Ereignis-, Performance- und Zustandsüberwachung

ONTAP 9

NetApp
February 12, 2026

Inhalt

Ereignis-, Performance- und Zustandsüberwachung

Überwachen Sie die Cluster-Performance mit System Manager

Überwachen Sie die Clusterleistung mit ONTAP 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.

Über diese Aufgabe

Dieses Verfahren gilt für FAS-, AFF- und ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, folgen Sie "Diesen Schritten ausführen" um die Leistung Ihres Clusters zu überwachen. ASA r2 Systeme bieten eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden.

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 Systemzustand und Kapazität auf → , um zusätzliche Informationen anzuzeigen und Aufgaben auszuführen.

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

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

Erfahren Sie mehr über Ansichtscluster auf ONTAP System Manager-Dashboards

Die System Manager Konsole bietet zentralen Zugriff auf eine schnelle und umfassende Übersicht über Ihr ONTAP Cluster.

Über das System Manager Dashboard erhalten Sie auf einen Blick Informationen zu wichtigen Alarmmeldungen und Benachrichtigungen, zur Effizienz und Kapazität von Storage-Tiers und Volumes, zu den in einem Cluster verfügbaren Nodes, zum Status der Nodes in einem Hochverfügbarkeitspaar, zu den aktivsten Applikationen und Objekten, und die Performance-Kennzahlen eines Clusters oder Node.

Das Dashboard umfasst vier Bereiche, die wie folgt beschrieben werden:

Systemzustand

In der Ansicht Systemzustand werden Informationen zum allgemeinen Systemzustand aller erkennbaren Nodes im Cluster angezeigt.

Die Ansicht „Systemzustand“ zeigt außerdem die Fehler und Warnungen auf Cluster-Ebene an, z. B. nicht konfigurierte Node-Details, die die Merkmale angeben, die zur Verbesserung der Cluster-Performance geändert werden können.

Klicken Sie auf → , um die Ansicht „Systemzustand“ zu erweitern, um eine Übersicht über das Cluster zu erhalten, z. B. den Namen des Clusters, die Version, das Datum und die Uhrzeit der Cluster-Erstellung und vieles mehr. Sie können auch die Statistiken zum Systemzustand der Nodes überwachen, die einem Cluster zugeordnet sind. Sie können Tags verwalten, mit denen Sie Ressourcen in Ihrer Umgebung gruppieren und identifizieren können. Der Abschnitt Insights unterstützt Sie bei der Optimierung von Kapazität, Compliance und Konfiguration Ihres Systems.

Kapazität

In der Ansicht Kapazität wird der Speicherplatz eines Clusters angezeigt. Sie können den gesamten verwendeten logischen Speicherplatz, den gesamten verwendeten physischen Speicherplatz und den verfügbaren Festplattenspeicher anzeigen.

Sie können sich bei ActiveIQ registrieren, um historische Cluster-Daten anzuzeigen. Klicken Sie hier → , um die Ansicht Kapazität zu erweitern, um eine Übersicht über die Tiers anzuzeigen, die einem Cluster zugeordnet sind. Sie können Kapazitätsinformationen zu den einzelnen Tiers anzeigen: Den Gesamtspeicherplatz, den belegten Speicherplatz und den verfügbaren Speicherplatz. Details werden für Durchsatz, IOPS und Latenz angezeigt. "Weitere Informationen zu diesen Kapazitätsmessungen in System Manager".

Sie können in der Kapazitätsansicht einen lokalen Tier oder einen Cloud-Tier hinzufügen. Weitere Informationen finden Sie unter "Anzeige der Kapazität eines Clusters".

Netzwerk

In der Ansicht Netzwerk werden die physischen Ports, Netzwerkschnittstellen und Speicher-VMs angezeigt, die Teil des Netzwerks sind.

In der Ansicht Netzwerk wird der Typ der mit dem Netzwerk verbundenen Clients angezeigt. Jeder dieser netzwerkverbundenen Clients wird durch eine Zahl dargestellt (z. B. „NVMe/FC 16“). Wählen Sie die Nummer aus, um spezifische Details zu jedem dieser Netzwerkelemente anzuzeigen.

Klicken Sie hier → , um eine umfassende Netzwerkansicht mit Ports, Netzwerkschnittstellen, Storage-VMs und Hosts im Netzwerk zu erhalten.

Performance

Die Performance-Ansicht zeigt Performance-Statistiken an, die Sie bei der Überwachung des Systemzustands und der Effizienz Ihres ONTAP-Clusters unterstützen. Die Statistiken umfassen wichtige Cluster-Performance-Indikatoren wie Latenz, Durchsatz und IOPS, die als Diagramme dargestellt sind.

In der Performance-Ansicht werden Leistungsstatistiken in verschiedenen Zeitintervallen nach Tag, Stunde, Woche oder Jahr angezeigt. Sie können die Cluster-Performance mithilfe der verschiedenen Diagramme schnell analysieren und charakteristische Merkmale identifizieren, die möglicherweise eine Optimierung erfordern. Diese schnelle Analyse hilft bei der Entscheidung, wie Sie Workloads hinzufügen oder verschieben

können. Sie können auch die Spitzenzeiten nutzen, um potenzielle Änderungen zu planen.

In der Performance-Ansicht werden die gesamten Performance-Metriken in Bezug auf Latenz, Durchsatz und IOPS angezeigt.

Ab Version 9.15.1 ist die Performance-Ansicht erweitert, um Diagramme für Lese-, Schreib- und sonstige Performance-Metriken sowie Diagramme in Bezug auf Latenz, Durchsatz und IOPS anzuzeigen. Weitere Metriken sind beispielsweise Vorgänge, die nicht gelesen oder geschrieben werden.

Die Leistungswerte werden alle 3 Sekunden aktualisiert, und das Performance-Diagramm wird alle 15 Sekunden aktualisiert. Es wird kein Diagramm angezeigt, wenn Informationen zur Cluster-Performance nicht verfügbar sind.

Klicken Sie hier  , um eine ganzseitige Ansicht der Leistungskennzahlen nach Stunden, Tagen, Wochen, Monaten und Jahr anzuzeigen. Sie können auch einen Bericht der Leistungskennzahlen in Ihrem lokalen System herunterladen.

Identifizieren Sie Hot Volumes und andere Objekte im ONTAP System Manager

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 im ONTAP System Manager ändern

Ab ONTAP 9.8 Servicequalität (QoS)ist bei der Bereitstellung von Storage 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 QoS ändern möchten, ⋮ dann **Bearbeiten**.

Überwachen Sie Risiken im ONTAP System Manager

Ab ONTAP 9.10.0 können Sie mit System Manager die von Active IQ Digital Advisor (auch als digitaler Berater bezeichnet) gemeldeten Risiken überwachen. Ab ONTAP 9.10.1 erkennen Sie mit System Manager auch die Risiken.

NetApp Digital Advisor meldet Chancen zur Risikominimierung und zur Verbesserung der Performance und Effizienz Ihrer Storage-Umgebung. Mit System Manager erfahren Sie mehr über die von Digital Advisor

gemeldeten Risiken und erhalten verwertbare Informationen, mit denen Sie Storage-Verwaltung, höhere Verfügbarkeit, verbesserte Sicherheit und eine bessere Storage-Performance erreichen.

Link zu Ihrem Digital Advisor-Konto

Um Informationen über Risiken von Digital Advisor zu erhalten, sollten Sie zunächst einen Link zu Ihrem Digital Advisor-Konto von System Manager erstellen.

Schritte

1. Klicken Sie in System Manager auf **Cluster > Einstellungen**.
2. Klicken Sie unter **Active IQ-Registrierung** auf **Registrieren**.
3. Geben Sie Ihre Anmeldedaten für Digital Advisor 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 im Dashboard in System Manager die Anzahl der von Digital Advisor gemeldeten Risiken anzeigen.

Bevor Sie beginnen

Sie müssen eine Verbindung von System Manager zu Ihrem Digital Advisor-Konto herstellen. Siehe Link zu Ihrem Digital Advisor-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 zeigen Sie in System Manager an, wie die von Digital Advisor gemeldeten Risiken nach Impact-Bereichen 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 von System Manager zu Ihrem Digital Advisor-Konto herstellen. Siehe Link zu Ihrem Digital Advisor-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 in System Manager die Liste der Risiken an, indem Sie das Verfahren in ausführenDetails 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 ein paar Minuten, bis die Änderung in die Liste der Digital Advisor-Vorschläge übernommen wird.

Risiken nicht anerkennen

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

Schritte

1. Zeigen Sie in System Manager die Liste der Risiken an, indem Sie das Verfahren in ausführenDetails 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 zurückgenommen haben, dauert es einige Minuten, bis die Änderung in die Liste der Vorschläge von Digital Advisor übernommen wird.

Optimieren Sie Ihr System mit den Erkenntnissen des ONTAP System Manager

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

Über diese Aufgabe

Dieses Verfahren gilt für FAS-, AFF- und ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, folgen Sie "Diesen Schritten ausführen" um Erkenntnisse anzuzeigen, die Ihnen bei der Optimierung Ihres Systems helfen. ASA r2 Systeme bieten eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden.

Ab ONTAP 9.11.1 können Sie im System Manager Einblicke erhalten, die Ihnen dabei helfen, die Kapazität, Sicherheitskonformität und Konfiguration Ihres Systems zu optimieren.

Das Blockieren von Erweiterungen kann zu unerwarteten Ergebnissen führen. Ab ONTAP 9.11.1 können Sie native FPolicy für Storage-VMs mithilfe von System Manager aktivieren. Eventuell erhalten Sie eine System Manager Insight Meldung, die Sie "Konfigurieren Sie nativen FPolicy" für eine Storage-VM empfiehlt.

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 nativer 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 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 Erkenntnisse an.

-  Zeigt die kapazitätsbezogenen Einblicke an.
-  Zeigt die konfigurationsbezogenen Einblicke 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 entblssen, 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 diese Einsicht rückgängig zu machen, siehe [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 ⋮, und 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 Sie eine Erkenntnis zuvor verworfen haben, können Sie deren Verwerfung rückgängig machen, indem Sie sicherstellen, dass das entsprechende Kontrollkästchen aktiviert 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 in der rechten oberen Ecke der Seite auf ⋮, und wählen Sie dann **Export**.

Konfigurieren Sie native FPolicies im ONTAP System Manager

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:

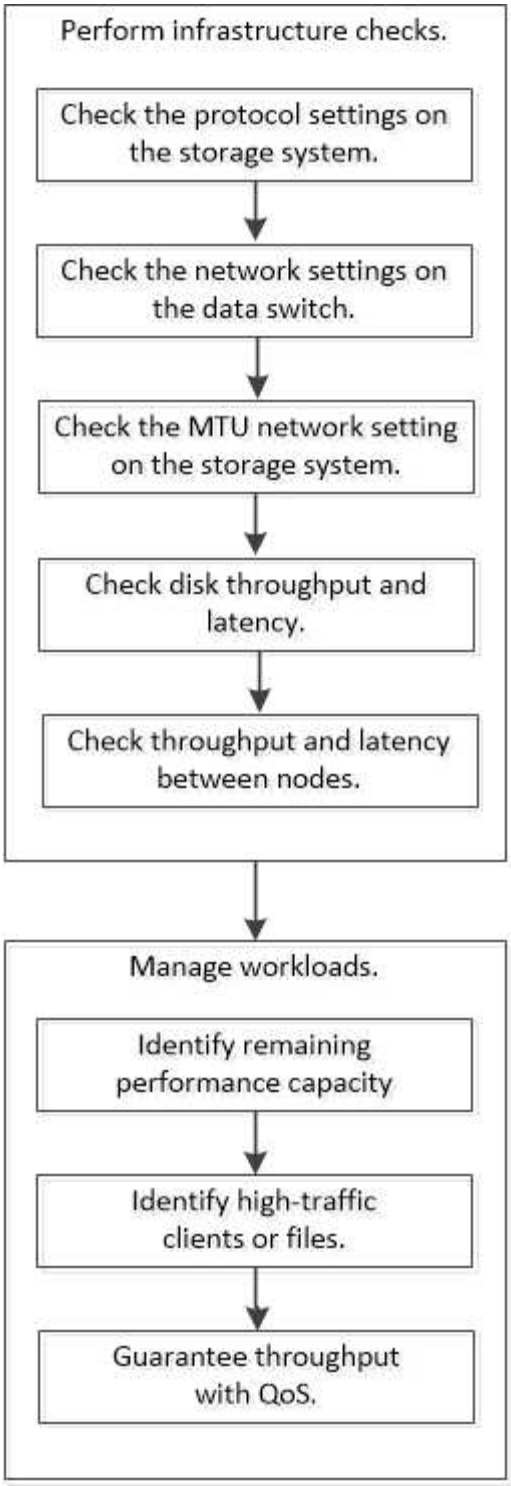
> **Das Blockieren von Erweiterungen kann zu unerwarteten Ergebnissen führen.** Ab ONTAP 9.11.1 können Sie native FPolicy für Storage-VMs mithilfe von System Manager aktivieren. Im FPolicy Native Mode können Sie bestimmte Dateierweiterungen zulassen oder untersagen. System Manager empfiehlt mehr als 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".

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

ONTAP 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 ONTAP NFS TCP-Übertragungsgröße

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.

Bevor Sie beginnen

- 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 `SVM1` auf 1048576 geändert:

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

Überprüfen Sie die ONTAP 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.

Bevor Sie beginnen

Für diese Aufgabe sind erweiterte Befehle auf Berechtigungsebene erforderlich.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

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

   ```
   vserver iscsi show -vserv,er vserver_name -instance
   ```

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

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

4. Zurück zur Administratorberechtigung:

```
set -privilege admin
```

Beispiel

Im folgenden Beispiel wird die TCP-Fenstergröße `SVM1` auf 131,400 Byte geändert:

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

Überprüfen Sie die ONTAP CIFS/SMB-Multiplexeinstellungen

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 auf `SVM1` 255 geändert:

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

Überprüfen Sie die Portgeschwindigkeit des ONTAP FC-Adapters

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.

