte einzelne E-Mail-Adressen oder Verteilerlisten in Ihrer internen Support-Organisation, die wichtige AutoSupport-Nachrichten empfangen
<code>-noteto</code>	Bis zu fünf kommagetrennte einzelne E-Mail-Adressen oder Verteilerlisten in Ihrer internen Support-Organisation, die eine verkürzte Version von wichtigen AutoSupport-Nachrichten erhalten, die für Mobiltelefone und andere mobile Geräte entwickelt wurden
<code>-partner-address</code>	Bis zu fünf kommagetrennte einzelne E-Mail-Adressen oder Verteilerlisten in Ihrer Support-Partnerorganisation, die alle AutoSupport Meldungen erhalten

- b. Überprüfen Sie, ob die Adressen richtig konfiguriert sind, indem Sie die Ziele mithilfe des auflisten `system node autosupport destinations show` Befehl.

5. Wenn Sie Meldungen an Ihre interne Support-Organisation senden oder SMTP-Transport für Meldungen an den technischen Support gewählt haben, konfigurieren Sie SMTP, indem Sie die folgenden Parameter

des festlegen `system node autosupport modify` Befehl:

- Einstellen `-mail-hosts` An einen oder mehrere E-Mail-Hosts, getrennt durch Kommas.

Sie können maximal fünf festlegen.

Sie können einen Portwert für jeden Mail-Host konfigurieren, indem Sie einen Doppelpunkt und eine Portnummer nach dem Namen des Mail-Hosts angeben: Z. B. `mymailhost.example.com:5678`, Wo 5678 ist der Port für den Mail-Host.

- Einstellen `-from` An die E-Mail-Adresse, die die AutoSupport-Nachricht sendet.

6. Konfigurieren Sie DNS.

7. Optional können Sie Befehlsoptionen hinzufügen, wenn Sie bestimmte Einstellungen ändern möchten:

Wenn Sie das wollen...	Stellen Sie dann die folgenden Parameter des ein <code>system node autosupport modify</code> Befehl...
Verbergen Sie private Daten, indem Sie sensible Daten in den Nachrichten entfernen, maskieren oder kodieren	Einstellen <code>-remove-private-data</code> Bis <code>true</code> . Wenn Sie von wechseln <code>false</code> Bis <code>true</code> , Alle AutoSupport-Verlauf und alle zugehörigen Dateien werden gelöscht.
Beenden Sie das Senden von Performance-Daten in regelmäßigen AutoSupport Meldungen	Einstellen <code>-perf</code> Bis <code>false</code> .

8. Überprüfen Sie die Gesamtkonfiguration mithilfe von `system node autosupport show` Befehl mit dem `-node` Parameter.

9. Überprüfen Sie den AutoSupport-Vorgang mit `system node autosupport check show` Befehl.

Wenn Probleme gemeldet werden, verwenden Sie das `system node autosupport check show-details` Befehl zum Anzeigen weiterer Informationen.

10. Testen, ob AutoSupport Meldungen gesendet und empfangen werden:

- a. Verwenden Sie die `system node autosupport invoke` Befehl mit dem `-type` Parameter auf gesetzt `test`.

```
cluster1::> system node autosupport invoke -type test -node node1
```

- b. Bestätigen Sie, dass NetApp Ihre AutoSupport Mitteilungen erhält:

AutoSupport-Verlauf des System-Node wird `-Node` lokal angezeigt

Der Status der letzten ausgehenden AutoSupport-Meldung sollte schließlich in geändert werden `sent-successful` Für alle geeigneten Protokollziele.

- a. Optional können Sie überprüfen, ob die AutoSupport-Nachricht an Ihre interne Support-Organisation oder an Ihren Support-Partner gesendet wird, indem Sie die E-Mail-Adresse überprüfen, die Sie für das konfiguriert haben `-to`, `-noteto`, Oder `-partner-address` Parameter des `system node`

`autosupport modify` Befehl.

Laden Sie Core Dump-Dateien hoch

Wenn eine Core Dump-Datei gespeichert wird, wird eine Ereignismeldung generiert. Wenn der AutoSupport Service aktiviert und konfiguriert ist, um Meldungen an den NetApp Support zu senden, wird eine AutoSupport-Meldung übertragen und eine automatische E-Mail-Bestätigung an Sie gesendet.

Was Sie benötigen

- Sie müssen AutoSupport mit den folgenden Einstellungen einrichten:
 - AutoSupport ist auf dem Node aktiviert.
 - AutoSupport wurde konfiguriert, um Meldungen an den technischen Support zu senden.
 - AutoSupport ist für die Verwendung des HTTP- oder HTTPS-Transportprotokolls konfiguriert.

Das SMTP-Transportprotokoll wird nicht unterstützt, wenn Meldungen mit großen Dateien, wie z. B. Core Dump-Dateien, gesendet werden.

Über diese Aufgabe

Sie können die Core Dump-Datei auch über den AutoSupport-Service über HTTPS hochladen, indem Sie die verwenden `system node autosupport invoke-core-upload` Befehl, falls durch den NetApp Support angefordert.

"Wie zum Hochladen einer Datei auf NetApp"

Schritte

1. Zeigen Sie die Core Dump-Dateien für einen Node an, indem Sie den verwenden `system node coredump show` Befehl.

Im folgenden Beispiel werden Core Dump-Dateien für den lokalen Node angezeigt:

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
-----
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. Generieren Sie eine AutoSupport Meldung und laden Sie mithilfe der eine Core Dump-Datei hoch `system node autosupport invoke-core-upload` Befehl.

Im folgenden Beispiel wird eine AutoSupport Meldung generiert und an den Standardspeicherort gesendet, d. h. technischen Support. Und die Core Dump-Datei wird an den Standardspeicherort hochgeladen, der die NetApp Support Site ist:

```
cluster1::> system node autosupport invoke-core-upload -core-filename  
core.4073000068.2013-09-11.15_05_01.nz -node local
```

Im folgenden Beispiel wird eine AutoSupport Meldung generiert und an den in der URI angegebenen Speicherort gesendet, und die Core Dump-Datei wird auf den URI hochgeladen:

```
cluster1::> system node autosupport invoke-core-upload -uri  
https://files.company.com -core-filename  
core.4073000068.2013-09-11.15_05_01.nz -node local
```

Archivdateien für die Performance werden hochgeladen

Sie können eine AutoSupport Nachricht generieren und senden, die ein Performance-Archiv enthält. Standardmäßig erhält der technische Support von NetApp die Meldung „AutoSupport“, und das Performance-Archiv wird auf die NetApp Support Site hochgeladen. Sie können ein anderes Ziel für die Nachricht angeben und hochladen.

Was Sie benötigen

- Sie müssen AutoSupport mit den folgenden Einstellungen einrichten:
 - AutoSupport ist auf dem Node aktiviert.
 - AutoSupport wurde konfiguriert, um Meldungen an den technischen Support zu senden.
 - AutoSupport ist für die Verwendung des HTTP- oder HTTPS-Transportprotokolls konfiguriert.

Das SMTP-Transportprotokoll wird nicht unterstützt, wenn Meldungen mit großen Dateien, z. B. Performance-Archivdateien, gesendet werden.

Über diese Aufgabe

Sie müssen ein Startdatum für die Performance-Archivdaten angeben, die Sie hochladen möchten. Bei den meisten Storage-Systemen werden Performance-Archive für zwei Wochen aufbewahrt, wodurch Sie ein Startdatum bis vor zwei Wochen angeben können. Wenn beispielsweise heute Januar 15 ist, können Sie ein Startdatum vom 2. Januar angeben.

Schritt

1. Generieren Sie eine AutoSupport-Meldung, und laden Sie die Performance-Archivdatei mithilfe des hoch `system node autosupport invoke-performance-archive` Befehl.

Im folgenden Beispiel werden einer AutoSupport Meldung 4 Stunden an Performance-Archivdateien vom 12. Januar 2015 hinzugefügt und an den Standardspeicherort hochgeladen, die sich auf der NetApp Support Site befindet:

```
cluster1::> system node autosupport invoke-performance-archive -node  
local -start-date 1/12/2015 13:42:09 -duration 4h
```

Im folgenden Beispiel werden 4 Stunden Performance-Archivdateien vom 12. Januar 2015 einer