Bevor Sie beginnen

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
   ```

   Erfahren Sie mehr über `network fcp adapter modify` in der "ONTAP-Befehlsreferenz".

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

   ```
   fcp adapter show -instance
   ```

Erfahren Sie mehr über `fcp adapter show` in der "ONTAP-Befehlsreferenz".

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`

   Erfahren Sie mehr über `network interface modify` in der "ONTAP-Befehlsreferenz".

Beispiel

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

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

Überprüfen Sie die ONTAP -Netzwerkeinstellungen auf den Daten-Switches

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.

Schritte

1. 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 ONTAP MTU-Netzwerkeinstellung auf dem Speichersystem

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-Domäne ist, `broadcast-domain modify` ändern Sie mit dem Befehl die MTU für alle Ports in der geänderten Broadcast-Domäne.

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
   ```

   Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

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 ONTAP 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

Das folgende Beispiel zeigt die Gesamtsummen in jedem Benutzer-Lese- oder Schreibvorgang für `node2` ein an `cluster1`:

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                    Busy Total Read  Write  Read    Write   *Latency
  Disk       Node   (%)   Ops   Ops   Ops   (Bps)    (Bps)       (us)
------------ ----   ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

Verwandte Informationen

- "Statistik-Disk-Show"

Überprüfen Sie den ONTAP Durchsatz und die Latenz zwischen den Knoten

Mit dem `network test-path` Befehl können Sie Netzwerkengpässe identifizieren oder die Netzwerkpfade zwischen den Nodes vorqualifizieren. Sie können den Befehl zwischen Cluster Nodes oder Intracluster Nodes ausführen.

Bevor Sie beginnen

- 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.

Mit dem `network test-path` Befehl können Sie den Durchsatz und die Latenz zwischen Nodes messen. 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.

Die `session-type` Option gibt an, welche Art von Vorgang Sie über den Netzwerkpfad ausführen – z. B. „AsyncMirrorRemote“ für die SnapMirror-Replikation zu 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 „local“ für `-source-node` gibt den Node an, auf dem Sie den Befehl ausführen.

   Mit dem folgenden Befehl werden Durchsatz und Latenz für SnapMirror-Typ-Replikationsvorgänge zwischen `node1` dem lokalen Cluster und `node3` auf gemessen `cluster2`:

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

   Beispielausgabe (die Ausgabedetails können je nach Ihrer Version von ONTAP variieren):

   ```
   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
   ```

   Erfahren Sie mehr über `network test-path` in der "ONTAP-Befehlsreferenz".

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 in ONTAP

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.

Bevor Sie beginnen

Für diese Aufgabe sind erweiterte Befehle auf Berechtigungsebene erforderlich.

Über diese Aufgabe

Sie können die folgenden Werte für die `-object` Option verwenden, um Reservestatistiken zu sammeln und anzuzeigen:

- 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
   ```

   Erfahren Sie mehr über `statistics start` in der "ONTAP-Befehlsreferenz".

3. Anzeigen von Informationen zu Reservestatistiken in Echtzeit:

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

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 Node berechnen, indem Sie den `current_utilization` Zähler vom Zähler abziehen `optimal_point_utilization`. In diesem Beispiel `CPU_sti2520-213` liegt die Auslastungskapazität für bei -14% (72%-86%), was darauf hindeutet, dass die CPU in der letzten Stunde durchschnittlich überlastet ist.

Sie könnten angegeben haben `ewma_daily`, , `ewma_weekly` oder `ewma_monthly` die gleichen Informationen über längere Zeiträume gemittelt 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.
```

Erfahren Sie mehr über `statistics show` in der "ONTAP-Befehlsreferenz".

Identifizieren Sie Clients oder Dateien mit hohem Datenverkehr in ONTAP

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.

Bevor Sie beginnen

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`*

   Der folgende Befehl zeigt die obersten Clients an, auf die zugegriffen `cluster1`wird:

   ```
   cluster1::> statistics top client show

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


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

   Erfahren Sie mehr über `statistics top client show` in der "ONTAP-Befehlsreferenz".

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`*

   Der folgende Befehl zeigt die wichtigsten Dateien auf `cluster1`:

```
cluster1::> statistics top file show

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

                                    *Total
                     File Volume Vserver          Node    Ops
------------------------ ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

Erfahren Sie mehr über `statistics top file show` in der "ONTAP-Befehlsreferenz".

Garantierter Durchsatz durch QoS

Sichern Sie den Durchsatz mit einer QoS-Übersicht in ONTAP

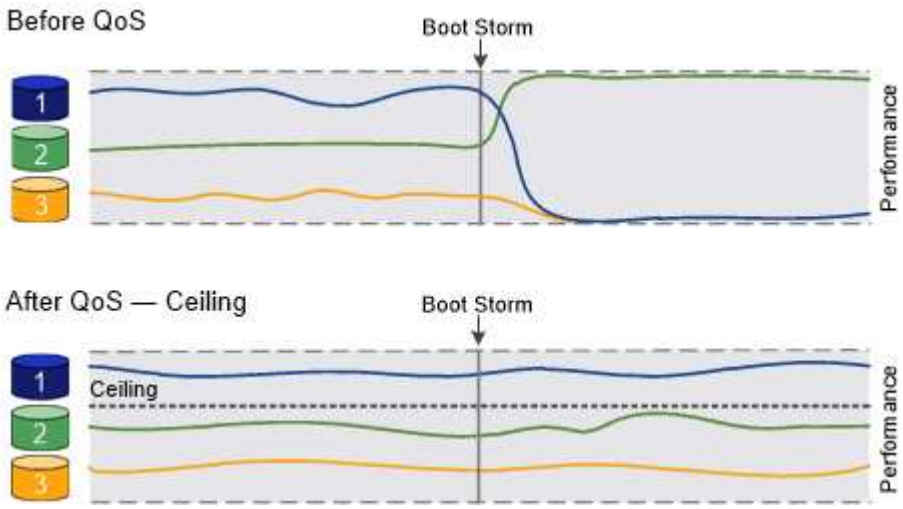
Dank Storage-Servicequalität (QoS) kann die Performance kritischer Workloads nicht durch konkurrierende Workloads beeinträchtigt werden. Sie können für einen konkurrierenden Workload eine Durchsatzbegrenzung festlegen, um die Auswirkungen auf Systemressourcen zu begrenzen oder für einen kritischen Workload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

Durchsatzgrenzen (QoS max)

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

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

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



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.

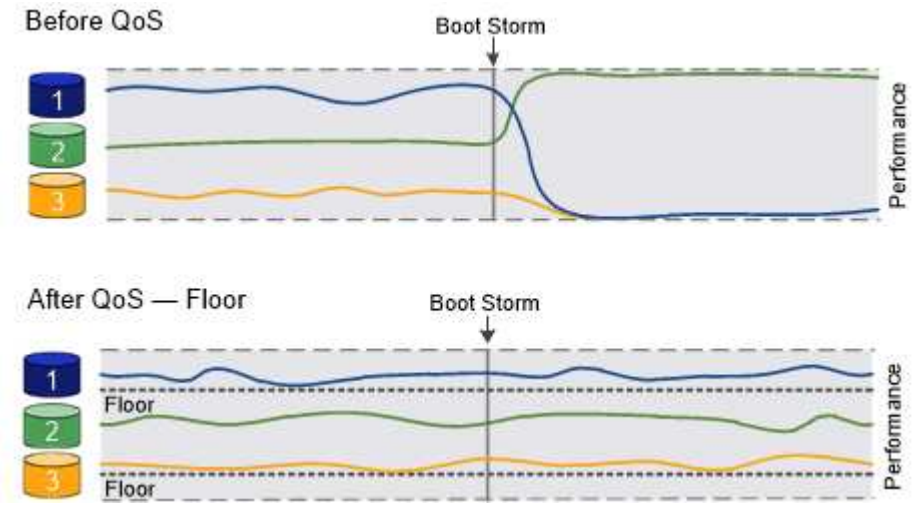
Sie können den Boden beim Erstellen der Richtliniengruppe angeben oder warten, bis Sie die Workloads überwachen, um sie anzugeben.

Ab ONTAP 9.13.1 lassen sich Durchsatzböden im SVM-Bereich mit einstellen[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. Eine Arbeitslast könnte während kritischer Vorgänge wie `volume move trigger-cutover`z. B. unter die angegebene Arbeitslast fallen. 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.



Shared-QoS-Richtliniengruppen und nicht-Shared-Richtliniengruppen

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.

Anpassungsfähige QoS

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

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

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

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

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

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

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

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

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

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

Ab ONTAP 9.6 werden Durchsatzböden 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. `vserver modify` `-qos-adaptive-policy-group-template`Legen Sie die Richtlinie mit dem Befehl mit dem Parameter fest.

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	• AFF • C190^ 1 ^ • ONTAP Select Premium mit SSD [1]	• 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
SnapMirror Synchronous	Ja.	Nein	Nein	Ja.

[1] C190 und ONTAP Select Unterstützung gestartet mit ONTAP 9.6 Version.

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-Unterstützung	ONTAP 9.8 und höher	ONTAP 9.7 bis 9.4	ONTAP 9.3 und frühere Versionen
Datenmenge	ja	ja	ja
Datei	ja	ja	ja
LUN	ja	ja	ja
SVM	ja	ja	ja

Workload-Unterstützung	ONTAP 9.8 und höher	ONTAP 9.7 bis 9.4	ONTAP 9.3 und frühere Versionen
FlexGroup Volume	ja	ja	ja (nur ONTAP 9.3)
Qtrees [1]	ja	Nein	Nein
Mehrere Workloads pro Richtliniengruppe	ja	ja	ja
Nicht gemeinsam genutzte Richtliniengruppen	ja	ja	Nein

[1] Ab ONTAP 9.9.1 wird der SMB-Zugriff auch in Qtrees in FlexVol und FlexGroup -Volumes mit aktiviertem SMB unterstützt. Ab ONTAP 9.8 wird der NFS-Zugriff in Qtrees in FlexVol und FlexGroup -Volumes mit aktiviertem NFS 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-Unterstützung	ONTAP 9.13.1 und höher	ONTAP 9.8 bis 9.13.0	ONTAP 9.4 bis 9.7	ONTAP 9,3
Datenmenge	ja	ja	ja	ja
Datei	ja	ja	ja	ja
LUN	ja	ja	ja	ja
SVM	ja	Nein	Nein	Nein
FlexGroup Volume	ja	ja	ja	Nein
Qtrees [1]	ja	ja	Nein	Nein
Mehrere Workloads pro Richtliniengruppe	ja	ja	ja	Nein
Nicht gemeinsam genutzte Richtliniengruppen	ja	ja	ja	Nein

[1] 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	ONTAP 9.13.1 und höher	ONTAP 9.4 bis 9.13.0	ONTAP 9,3
Datenmenge	ja	ja	ja
Datei	ja	ja	Nein
LUN	ja	ja	Nein
SVM	ja	Nein	Nein
FlexGroup Volume	ja	ja	Nein
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 9.4 und höher	ONTAP 9.3 und frühere Versionen
Maximale Workloads pro Cluster	40.000	12.000
Maximale Workloads pro Node	40.000	12.000
Maximale Anzahl von Richtliniengruppen	12.000	12.000

Aktivieren oder Deaktivieren von ONTAP Throughput Floors v2

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

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Geben Sie einen der folgenden Befehle ein:

Ihr Ziel ist	Verwenden Sie den folgenden Befehl:
Deaktivieren Sie die Etagen v2	`qos settings throughput-floors-v2 -enable false`

Ihr Ziel ist	Verwenden Sie den folgenden Befehl:
Ebenen v2 aktivieren	`qos settings throughput-floors-v2 -enable true`

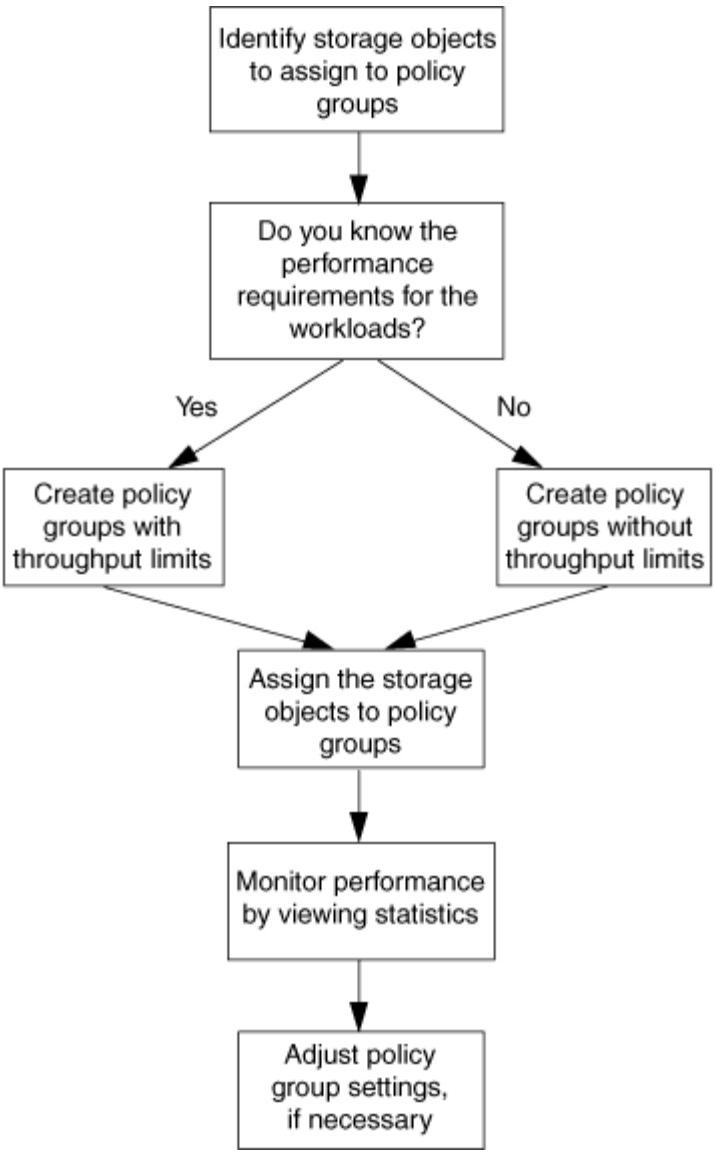
> Um Durchsatzböden v2 in einem MetroCluster Cluster zu deaktivieren, müssen Sie die ausführen
>
> `qos settings throughput-floors-v2 -enable false`
>
> Befehl auf Quell- und Ziel-Clustern.

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

Erfahren Sie mehr über `qos settings throughput-floors-v2` in der "ONTAP-Befehlsreferenz".

ONTAP Speicher-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.



Legen Sie mit QoS in ONTAP eine Durchsatzobergrenze fest

Über das `max-throughput` Feld für eine Richtliniengruppe können Sie eine Durchsatzobergrenze für Storage-Objekt-Workloads definieren (QoS max). Sie können die Richtliniengruppe anwenden, wenn Sie das Speicherobjekt erstellen oder ändern.

Bevor Sie beginnen

- 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.

  Legen Sie `-is-shared=false` für den `qos policy-group create` Befehl fest, um eine nicht freigegebene Richtliniengruppe anzugeben.

- 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`

   Erfahren Sie mehr über `qos policy-group create` in der "ONTAP-Befehlsreferenz".

   Sie können die `qos policy-group modify` Durchsatzdecken mit dem Befehl anpassen.

   Mit dem folgenden Befehl wird die Gruppe für gemeinsam genutzte Richtlinien `pg-vs1` mit einem maximalen Durchsatz von 5,000 IOPS erstellt:

   ```
   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 `pg-vs3` mit einem maximalen Durchsatz von 100 IOPS und 400 KB/s erstellt:

   ```
   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 `pg-vs4` ohne Durchsatzbegrenzung erstellt:

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

   Erfahren Sie mehr über `qos policy-group modify` in der "ONTAP-Befehlsreferenz".

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

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

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz". Sie können mit dem *storage_object* `modify` Befehl eine andere Richtliniengruppe auf das Speicherobjekt anwenden.

Der folgende Befehl wendet Policy Group `pg-vs1` auf SVM an `vs1`:

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

Die folgenden Befehle wenden Policy Group `pg-app` auf die Volumes `app1` und `app2`an:

```
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`

   Erfahren Sie mehr über `qos statistics performance show` in der "ONTAP-Befehlsreferenz".

   > 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`

   > 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
```

Erfahren Sie mehr über `qos statistics workload performance show` in der "ONTAP-Befehlsreferenz".

Sie können mit dem `qos statistics workload latency show` Befehl detaillierte Latenzstatistiken für QoS-Workloads anzeigen. Erfahren Sie mehr über `qos statistics workload latency show` in der "ONTAP-Befehlsreferenz".

Richten Sie mit QoS in ONTAP eine Durchsatzebene ein

Über das `min-throughput` Feld für eine Richtliniengruppe kann eine Durchsatzmenge für Storage-Objekt-Workloads definiert werden (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

- Zum Erstellen einer Richtliniengruppe müssen Sie ein Cluster-Administrator sein.
- Ab ONTAP 9.13.1 lassen sich Durchsatzwerte auf SVM-Ebene mithilfe eines erzwingenVorlage 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.

  Legen Sie `-is-shared=false` für den `qos policy-group create` Befehl fest, um eine nicht freigegebene Richtliniengruppe anzugeben.

- 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 zur "Identifizierung der verbleibenden Performance-Kapazität"Verfügung steht, wie in beschrieben.
2. Erstellen einer Richtliniengruppe:

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

   Erfahren Sie mehr über `qos policy-group create` in der "ONTAP-Befehlsreferenz".

3. Sie können den `qos policy-group modify` Befehl verwenden, um Durchsatzböden anzupassen.

   Mit dem folgenden Befehl wird die Gruppe für gemeinsam genutzte Richtlinien `pg-vs2` mit einem Mindestdurchsatz von 1,000 IOPS erstellt:

   ```
   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 `pg-vs4` ohne Durchsatzbegrenzung erstellt:

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

   Erfahren Sie mehr über `qos policy-group modify` in der "ONTAP-Befehlsreferenz".

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

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*`Sie können die _storage_object_modify` Befehl, um eine andere Richtliniengruppe auf das Speicherobjekt anzuwenden.

   Mit dem folgenden Befehl wird die Richtliniengruppe `pg-app2` auf das Volume angewendet `app2`:

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

   Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

5. Überwachung der Richtliniengruppenleistung:

   `qos statistics performance show`

   > 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
```

Erfahren Sie mehr über `qos statistics performance show` in der "ONTAP-Befehlsreferenz".

6. Monitoring der Workload-Performance:

   `qos statistics workload performance show`

   > 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
```

Erfahren Sie mehr über `qos statistics workload performance show` in der "ONTAP-Befehlsreferenz".

> Sie können mit dem `qos statistics workload latency show` Befehl detaillierte Latenzstatistiken für QoS-Workloads anzeigen. Erfahren Sie mehr über `qos statistics workload latency show` in der "ONTAP-Befehlsreferenz".

Verwenden Sie adaptive QoS-Richtliniengruppen in ONTAP

Sie können eine *adaptive QoS*-Richtliniengruppe verwenden, um eine Durchsatzobergrenze oder -untergrenze automatisch an die Volumengröße anzupassen und dabei das Verhältnis von IOPS zu TB/GB beizubehalten, wenn sich die Größe des Volumens ändert. Das ist ein erheblicher Vorteil, wenn man Hunderte oder Tausende von Workloads in einer großen Implementierung verwaltet.

Bevor Sie beginnen

- Sie müssen ONTAP 9.3 oder höher ausführen. Adaptive QoS-Richtliniengruppen sind ab ONTAP 9.3

verfügbar.

- Zum Erstellen einer Richtliniengruppe müssen Sie ein Cluster-Administrator sein.

Über diese Aufgabe

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

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

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

- `expected-iops`ist die minimale erwartete IOPS-Zahl pro zugewiesenem TB/GB.

> `expected-iops` Garantiert nur auf AFF-Plattformen. `expected-iops` Eine Garantie für FabricPool ist nur dann gegeben, wenn die Tiering-Richtlinie auf „keine" gesetzt ist und sich keine Blöcke in der Cloud befinden. `expected-iops` Garantiert für Volumes, die sich nicht in einer synchronen SnapMirror-Beziehung befinden.

- `peak-iops`ist die maximal mögliche IOPS-Zahl pro zugewiesenem oder verwendetem TB/GB.
- `expected-iops-allocation` Gibt an, ob zugewiesener Speicherplatz (Standard) oder belegter Speicherplatz für erwartete iops verwendet wird.

> `expected-iops-allocation` Ist verfügbar in ONTAP 9.5 und später. Es wird nicht unterstützt in ONTAP 9.4 und früher.

- `peak-iops-allocation` Gibt an, ob zugewiesener oder genutzter Speicherplatz (Standard) für verwendet wird `peak-iops`.
- `absolute-min-iops` Ist die absolute Mindestanzahl an IOPS. Sie können dieses Feld mit sehr kleinen Speicherobjekten verwenden. Es überschreibt sowohl `peak-iops` und/oder `expected-iops` wenn `absolute-min-iops` größer als der berechnete ist `expected-iops`.

  Wenn Sie beispielsweise `expected-iops` 1,000 IOPS/TB festlegen und die Volume-Größe weniger als 1 GB beträgt, `expected-iops` wird als Berechnung ein fraktionaler IOP berechnet. Der berechnete `peak-iops` Anteil wird noch kleiner sein. Sie können dies vermeiden, indem Sie `absolute-min-iops` einen realistischen Wert einstellen.

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

Standardmäßige adaptive QoS-Richtliniengruppen

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

Einschränkungen bei der Zuweisung von Speicherobjektrichtliniengruppen

In einigen Fällen können Sie ein Speicherobjekt keiner Richtliniengruppe zuordnen, wenn das enthaltende Objekt oder seine untergeordneten Objekte zu einer Richtliniengruppe gehören.

Ab ONTAP 9.18.1 können Sie verschachtelte QoS-Richtlinien verwenden, die es ermöglichen, Richtliniengruppen sowohl dem übergeordneten Objekt, wie z. B. einer SVM, als auch dessen untergeordneten Objekten, wie z. B. einem Volume, zuzuweisen. In einer Multi-Tenant-Umgebung ermöglichen verschachtelte QoS-Richtlinien den Administratoren, die QoS-Limits für SVMs auf die Volumes und Qtrees innerhalb der SVM aufzuteilen und die Speicherressourcen über verschiedene Rechenumgebungen hinweg auszugleichen, während gleichzeitig die Priorisierung geschäftskritischer Workloads ermöglicht wird.

Verschachtelte QoS-Richtlinien werden für die folgenden Objektpaare unterstützt:

- SVMs und FlexVol oder FlexGroup -Volumes, die von der SVM enthalten sind.
- FlexVol oder FlexGroup Volumes und Qtrees innerhalb der Volumes.

Bei verschachtelten QoS-Richtlinien wird die restriktivste anwendbare Richtlinie verwendet.

Die Einschränkungen sind in der folgenden Tabelle aufgeführt.

Wenn Sie die folgende Zuordnung zuweisen:	**Dann können Sie die Richtlinie keiner Richtliniengruppe zuweisen…**
SVM einer Richtliniengruppe	Alle im SVM enthaltenen Speicherobjekte. Wenn Sie ONTAP 9.18.1 verwenden, können FlexVol und FlexGroup -Volumes, die in SVMs enthalten sind, einer Richtliniengruppe zugewiesen werden.
Volume zu einer Richtliniengruppe	Die SVM, die das Volume oder alle untergeordneten LUNs enthält. Wenn Sie ONTAP 9.18.1 oder höher verwenden, kann die SVM, die das Volume enthält, einer Richtliniengruppe zugewiesen werden. Zusätzlich können Qtrees in FlexVol oder FlexGroup -Volumes zugewiesen werden.

Wenn Sie die folgende Zuordnung zuweisen:	Dann können Sie die Richtlinie keiner Richtliniengruppe zuweisen…
LUN einer Richtliniengruppe	Das Volume oder SVM, das die LUNs enthält
Datei zu einer Richtliniengruppe	Das Volume oder SVM, das die Datei enthält

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`

   Erfahren Sie mehr über `qos adaptive-policy-group create` in der "ONTAP-Befehlsreferenz".

   > `-expected-iops-allocation` Und `-block-size` ist in ONTAP 9.5 und später verfügbar. Diese Optionen werden in ONTAP 9.4 und früher nicht unterstützt.

   Mit dem folgenden Befehl wird eine Richtliniengruppe `adpg-app1` für adaptive QoS mit `-expected-iops` einem Wert von 300 IOPS/ `-peak-iops`TB erstellt, `-peak-iops-allocation` auf 1,000 IOPS/TB `used-space -absolute-min-iops` festgelegt, auf festgelegt und auf 50 IOPS festgelegt:

   ```
   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`*

   Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

   Mit dem folgenden Befehl wird die Richtliniengruppe der adaptiven QoS `adpg-app1` auf das Volume angewendet `app1`:

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

   Mit den folgenden Befehlen wenden Sie die standardmäßige Richtliniengruppe adaptive QoS `extreme` auf das neue Volume `app4` und auf das vorhandene Volume `app5`an. 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 in ONTAP 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. Die Durchsatzmenge wird jedoch 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 und verwalten Sie die Clusterleistung mit Unified Manager.

Überwachen Sie die Clusterleistung mit ONTAP 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 Linus"
- "Erste Schritte mit Active IQ Unified Manager für Windows"

Erfahren Sie mehr über die Leistungsüberwachung und -verwaltung von ONTAP Active IQ Unified Manager

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 verwenden die ONTAP-Befehlszeilenschnittstelle, um Storage Quality of Service (QoS) zu konfigurieren. QoS ist außerdem über die folgenden Optionen verfügbar:
  - System Manager
  - ONTAP REST API
  - ONTAP Tools für VMware vSphere
  - NetApp-Service-Level-Manager (NSLM)
  - OnCommand Workflow Automation (WFA)
- Sie möchten Active IQ Unified Manager mithilfe einer virtuellen Appliance installieren, anstatt eine Linux- oder Windows-basierte Installation durchzuführen.
- 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

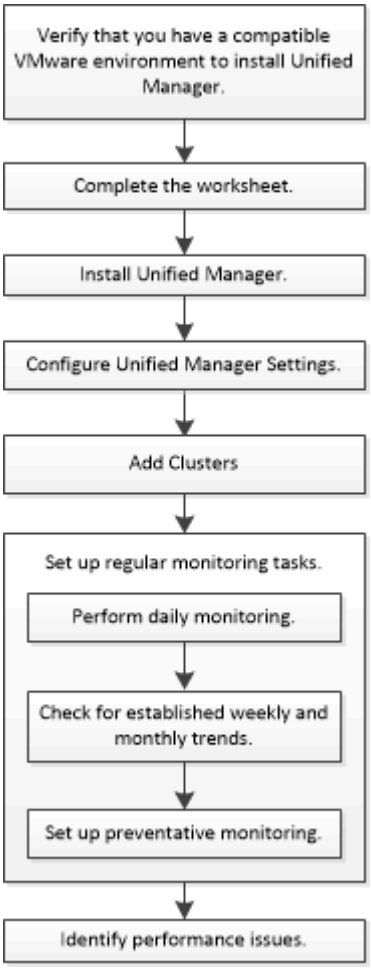
Wenn diese Annahmen für Ihre Situation nicht richtig sind, sollten Sie die folgenden Ressourcen sehen:

- "Installation von Active IQ Unified Manager 9.8"
- "Systemadministration"

Monitoring der Performance

Erfahren Sie mehr über den Leistungsüberwachungs- und Wartungsworkflow von ONTAP Active IQ Unified Manager

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.



Überprüfen Sie die VMware-Umgebungsanforderungen für ONTAP Active IQ Unified Manager

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. "Interoperabilitätsmatrix"Überprüfen Sie im, ob eine unterstützte Kombination der folgenden Komponenten verwendet wird:
   - ONTAP-Version
   - ESXi-Betriebssystemversion
   - VMware vCenter Server-Version
   - VMware Tools-Version
   - Browsertyp und -Version

   In der Interoperabilitäts-Matrix werden die unterstützten Konfigurationen für Unified Manager aufgeführt.
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

ONTAP Active IQ Unified Manager Arbeitsblatt

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

Informationen zur Installation von Unified Manager

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

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

Informationen zur Unified Manager-Konfiguration

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

Cluster-Informationen

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

Cluster 1 von N	Ihr Wert
Host-Name oder Cluster-Management-IP-Adresse	
Benutzername des ONTAP-Administrators Dem Administrator muss die Rolle „admin“ zugewiesen worden sein.	
ONTAP-Administratorpasswort	
Protokoll (HTTP oder HTTPS)	

Verwandte Informationen

"Administratorauthentifizierung und RBAC"

Installation von Active IQ Unified Manager

ONTAP Active IQ Unified Manager herunterladen und bereitstellen

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 der anfänglichen ONTAP Active IQ Unified Manager -Einstellungen

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

Schritte

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

Nachdem Sie fertig sind

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

Geben Sie die zu überwachenden ONTAP Cluster im Active IQ Unified Manager 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.

Bevor Sie beginnen

- 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.

  Sie können dies mit dem Befehl ONTAP 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

Führen Sie täglich eine ONTAP Active IQ Unified Manager Überwachung durch

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**, `Active Performance Events` und bestimmen Sie, welche Aktion erforderlich ist.