AutoSupport-Nachricht hinzugefügt und an den von der URI angegebenen Speicherort hochgeladen:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h -uri
https://files.company.com
```

Informieren Sie sich über die Beschreibungen von AutoSupport Meldungen

Die Beschreibungen der AutoSupport Meldungen, die Sie erhalten, sind über den ONTAP Syslog Translator verfügbar.

Schritte

1. Wechseln Sie zum ["Syslog Translator"](#).
2. Geben Sie im Feld **Release** die Version von ONTAP ein, die Sie verwenden. Geben Sie im Feld **Suche Zeichenfolge** „Callhome“ ein. Wählen Sie **Übersetzen**.
3. Der Syslog Translator führt in alphabetischer Reihenfolge alle Ereignisse auf, die mit der eingegebenen Meldungszeichenfolge übereinstimmen.

Befehle zum Verwalten von AutoSupport

Sie verwenden das `system node autosupport` Befehle zum Ändern oder Anzeigen der AutoSupport Konfiguration, zum Anzeigen von Informationen über frühere AutoSupport Meldungen und zum Senden, Neusenden oder Abbrechen einer AutoSupport Meldung.

Konfigurieren Sie AutoSupport

Ihr Ziel ist	Befehl
Steuern, ob AutoSupport Meldungen gesendet werden	<code>system node autosupport modify</code> Mit dem -state Parameter
Steuern, ob AutoSupport Meldungen an den technischen Support gesendet werden	<code>system node autosupport modify</code> Mit dem -support Parameter
Richten Sie AutoSupport ein, oder ändern Sie die Konfiguration von AutoSupport	<code>system node autosupport modify</code>
Aktivieren und deaktivieren Sie AutoSupport Meldungen für einzelne Triggerereignisse an Ihre interne Support-Abteilung und legen Sie zusätzliche Subsystemberichte fest, die als Antwort auf einzelne Trigger-Ereignisse gesendete Meldungen enthalten	<code>system node autosupport trigger modify</code>



Zeigt Informationen zur AutoSupport-Konfiguration an

Ihr Ziel ist	Befehl
Zeigt die AutoSupport-Konfiguration an	<code>system node autosupport show</code> Mit dem <code>-node</code> Parameter
Zeigen Sie eine Zusammenfassung aller Adressen und URLs an, die AutoSupport Meldungen erhalten	<code>system node autosupport destinations show</code>
Anzeige der AutoSupport Meldungen, die an Ihre interne Support-Abteilung gesendet werden, für einzelne Auslöser	<code>system node autosupport trigger show</code>
Anzeige des Status der AutoSupport-Konfiguration sowie der Lieferung an verschiedene Ziele	<code>system node autosupport check show</code>
Anzeige des detaillierten Status der AutoSupport-Konfiguration sowie Lieferung an verschiedene Ziele	<code>system node autosupport check show-details</code>

Zeigt Informationen zu früheren AutoSupport Meldungen an

Ihr Ziel ist	Befehl
Zeigt Informationen zu mindestens einer der 50 neuesten AutoSupport Meldungen an	<code>system node autosupport history show</code>
Informationen über kürzlich generierte AutoSupport-Meldungen anzeigen, um Core Dump- oder Performance-Archivdateien auf die technische Support-Website oder einen angegebenen URI hochzuladen	<code>system node autosupport history show-upload-details</code>
Anzeigen der Informationen in den AutoSupport Meldungen, einschließlich Name und Größe der einzelnen für die Nachricht gesammelten Dateien sowie etwaiger Fehler	<code>system node autosupport manifest show</code>

Senden, erneutes Senden oder Abbrechen von AutoSupport Meldungen

Ihr Ziel ist	Befehl
<p>Übertragen Sie eine lokal gespeicherte AutoSupport-Nachricht, die durch die AutoSupport-Sequenznummer gekennzeichnet ist, erneut</p> <div>  <p>Wenn Sie eine AutoSupport-Meldung erneut senden und die Unterstützung diese Meldung bereits erhalten hat, erstellt das Support-System keinen doppelten Fall. Wenn andererseits der Support diese Meldung nicht erhalten hat, analysiert das AutoSupport System die Meldung und erstellt bei Bedarf einen Case.</p> </div>	<pre>system node autosupport history retransmit</pre>
<p>Generieren und senden Sie eine AutoSupport Message – zum Beispiel zu Testzwecken</p>	<pre>system node autosupport invoke</pre> <div>  <p>Verwenden Sie die <code>-force</code> Parameter zum Senden einer Meldung, selbst wenn AutoSupport deaktiviert ist. Verwenden Sie die <code>-uri</code> Parameter, um die Meldung an das Ziel zu senden, das Sie anstelle des konfigurierten Ziels angeben.</p> </div>
<p>Abbrechen einer AutoSupport Nachricht</p>	<pre>system node autosupport history cancel</pre>

Verwandte Informationen

["ONTAP 9-Befehle"](#)

Informationen, die im AutoSupport-Manifest enthalten sind

Das AutoSupport Manifest bietet Ihnen eine detaillierte Ansicht der Dateien, die für jede AutoSupport Nachricht gesammelt wurden. Das AutoSupport-Manifest enthält auch Informationen über Erfassungsfehler, wenn AutoSupport die benötigten Dateien nicht sammeln kann.

Das AutoSupport-Manifest enthält folgende Informationen:

- Sequenznummer der AutoSupport-Meldung
- Welche Dateien AutoSupport in der AutoSupport Nachricht enthalten
- Größe jeder Datei in Byte
- Der Status der AutoSupport Manifest-Sammlung
- Fehlerbeschreibung, falls AutoSupport eine oder mehrere Dateien nicht sammeln konnte

Sie können das AutoSupport-Manifest mit dem anzeigen `system node autosupport manifest show` Befehl.

Das AutoSupport-Manifest ist in jeder AutoSupport-Nachricht enthalten und im XML-Format dargestellt, was bedeutet, dass Sie entweder einen generischen XML-Viewer zum Lesen verwenden oder es mit dem Active IQ-Portal (früher bekannt als My AutoSupport) anzeigen können.

Unterdrückung von AutoSupport-Cases während geplanter Wartungszeiten

Durch die AutoSupport-Fallunterdrückung können Sie verhindern, dass unnötige Fälle durch AutoSupport Meldungen erstellt werden, die während eines geplanten Wartungsfensters ausgelöst werden.

Um AutoSupport-Fälle zu unterdrücken, müssen Sie eine AutoSupport-Nachricht manuell mit einer speziell formatierten Textzeichenfolge aufrufen: `MAINT=xh`. `x` ist die Dauer des Wartungsfensters in Stundeneinheiten.

Verwandte Informationen

["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#)

Beheben Sie AutoSupport, wenn keine Meldungen empfangen werden

Wenn das System die AutoSupport Meldung nicht sendet, können Sie bestimmen, ob das der Fall ist, weil AutoSupport die Meldung nicht generieren kann oder die Meldung nicht liefern kann.

Schritte

1. Überprüfen Sie den Zustellungsstatus der Meldungen mithilfe der `system node autosupport history show` Befehl.
2. Lesen Sie den Status.

Diesem Status	Bedeutet
Initialisierung	Der Erfassungsprozess wird gestartet. Wenn dieser Zustand vorübergehend ist, ist alles gut. Wenn dieser Status jedoch weiterhin besteht, gibt es ein Problem.
Sammlung fehlgeschlagen	AutoSupport kann den AutoSupport-Inhalt im Spool-Verzeichnis nicht erstellen. Sie können anzeigen, was AutoSupport zu erfassen versucht, indem Sie die eingeben <code>system node autosupport history show -detail</code> Befehl.
Inkassovorgang läuft	AutoSupport sammelt AutoSupport-Inhalte. Sie können anzeigen, was AutoSupport erfasst, indem Sie die eingeben <code>system node autosupport manifest show</code> Befehl.
Warteschlange	AutoSupport Nachrichten werden für die Lieferung in die Warteschlange eingereicht, aber noch nicht geliefert.
Übertragung	AutoSupport stellt derzeit Meldungen aus.

Diesem Status	Bedeutet
Gesendet-erfolgreich	AutoSupport hat die Meldung erfolgreich übermittelt. Finden Sie heraus, an welchen Stellen AutoSupport die Nachricht geliefert hat, indem Sie den eingeben <code>system node autosupport history show -delivery</code> Befehl.
Ignorieren	AutoSupport verfügt über keine Ziele für die Meldung. Sie können die Lieferdetails anzeigen, indem Sie die eingeben <code>system node autosupport history show -delivery</code> Befehl.
Erneut in Warteschlange gestellt	AutoSupport hat versucht, Nachrichten zu senden, aber der Versuch ist fehlgeschlagen. Infolgedessen wurden die Nachrichten von AutoSupport wieder in die Ausgabewarteschlange für einen anderen Versuch platziert. Sie können den Fehler anzeigen, indem Sie die eingeben <code>system node autosupport history show</code> Befehl.
Übertragung fehlgeschlagen	AutoSupport konnte die Nachricht nicht mit der angegebenen Anzahl von Zeiten senden und hörte nicht auf, die Nachricht zu liefern. Sie können den Fehler anzeigen, indem Sie die eingeben <code>system node autosupport history show</code> Befehl.
ondemand-Ignorieren	Die AutoSupport Meldung wurde erfolgreich verarbeitet, aber der AutoSupport OnDemand Dienst wählte, um sie zu ignorieren.

3. Führen Sie eine der folgenden Aktionen aus:

Für diesen Status	Tun Sie das
Initialisierung oder Sammlung fehlgeschlagen	Wenden Sie sich an den NetApp Support, da AutoSupport die Nachricht nicht generieren kann. Erwähnen Sie den folgenden Knowledge Base-Artikel: "AutoSupport kann nicht liefern: Der Status befindet sich in Initialisierung"
Ignorieren, erneute Warteschlange oder Übertragung fehlgeschlagen	Überprüfen Sie, ob die Ziele für SMTP, HTTP oder HTTPS richtig konfiguriert sind, da AutoSupport die Meldung nicht senden kann.

Fehlerbehebung bei der Bereitstellung von AutoSupport Meldungen über HTTP oder HTTPS

Wenn das System die erwartete AutoSupport-Meldung nicht sendet und Sie HTTP oder HTTPS verwenden oder die Funktion zum automatischen Aktualisieren nicht funktioniert, können Sie eine Reihe von Einstellungen überprüfen, um das Problem zu beheben.

Was Sie benötigen

Sie sollten die grundlegende Netzwerkverbindung und das DNS-Lookup bestätigt haben:

- Die Node-Management-LIF muss den Status „Betriebs“ und „Administration“ aufweisen.
- Sie müssen in der Lage sein, einen funktionierenden Host in demselben Subnetz von der Cluster-Management-LIF zu pingen (keine LIF auf keinem der Nodes).
- Sie müssen in der Lage sein, einen funktionierenden Host außerhalb des Subnetzes von der Cluster-Management-LIF zu pingen.
- Sie müssen in der Lage sein, einen funktionierenden Host außerhalb des Subnetzes von der Cluster-Management-LIF mit dem Namen des Hosts (nicht die IP-Adresse) anzupingen.

Über diese Aufgabe

Diese Schritte sind für Fälle, in denen Sie festgestellt haben, dass AutoSupport die Meldung generieren kann, die Meldung jedoch nicht über HTTP oder HTTPS übermitteln kann.

Wenn bei diesem Vorgang Fehler auftreten oder ein Schritt nicht ausgeführt werden kann, ermitteln und beheben Sie das Problem, bevor Sie mit dem nächsten Schritt fortfahren.

Schritte

1. Anzeigen des detaillierten Status des AutoSupport-Subsystems:

```
system node autosupport check show-details
```

Dazu gehört auch die Überprüfung der Verbindung zu AutoSupport Zielen durch Senden von Testmeldungen und Bereitstellen einer Liste möglicher Fehler in Ihren AutoSupport Konfigurationseinstellungen.

2. Überprüfen Sie den Status der Node-Management-LIF:

```
network interface show -home-node local -role node-mgmt -fields
vserver,lif,status-oper,status-admin,address,role
```

Der status-oper Und status-admin Felder sollten „up“ zurückgeben.

3. Notieren Sie den SVM-Namen, den LIF-Namen und die LIF-IP-Adresse für die spätere Verwendung.
4. Stellen Sie sicher, dass DNS richtig aktiviert und konfiguriert ist:

```
vserver services name-service dns show
```

5. Beheben Sie alle Fehler, die von der AutoSupport Meldung zurückgegeben werden:

```
system node autosupport history show -node * -fields node,seq-
num,destination,last-update,status,error
```

Informationen zur Fehlerbehebung bei zurückgegebenen Fehlern finden Sie im ["ONTAP AutoSupport \(Transport HTTPS und HTTP\) Auflösungsleitfaden"](#).

6. Vergewissern Sie sich, dass das Cluster sowohl auf die Server zugreifen kann, die es benötigt, als auch auf das Internet:

```
a. network traceroute -lif node-management_LIF -destination DNS server
```

```
b. network traceroute -lif node_management_LIF -destination support.netapp.com
```



Die Adresse `support.netapp.com` Selbst reagiert nicht auf Ping/Traceroute, aber die Informationen pro Hop sind wertvoll.

c. `system node autosupport show -fields proxy-url`

d. `network traceroute -node node_management_LIF -destination proxy_url`

Wenn eine dieser Routen nicht funktioniert, versuchen Sie die gleiche Route von einem funktionierenden Host im selben Subnetz wie das Cluster, indem Sie das Dienstprogramm „traceroute“ oder „tracert“ verwenden, das auf den meisten Netzwerk-Clients von Drittanbietern gefunden wurde. Dadurch können Sie herausfinden, ob das Problem in Ihrer Netzwerkkonfiguration oder der Cluster-Konfiguration vorliegt.

7. Wenn Sie HTTPS für Ihr AutoSupport-Transportprotokoll verwenden, stellen Sie sicher, dass HTTPS-Datenverkehr das Netzwerk beenden kann:

a. Konfigurieren Sie einen Web-Client im gleichen Subnetz wie die Cluster-Management-LIF.

Stellen Sie sicher, dass alle Konfigurationsparameter dieselben Werte wie für die AutoSupport-Konfiguration sind, einschließlich der Verwendung desselben Proxy-Servers, Benutzernamens, Passworts und Ports.

b. Datenzugriff `https://support.netapp.com` Mit dem Web-Client.

Der Zugriff sollte erfolgreich sein. Wenn nicht, stellen Sie sicher, dass alle Firewalls richtig konfiguriert sind, um HTTPS- und DNS-Datenverkehr zu ermöglichen, und dass der Proxy-Server korrekt konfiguriert ist. Weitere Informationen zum Konfigurieren der statischen Namensauflösung für `support.netapp.com` finden Sie im Knowledge Base-Artikel "[Wie würde ein HOST-Eintrag in ONTAP für support.netapp.com? hinzugefügt werden](#)"

8. Wenn Sie mit ONTAP 9.10.1 die Funktion Automatische Aktualisierung aktiviert haben, stellen Sie sicher, dass Sie über eine HTTPS-Verbindung zu den folgenden zusätzlichen URLs verfügen:

- `https://support-sg-emea.netapp.com`
- `https://support-sg-naeast.netapp.com`
- `https://support-sg-nawest.netapp.com`

Fehlerbehebung bei der AutoSupport Nachrichtenübermittlung über SMTP

Wenn das System keine AutoSupport Meldungen über SMTP liefern kann, können Sie eine Reihe von Einstellungen überprüfen, um das Problem zu lösen.

Was Sie benötigen

Sie sollten die grundlegende Netzwerkverbindung und das DNS-Lookup bestätigt haben:

- Die Node-Management-LIF muss den Status „Betriebs“ und „Administration“ aufweisen.
- Sie müssen in der Lage sein, einen funktionierenden Host in demselben Subnetz von der Cluster-Management-LIF zu pingen (keine LIF auf keinem der Nodes).
- Sie müssen in der Lage sein, einen funktionierenden Host außerhalb des Subnetzes von der Cluster-Management-LIF zu pingen.
- Sie müssen in der Lage sein, einen funktionierenden Host außerhalb des Subnetzes von der Cluster-Management-LIF mit dem Namen des Hosts (nicht die IP-Adresse) anzupingen.

Über diese Aufgabe

Diese Schritte sind für Fälle, in denen Sie festgestellt haben, dass AutoSupport die Meldung generieren kann, die Meldung jedoch nicht über SMTP liefern kann.

Wenn bei diesem Vorgang Fehler auftreten oder ein Schritt nicht ausgeführt werden kann, ermitteln und beheben Sie das Problem, bevor Sie mit dem nächsten Schritt fortfahren.

Sofern nicht anders angegeben, werden alle Befehle über die ONTAP-Befehlszeilenschnittstelle eingegeben.

Schritte

1. Überprüfen Sie den Status der Node-Management-LIF:

```
network interface show -home-node local -role node-mgmt -fields  
vserver,lif,status-oper,status-admin,address,role
```

Der status-oper Und status-admin Die Felder sollten zurückgegeben werden up.

2. Notieren Sie den SVM-Namen, den LIF-Namen und die LIF-IP-Adresse für die spätere Verwendung.
3. Stellen Sie sicher, dass DNS richtig aktiviert und konfiguriert ist:

```
vserver services name-service dns show
```

4. Alle Server anzeigen, die für die Verwendung durch AutoSupport konfiguriert sind:

```
system node autosupport show -fields mail-hosts
```

Notieren Sie alle angezeigten Servernamen.

5. Für jeden Server, der im vorherigen Schritt angezeigt wird, und `support.netapp.com`, Stellen Sie sicher, dass der Server oder die URL durch den Knoten erreicht werden kann:

```
network traceroute -node local -destination server_name
```

Wenn eine dieser Routen nicht funktioniert, versuchen Sie die gleiche Route von einem funktionierenden Host im selben Subnetz wie das Cluster, indem Sie das Dienstprogramm „traceroute“ oder „tracert“ verwenden, das auf den meisten Netzwerk-Clients von Drittanbietern gefunden wurde. Dadurch können Sie herausfinden, ob das Problem in Ihrer Netzwerkkonfiguration oder der Cluster-Konfiguration vorliegt.

6. Melden Sie sich beim Host an, der als E-Mail-Host bezeichnet wird, und stellen Sie sicher, dass er SMTP-Anforderungen bereitstellen kann:

```
netstat -aAn|grep 25
```

25 Ist die SMTP-Port-Nummer des Listeners.

Es wird eine Meldung wie der folgende Text angezeigt:

```
ff64878c tcp          0      0 *.25    *.*    LISTEN.
```

7. Öffnen Sie von einem anderen Host eine Telnet-Sitzung mit dem SMTP-Port des Mail-Hosts:

```
telnet mailhost 25
```

Es wird eine Meldung wie der folgende Text angezeigt:

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

8. Stellen Sie an der Eingabeaufforderung Telnet sicher, dass eine Nachricht von Ihrem Mail-Host weitergeleitet werden kann:

```
HELO domain_name
```

```
MAIL FROM: your_email_address
```

```
RCPT TO: autosupport@netapp.com
```

domain_name ist der Domain-Name Ihres Netzwerks.

Wenn ein Fehler zurückgegeben wird, der besagt, dass das Relying verweigert wird, ist das Relying auf dem Mail-Host nicht aktiviert. Wenden Sie sich an Ihren Systemadministrator.

9. Senden Sie an der Eingabeaufforderung Telnet eine Testmeldung:

```
DATA
```

```
SUBJECT: TESTING
```

```
THIS IS A TEST
```

```
.
```



Stellen Sie sicher, dass Sie den letzten Zeitraum (.) in einer Zeile selbst eingeben. Der Zeitraum gibt dem Mail-Host an, dass die Nachricht abgeschlossen ist.

Wenn ein Fehler zurückgegeben wird, ist Ihr Mail-Host nicht richtig konfiguriert. Wenden Sie sich an Ihren Systemadministrator.

10. Senden Sie über die ONTAP Befehlszeilenschnittstelle eine AutoSupport-Testmeldung an eine vertrauenswürdige E-Mail-Adresse, auf die Sie Zugriff haben:

```
system node autosupport invoke -node local -type test
```

11. Suchen Sie die Sequenznummer des Versuchs:

```
system node autosupport history show -node local -destination smtp
```

Suchen Sie die Sequenznummer Ihres Versuchs basierend auf dem Zeitstempel. Es ist wahrscheinlich der jüngste Versuch.

12. Zeigen Sie den Fehler für den Versuch der Testmeldung an:

```
system node autosupport history show -node local -seq-num seq_num -fields error
```

Wenn der Fehler angezeigt wird `Login denied`, Ihr SMTP-Server akzeptiert keine Anfragen von der

Cluster-Management-LIF. Wenn Sie als Transportprotokoll nicht zu HTTPS wechseln möchten, wenden Sie sich an den Standortnetzwerkadministrator, um die SMTP-Gateways zu konfigurieren, um dieses Problem zu beheben.

Wenn dieser Test erfolgreich ist, aber dieselbe Nachricht an `mailto:autosupport@netapp.com` nicht gesendet wird, stellen Sie sicher, dass SMTP-Relais auf allen Ihren SMTP-Mail-Hosts aktiviert ist, oder verwenden Sie HTTPS als Transportprotokoll.

Wenn auch die Meldung an das lokal verwaltete E-Mail-Konto nicht erfolgreich ist, bestätigen Sie, dass Ihre SMTP-Server so konfiguriert sind, dass Anlagen mit beiden folgenden Eigenschaften weitergeleitet werden:

- Das Suffix „7z“
- Der Typ „Application/x-7x-compressed“ MIME.

Fehler beim AutoSupport-Subsystem

Der `system node check show` Mit diesen Befehlen können Probleme hinsichtlich der AutoSupport-Konfiguration und -Bereitstellung überprüft und behoben werden.

Schritt

1. Zeigen Sie mit den folgenden Befehlen den Status des AutoSupport-Subsystems an.

Befehl	Hier...
<code>system node autosupport check show</code>	Zeigt den Gesamtstatus des AutoSupport-Subsystems an, z. B. den Status von AutoSupport HTTP- oder HTTPS-Ziel, AutoSupport SMTP-Ziele, AutoSupport OnDemand Server und AutoSupport-Konfiguration
<code>system node autosupport check show-details</code>	Anzeige des detaillierten Status des AutoSupport-Subsystems, z. B. detaillierte Beschreibungen der Fehler und der Korrekturmaßnahmen

Monitoring des Systemzustands

Überwachen Sie den Systemzustand Ihrer Systemübersicht

Zustandsüberwachung überwachen proaktiv bestimmte kritische Bedingungen in Ihrem Cluster und Warnmeldungen, wenn ein Fehler oder Risiko erkannt wird, aus. Wenn aktive Meldungen vorliegen, wird der Systemzustand den Status des Systems für das Cluster mit einem Status „beeinträchtigt“ angezeigt. Die Meldungen enthalten die Informationen, die Sie benötigen, um auf den beeinträchtigten Systemzustand zu reagieren.

Wenn der Status „beeinträchtigt“ lautet, können Sie Details zum Problem anzeigen, einschließlich der wahrscheinlichen Ursache und der empfohlenen Wiederherstellungsmaßnahmen. Nachdem Sie das Problem behoben haben, kehrt der Systemzustand automatisch zu OK zurück.

Der Systemzustand gibt mehrere separate Integritätsmonitore wieder. Ein Status „beeinträchtigt“ in einer einzelnen Systemzustandsüberwachung bewirkt einen Status „beeinträchtigt“ für den gesamten Systemzustand.

Details dazu, wie ONTAP Cluster Switches für die Überwachung des Systemzustands im Cluster unterstützt, finden Sie unter *Hardware Universe*.

["Unterstützte Switches im Hardware Universe"](#)

Einzelheiten zu den Ursachen von AutoSupport-Meldungen (Cluster Switch Health Monitor, CSHM) und den zur Behebung dieser Warnmeldungen erforderlichen Maßnahmen finden Sie im Knowledgebase Artikel.

["AutoSupport Meldung: Health Monitor Prozess CSHM"](#)

Funktionsweise der Statusüberwachung

Individuelle Systemzustandsüberwachung verfügen über eine Reihe von Richtlinien, die Warnungen auslösen, wenn bestimmte Bedingungen auftreten. Wenn Sie verstehen, wie das Statusüberwachung funktioniert, können Sie auf Probleme reagieren und zukünftige Warnmeldungen steuern.

Die Statusüberwachung besteht aus den folgenden Komponenten:

- Individuelle Gesundheitsmonitore für bestimmte Subsysteme, von denen jeder seinen eigenen Gesundheitszustand hat

Beispielsweise verfügt das Storage-Subsystem über eine Systemzustandsüberwachung für die Node-Konnektivität.

- Eine allgemeine Systemzustandsüberwachung, die den Systemzustand der einzelnen Systemzustandsüberwachung konsolidiert

Ein Status „beeinträchtigt“ in einem einzelnen Subsystem führt zu einem Status „beeinträchtigt“ für das gesamte System. Wenn keine Subsysteme Warnmeldungen enthalten, ist der gesamte Systemstatus OK.

Jede Systemzustandsüberwachung setzt sich aus den folgenden wichtigen Elementen zurück:

- Meldungen, die von der Systemzustandsüberwachung potenziell angehoben werden können

Jede Meldung hat eine Definition, die Details wie den Schweregrad der Warnmeldung und die wahrscheinliche Ursache enthält.

- Integritätsrichtlinien, die festlegen, wann jede Meldung ausgelöst wird

Jede Systemzustandsüberwachung verfügt über einen Regelausdruck. Dies ist die genaue Bedingung oder Änderung, durch die die Meldung ausgelöst wird.

Eine Systemzustandsüberwachung überwacht kontinuierlich die Ressourcen in ihrem Subsystem auf ihre Zustandsänderungen. Wenn eine Änderung einer Bedingung oder eines Status mit einem Regelausdruck in einer Systemzustandsüberwachung übereinstimmt, erhöht die Systemzustandsüberwachung eine Meldung. Eine Meldung bewirkt, dass der Systemzustand des Subsystems und der gesamte Systemzustand beeinträchtigt werden.

Möglichkeiten zur Reaktion auf Systemzustandsmeldungen

Wenn eine Systemzustandsmeldung auftritt, können Sie sie bestätigen, mehr darüber erfahren, den zugrunde liegenden Zustand reparieren und verhindern, dass er erneut auftritt.

Wenn eine Systemzustandsüberwachung eine Meldung aufwirft, können Sie auf folgende Arten reagieren:

- Informieren Sie sich über die Meldung, zu der die betroffene Ressource, der Schweregrad der Warnmeldung, die wahrscheinliche Ursache, die mögliche Auswirkung und die Korrekturmaßnahmen gehören.
- Detaillierte Informationen über die Warnmeldung, z. B. den Zeitpunkt, zu dem die Warnmeldung ausgegeben wurde und ob jemand anderer die Warnmeldung bereits bestätigt hat.
- Abrufen von Systemzustandsinformationen zum Status der betroffenen Ressource oder Subsysteme, z. B. ein bestimmtes Shelf oder eine bestimmte Festplatte
- Bestätigen Sie den Alarm, um anzuzeigen, dass jemand an dem Problem arbeitet und identifizieren Sie sich als „Danker“.
- Beheben Sie das Problem, indem Sie die in der Warnmeldung angegebenen Korrekturmaßnahmen ergreifen, z. B. Kabelbefestigung zur Behebung eines Verbindungsproblems.
- Löschen Sie die Meldung, wenn sie vom System nicht automatisch gelöscht wurde.
- Unterdrücken einer Meldung, um zu verhindern, dass sie den Integritätsstatus eines Subsystems beeinflusst.

Das Unterdrücken ist nützlich, wenn Sie ein Problem verstehen. Nachdem Sie eine Meldung unterdrückt haben, kann sie weiterhin auftreten, der Systemzustand des Subsystems wird jedoch als „ok-with-underdrückung“ angezeigt, wenn die unterdrückte Meldung auftritt.

Anpassung der Systemzustandsmeldung

Sie können steuern, welche Meldungen eine Systemzustandsüberwachung generiert, indem Sie die Systemintegritätsrichtlinien aktivieren und deaktivieren, die definieren, wann Meldungen ausgelöst werden. So können Sie das System zur Statusüberwachung für Ihre spezifische Umgebung anpassen.

Sie können den Namen einer Richtlinie erlernen, indem Sie ausführliche Informationen über eine generierte Meldung anzeigen oder Richtliniendefinitionen für eine bestimmte Systemzustandsüberwachung, Node oder Alarm-ID anzeigen.

Das Deaktivieren von Integritätsrichtlinien unterscheidet sich vom Unterdrücken von Meldungen. Wenn Sie eine Meldung unterdrücken, hat dies keine Auswirkung auf den Systemzustand des Subsystems, aber die Meldung kann immer noch auftreten.

Wenn Sie eine Richtlinie deaktivieren, löst die im Richtlinienausdruck definierte Bedingung oder der Status keine Meldung mehr aus.

Beispiel für eine Meldung, die Sie deaktivieren möchten

Angenommen, eine Meldung tritt auf, die für Sie nicht hilfreich ist. Sie verwenden das `system health alert show -instance` Befehl zum Abrufen der Richtlinien-ID für die Meldung. Sie verwenden die Richtlinien-ID im `system health policy definition show` Befehl zum Anzeigen von Informationen zur

Richtlinie. Nachdem Sie den Regelausdruck und andere Informationen über die Richtlinie geprüft haben, entscheiden Sie, die Richtlinie zu deaktivieren. Sie verwenden das `system health policy definition modify` Befehl zum Deaktivieren der Richtlinie

Wie Systemzustandsmeldungen AutoSupport Meldungen und Ereignisse auslösen

Systemzustandsmeldungen lösen AutoSupport-Meldungen und Ereignisse im Event Management System (EMS) aus, so dass Sie den Systemzustand mithilfe von AutoSupport-Meldungen und dem EMS sowie die direkte Verwendung des Integritätsüberwachungssystems überwachen können.

Das System sendet eine AutoSupport Meldung innerhalb von fünf Minuten nach einer Meldung. Die AutoSupport Meldung enthält alle seit der letzten AutoSupport Meldung generierten Warnmeldungen, mit Ausnahme von Warnungen, die eine Meldung für dieselbe Ressource und wahrscheinliche Ursache innerhalb der vorherigen Woche duplizieren.


Einige Meldungen lösen keine AutoSupport-Meldungen aus. Eine Meldung löst keine AutoSupport Meldung aus, wenn ihre Integritätsrichtlinie das Senden von AutoSupport Meldungen deaktiviert. Beispielsweise kann eine Systemzustandsüberwachung standardmäßig AutoSupport Meldungen deaktivieren, da AutoSupport bereits eine Meldung generiert, wenn das Problem auftritt. Sie können Richtlinien so konfigurieren, dass AutoSupport-Meldungen nicht mit dem ausgelöst werden `system health policy definition modify` Befehl.

Sie können eine Liste aller AutoSupport Meldungen, die in der vorherigen Woche über die gesendet wurden, anzeigen `system health autosupport trigger history show` Befehl.

Warnmeldungen auslösen außerdem die Generierung von Ereignissen an das EMS. Jedes Mal, wenn eine Meldung erstellt wird, wird ein Ereignis generiert, wenn eine Meldung gelöscht wird.

Verfügbare Cluster-Zustandsmonitore

Verschiedene Systemzustandsüberwachung überwachen verschiedene Teile eines Clusters. Die Zustandsüberwachung unterstützen Sie bei der Wiederherstellung nach Fehlern in ONTAP Systemen. Dazu werden Ereignisse erkannt, Warnmeldungen an Sie gesendet und Ereignisse gelöscht, sobald sie gelöscht werden.

Name der Systemzustandsüberwachung (Kennung)	Subsystemname (Kennung)	Zweck
Cluster-Switch (Cluster-Switch)	Switch (Switch-Health)	<p>Überwacht Cluster-Netzwerk-Switches und Management-Netzwerk-Switches auf Temperatur, Auslastung, Schnittstellenkonfiguration, Redundanz (nur Cluster-Netzwerk-Switches) sowie Lüfter- und Netzteilbetrieb. Die Cluster-Switch-Systemzustandsüberwachung kommuniziert mit Switches über SNMP. SNMPv2c ist die Standardeinstellung.</p> <div>  <p>Ab ONTAP 9.2 kann dieser Monitor erkennen und melden, wenn ein Cluster-Switch seit der letzten Abrufzeit neu gestartet wurde.</p> </div>
MetroCluster Fabric	Switch	Überwacht die Back-End-Fabric-Topologie der MetroCluster Konfiguration und erkennt Fehlkonfigurationen wie falsche Verkabelung und Zoning oder ISL-Ausfälle.
Systemzustand von MetroCluster	Interconnect, RAID und Storage	Überwacht FC-VI-Adapter, FC Initiator-Adapter, Aggregate und Festplatten im Hintergrund sowie Cluster-Ports
Node-Konnektivität (Node-Connect)	Unterbrechungsfreier CIFS-Betrieb (CIFS-NDO)	Überwachung von SMB-Verbindungen für unterbrechungsfreien Betrieb von Hyper-V Applikationen
Storage (SAS-Connect)	Überwacht Shelves, Festplatten und Adapter auf Node-Ebene für entsprechende Pfade und Verbindungen.	System
Keine Angabe	Fasst Informationen aus anderen Zustandsmonitoren zusammen.	Systemkonnektivität (System-connect)

Automatisches Empfangen von Systemzustandsmeldungen

Sie können Systemzustandsmeldungen manuell mit der anzeigen `system health alert show` Befehl. Sie sollten jedoch bestimmte EMS-Meldungen (Event Management System) abonnieren, um Benachrichtigungen automatisch zu erhalten, wenn eine Systemzustandsüberwachung eine Meldung generiert.

Über diese Aufgabe

Das folgende Verfahren zeigt Ihnen, wie Sie Benachrichtigungen für alle `hm.alert.alert.hopped` Nachrichten und alle `hm.alert.cleaned` Nachrichten einrichten.

Alle `hm.alert.alerted` Nachrichten und alle `hm.alert.cleaned` Nachrichten enthalten einen SNMP-Trap. Die Namen der SNMP-Traps sind `HealthMonitorAlertRaised` Und `HealthMonitorAlertCleared`. Informationen zu SNMP-Traps finden Sie im *Network Management Guide*.

Schritte

1. Verwenden Sie die `event destination create` Befehl zum Festlegen des Ziels, an das Sie die EMS-Nachrichten senden möchten.