Verwenden Sie die wöchentlichen und monatlichen Leistungstrends von ONTAP Active IQ Unified Manager, um Leistungsprobleme zu identifizieren

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.

Leistungsschwellenwerte für ONTAP Active IQ Unified Manager festlegen

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.

ONTAP Active IQ Unified Manager Warnmeldungen hinzufügen

Ereignisse sind Benachrichtigungen, die der Active IQ Unified Manager automatisch generiert, wenn eine vordefinierte Bedingung eintritt oder wenn ein Leistungsindikator einen Schwellenwert überschreitet. Ereignisse helfen Ihnen, Leistungsprobleme in den von Ihnen überwachten Clustern zu identifizieren.

Sie können Warnmeldungen konfigurieren, die Sie benachrichtigen, wenn ein bestimmtes Ereignis generiert wird. Sie können Warnungen für eine einzelne Ressource, für eine Gruppe von Ressourcen oder für Ereignisse eines bestimmten Schweregrads konfigurieren. Sie können die Benachrichtigungshäufigkeit angeben und der Warnung ein Skript zuordnen.

Bevor Sie beginnen

- 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 `HealthTest` das Feld **Alert Name** ein.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
   a. Geben Sie `abc` in das Feld **Name enthält** ein, um die Volumes anzuzeigen, deren Name "abc" enthält.
   b. Wählen Sie[All Volumes whose name contains 'abc'] im Bereich „Verfügbare Ressourcen“ die Option **++** aus, und verschieben Sie sie in den Bereich „Ausgewählte Ressourcen“.
   c. Klicken Sie auf **exclude** und geben Sie `xyz` das Feld **Name enthält** ein, und klicken Sie dann auf **Add**.
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 **actions**, und geben Sie `sample@domain.com` in das Feld Alert these users ein.
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 der Warneinstellungen für ONTAP Active IQ Unified Manager

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.

Bevor Sie beginnen

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**.

Identifizieren Sie Leistungsprobleme im ONTAP Active IQ Unified Manager

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 ONTAP 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. Digital Advisor zeigt die Systemperformance 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.

Zusätzlich zu diesen Performance-Daten zeigt Digital Advisor Ihre Storage-Effizienz nach Workload auf und vergleicht diese Effizienz mit der erwarteten Effizienz für diesen Workload. 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

- "Digital Advisor Dokumentation"

- "Digital Advisor Video-Playliste"
- "Digital Advisor Webportal"

Überwachen Sie die Cluster-Leistung mit ONTAP Data Infrastructure Insights

NetApp Data Infrastructure Insights ist ein Überwachungstool, das Ihnen Einblick in Ihre gesamte Infrastruktur bietet. Mit Data Infrastructure Insights können Sie alle Ihre Ressourcen, einschließlich Ihrer öffentlichen Clouds und privaten Rechenzentren, überwachen, Fehler beheben und optimieren.

Alle Ressourcen überwachen, optimieren und Fehler beheben

Mithilfe von Data Infrastructure Insights können Sie die Zeit zur Lösung von Problemen erheblich verkürzen und verhindern, dass diese Auswirkungen auf die Endbenutzer haben. 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.

Data Infrastructure Insights bietet Ihnen an einem Ort Einblick in Ihre gesamte Hybridinfrastruktur – von der öffentlichen Cloud bis zu Ihrem Rechenzentrum. 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.

Data Infrastructure Insights visualisiert Ihre Systemtopologie, um ein Verständnis Ihrer Kubernetes-Architektur zu erlangen. Kunden können den Zustand der Kubernetes Cluster einschließlich problematischer Nodes überwachen und im Problemfall weitere Details einlesen.

Data Infrastructure Insights hilft Ihnen dabei, Unternehmensdaten vor Missbrauch durch böswillige oder kompromittierte Benutzer zu schützen. Dies geschieht durch fortschrittliches maschinelles Lernen und Anomalieerkennung, die Ihnen verwertbare Informationen zu Insider-Bedrohungen liefert.

Data Infrastructure Insights hilft Ihnen, Kubernetes-Metriken zu visualisieren, damit Sie die Beziehungen zwischen Ihren Pods, Knoten und Clustern vollständig verstehen. 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

- "Erste Schritte mit Data Infrastructure Insights"

Audit-Protokollierung

Erfahren Sie mehr über die Implementierung von ONTAP Audit-Protokollierung

Die im Audit-Protokoll aufgezeichneten Verwaltungsaktivitäten sind in den Standardberichten von AutoSupport enthalten, und bestimmte Protokollierungsaktivitäten sind in EMS-Nachrichten enthalten. Sie können das Audit-Protokoll auch an von Ihnen angegebene Ziele weiterleiten und Audit-Protokolldateien über die ONTAP -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.

Beginnend mit ONTAP 9.17.1 und mit ONTAP 9.16.1 P4 und späteren 9.16.1 Patch-Releases, "Remote-Verwaltungsaktivitäten, die von einem Peering-Cluster mithilfe von Cluster-übergreifenden Operationen initiiert werden, können ebenfalls protokolliert werden" . Diese Aktivitäten umfassen benutzergesteuerte und interne Vorgänge, die aus einem anderen Cluster stammen.

In ONTAP protokollierte Verwaltungsaktivitäten

ONTAP protokolliert Verwaltungsaktivitäten, die auf einem Cluster ausgeführt werden, z. B. welche Anfrage gestellt wurde, welcher Benutzer die Anfrage ausgelöst hat, die Zugriffsmethode des Benutzers und den Zeitpunkt der Anfrage.

Es gibt folgende Arten von Managementaktivitäten:

- **SET-Anfragen**:
  - Diese Anforderungen beziehen sich normalerweise auf Befehle oder Vorgänge, die keine Anzeigevorgänge sind.
  - Diese Anforderungen werden ausgegeben, wenn Sie `create` `modify` `delete` beispielsweise einen, , oder -Befehl ausführen.
  - SET-Anfragen werden standardmäßig protokolliert.
- **GET-Anfragen**:
  - Diese Anfragen rufen Informationen ab und zeigen sie in der Verwaltungsschnittstelle an.
  - Diese Anforderungen werden ausgegeben, wenn Sie `show` beispielsweise einen Befehl ausführen.
  - GET-Anfragen werden standardmäßig nicht protokolliert, Sie können jedoch steuern, ob GET-Anfragen, die von der ONTAP CLI gesendet werden, (`-cliget`), aus der ONTAP API (`-ontapiget`) oder über die ONTAP REST API (`-httpget`) werden in der Datei protokolliert.

Aufzeichnung und Rotation von Überwachungsprotokollen

ONTAP Records Management-Aktivitäten in der `/mroot/etc/log/mlog/audit.log` Datei eines Knotens. Befehle der drei Shells für CLI-Befehle (Cluster-Shell, Nodeshell und nicht-interaktive Systemshell) sowie API-Befehle werden hier protokolliert. Interaktive Systemshell-Befehle werden nicht protokolliert. Audit-Protokolle enthalten Zeitstempel, um zu zeigen, ob alle Knoten in einem Cluster synchronisiert sind.

Die `audit.log` 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.

Die `audit.log` 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.

Wenn Sie die GET-Überwachung aktivieren, sollten Sie die Protokollweiterleitung konfigurieren, um Datenverluste durch schnelle Protokollrotation zu vermeiden. Weitere Informationen finden Sie im folgenden Knowledge Base-Artikel: "Aktivieren der Weiterleitung von Überwachungsprotokollen" .

Erfahren Sie mehr über Änderungen an der ONTAP-Audit-Protokollierung

Beginnend mit ONTAP 9 `command-history.log` wird die Datei durch `audit.log`, ersetzt und die `mgwd.log` 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 `command-history.log` bleiben vorhandene Dateien erhalten. Sie werden gedreht (gelöscht), wenn neue `audit.log` Dateien in gedreht (erstellt) werden.

Werkzeuge und Skripte, die die `command-history.log` Datei prüfen, funktionieren möglicherweise weiterhin, da `command-history.log` `audit.log` beim Upgrade ein Softlink von zu erstellt wird. Werkzeuge und Skripte, die die `mgwd.log` Datei prüfen, schlagen jedoch 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.

Anzeigen des Inhalts des ONTAP-Überwachungsprotokolls

Sie können den Inhalt der Cluster- `/mroot/etc/log/mlog/audit.log`Dateien mit der ONTAP CLI, mit System Manager oder mit einem Webbrowser anzeigen.

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.

Status
: Der aktuelle Status der Prüfungsanforderung, der sein könnte `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

Zeigt an `svm`, wenn sich die Anforderung auf einer Datenspeicher-VM befindet; andernfalls wird 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 Überwachungseinträge anzuzeigen, die aus mehreren Knoten im Cluster zusammengeführt wurden, geben Sie Folgendes ein:
`security audit log show <[parameters]>`

Mit dem `security audit log show` Befehl können Sie Überwachungseinträge für einzelne Nodes anzeigen oder aus mehreren Nodes im Cluster zusammengeführt werden. Sie können den Inhalt des `/mroot/etc/log/mlog` Verzeichnisses auch mit einem Webbrowser auf einem einzelnen Knoten anzeigen. Erfahren Sie mehr über `security audit log show` in der "ONTAP-Befehlsreferenz".

Webbrowser

Sie können den Inhalt des `/mroot/etc/log/mlog` Verzeichnisses mit einem Webbrowser auf einem einzelnen Knoten anzeigen. "Hier erfahren Sie, wie Sie mit einem Webbrowser auf die Protokoll-, Core Dump- und MIB-Dateien eines Node zugreifen".

Managen der Einstellungen für ONTAP Audit GET-Anforderungen

Während FESTGELEGTE Anforderungen standardmäßig protokolliert werden, sind GET-Anforderungen nicht. Sie können jedoch steuern, ob GET Requests(`-httpget`, die von ONTAP HTML), der ONTAP-CLI (`-cliget`) oder von den ONTAP-APIs (`-ontapiget`)

gesendet werden, in der Datei protokolliert werden.

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 oben rechts auf , und wählen Sie dann die Anforderungen aus, die Sie hinzufügen oder entfernen möchten.

CLI

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

Erfahren Sie mehr über `security audit show` in der "ONTAP-Befehlsreferenz".

Aktivieren Sie ONTAP Cross-Cluster-Audits

Ab ONTAP 9.17.1 und ab ONTAP 9.16.1 P4 sowie späteren Patch-Versionen 9.16.1 können Sie in ONTAP Cluster-übergreifendes Auditing aktivieren, um von einem Peering-Cluster initiierte Vorgänge zu protokollieren. Dieses Remote-Auditing ist besonders wertvoll in Umgebungen, in denen mehrere ONTAP Cluster interagieren, da es die Nachvollziehbarkeit und Verantwortlichkeit von Remote-Aktionen ermöglicht.

Die clusterübergreifende Überwachung kann zwischen benutzerinitiierten GET- (Lesen) oder SET- (Erstellen/Ändern/Entfernen) Operationen unterscheiden. Standardmäßig werden nur benutzerinitiierte SET-Operationen auf Zielclustern überwacht. Jede Anfrage, die Daten liest, wie z. B. eine GET- oder `show` Befehl in der CLI wird standardmäßig nicht geprüft, unabhängig davon, ob die Anforderung clusterübergreifend ist.

Bevor Sie beginnen

- Sie müssen `advanced` Ebenenberechtigungen
- Der Cluster muss mit einem anderen Cluster verbunden sein und auf beiden Clustern muss ONTAP 9.16.1 P4 oder höher ausgeführt werden.

> In Umgebungen, in denen einige, aber nicht alle Knoten auf ONTAP 9.16.1 P4 oder höher aktualisiert wurden, erfolgt die Audit-Protokollierung nur auf Knoten mit der aktualisierten Version. Es wird empfohlen, alle Knoten auf eine unterstützte Version zu aktualisieren, um ein konsistentes Audit-Verhalten zu gewährleisten.

Aktivieren oder Deaktivieren der clusterübergreifenden Überwachung

Schritte

1. Aktivieren (oder deaktivieren) Sie die Cluster-übergreifende Überwachung auf dem Cluster, indem Sie die `cluster-peer` Parameter auf `on` oder `off` :

```
security audit modify -cluster-peer {on|off}
```

2. Bestätigen Sie, dass die Cluster-Peer-Einstellung aktiviert oder deaktiviert ist, indem Sie den aktuellen Überwachungsstatus prüfen:

```
security audit show
```

Antwort:

```
    Audit Setting State
    ------------- -----
         CLI GET: off
        HTTP GET: off
      ONTAPI GET: off
    Cluster Peer: on
```

Auswirkungen der Aktivierung der GET-Überwachung

Ab ONTAP 9.17.1, wenn Sie "Aktivieren Sie CLI, HTTP, ONTAPI GET-Auditing" In einem Peering-Cluster aktivieren Sie auch die Überwachung clusterübergreifender, benutzerinitiierter GET-Anfragen. In früheren ONTAP Versionen bezog sich die GET-Überwachung nur auf Anfragen in einem lokalen Cluster. Mit ONTAP 9.17.1 aktivieren Sie die GET-Überwachung mit dem `cluster-peer` Option eingestellt auf `on` , sowohl lokale Cluster- als auch clusterübergreifende Anforderungen werden geprüft.

ONTAP-Audit-Protokoll-Ziele verwalten

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

Um die Weiterleitung zu konfigurieren, müssen Sie die IP-Adresse des Syslog- oder Splunk-Hosts, seine Portnummer, ein Übertragungsprotokoll und die Syslog-Funktion angeben, die für die weitergeleiteten Protokolle verwendet werden soll. "Hier erfahren Sie mehr über Syslog-Funktionen".

Mit dem `-protocol` Parameter können Sie 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.

Der Standardport ist 514 für UDP und 6514 für TCP, aber Sie können jeden Port festlegen, der die Anforderungen Ihres Netzwerks erfüllt.