```
cluster1::> event destination create -name health_alerts -mail  
admin@example.com
```

2. Verwenden Sie die `event route add-destinations` Befehl zum Umleiten des `hm.alert.raised` Botschaft und der `hm.alert.cleaned` Nachricht an ein Ziel senden.

```
cluster1::> event route add-destinations -messageName hm.alert*  
-destinations health_alerts
```

Verwandte Informationen

["Netzwerkmanagement"](#)

Reagieren Sie auf den eingeschränkten Systemzustand

Wenn der Systemzustand des Systems beeinträchtigt ist, können Sie Meldungen anzeigen, die wahrscheinliche Ursache und die möglichen Korrekturmaßnahmen lesen, Informationen zum beeinträchtigten Subsystem anzeigen und das Problem lösen. Unterdrückte Warnungen werden ebenfalls angezeigt, damit Sie sie ändern und sehen können, ob sie bestätigt wurden.

Über diese Aufgabe

Sie können feststellen, dass eine Meldung durch die Anzeige einer AutoSupport Meldung, eines EMS-Ereignisses oder mithilfe des generiert wurde `system health` Befehle.

Schritte

1. Verwenden Sie die `system health alert show` Befehl zum Anzeigen der Meldungen, die den Systemzustand beeinträchtigen.

2. Lesen Sie die wahrscheinliche Ursache, die mögliche Auswirkung und die Korrekturmaßnahmen der Meldung, um zu ermitteln, ob Sie das Problem beheben oder weitere Informationen benötigen.
3. Wenn Sie weitere Informationen benötigen, verwenden Sie das `system health alert show -instance` Befehl zum Anzeigen weiterer Informationen, die für die Meldung verfügbar sind.
4. Verwenden Sie die `system health alert modify` Befehl mit dem `-acknowledge` Parameter, um anzugeben, dass Sie an einer bestimmten Warnmeldung arbeiten.
5. Führen Sie Korrekturmaßnahmen durch, um das Problem zu lösen, wie im beschriebenen `Corrective Actions` Feld in der Meldung.

Die Korrekturmaßnahmen können ein Neubooten des Systems umfassen.

Nach Behebung des Problems wird die Meldung automatisch behoben. Wenn das Subsystem keine weiteren Warnmeldungen aufweist, ändert sich der Systemzustand des Subsystems in `OK`. Wenn der Systemzustand aller Subsysteme in Ordnung ist, ändert sich der Gesamtzustand des Systems in `OK`.

6. Verwenden Sie die `system health status show` Befehl zur Bestätigung, dass der Systemzustand lautet `OK`.

Wenn der Systemstatus nicht lautet `OK`, Wiederholen Sie dieses Verfahren.

Beispiel der Reaktion auf den eingeschränkten Systemzustand

Durch Überprüfung eines bestimmten Beispiels des beeinträchtigten Systemzustands, der durch ein Shelf verursacht wurde, in dem zwei Pfade zu einem Node fehlen, werden Sie sehen, was die CLI zeigt, wenn Sie auf eine Meldung antworten.

Nach dem Starten von ONTAP überprüfen Sie den Systemzustand, und Sie stellen fest, dass der Status „beeinträchtigt“ lautet:

```
cluster1::>system health status show
Status
-----
degraded
```

Sie zeigen die Meldungen an, um herauszufinden, wo das Problem ist, und sehen, dass Shelf 2 keine zwei Pfade zu node1 hat:

```
cluster1::>system health alert show
```

```
Node: node1
```

```
Resource: Shelf ID 2
```

```
Severity: Major
```

```
Indication Time: Mon Nov 10 16:48:12 2013
```

```
Probable Cause: Disk shelf 2 does not have two paths to controller  
node1.
```

```
Possible Effect: Access to disk shelf 2 via controller node1 will be  
lost with a single hardware component failure (e.g.  
cable, HBA, or IOM failure).
```

```
Corrective Actions: 1. Halt controller node1 and all controllers attached  
to disk shelf 2.
```

```
2. Connect disk shelf 2 to controller node1 via two  
paths following the rules in the Universal SAS and ACP Cabling Guide.
```

```
3. Reboot the halted controllers.
```

```
4. Contact support personnel if the alert persists.
```

Sie zeigen Details über die Meldung an, um weitere Informationen zu erhalten, einschließlich der Warn-ID:


```

cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
    Node: node1
    Monitor: node-connect
    Alert ID: DualPathToDiskShelf_Alert
    Alerting Resource: 50:05:0c:c1:02:00:0f:02
    Subsystem: SAS-connect
    Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
    Probable Cause: Connection_establishment_error
    Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
    Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
    hardware component failure (e.g. cable, HBA, or IOM failure).
    Acknowledge: false
    Suppress: false
    Policy: DualPathToDiskShelf_Policy
    Acknowledger: -
    Suppressor: -
    Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
    Alerting Resource Name: Shelf ID 2

```

Sie bestätigen die Meldung, dass Sie daran arbeiten.