Sie können mit dem `-message-format` Befehl eines der folgenden Nachrichtenformate auswählen:

Legacy-NetApp

Eine Variation des RFC-3164 Syslog-Formats (Format: <PRIVAL> TIMESTAMP HOSTNAME: MSG)

rfc-5424

Syslog-Format gemäß RFC-5424 (Format: <PRIVAL> SION ZEITSTEMPEL HOSTNAME: MSG)

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 hier, ⋮ 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 Sie auf + Add , oder klicken Sie ⋮ in die Spalte **Host-Adresse**, um Einträge zu bearbeiten oder zu 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 6514 -protocol tcp-encrypted -facility user
```

   - Wenn der `cluster log-forwarding create` Befehl keinen Ping-Befehl an den Ziel-Host senden kann, um die Konnektivität zu überprüfen, schlägt der Befehl mit einem Fehler fehl. Obwohl nicht empfohlen, wird `-force` die Konnektivitätsprüfung mit dem Parameter mit dem Befehl umgangen.
   - Wenn Sie den `-verify-server` Parameter auf setzen `true`, wird die Identität des Protokollweiterleitungsziels durch Validierung des Zertifikats überprüft. Sie können den Wert `true` nur einstellen, wenn Sie den `tcp-encrypted` Wert im `-protocol` Feld auswählen.

2. Überprüfen Sie mit dem `cluster log-forwarding show` Befehl, ob die Zieldatensätze korrekt sind.

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

                                                Verify Syslog
Destination Host          Port   Protocol       Server Facility
------------------------- ------ -------------- ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            6514   tcp-encrypted  true   user
2 entries were displayed.
```

Verwandte Informationen

- "Cluster-Log-Forwarding wird angezeigt"
- "Erstellung von Cluster-Protokollweiterleitungsfunktion"

AutoSupport

Erfahren Sie mehr über AutoSupport

Erfahren Sie mehr über ONTAP AutoSupport

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"
- "ONTAP-Befehlsreferenz"

Erfahren Sie mehr über Digital Advisor und ONTAP AutoSupport

Die AutoSupport-Komponente von ONTAP erfasst Telemetrie und sendet diese zur Analyse. Digital Advisor analysiert die Daten von AutoSupport und bietet proaktive Betreuung und Optimierung. Mithilfe von künstlicher Intelligenz kann Digital Advisor potenzielle Probleme identifizieren und lösen, bevor sie sich auf Ihr Unternehmen auswirken.

Mit Digital Advisor optimieren Sie Ihre Dateninfrastruktur in der gesamten globalen Hybrid Cloud. Dazu bieten wir Ihnen konkrete prädiktive Analysen und proaktiven Support über ein Cloud-basiertes Portal und mobile App. Mit einem aktiven SupportEdge-Vertrag stehen allen NetApp Kunden mit Daten-fokussierten Einblicken und Empfehlungen von Digital Advisor zur Verfügung (Funktionen variieren je nach Produkt und Support-Stufe).

Hier einige Dinge, die Sie mit Digital Advisor tun können:

- Planung von Upgrades: Digital Advisor erkennt Probleme in Ihrer Umgebung, die durch ein Upgrade auf eine neuere Version von ONTAP behoben werden können. Die Komponente Upgrade Advisor unterstützt Sie bei der Planung eines erfolgreichen Upgrades.
- Sehen Sie sich das Wellness-System an. Ihr Digital Advisor Dashboard meldet alle Probleme mit dem Wellness-Center und hilft Ihnen bei der Behebung dieser Probleme. Überwachen Sie die Systemkapazität, um sicherzugehen, dass nie mehr Speicherplatz belegt wird. Zeigen Sie Support-Cases für Ihr System an.
- Performance-Management: Digital Advisor zeigt die Systemperformance 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 Digital Advisor zeigt den gesamten Bestand sowie Informationen zur 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: Digitaler Berater"

"Starten Sie Digital Advisor"

"SupportEdge Services"

Hier erfahren Sie, wann und wo ONTAP AutoSupport Meldungen gesendet werden

AutoSupport sendet je nach Nachrichtentyp Meldungen an verschiedene Empfänger. Wenn Sie erfahren, wann und wo AutoSupport Nachrichten sendet, können Sie die Nachrichten verstehen, die Sie per E-Mail erhalten oder auf der Digital Advisor Website aufrufen.

Sofern nicht anders angegeben, sind die Einstellungen in den folgenden Tabellen Parameter des `system node autosupport modify` Befehls.

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	In `-to` und angegebene Adressen `-noteto`. (Es werden nur kritische Ereignisse gesendet, die sich auf den Service auswirken.) In angegebene Adressen `-partner-address` Technischer Support, wenn `-support` auf eingestellt ist `enable`

Geplante Nachrichten

AutoSupport sendet automatisch mehrere Meldungen zu einem regelmäßigen Zeitplan.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
Täglich (standardmäßig zwischen 12:00 und 1:00 Uhr als Protokollnachricht gesendet)	In angegebene Adressen `-partner-address` Technischer Support, wenn `-support` auf eingestellt ist `enable`
Täglich (standardmäßig wird zwischen 12:00 und 1:00 Uhr als Performance-Meldung gesendet), wenn der `-perf` Parameter auf festgelegt ist `true`	Adressen angegeben in -Partner-address`  Technischer Support, wenn `-support` auf eingestellt ist `enable`
Wöchentlich (standardmäßig Sonntag zwischen 12:00 und 1:00 Uhr)	In angegebene Adressen `-partner-address` Technischer Support, wenn `-support` auf eingestellt ist `enable`

Manuell ausgelöste Nachrichten

Sie können eine AutoSupport Meldung manuell initiieren oder erneut senden.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
Sie initiieren eine Meldung manuell mit dem `system node autosupport invoke` Befehl	Wenn ein URI mit dem `-uri` Parameter im `system node autosupport invoke` Befehl angegeben wird, wird die Meldung an diesen URI gesendet. Wenn `-uri` nicht angegeben, wird die Nachricht an die in `-to` und angegebenen Adressen gesendet `-partner-address`. Die Nachricht wird auch an den technischen Support gesendet, wenn `-support` auf eingestellt ist `enable`.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
Sie initiieren eine Meldung manuell mit dem `system node autosupport invoke-core-upload` Befehl	Wenn eine URI mit dem `-uri` Parameter im `system node autosupport invoke-core-upload` Befehl angegeben wird, wird die Meldung an diesen URI gesendet und die Core Dump-Datei in den URI hochgeladen. Wenn `-uri` im `system node autosupport invoke-core-upload` Befehl nicht angegeben wird, wird die Meldung an den technischen Support gesendet und die Core Dump-Datei auf die technische Support-Website hochgeladen. Beide Szenarien erfordern, dass `-support` auf gesetzt ist `enable` und `-transport` auf `https` oder gesetzt ist `http`. Aufgrund der großen Größe von Core Dump-Dateien wird die Meldung nicht an die in den `-to -partner -addresses` Parametern und angegebenen Adressen gesendet.
Sie initiieren eine Meldung manuell mit dem `system node autosupport invoke-performance-archive` Befehl	Wenn ein URI mit dem `-uri` Parameter im `system node autosupport invoke-performance-archive` Befehl angegeben wird, wird die Meldung an diesen URI gesendet und die Performance-Archivdatei in den URI hochgeladen. Wenn `-uri` in der nicht angegeben `system node autosupport invoke-performance-archive` ist, wird die Meldung an den technischen Support gesendet und die Performance-Archivdatei auf die technische Support-Website hochgeladen. Beide Szenarien erfordern, dass `-support` auf gesetzt ist `enable` und `-transport` auf `https` oder gesetzt ist `http`. Aufgrund der großen Größe von Performance-Archivdateien wird die Nachricht nicht an die in den `-to -partner-addresses` Parametern und angegebenen Adressen gesendet.
Sie senden eine vergangene Nachricht manuell mit dem `system node autosupport history retransmit` Befehl erneut	Nur an den URI, den Sie im `-uri` Parameter des `system node autosupport history retransmit` Befehls angeben

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	In angegebene Adressen `-partner-address` Technischer Support, wenn `-support` auf festgelegt ist `enable` und `-transport` auf eingestellt ist `https`
Wenn AutoSupport Lieferanweisungen erhält, um frühere AutoSupport Meldungen erneut zu senden	Technischer Support, wenn `-support` auf festgelegt ist `enable` und `-transport` auf eingestellt ist `https`
Wenn AutoSupport Anweisungen zur Bereitstellung erhält, um neue AutoSupport Meldungen zu generieren, die Core Dump- oder Performance-Archivdateien hochladen	Technischer Support, wenn `-support` auf eingestellt ist `enable` und `-transport` auf eingestellt ist `https`. Die Core Dump- oder Performance-Archivdatei wird auf die technische Support-Website hochgeladen.

Erfahren Sie mehr über ereignisgesteuerte ONTAP AutoSupport Meldungen

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

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 mit dem `system node autosupport trigger modify` Befehl weitere Subsysteme mit einem Trigger verknüpfen.

3. AutoSupport sendet die ereignisausgelöste AutoSupport-Nachricht an die Empfänger `system node autosupport modify -to`, die mit den `-noteto` `-partner-address` `-support` Parametern ,, und definiert werden.

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

Beispiel für Daten, die für ein bestimmtes Ereignis gesendet werden

Das `storage shelf PSU failed` EMS-Ereignis löst eine Meldung aus, die grundlegende Daten aus den Subsystemen obligatorisch, Protokolldateien, Speicher, RAID, HA, Plattform und Netzwerk sowie Fehlerbehebungsdaten aus den Subsystemen obligatorisch, Protokolldateien und Speicher enthält.

Sie entscheiden, dass Sie Daten über NFS in alle AutoSupport-Nachrichten aufnehmen möchten `storage shelf PSU failed`, die als Antwort auf ein zukünftiges Ereignis gesendet werden. Sie geben den folgenden Befehl ein, um Daten zur Fehlerbehebung für NFS für das `callhome.shlf.ps.fault` Ereignis zu aktivieren:

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Beachten Sie, dass das `callhome.` Präfix vom `callhome.shlf.ps.fault` Ereignis entfernt wird `system node autosupport trigger`, wenn Sie die Befehle verwenden oder wenn in der CLI auf AutoSupport- und EMS-Ereignisse verwiesen wird.

Arten von ONTAP AutoSupport-Nachrichten und deren Inhalt

AutoSupport-Meldungen enthalten Statusinformationen zu unterstützten Subsystemen. Wenn Sie erfahren, welche AutoSupport-Nachrichten enthalten, können Sie Nachrichten, die Sie per E-Mail erhalten oder auf der Digital Advisor-Website anzeigen, interpretieren oder darauf antworten.

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
Performance	Performance-Daten, die in den letzten 24 Stunden erfasst wurden
Wöchentlich	Konfigurations- und Statusdaten

Nachrichtentyp	Typ der Daten, die die Nachricht enthält
Wird durch den `system node autosupport invoke` Befehl ausgelöst	Abhängig vom im `-type` Parameter angegebenen Wert: • `test` Sendet eine vom Benutzer ausgelöste Meldung mit einigen Basisdaten. Diese Meldung löst außerdem eine automatische E-Mail-Antwort des technischen Supports an beliebige angegebene E-Mail-Adressen aus `-to`, sodass Sie mit der Option den Empfang von AutoSupport Meldungen bestätigen können. • `performance` Sendet Leistungsdaten. • `all` Sendet eine vom Benutzer ausgelöste Meldung mit einem vollständigen Datensatz ähnlich der wöchentlichen Meldung, einschließlich der Fehlerbehebungsdaten von jedem Subsystem. Technischer Support fordert diese Meldung in der Regel an.
Wird durch den `system node autosupport invoke-core-upload` Befehl ausgelöst	Core Dump-Dateien für einen Node
Wird durch den `system node autosupport invoke-performance-archive` Befehl ausgelöst	Performance-Archivdateien für einen bestimmten Zeitraum
Wird von AutoSupport OnDemand ausgelöst	AutoSupport OnDemand kann neue Nachrichten oder frühere Nachrichten anfordern: • Neue Nachrichten, je nach Typ der AutoSupport-Sammlung, können `test` , `all` oder sein `performance`. • Frühere Nachrichten hängen von der Art der Nachricht ab, die neu gesendet wird. AutoSupport OnDemand kann neue Nachrichten anfordern, die die folgenden Dateien auf die NetApp Support-Website hochladen "mysupport.netapp.com": • Core Dump • Performance-Archivierung

Zeigen Sie ONTAP AutoSupport-Subsysteme an

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.

Schritte

1. Informationen zu Subsystemen und Triggerereignissen anzeigen:

```
system node autosupport trigger show
```

Informieren Sie sich über Größe und Zeitbudgets von ONTAP 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 die Standardzeitbudgets der Subsysteme mit dem `autosupport manifest show` Befehl überprüfen.

Erfahren Sie mehr über Dateien, die in ereignisausgelösten ONTAP AutoSupport Meldungen gesendet werden

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.

Mit dem `system node autosupport trigger show` Befehl mit dem `-instance` Parameter können Sie alle möglichen Ereignisse anzeigen und bestimmen, welche Subsysteme in Meldungen zu den einzelnen Ereignissen enthalten sind.

Zusätzlich zu den Subsystemen, die standardmäßig für jedes Ereignis enthalten sind, können Sie mit dem `system node autosupport trigger modify` Befehl zusätzliche Subsysteme entweder auf Basis- oder auf Fehlerbehebungsebene hinzufügen.

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
• Protokolldateien aus dem `/mroot/etc/log/mlog/` Verzeichnis • DIE MELDUNGSPROTOKOLLDATEI	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. (Log-Dateien von Partnern sind ausgenommen, für Partner sind maximal zulässige Daten enthalten.)
• Protokolldateien aus dem `/mroot/etc/log/shelflog/` Verzeichnis • Protokolldateien aus dem `/mroot/etc/log/acp/` Verzeichnis • Ereignimanagementsystem (EMS) Protokolldaten	Die letzten Datenzeilen bis zu einem festgelegten Maximum.

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

Erfahren Sie, wie ONTAP AutoSupport OnDemand Lieferanweisungen vom 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:

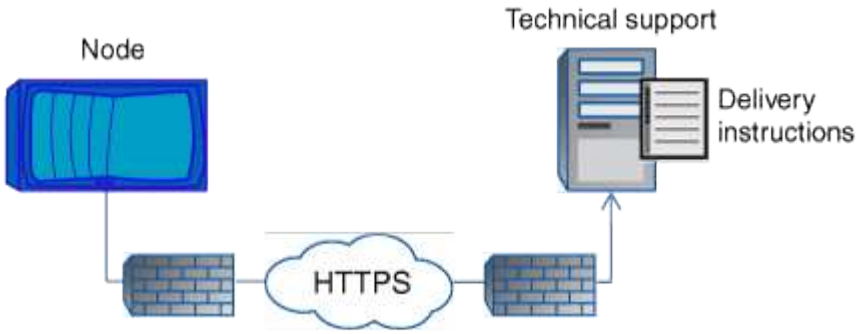
- AutoSupport ist aktiviert.
- AutoSupport wurde konfiguriert, um Meldungen an den technischen Support zu senden.
- AutoSupport ist für die Verwendung des HTTPS-Transportprotokolls konfiguriert.