```

cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true

```

Sie reparieren die Verkabelung zwischen Shelf 2 und node1 und booten das System dann neu. Anschließend überprüfen Sie den Systemzustand wieder und sehen, dass der Status lautet OK:

```
cluster1::>system health status show
Status
-----
OK
```

Konfigurieren der Erkennung von Cluster- und Management-Netzwerk-Switches

Die Cluster-Switch-Systemzustandsüberwachung versucht automatisch, die Cluster- und Management-Netzwerk-Switches mithilfe des Cisco Discovery Protocol (CDP) zu erkennen. Sie müssen die Systemzustandsüberwachung konfigurieren, wenn ein Switch nicht automatisch erkannt werden kann oder wenn Sie nicht für die automatische Erkennung CDP verwenden möchten.

Über diese Aufgabe

Der `system cluster-switch show` Mit dem Befehl werden die Switches aufgeführt, die die Systemzustandsüberwachung erkannt hat. Wenn für Sie keinen Schalter in der Liste angezeigt wird, kann die Systemzustandsüberwachung ihn nicht automatisch erkennen.

Schritte

1. Wenn Sie CDP für die automatische Erkennung verwenden möchten, gehen Sie wie folgt vor:

- a. Stellen Sie sicher, dass das Cisco Discovery Protocol (CDP) auf Ihren Switches aktiviert ist.

Anweisungen hierzu finden Sie in der Switch-Dokumentation.

- b. Führen Sie für jeden Knoten im Cluster den folgenden Befehl aus, um zu überprüfen, ob CDP aktiviert oder deaktiviert ist:

```
run -node node_name -command options cdpd.enable
```

Wenn CDP aktiviert ist, fahren Sie mit Schritt d. fort Wenn CDP deaktiviert ist, mit Schritt c fortfahren

- c. Führen Sie den folgenden Befehl aus, um CDP zu aktivieren:

```
run -node node_name -command options cdpd.enable on
```

Warten Sie fünf Minuten, bevor Sie mit dem nächsten Schritt fortfahren.

- a. Verwenden Sie die `system cluster-switch show` Befehl zum Überprüfen, ob ONTAP die Switches jetzt automatisch erkennen kann.

2. Wenn die Systemzustandsüberwachung keinen Switch automatisch erkennt, verwenden Sie den `system cluster-switch create` Befehl zum Konfigurieren der Erkennung des Switches:

```
cluster1::> system cluster-switch create -device switch1 -address
192.0.2.250 -snmp-version SNMPv2c -community cshml! -model NX5020 -type
cluster-network
```

Warten Sie fünf Minuten, bevor Sie mit dem nächsten Schritt fortfahren.

3. Verwenden Sie die `system cluster-switch show` Befehl um zu überprüfen, ob ONTAP den Switch erkennen kann, für den Sie Informationen hinzugefügt haben.

Nachdem Sie fertig sind

Überprüfen Sie, ob die Systemzustandsüberwachung Ihre Switches überwachen kann.

Überprüfen Sie die Überwachung von Cluster- und Managementnetzwerk-Switches

Die Cluster-Switch-Systemzustandsüberwachung versucht automatisch, die Switches zu überwachen, die sie erkannt haben. Die Überwachung erfolgt jedoch möglicherweise nicht automatisch, wenn die Switches nicht richtig konfiguriert sind. Sie sollten überprüfen, ob die Systemzustandsüberwachung ordnungsgemäß für das Monitoring Ihrer Switches konfiguriert ist.

Schritte

1. Geben Sie den folgenden Befehl ein, um die Switches zu identifizieren, die die Systemzustandsüberwachung des Cluster-Switch erkannt haben:

ONTAP 9.8 und höher

```
system switch ethernet show
```

ONTAP 9.7 und früher

```
system cluster-switch show
```

Wenn der `Model` Spalte zeigt den Wert an `OTHER`, Dann kann ONTAP den Schalter nicht überwachen. ONTAP setzt den Wert auf `OTHER` Wenn ein automatisch erkannte Switch nicht für das Monitoring des Systemzustands unterstützt wird.



Wenn in der Befehlsausgabe des Befehls kein Switch angezeigt wird, müssen Sie die Erkennung des Switches konfigurieren.

2. Führen Sie ein Upgrade auf die neueste unterstützte Switch-Software durch, und verwenden Sie die Konfigurationsdatei (RCF) von der NetApp Support Site.

["NetApp Support Downloads Seite"](#)

Die Community-Zeichenfolge in der RCF des Switches muss mit der Community-Zeichenfolge übereinstimmen, die die Systemzustandsüberwachung konfiguriert ist. Standardmäßig verwendet die Systemzustandsüberwachung die Community-Zeichenfolge `cshml!`.



Derzeit unterstützt die Systemzustandsüberwachung nur SNMPv2.

Wenn Sie Informationen über einen Switch ändern müssen, der vom Cluster überwacht wird, können Sie den Community-String, den die Systemzustandsüberwachung mit dem folgenden Befehl verwendet, ändern:

ONTAP 9.8 und höher