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 möchten, aber AutoSupport aktiviert lassen möchten, verwenden Sie den Befehl `system node autosupport modify -ondemand-state disable`. Erfahren Sie mehr über `system node autosupport modify -ondemand-state disable` in der "ONTAP-Befehlsreferenz".

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.

Erfahren Sie mehr über die Struktur der per E-Mail gesendeten ONTAP 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 `body.7z` mit dem Namen komprimiert und an die Nachricht angehängt werden.

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

Informieren Sie sich über ONTAP 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.

Beschreibungen von ONTAP AutoSupport-Meldungen abrufen

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

Schritte

1. Gehen 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 ONTAP AutoSupport

Mit den `system node autosupport` Befehlen können Sie die AutoSupport-Konfiguration ändern oder anzeigen, Informationen zu früheren AutoSupport Meldungen

anzeigen und eine AutoSupport Meldung senden, erneut senden oder abbrechen.

Konfigurieren Sie AutoSupport

Ihr Ziel ist	Befehl
Steuern, ob AutoSupport Meldungen gesendet werden	`system node autosupport modify` Mit dem `-state` Parameter
Steuern, ob AutoSupport Meldungen an den technischen Support gesendet werden	`system node autosupport modify` Mit dem `-support` Parameter
Richten Sie AutoSupport ein, oder ändern Sie die Konfiguration von AutoSupport	`system node autosupport modify`
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	`system node autosupport trigger modify`

Zeigt Informationen zur AutoSupport-Konfiguration an

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

Zeigt Informationen zu früheren AutoSupport Meldungen an

Ihr Ziel ist	Befehl
Zeigt Informationen zu mindestens einer der 50 neuesten AutoSupport Meldungen an	`system node autosupport history show`

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

Senden, erneutes Senden oder Abbrechen von AutoSupport Meldungen

Ihr Ziel ist	Befehl
Übertragen Sie eine lokal gespeicherte AutoSupport-Nachricht, die durch die AutoSupport-Sequenznummer gekennzeichnet ist, erneut 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.	`system node autosupport history retransmit`
Generieren und senden Sie eine AutoSupport Message – zum Beispiel zu Testzwecken	`system node autosupport invoke` Mit dem `-force` Parameter können Sie eine Meldung senden, auch wenn AutoSupport deaktiviert ist. Verwenden Sie den `-uri` Parameter, um die Meldung an das angegebene Ziel statt an das konfigurierte Ziel zu senden.
Abbrechen einer AutoSupport Nachricht	`system node autosupport history cancel`

Erfahren Sie mehr über `system node autosupport` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

"ONTAP-Befehlsreferenz"

Erfahren Sie mehr über die im ONTAP AutoSupport Manifest enthaltenen Informationen

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 `system node autosupport manifest show` Befehl anzeigen.

Das AutoSupport-Manifest ist bei jeder AutoSupport-Nachricht enthalten und wird im XML-Format dargestellt. Das bedeutet, dass Sie entweder einen allgemeinen XML-Viewer verwenden oder ihn über das Digital Advisor-Portal anzeigen können.

Planen

Bereiten Sie die Verwendung von ONTAP AutoSupport vor

Sie können ein ONTAP-Cluster konfigurieren, um AutoSupport-Meldungen an NetApp zu übermitteln. In diesem Zusammenhang können Sie auch eine Kopie der Nachrichten an lokale E-Mail-Adressen senden, normalerweise innerhalb Ihres Unternehmens. Sie sollten die Konfiguration von AutoSupport vorbereiten, indem Sie die verfügbaren Optionen überprüfen.

AutoSupport-Nachrichten an NetApp senden

AutoSupport-Meldungen können entweder über HTTPS- oder SMTP-Protokolle an NetApp gesendet werden. Ab ONTAP 9.15.1 können Sie TLS auch mit SMTP verwenden.

Verwenden Sie nach Möglichkeit HTTPS zur Kommunikation mit AutoSupport OnDemand und zum Hochladen großer Dateien.

Beachten Sie auch Folgendes:

- Für die AutoSupport-Meldungen kann nur ein Ausgabekanal an NetApp konfiguriert werden. Sie können nicht zwei Protokolle verwenden, um AutoSupport Meldungen an NetApp zu übermitteln.
- AutoSupport begrenzt die maximale Dateigröße für jedes Protokoll. Wenn die Größe einer AutoSupport Meldung das konfigurierte Limit überschreitet, liefert AutoSupport so viele Meldungen wie möglich, doch wird ein Trunking durchgeführt.
- Sie können die maximale Dateigröße bei Bedarf ändern. Erfahren Sie mehr über `system node autosupport modify` in der "ONTAP-Befehlsreferenz".

- Beide Protokolle können basierend auf der Adressenfamilie, in die der Name aufgelöst wird, über IPv4 oder IPv6 übertragen werden.
- Die TCP-Verbindung, die von ONTAP zum Senden von AutoSupport-Nachrichten eingerichtet wurde, ist vorübergehend und nur von kurzer Dauer.

HTTPS

Dies bietet die robustesten Funktionen. Beachten Sie Folgendes:

- AutoSupport OnDemand und die Übertragung großer Dateien werden unterstützt.
- Es wird zuerst versucht, eine HTTPS-PUT-Anforderung zu stellen. Wenn die Anforderung während der Übertragung fehlschlägt, wird die Anforderung an der Stelle neu gestartet, an der sie angehalten wurde.
- Wenn der Server PUT nicht unterstützt, wird stattdessen die HTTPS-POST-Methode verwendet.
- Die Standardeinstellung für HTTPS-Übertragungen ist 50 MB.
- Das HTTPS-Protokoll verwendet Port 443.

SMTP

Als allgemeine Regel sollten Sie SMTP nur verwenden, wenn HTTPS nicht zulässig ist oder nicht unterstützt wird. Beachten Sie Folgendes:

- AutoSupport OnDemand und Übertragungen großer Dateien werden nicht unterstützt.
- Wenn SMTP-Anmeldeinformationen konfiguriert sind, werden sie unverschlüsselt und im Klaren gesendet.
- Die Standardgrenze für Übertragungen beträgt 5 MB.
- Das ungesicherte SMTP-Protokoll verwendet Port 25.

Verbessern Sie die SMTP-Sicherheit mit TLS

Bei Verwendung von SMTP ist der gesamte Datenverkehr unverschlüsselt und kann leicht abgefangen und gelesen werden. Ab ONTAP 9.15.1 können Sie TLS auch mit SMTP (SMTPS) verwenden. In diesem Fall wird *Explicit TLS* verwendet, der den sicheren Kanal aktiviert, nachdem die TCP-Verbindung hergestellt wurde.

Der folgende Port wird normalerweise für SMTPS verwendet: Port 587

Weitere Überlegungen zur Konfiguration

Bei der Konfiguration von AutoSupport müssen zusätzlich einige Überlegungen angestellt werden.

Weitere Informationen zu den Befehlen, die für diese Überlegungen relevant sind, finden Sie unter "AutoSupport einrichten".

Senden Sie eine lokale Kopie per E-Mail

Unabhängig vom Protokoll, das zum Senden von AutoSupport-Nachrichten an NetApp verwendet wird, können Sie auch eine Kopie jeder Nachricht an eine oder mehrere lokale E-Mail-Adressen senden. Beispielsweise können Sie Meldungen an Ihre interne Support-Organisation oder an eine Partnerorganisation senden.

> Wenn Sie Nachrichten über SMTP (oder SMTPS) an NetApp senden und gleichzeitig lokale E-Mail-Kopien dieser Nachrichten senden, wird dieselbe E-Mail-Server-Konfiguration verwendet.

HTTP-Proxy

Je nach Netzwerkkonfiguration erfordert das HTTPS-Protokoll möglicherweise eine zusätzliche Konfiguration einer Proxy-URL. Wenn HTTPS zum Senden von AutoSupport-Nachrichten an den technischen Support verwendet wird und Sie über einen Proxy verfügen, müssen Sie die URL für den Proxy angeben. Wenn der Proxy einen anderen Port als den Standardport (Port 3128) verwendet, können Sie den Port für diesen Proxy angeben. Optional können Sie auch einen Benutzernamen und ein Passwort für die Proxy-Authentifizierung angeben.

Installieren Sie das Serverzertifikat

Mit TLS (HTTPS oder SMTPS) wird das vom Server heruntergeladene Zertifikat anhand des Stammzertifizierungszertifikats von ONTAP validiert. Bevor Sie HTTPS oder SMTPS verwenden, müssen Sie sicherstellen, dass das Stammzertifikat in ONTAP installiert ist und dass ONTAP das Serverzertifikat validieren kann. Diese Validierung erfolgt auf der Grundlage der Zertifizierungsstelle, die das Serverzertifikat signiert hat.

ONTAP enthält eine große Anzahl vorinstallierter Stammzertifizierungsstellen-Zertifikate. In vielen Fällen wird das Zertifikat für Ihren Server ohne zusätzliche Konfiguration sofort von ONTAP erkannt. Je nachdem, wie das Serverzertifikat signiert wurde, müssen Sie möglicherweise ein Stammzertifizierungsstellenzertifikat und alle Zwischenzertifikate installieren.

Gehen Sie wie folgt vor, um das Zertifikat bei Bedarf zu installieren. Installieren Sie alle erforderlichen Zertifikate auf Cluster-Ebene.

Beispiel 1. Schritte

System Manager

1. Wählen Sie im System Manager **Cluster** > **Einstellungen** aus.
2. Scrollen Sie nach unten zum Abschnitt **Sicherheit**.
3. Wählen Sie → neben **Certificates** aus.
4. Klicken Sie auf der Registerkarte **Vertrauenswürdige Zertifizierungsstellen** auf **Hinzufügen**.
5. Klicken Sie auf **Import** und wählen Sie die Zertifikatdatei aus.
6. Vervollständigen Sie die Konfigurationsparameter für Ihre Umgebung.
7. Klicken Sie Auf **Hinzufügen**.

CLI

1. Starten Sie die Installation:

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

   Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".

2. Suchen Sie nach der folgenden Konsolenmeldung:

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Öffnen Sie die Zertifikatdatei mit einem Texteditor.
4. Kopieren Sie das gesamte Zertifikat einschließlich der folgenden Zeilen:

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. Fügen Sie das Zertifikat nach der Eingabeaufforderung in das Terminal ein.
6. Drücken Sie **Enter**, um die Installation abzuschließen.
7. Überprüfen Sie, ob das Zertifikat installiert ist, indem Sie einen der folgenden Befehle ausführen:

   ```
   security certificate show-user-installed
   ```

   ```
   security certificate show
   ```

   Erfahren Sie mehr über `security certificate show` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "AutoSupport einrichten"
- "ONTAP-Befehlsreferenz"

Richten Sie ONTAP AutoSupport ein

Sie können einen ONTAP Cluster so konfigurieren, dass AutoSupport-Nachrichten an den technischen Support von NetApp gesendet werden, und E-Mail-Kopien an den internen Support senden. Im Rahmen dieser Funktion können Sie die Konfiguration auch testen, bevor Sie sie in einer Produktionsumgebung verwenden.

Über diese Aufgabe

Ab ONTAP 9.5 können Sie AutoSupport für alle Nodes eines Clusters gleichzeitig aktivieren und konfigurieren. Wenn ein neuer Node dem Cluster Beitritt, übernimmt der Node automatisch die gleiche AutoSupport-Konfiguration. Zur Unterstützung dieses Befehls `system node autosupport modify` dient der CLI-Befehl als Cluster-Ebene. Die `-node` Befehlsoption wird aus Gründen der Abwärtskompatibilität beibehalten, wird jedoch ignoriert.

> In ONTAP 9.4 und früheren Versionen `system node autosupport modify` ist der Befehl für jeden Knoten spezifisch. Wenn auf dem Cluster ONTAP 9.4 oder eine frühere Version ausgeführt wird, müssen Sie auf jedem Node im Cluster AutoSupport aktivieren und konfigurieren.

Bevor Sie beginnen

Die empfohlene Transportkonfiguration für die Übertragung von AutoSupport Meldungen an NetApp ist HTTPS (HTTP mit TLS). Diese Option bietet die robustesten Funktionen und die beste Sicherheit.

Überprüfen "Bereiten Sie die Verwendung von AutoSupport vor" Sie vor der Konfiguration des ONTAP-Clusters, ob weitere Informationen vorhanden sind.

Schritte

1. Vergewissern Sie sich, dass AutoSupport aktiviert ist:

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

2. Wenn der technische Support von NetApp AutoSupport Meldungen erhalten soll, 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.

   > AutoSupport OnDemand ist standardmäßig aktiviert und funktioniert, wenn es so konfiguriert ist, dass über das HTTPS-Transportprotokoll Meldungen an den technischen Support gesendet werden.

3. Wenn Sie den technischen Support von NetApp zum Empfang von AutoSupport Meldungen aktiviert haben, geben Sie das für diese Meldungen zu verwendende Transportprotokoll an.

   Sie können aus folgenden Optionen wählen:

Ihr Ziel ist	Legen Sie dann die folgenden Parameter des `system node autosupport modify` Befehls fest…
Verwenden Sie das HTTPS-Standardprotokoll	a. Setzen Sie `-transport` auf `https`. b. Wenn Sie einen Proxy verwenden, legen Sie `-proxy-url` die URL Ihres Proxys fest. Diese Konfiguration unterstützt die Kommunikation mit AutoSupport OnDemand und das Hochladen großer Dateien.
Verwenden Sie SMTP	Setzen Sie `-transport` auf `smtp`. Diese Konfiguration unterstützt weder AutoSupport OnDemand noch Uploads großer Dateien.

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 `system node autosupport modify` Befehls festlegen:

Diesen Parameter festlegen…	Künftige Situation
`-to`	Bis zu fünf kommagetrennte einzelne E-Mail-Adressen oder Verteilerlisten in Ihrer internen Support-Organisation, die wichtige AutoSupport-Nachrichten empfangen
`-noteto`	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
`-partner-address`	Bis zu fünf kommagetrennte einzelne E-Mail-Adressen oder Verteilerlisten in Ihrer Support-Partnerorganisation, die alle AutoSupport Meldungen erhalten

   b. Überprüfen Sie, ob Adressen richtig konfiguriert `system node autosupport destinations show` sind, indem Sie die Ziele mit dem Befehl auflisten.
5. Wenn Sie im vorherigen Schritt die Empfängeradressen für Ihre interne Supportorganisation konfiguriert haben oder SMTP-Übertragung für Meldungen an den technischen Support gewählt haben, konfigurieren

Sie SMTP, indem Sie die folgenden Parameter des Befehls festlegen `system node autosupport modify`:

- Legen Sie `-mail-hosts` einen oder mehrere E-Mail-Hosts fest, die durch Kommas getrennt sind.

  Sie können maximal fünf festlegen.

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

- Legen Sie `-from` die E-Mail-Adresse fest, an die die AutoSupport-Nachricht gesendet wird.

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

Wenn Sie das wollen…	Legen Sie dann die folgenden Parameter des `system node autosupport modify` Befehls fest…
Verbergen Sie private Daten, indem Sie sensible Daten in den Nachrichten entfernen, maskieren oder kodieren	Setzen Sie `-remove-private-data` auf `true`. Wenn Sie von `false` in wechseln `true`, werden alle AutoSupport-Historie und alle zugehörigen Dateien gelöscht.
Beenden Sie das Senden von Performance-Daten in regelmäßigen AutoSupport Meldungen	Setzen Sie `-perf` auf `false`.

8. Wenn Sie SMTP verwenden, um AutoSupport-Nachrichten an NetApp zu senden, können Sie TLS optional aktivieren, um die Sicherheit zu verbessern.
   a. Zeigt die für den neuen Parameter verfügbaren Werte an:

   ```
   cluster1::> system node autosupport modify -smtp-encryption ?
   ```

   b. TLS für SMTP-Nachrichtenversand aktivieren:

   ```
   cluster1::> system node autosupport modify -smtp-encryption start_tls
   ```

   c. Aktuelle Konfiguration anzeigen:

   ```
   cluster1::> system node autosupport show -fields smtp-encryption
   ```

9. Überprüfen Sie die Gesamtkonfiguration mit dem `system node autosupport show` Befehl mit dem `-node` Parameter.
10. Überprüfen Sie die AutoSupport-Operation mit dem `system node autosupport check show` Befehl.

Wenn Probleme gemeldet werden, verwenden Sie den `system node autosupport check show-details` Befehl, um weitere Informationen anzuzeigen.

11. Testen, ob AutoSupport Meldungen gesendet und empfangen werden:
    a. Verwenden Sie den `system node autosupport invoke` Befehl mit dem `-type` Parameter auf `test`:

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

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

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

    Der Status der letzten ausgehenden AutoSupport-Nachricht sollte sich schließlich `sent-successful` für alle geeigneten Protokollziele in ändern.

    c. Bestätigen Sie optional, dass AutoSupport-Nachrichten an Ihre interne Support-Organisation oder an Ihren Support-Partner gesendet werden, indem Sie die E-Mail-Adresse einer Adresse überprüfen, die Sie für die `-to`, `-noteto` oder- `-partner-address`Parameter des `system node autosupport modify` Befehls konfiguriert haben.

Verwandte Informationen

- "Bereiten Sie die Verwendung von AutoSupport vor"
- "ONTAP-Befehlsreferenz"

Konfigurieren

Managen der ONTAP AutoSupport-Einstellungen

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

Weitere Informationen zu AutoSupport-Konfigurationsoptionen, einschließlich Einstellungen, die in System Manager nicht verfügbar sind, finden Sie unter `system-node-autosupport-modify` in "ONTAP-Befehlsreferenz" .

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 ⋮, und wählen Sie dann **Weitere Optionen** aus.

   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 ⋮, und wählen Sie dann **Generieren und Senden** aus.
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 ⋮, und 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 sich bewusst sein, dass Sie das NetApp Call Home-System ausschalten und dabei die folgenden Vorteile verlieren:

- **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, beispielsweise einige Workflows in der NetApp Konsole.

Schritte

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

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 ⋮, und wählen Sie dann **Support-Case-Erstellung 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 ⋮, und 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 ⋮, und wählen Sie dann **Weitere Optionen** aus.
3. Wählen Sie im Abschnitt **Verbindungen** oder im Abschnitt **E-Mail** aus, Edit um die Einstellungen für einen der beiden Bereiche zu ändern.

Verwandte Informationen

- "Bereiten Sie die Verwendung von AutoSupport vor"
- "AutoSupport einrichten"

Unterdrücken Sie die Erstellung von ONTAP AutoSupport-Fällen während geplanter Wartungsfenster

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

Schritte

1. Rufen Sie manuell eine AutoSupport-Meldung mit der Textzeichenfolge auf `MAINT=xh`, wobei `x` die Dauer des Wartungsfensters in Stunden ist. Ersetzen Sie <node> durch den Namen des Node, von dem die AutoSupport Meldung gesendet werden soll:

```
system node autosupport invoke -node <node> -message MAINT=xh
```

Verwandte Informationen

- "ONTAP-Befehlsreferenz"
- "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"

Laden Sie Dateien mit AutoSupport hoch

Laden Sie ONTAP AutoSupport 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.

Bevor Sie beginnen

- Sie haben AutoSupport mit den folgenden Einstellungen eingerichtet:
  - AutoSupport ist auf dem Node aktiviert.
  - AutoSupport wurde konfiguriert, um Meldungen an den technischen Support zu senden.
  - AutoSupport ist für das HTTPS-Transportprotokoll 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 auch die Core Dump-Datei über den AutoSupport-Service mit dem `system node autosupport invoke-core-upload` Befehl über HTTPS hochladen, sofern die NetApp Unterstützung dies wünscht.

"Hochladen einer ONTAP 9-Kerndatei zur Analyse"

Schritte

1. Zeigen Sie mit dem `system node coredump show` Befehl die Core Dump-Dateien für einen Node an.

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 Nachricht und laden Sie eine Core Dump-Datei mit dem `system node autosupport invoke-core-upload` Befehl hoch.

   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
   ```

Laden Sie Archivdateien zur ONTAP AutoSupport Performance hoch

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.

Bevor Sie beginnen

- 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 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 Nachricht und laden Sie die Performance-Archivdatei mit dem `system node autosupport invoke-performance-archive` Befehl hoch.

   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
   ```

Fehlerbehebung

Fehlerbehebung bei ONTAP 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 mit dem `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 `system node autosupport history show -detail`, indem Sie den Befehl eingeben.

Diesem Status	Bedeutet
Inkassovorgang läuft	AutoSupport sammelt AutoSupport-Inhalte. Sie können anzeigen, was AutoSupport sammelt, indem Sie den `system node autosupport manifest show` Befehl eingeben.
Warteschlange	AutoSupport Nachrichten werden für die Lieferung in die Warteschlange eingereiht, aber noch nicht geliefert.
Übertragung	AutoSupport stellt derzeit Meldungen aus.
Gesendet-erfolgreich	AutoSupport hat die Meldung erfolgreich übermittelt. Sie können herausfinden, wo AutoSupport die Nachricht zugestellt hat `system node autosupport history show -delivery`, indem Sie den Befehl eingeben.
Ignorieren	AutoSupport verfügt über keine Ziele für die Meldung. Sie können die Lieferdetails durch Eingabe des `system node autosupport history show -delivery` Befehls anzeigen.
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 den `system node autosupport history show` Befehl eingeben.
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 den `system node autosupport history show` Befehl eingeben.
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 ONTAP AutoSupport Nachrichtenübermittlung über HTTPS

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

Bevor Sie beginnen

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 HTTPS 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.