```
system switch ethernet modify
```

ONTAP 9.7 und früher

```
system cluster-switch modify
```

3. Vergewissern Sie sich, dass der Managementport des Switch mit dem Managementnetzwerk verbunden ist.

Diese Verbindung ist erforderlich, um SNMP-Abfragen durchzuführen.

Befehle für das Monitoring des Systemzustands Ihres Systems

Sie können das verwenden `system health` Befehle zum Anzeigen von Informationen über den Systemzustand der Systemressourcen, zum Reagieren auf Meldungen und zum Konfigurieren zukünftiger Warnmeldungen. Mithilfe der CLI-Befehle können Sie detaillierte Informationen über das Konfigurieren des Systemzustands anzeigen. Die man-Pages für die Befehle enthalten weitere Informationen.

Zeigt den Status des Systemzustands an

Ihr Ziel ist	Befehl
Anzeigen des Integritätsstatus des Systems, der den Gesamtstatus einzelner Integritätsmonitore wiedergibt	<code>system health status show</code>
Anzeigen des Funktionszustands von Subsystemen, für die ein Zustandsüberwachung verfügbar ist	<code>system health subsystem show</code>

Zeigt den Status der Node-Konnektivität an

Ihr Ziel ist	Befehl
Zeigt Details zur Konnektivität vom Node zum Storage Shelf an, einschließlich Portinformationen, HBA-Port-Geschwindigkeit, I/O-Durchsatz und der Geschwindigkeit von I/O-Vorgängen pro Sekunde	<code>storage shelf show -connectivity</code> Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu jedem Shelf.
Anzeigen von Informationen zu Laufwerken und Array-LUNs, einschließlich des nutzbaren Speicherplatzes, Shelf- und Einschubnummern sowie des eigenen Node-Namens	<code>storage disk show</code> Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu jedem Laufwerk.

Ihr Ziel ist	Befehl
Zeigt detaillierte Informationen über Storage-Shelf-Ports an, einschließlich Porttyp, Geschwindigkeit und Status	<pre>storage port show</pre> <p>Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu den einzelnen Adaptern.</p>

Managen Sie die Erkennung von Cluster-, Storage- und Management-Netzwerk-Switches

Ihr Ziel ist	Verwenden Sie diesen Befehl.. (ONTAP 9.8 und höher)	Verwenden Sie diesen Befehl.. (ONTAP 9.7 und früher)
Zeigen Sie die Switches an, die das Cluster überwacht	<pre>system switch ethernet show</pre>	<pre>system cluster-switch show</pre>
<p>Zeigen Sie die Switches an, die das Cluster derzeit überwacht, einschließlich der von Ihnen gelöschten Switches (siehe Spalte „Grund“ der Befehlsausgabe), und Konfigurationsinformationen, die Sie für den Netzwerkzugriff auf das Cluster und auf die Management-Netzwerk-Switches benötigen.</p> <p>Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar.</p>	<pre>system switch ethernet show-all</pre>	<pre>system cluster-switch show-all</pre>
Konfigurieren Sie die Erkennung eines nicht erkannten Switches	<pre>system switch ethernet create</pre>	<pre>system cluster-switch create</pre>
Ändern von Informationen über einen vom Cluster überwachten Switch (z. B. Gerätenamen, IP-Adresse, SNMP-Version und Community String)	<pre>system switch ethernet modify</pre>	<pre>system cluster-switch modify</pre>
Deaktivieren Sie die Überwachung eines Switches	<pre>system switch ethernet modify -disable-monitoring</pre>	<pre>system cluster-switch modify -disable-monitoring</pre>
Deaktivieren Sie die Erkennung und Überwachung eines Switch und löschen Sie die Switch-Konfigurationsinformationen	<pre>system switch ethernet delete</pre>	<pre>system cluster-switch delete</pre>

Ihr Ziel ist	Verwenden Sie diesen Befehl.. (ONTAP 9.8 und höher)	Verwenden Sie diesen Befehl.. (ONTAP 9.7 und früher)
Entfernen Sie die in der Datenbank gespeicherten Switch-Konfigurationsinformationen dauerhaft (wodurch die automatische Erkennung des Switch wieder möglich ist).	<code>system switch ethernet delete -force</code>	<code>system cluster-switch delete -force</code>
Aktivieren Sie die automatische Protokollierung zum Senden mit AutoSupport-Nachrichten.	<code>system switch ethernet log</code>	<code>system cluster-switch log</code>




Reagieren Sie auf generierte Warnmeldungen

Ihr Ziel ist	Befehl
Anzeige von Informationen zu generierten Meldungen, z. B. Ressource und Node, auf dem die Meldung ausgelöst wurde, sowie des Schweregrads und der wahrscheinlichen Ursache der Meldung	<code>system health alert show</code>
Zeigt Informationen zu jeder generierten Meldung an	<code>system health alert show -instance</code>
Geben Sie an, dass jemand an einer Warnung arbeitet	<code>system health alert modify</code>
Bestätigen Sie eine Meldung	<code>system health alert modify -acknowledge</code>
Unterdrücken Sie eine nachfolgende Meldung, damit sie den Integritätsstatus eines Subsystems nicht beeinflusst	<code>system health alert modify -suppress</code>
Löschen Sie eine Meldung, die nicht automatisch gelöscht wurde	<code>system health alert delete</code>
Informationen zu den AutoSupport Meldungen, die innerhalb der letzten Woche ausgelöst wurden, anzeigen, um z. B. zu bestimmen, ob eine Meldung eine AutoSupport Meldung ausgelöst hat	<code>system health autosupport trigger history show</code>

Konfigurieren Sie zukünftige Warnmeldungen

Ihr Ziel ist	Befehl
Aktivieren oder deaktivieren Sie die Richtlinie, die steuert, ob ein bestimmter Ressourcenzustand eine bestimmte Warnmeldung ausgibt	<code>system health policy definition modify</code>

Zeigt Informationen zur Konfiguration der Systemzustandsüberwachung an

Ihr Ziel ist	Befehl
Anzeigen von Informationen über Systemzustandsüberwachung, z. B. ihre Nodes, Namen, Subsysteme und Status	<code>system health config show</code> <div>  <p>Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu jeder Systemzustandsüberwachung.</p> </div>
Zeigen Sie Informationen zu den Meldungen an, die eine Systemzustandsüberwachung möglicherweise generiert werden kann	<code>system health alert definition show</code> <div>  <p>Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu jeder Meldungsdefinition.</p> </div>
Anzeigen von Informationen über Richtlinien der Systemzustandsüberwachung, die bestimmen, wann Meldungen ausgegeben werden	<code>system health policy definition show</code> <div>  <p>Verwenden Sie die <code>-instance</code> Parameter zum Anzeigen detaillierter Informationen zu jeder Richtlinie. Verwenden Sie andere Parameter, um die Meldungsliste zu filtern, z. B. nach Richtlinienstatus (aktiviert oder nicht), Systemzustandsüberwachung, Meldung usw.</p> </div>

Zeigt Umgebungsinformationen an

Sensoren helfen Ihnen dabei, die Umgebungskomponenten Ihres Systems zu überwachen. Die Informationen, die Sie zu Umgebungssensoren anzeigen können, umfassen ihren Typ, ihren Namen, den Zustand, ihren Wert und ihre Schwellenwerte.

Schritt

1. Verwenden Sie das, um Informationen zu Umgebungssensoren anzuzeigen `system node environment sensors show` Befehl.

Filesystem-Analyse

File System Analytics – Übersicht

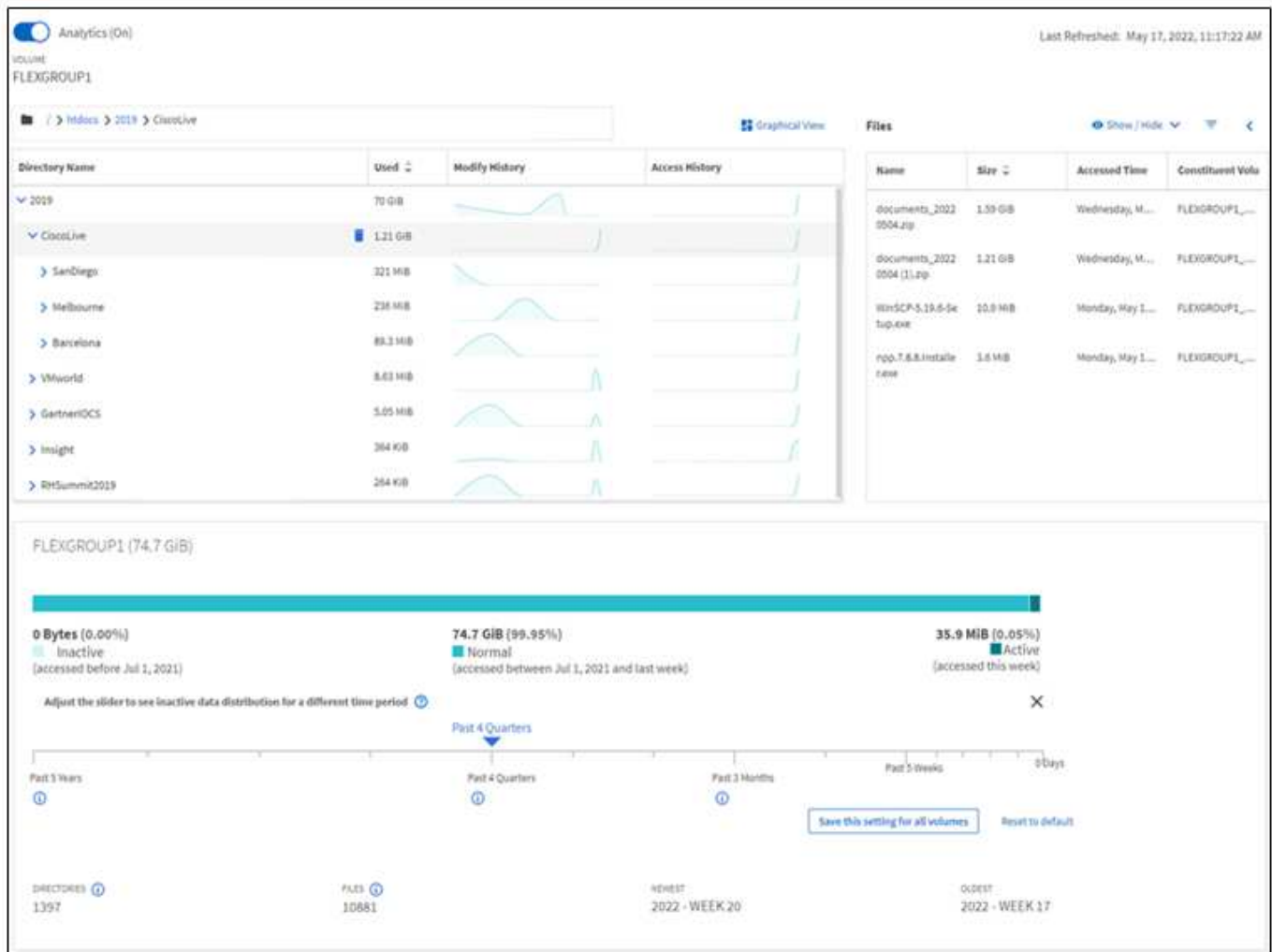
Die File System Analytics (FSA) wurde erstmals in ONTAP 9.8 eingeführt, um Echtzeiteinblick in die Dateinutzung und die Trends in der Storage-Kapazität in ONTAP FlexGroup oder FlexVol Volumes zu bieten. Diese native Funktion macht externe Tools überflüssig und bietet wichtige Einblicke in die Auslastung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

Mit FSA haben Sie Einblick 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 Bereich der Dateisystemanalyse.

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
Visualisierung in System Manager	✓	✓	✓	✓	✓	✓	✓
Kapazitätsanalysen	✓	✓	✓	✓	✓	✓	✓
Informationen zu inaktiven Daten	✓	✓	✓	✓	✓	✓	✓
Unterstützung für Volumes, die aus Data ONTAP 7-Mode migriert wurden	✓	✓	✓	✓	✓	✓	

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
Möglichkeit zum Anpassen inaktiver Perioden in System Manager	✓	✓	✓	✓	✓	✓	
Aktivitätenverfolgung auf Volume-Ebene	✓	✓	✓	✓	✓		
Vorgangsverfolgungsdaten in CSV herunterladen	✓	✓	✓	✓	✓		
Aktivitätsverfolgung auf SVM-Ebene	✓	✓	✓	✓			
Zeitachse	✓	✓	✓	✓			
Nutzungsanalysen	✓	✓	✓				
Option zum Aktivieren der Dateisystemanalyse standardmäßig	✓	✓					
Fortschrittsüberwachung für Initialisierungsscan	✓						


Erfahren Sie mehr über die Dateisystemanalyse

ONTAP File System Analytics

Daniel Tennant
Director of Software Engineering
December 13, 2020

© 2020 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —







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.

Über diese Aufgabe

- 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.
- 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 volume analytics show` verwenden.

Ab ONTAP 9.14.1 bietet ONTAP neben Benachrichtigungen über Drosselungsereignisse, die den Scanfortschritt beeinflussen, auch die Fortschrittsverfolgung für die Initialisierungsscan.

Weitere Überlegungen zum Initialisierungsscan finden Sie unter [Überlegungen zum Scannen](#).

Schritte

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

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. Nachdem Sie die Dateisystemanalyse erfolgreich aktiviert haben, können Sie die Analysedaten mit System Manager oder der ONTAP REST API anzeigen.


Ändern Sie die Standardeinstellungen für die Dateisystemanalyse

Ab ONTAP 9.13.1 können Sie die SVM- oder Clustereinstellungen ändern, um die Dateisystemanalyse auf neuen Volumes standardmäßig zu aktivieren.

System Manager

Wenn Sie System Manager verwenden, können Sie die Storage-VM- oder Cluster-Einstellungen ändern, um die Kapazitätsanalyse und die Aktivitätsverfolgung bei der Volume-Erstellung standardmäßig zu aktivieren. Die Standard-Aktivierung gilt nur für Volumes, die nach dem Ändern der Einstellungen erstellt wurden, nicht für vorhandene Volumes.

Einstellungen für Dateisystemanalysen in einem Cluster ändern

1. Navigieren Sie im System Manager zu **Cluster settings**.
2. Überprüfen Sie in **Cluster settings** die Registerkarte File System Settings. Um die Einstellungen zu ändern, wählen Sie die aus  Symbol.
3. Geben Sie im Feld **Activity Tracking** die Namen der SVMs ein, für die standardmäßig Activity Tracking aktiviert werden soll. Wenn Sie das Feld leer lassen, wird die Aktivitätsverfolgung für alle SVMs deaktiviert.

Deaktivieren Sie das Kontrollkästchen **bei neuen Storage-VMs aktivieren**, um die Aktivitätsverfolgung bei neuen Storage-VMs standardmäßig zu deaktivieren.

4. Geben Sie im Feld **Analytics** die Namen der Storage-VMs ein, für die die Kapazitätsanalyse standardmäßig aktiviert werden soll. Wenn Sie dieses Feld leer lassen, sind die Kapazitätsanalysen für alle SVMs deaktiviert.

Deaktivieren Sie das Kontrollkästchen **bei neuen Storage VMs aktivieren**, um die Kapazitätsanalyse bei neuen Storage VMs standardmäßig zu deaktivieren.

5. Wählen Sie **Speichern**.

Einstellungen für Dateisystemanalysen auf einer SVM ändern

1. Wählen Sie die SVM, die Sie ändern möchten, dann **Storage VM Einstellungen**.
2. Verwenden Sie in der Karte **File System Analytics** die Umschaltfunktionen, um Activity Tracking und Capacity Analytics für alle neuen Volumes auf der Speicher-VM zu aktivieren oder zu deaktivieren.

CLI

Sie können die Storage-VM so konfigurieren, dass die Dateisystemanalyse standardmäßig auf neuen Volumes mit der ONTAP-CLI aktiviert wird.

Aktivieren Sie File System Analytics standardmäßig auf einer SVM

1. Ändern Sie die SVM für alle neu erstellten Volumes so, dass die Kapazitätsanalyse und die Aktivitätsverfolgung standardmäßig aktiviert werden:

```
vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto-enable-analytics true
```

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

Ab ONTAP 9.10.1 umfasst die Dateisystemanalyse eine Funktion zur Verfolgung von Aktivitäten, mit der Sie Hot Objects identifizieren und die Daten 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. Zeitachsensdaten 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 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](#)

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 -vserver svm_name -volume volume_name
```

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

```
volume activity-tracking show -vserver 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 die Aktivitätsüberwachung für mehrere Volumes mit System Manager oder der 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

Aktivieren Sie für spezifische Volumes

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 aktivieren

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.

CLI

Ab ONTAP 9.13.1 können Sie die Aktivitätsverfolgung für mehrere Volumes mithilfe der ONTAP-CLI aktivieren.

Schritte

1. Verfolgung Von Aktivitäten Aktivieren:

```
volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
```

Nutzung * Aktivieren der Aktivitätsüberwachung für alle Volumes auf der angegebenen Speicher-VM

Nutzung ! Gefolgt von Volume-Namen, um Activity Tracking für alle Volumes auf der SVM mit Ausnahme der benannten Volumes zu aktivieren.

2. Bestätigen Sie, dass der Vorgang erfolgreich war:

```
volume show -fields activity-tracking-state
```

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

Analysen von der Nutzung ermöglichen

Ab ONTAP 9.12.1 können Sie die Nutzungsanalyse aktivieren, um festzustellen, welche Verzeichnisse innerhalb eines Volumes den größten Speicherplatz belegen. Sie können die Gesamtzahl der Verzeichnisse in einem Volume oder die Gesamtzahl der Dateien in einem Volume anzeigen. Die Berichterstellung ist auf die 25 Verzeichnisse beschränkt, die den größten Speicherplatz verwenden.

Analyse großer Verzeichnisse aktualisieren alle 15 Minuten. Sie können die letzte Aktualisierung überwachen, indem Sie den Zeitstempel der letzten Aktualisierung oben auf der Seite überprüfen. Sie können auch auf die Schaltfläche Herunterladen klicken, um Daten in eine Excel-Arbeitsmappe herunterzuladen. Der Download-Vorgang wird im Hintergrund ausgeführt und zeigt die zuletzt gemeldeten Informationen für das ausgewählte

Volume an. 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.

Um mehr Einblicke in ein bestimmtes Verzeichnis zu erhalten, können Sie dies tun [Aktivität auf einem Dateisystem anzeigen](#).

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.

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.)

Schritte

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.

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.

Schritte

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, um Storage-Kosten zu senken

Basierend auf Analyseanzeigen und Medienkostenvergleichen lassen sich Volumes auf kostengünstigeren Storage in lokalen Tiers verschieben.

Es kann jeweils nur ein Volume verglichen und verschoben werden.

Schritte

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` endpoint (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	<ul style="list-style-type: none">• /:uuid/top-metrics/directories• /:uuid/top-metrics/files• /:uuid/top-metrics/clients• /:uuid/top-metrics/users
Verfolgung von Aktivitäten auf SVMs	/api/svm/svms	<ul style="list-style-type: none">• /: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 Zugriff auf Administratoren 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"](#).

Überlegungen zum Scannen

Wenn Sie die Kapazitätsanalyse aktivieren, führt ONTAP einen Initialisierungsscan für Kapazitätsanalysen durch. Der Scan greift auf Metadaten für alle Dateien in Volumes zu, für die die Kapazitätsanalyse aktiviert ist. Während des Scans werden keine Dateidaten gelesen. Ab ONTAP 9.14.1 können Sie den Fortschritt des Scans mit der REST-API, auf der Registerkarte **Explorer** im System-Manager oder mit der verfolgen `volume analytics show` CLI-Befehl. Wenn ein Drosselungsereignis vorhanden ist, gibt ONTAP eine Benachrichtigung aus.

Nach Abschluss des Scans wird die Dateisystemanalyse kontinuierlich in Echtzeit aktualisiert, da sich das Dateisystem ändert, ohne dass der Scan erneut durchgeführt werden muss.

Die für den Scan benötigte Zeit ist proportional zur Anzahl der Verzeichnisse und Dateien auf dem Volume. Da beim Scan Metadaten erfasst werden, wirkt sich die Dateigröße nicht auf die Scan-Zeit aus.

Weitere Informationen zum Initialisierungsscan finden Sie unter ["TR-4867: Best Practice Guidelines for File System Analytics"](#).

Best Practices in sich vereint

Sie sollten den Scan auf Volumes starten, die Aggregate nicht gemeinsam nutzen. Mit dem Befehl können Sie sehen, welche Aggregate derzeit welche Volumes hosten:

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

Während der Scan ausgeführt wird, bedienen die Volumes weiterhin den Client-Datenverkehr. Es wird empfohlen, den Scan in Zeiträumen zu starten, in denen Sie mit einem geringeren Clientverkehr rechnen.

Wenn der Client-Datenverkehr zunimmt, verbraucht er Systemressourcen und führt dazu, dass der Scan länger dauert.

Ab ONTAP 9.12.1 können Sie die Datenerfassung in System Manager und über die ONTAP CLI anhalten.

- Wenn Sie die ONTAP-CLI verwenden:
 - Sie können die Datenerfassung mit dem folgenden Befehl anhalten: `volume analytics initialization pause -vserver svm_name -volume volume_name`
 - Sobald der Clientverkehr verlangsamt wurde, können Sie die Datenerfassung mit dem folgenden Befehl fortsetzen: `volume analytics initialization resume -vserver svm_name -volume volume_name`
- Wenn Sie den System Manager verwenden, verwenden Sie in der Ansicht **Explorer** des Volume-Menüs die Schaltflächen **Datensammlung anhalten** und **Datenerfassung fortsetzen**, um den Scan zu verwalten.

EMS-Konfiguration

EMS-Konfigurationsübersicht

Sie können ONTAP 9 so konfigurieren, dass wichtige EMS (Event Management System)-Ereignisbenachrichtigungen direkt an eine E-Mail-Adresse, Syslog-Server, Simple Management Network Protocol (SNMP) traphost oder Webhook-Anwendung gesendet werden, sodass Sie sofort über Systemprobleme benachrichtigt werden, die eine sofortige Aufmerksamkeit erfordern.

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

Überprüfen Sie die Release-spezifischen Versionen der ["ONTAP 9 EMS-Referenz"](#).

Wenn Ihre EMS-Ereigniszuordnung veraltete ONTAP-Befehlssätze verwendet (z. B. Ereignisziel, Ereignisroute), wird empfohlen, dass Sie Ihre Zuordnung aktualisieren. ["Erfahren Sie, wie Sie Ihre EMS-Zuordnung von veralteten ONTAP-Befehlen aktualisieren können"](#).

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



- "[ONTAP EMS-Referenz](#)"
- "[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	<ul style="list-style-type: none"> • TrapHost-Name


E-Mail (Ab 9.10.1)	<ul style="list-style-type: none"> • E-Mail-Adresse des Zielorts • Mailserver • Von E-Mail-Adresse
Syslog-Server (Ab 9.10.1)	<ul style="list-style-type: none"> • Hostname oder IP-Adresse des Servers • Syslog-Port (beginnend mit 9.12.1) • Syslog-Transport (ab 9.12.1) <p>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.</p>
Webhook (Ab 9.10.1)	<ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> 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` 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 `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 Webhook-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 skalierbaren 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
```

Name	Mail Dest.	SNMP Dest.	Syslog Dest.	Hide
------	------------	------------	--------------	------

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.*
```

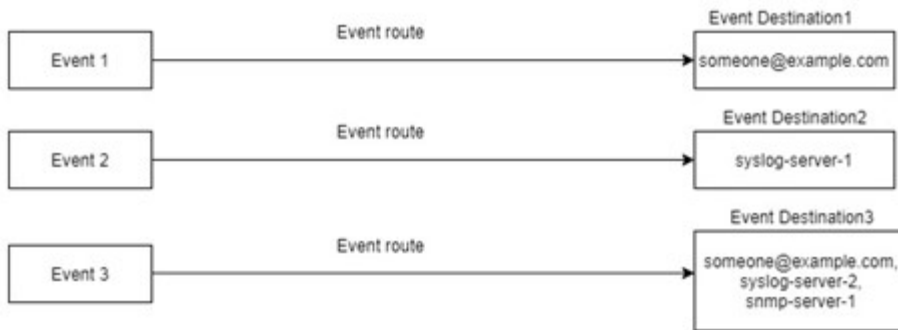
Time	Message	Severity	Destinations	Freq	Threshd
-----	-----	-----	-----	-----	-----
-----	-----	-----	-----	-----	-----
	raid.aggr.autoGrow.abort	NOTICE	test	0	0
	raid.aggr.autoGrow.success	NOTICE	test	0	0
	raid.aggr.lock.conflict	INFORMATIONAL	test	0	0
	raid.aggr.log.CP.count	DEBUG	test	0	0

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"](#)

Legacy routing based model



Event notification based model



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
```

Time	Message	Severity	Destinations	Threshd	Freq
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?: -
```

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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