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
   ```

   Die `status-oper` `status-admin` Felder und sollten zurückgegeben werden `up`. Erfahren Sie mehr über `up` in der "ONTAP-Befehlsreferenz".

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 per-Hop Informationen 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 dieselbe Route von einem funktionierenden Host im selben Subnetz wie das Cluster. Verwenden Sie dabei das Dienstprogramm oder `tracert`, das auf den meisten Netzwerk-Clients von `traceroute` Drittanbietern vorhanden ist. Sie können dann feststellen, ob das Problem in der Netzwerkkonfiguration oder in der Clusterkonfiguration liegt. Erfahren Sie mehr über `network traceroute` in der "ONTAP-Befehlsreferenz".

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. Zugriff `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-Verkehr zuzulassen, und dass der Proxyserver richtig konfiguriert ist. Weitere Informationen zum Konfigurieren der statischen Namensauflösung für support.netapp.com finden Sie im"NetApp Knowledge Base: Wie wird in ONTAP ein HOST-Eintrag für support.netapp.com hinzugefügt?"

8. Wenn Sie ab ONTAP 9.10.1 die automatischen Aktualisierungen aktivieren, stellen Sie sicher, dass Sie über eine HTTPS-Verbindung zu den folgenden zusätzlichen URLs verfügen:
   - https://support-sg-naeast.NetApp.com
   - https://support-sg-nawest.NetApp.com

Fehlerbehebung bei der ONTAP 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.

Bevor Sie beginnen

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`

   Die `status-oper` `status-admin` Felder und sollten zurückgegeben werden `up`. Erfahren Sie mehr über `up` in der "ONTAP-Befehlsreferenz".

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. `support.netapp.com`Stellen Sie für jeden Server, der durch den vorherigen Schritt angezeigt wird, und sicher, dass der Server oder die URL vom 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 Listener-SMTP-Portnummer.

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 Domänenname 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 angezeigte Fehler lautet `Login denied`, akzeptiert der SMTP-Server keine Sendeanforderungen 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.

Fehlerbehebung für das ONTAP AutoSupport-Subsystem

Mit den `system node check show` Befehlen können Sie sämtliche Probleme in Verbindung mit der AutoSupport-Konfiguration und -Bereitstellung überprüfen und beheben.

Schritt

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

Befehl	Hier…
`system node autosupport check show`	Zeigt den Gesamtstatus des AutoSupport-Subsystems an, z. B. den Status des AutoSupport HTTPS-Ziels, der AutoSupport SMTP-Ziele, des AutoSupport OnDemand-Servers und der AutoSupport-Konfiguration
`system node autosupport check show-details`	Anzeige des detaillierten Status des AutoSupport-Subsystems, z. B. detaillierte Beschreibungen der Fehler und der Korrekturmaßnahmen

Monitoring des Systemzustands

Erfahren Sie mehr über die Überwachung des Systemzustands mit ONTAP

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"

Erfahren Sie mehr über die Monitoring-Komponenten von ONTAP

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.

Erfahren Sie mehr über die Reaktion von ONTAP 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-unterdrückung`“ angezeigt, wenn die unterdrückte Meldung auftritt.

Erfahren Sie mehr über die Anpassung von ONTAP Systemzustandswarnmeldungen

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 den `system health alert show -instance` Befehl, um die Richtlinien-ID für die Meldung zu erhalten. Sie verwenden die Richtlinien-ID im `system health policy definition show` Befehl, um Informationen zur Richtlinie anzuzeigen. Nachdem Sie den Regelausdruck und andere Informationen über die Richtlinie geprüft haben, entscheiden Sie, die Richtlinie zu deaktivieren. Sie verwenden den `system health policy definition modify` Befehl, um die Richtlinie zu deaktivieren.

Verwandte Informationen

- "Systemzustandswarnung anzeigen"

Weitere Informationen zu ONTAP AutoSupport-Systemzustandswarnauslösern

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 konfigurieren, damit keine AutoSupport Meldungen mit dem `system health policy definition modify` Befehl ausgelöst werden.

Mit dem `system health autosupport trigger history show` Befehl können Sie eine Liste aller warnungsausgelösten AutoSupport-Meldungen anzeigen, die in der vergangenen Woche gesendet wurden.

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.

Erfahren Sie mehr über verfügbare Systemzustandsüberwacher für ONTAP Cluster

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
Ethernet-Switch	Switch (Switch-Health)	Der ONTAP-Netzwerkswitch-Funktionsmonitor (CSHM) überwacht den Status von Cluster- und Speichernetzwerk-Switches, während er Protokolle zur Analyse erfasst. Standardmäßig fragt CSHM jeden Switch alle 5 Minuten über SNMPv2c ab, um Ressourcentabellen mit Informationen zu Supportfähigkeit, Überwachungsstatus, Temperatursensoren, CPU-Auslastung, Schnittstellenkonfigurationen und -Verbindungen, Cluster-Switch-Redundanz sowie Lüfter- und Netzteilvorgängen zu aktualisieren. Darüber hinaus erfasst CSHM bei entsprechender Konfiguration stündlich Protokolle über SSH/SCP, die zur weiteren Analyse über AutoSupport gesendet werden. Auf Anfrage kann CSHM auch eine ausführlichere Tech-Support-Protokollsammlung mithilfe von SSH/SCP durchführen. Weitere Informationen finden Sie unter "Überwachung des Switch-Systemzustands" .
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

Name der Systemzustandsüberwachung (Kennung)	Subsystemname (Kennung)	Zweck
Node-Konnektivität (Node-Connect)	Unterbrechungsfreier CIFS-Betrieb (CIFS-NDO)	Überwachung von SMB-Verbindungen für unterbrechungsfreien Betrieb von Hyper-V Applikationen
Storage (SAS-Connect)	Überwacht Shelfs, Festplatten und Adapter auf Node-Ebene für entsprechende Pfade und Verbindungen.	System
Keine Angabe	Fasst Informationen aus anderen Zustandsmonitoren zusammen.	Systemkonnektivität (System-connect)

Automatischer Empfang von ONTAP Systemzustandsmeldungen

Sie können Systemzustandsmeldungen mit dem `system health alert show` Befehl manuell anzeigen. 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.alered Nachrichten und alle hm.alert.cleaned Nachrichten enthalten einen SNMP-Trap. Die Namen der SNMP-Traps lauten `HealthMonitorAlertRaised` und `HealthMonitorAlertCleared`.

Erfahren Sie mehr über `system health alert show` in der "ONTAP-Befehlsreferenz".

Schritte

1. `event destination create`Definieren Sie mit dem Befehl das Ziel, an das die EMS-Meldungen gesendet werden sollen.

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

   Erfahren Sie mehr über `event destination create` in der "ONTAP-Befehlsreferenz".

2. Verwenden Sie den `event route add-destinations` Befehl, um die `hm.alert.raised` `hm.alert.cleared` Meldung und die Meldung an ein Ziel weiterzuleiten.

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

Erfahren Sie mehr über `event route add-destinations` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Visualisierung des ONTAP Netzwerks mit System Manager"
- "So konfigurieren Sie die SNMP-Überwachung auf DATA ONTAP"

Reaktion auf beeinträchtigten Zustand des ONTAP-Systems

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 Anzeigen einer AutoSupport Nachricht, eines EMS-Ereignisses oder mithilfe der `system health` Befehle generiert wurde.

Schritte

1. Mit dem `system health alert show` Befehl können Sie die Warnungen anzeigen, 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, können Sie mit dem `system health alert show -instance` Befehl weitere Informationen anzeigen, die für die Meldung verfügbar sind.
4. Verwenden Sie den `system health alert modify` Befehl mit dem `-acknowledge` Parameter, um anzugeben, dass Sie an einer bestimmten Meldung arbeiten.
5. Führen Sie Korrekturmaßnahmen durch, um das Problem gemäß dem `Corrective Actions` Feld in der Meldung zu lösen.

   Die Korrekturmaßnahmen können ein Neubooten des Systems umfassen.

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

6. `system health status show`Überprüfen Sie mit dem Befehl, ob der Systemzustandsstatus lautet `OK`.

   Wenn der Systemstatus nicht lautet `OK`, wiederholen Sie diesen Vorgang.

Verwandte Informationen

- "Systemzustandswarnung ändern"

Erfahren Sie mehr über die Reaktion auf den beeinträchtigten Zustand des ONTAP-Systems

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. Dann überprüfen Sie die Systemintegrität erneut und sehen, dass der Status lautet `OK`:

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

Verwandte Informationen

- "Systemzustandswarnung ändern"

Befehle zum Monitoring des Systemzustands Ihres ONTAP Systems

Sie können die `system health` Befehle verwenden, um Informationen zum Zustand der Systemressourcen anzuzeigen, auf Warnmeldungen zu antworten und zukünftige Warnmeldungen zu konfigurieren. Mithilfe der CLI-Befehle können Sie detaillierte Informationen über das Konfigurieren des Systemzustands anzeigen. Erfahren Sie mehr über `system health` in der "ONTAP-Befehlsreferenz".

Zeigt den Status des Systemzustands an

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

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	`storage shelf show -connectivity` Verwenden Sie den `-instance` Parameter, um detaillierte Informationen zu jedem Shelf anzuzeigen.
Anzeigen von Informationen zu Laufwerken und Array-LUNs, einschließlich des nutzbaren Speicherplatzes, Shelf- und Einschubnummern sowie des eigenen Node-Namens	`storage disk show` Verwenden Sie den `-instance` Parameter, um detaillierte Informationen zu jedem Laufwerk anzuzeigen.
Zeigt detaillierte Informationen über Storage-Shelf-Ports an, einschließlich Porttyp, Geschwindigkeit und Status	`storage port show` Verwenden Sie den `-instance` Parameter, um detaillierte Informationen zu den einzelnen Adaptern anzuzeigen.

Monitoring von Cluster- und Storage-Netzwerk-Switches

Ihr Ziel ist	Befehl (ONTAP 9.8 und höher)	Befehl (ONTAP 9.7 und früher)
Zeigen Sie die Switches an, die das Cluster überwacht	`system switch ethernet show`	`system cluster-switch show`
Zeigt die Switches an, die das Cluster derzeit überwacht, einschließlich der von Ihnen gelöschten Switches (in der Spalte „Reason“ der Befehlsausgabe angezeigt) Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar	`system switch ethernet show-all`	`system cluster-switch show-all`
Konfigurieren Sie die Überwachung eines nicht erkannten Switches	`system switch ethernet create`	`system cluster-switch create`
Ändern von Informationen über einen vom Cluster überwachen Switch (z. B. Gerätename, IP-Adresse, SNMP-Version und Community String)	`system switch ethernet modify`	`system cluster-switch modify`
Deaktivieren Sie die Überwachung eines Switches	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
Löschen Sie einen Schalter aus der Überwachung	`system switch ethernet delete`	`system cluster-switch delete`
Entfernen Sie die in der Datenbank gespeicherten Switch-Konfigurationsinformationen dauerhaft (wodurch die automatische Erkennung des Switch wieder möglich ist).	`system switch ethernet delete -force`	`system cluster-switch delete -force`
Führen Sie die Protokollerfassung mit einem Switch durch	`system switch ethernet log`	`system cluster-switch log`

Weitere Informationen finden Sie unter "Überwachung des Switch-Systemzustands" und"Konfigurieren der Protokollerfassung".

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	`system health alert show`
Zeigt Informationen zu jeder generierten Meldung an	`system health alert show -instance`
Geben Sie an, dass jemand an einer Warnung arbeitet	`system health alert modify`
Bestätigen Sie eine Meldung	`system health alert modify -acknowledge`
Unterdrücken Sie eine nachfolgende Meldung, damit sie den Integritätsstatus eines Subsystems nicht beeinflusst	`system health alert modify -suppress`
Löschen Sie eine Meldung, die nicht automatisch gelöscht wurde	`system health alert delete`
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	`system health autosupport trigger history show`

Konfigurieren Sie zukünftige Warnmeldungen

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

Zeigt Informationen zur Konfiguration der Systemzustandsüberwachung an

Ihr Ziel ist	Befehl
Anzeigen von Informationen über Systemzustandsüberwachung, z. B. ihre Nodes, Namen, Subsysteme und Status	`system health config show` Verwenden Sie den `-instance` Parameter, um detaillierte Informationen zu jeder Systemzustandsüberwachung anzuzeigen.

Ihr Ziel ist	Befehl
Zeigen Sie Informationen zu den Meldungen an, die eine Systemzustandsüberwachung möglicherweise generiert werden kann	`system health alert definition show` Verwenden Sie den `-instance` Parameter, um detaillierte Informationen zu den einzelnen Meldungsdefinitionen anzuzeigen.
Anzeigen von Informationen über Richtlinien der Systemzustandsüberwachung, die bestimmen, wann Meldungen ausgegeben werden	`system health policy definition show` Mit dem `-instance` Parameter können Sie detaillierte Informationen zu den einzelnen Richtlinien anzeigen. Verwenden Sie andere Parameter, um die Meldungsliste zu filtern, z. B. nach Richtlinienstatus (aktiviert oder nicht), Systemzustandsüberwachung, Meldung usw.

Verwandte Informationen

- "Speicherport anzeigen"
- "Lagerregal anzeigen"
- "Systemzustandswarnung löschen"

Zeigen Sie Umgebungsinformationen zu ONTAP an

Sensoren helfen Ihnen dabei, die Umgebungskomponenten Ihres Systems zu überwachen. Zu den Informationen, die Sie über Umgebungssensoren anzeigen können, gehören Typ, Name, Status, Wert und Schwellenwertwarnungen.

Schritt

1. Um Informationen zu Umgebungssensoren anzuzeigen, verwenden Sie den `system node environment sensors show` Befehl.

Filesystem-Analyse

Weitere Informationen zur ONTAP Dateisystemanalyse

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. Durch diese native Funktion werden keine externen Tools benötigt und Sie erhalten wichtige Einblicke in die Verwendung Ihres Storage und Möglichkeiten zur Storage-Optimierung entsprechend Ihren Geschäftsanforderungen.

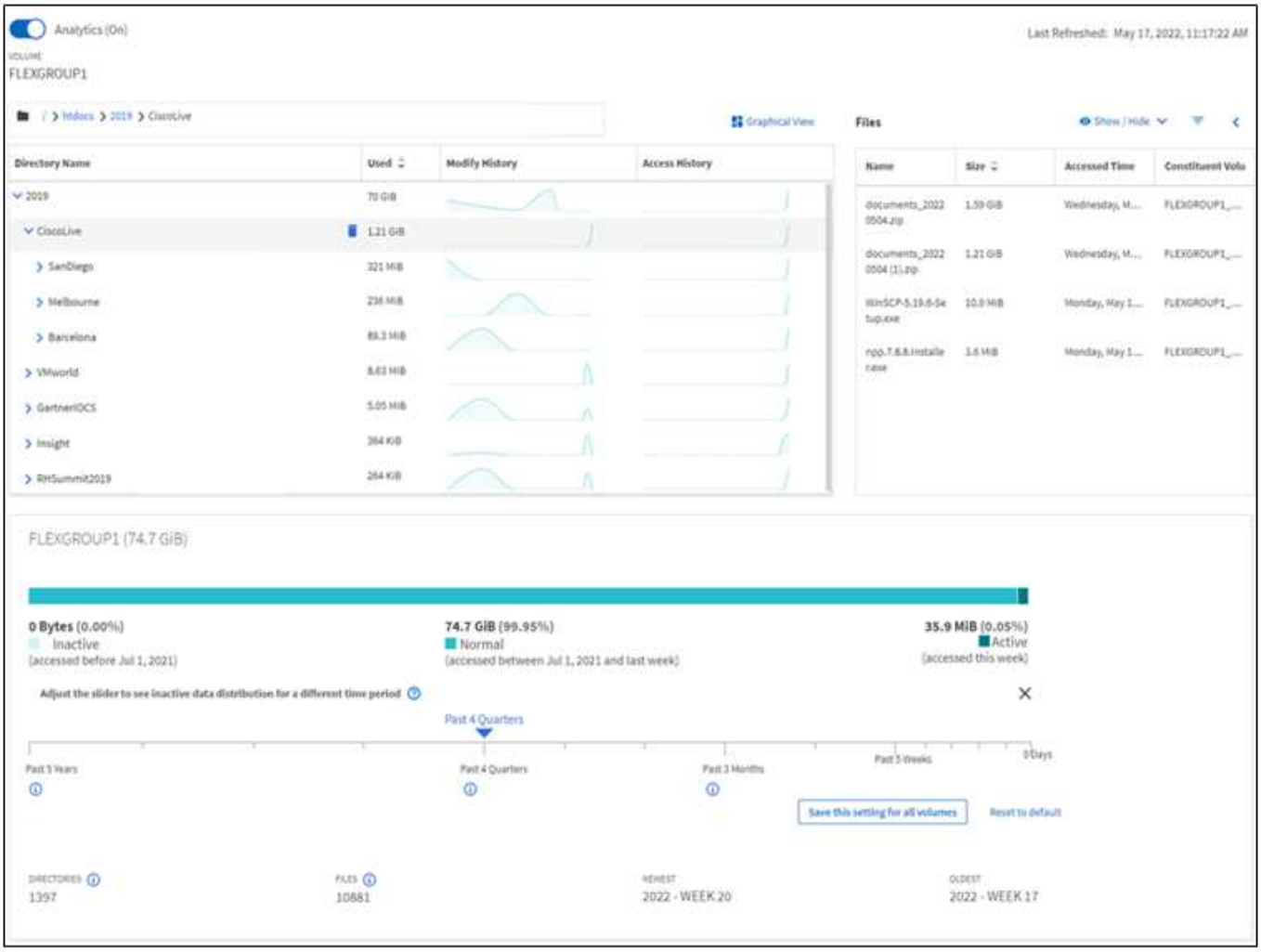
Mit FSA haben Sie Einblick auf allen Ebenen der Dateisystemhierarchie eines Volumes in NAS. Sie erhalten

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

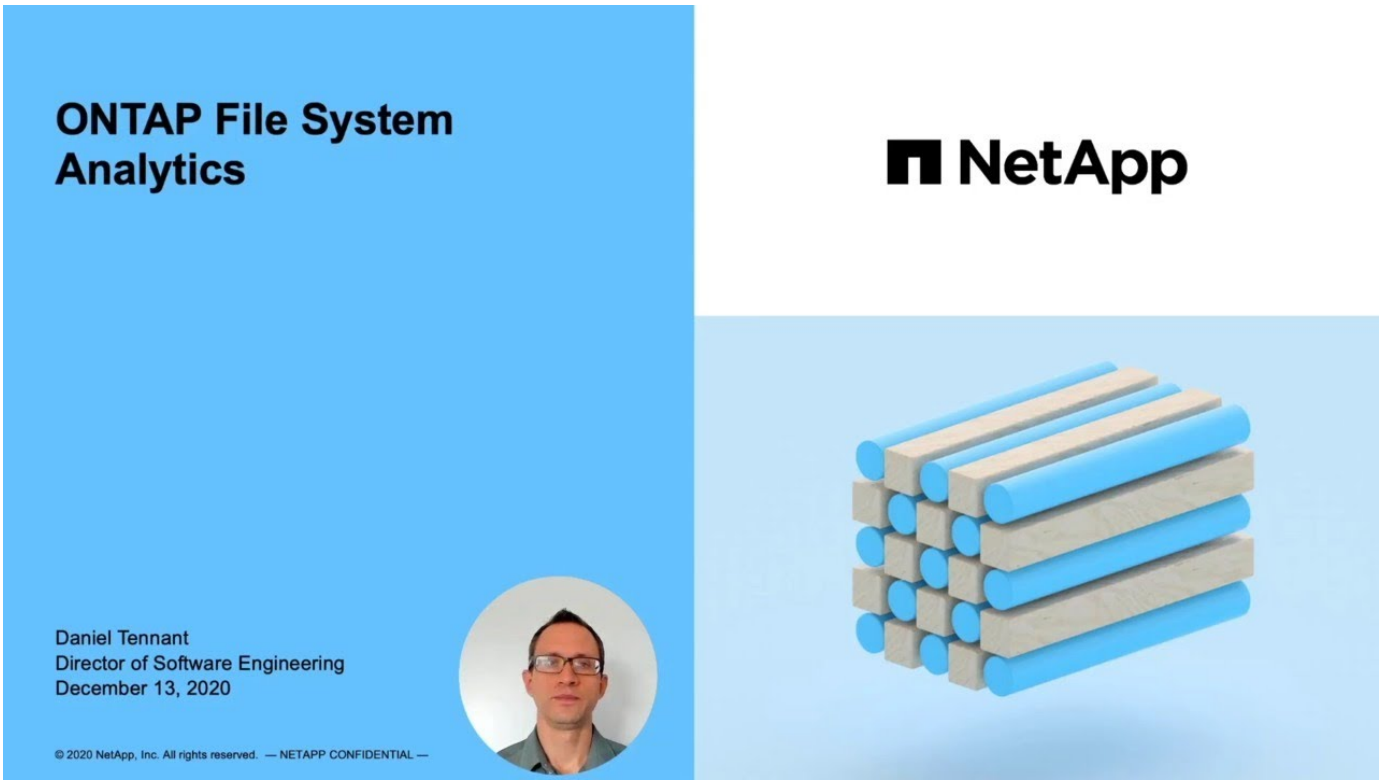
Die Dateisystemanalyse erlaubt Transparenz auf Volumes mit aktiven NAS-Daten mit Ausnahme von FlexCache Caches und SnapMirror Ziel-Volumes.

Verfügbarkeit der Filesystem-Analysefunktion

Jede ONTAP-Version erweitert den Bereich der Dateisystemanalyse.

	ONTAP 9.14.1 und höher	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	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.
Kapazitätsanalysen	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.
Informationen zu inaktiven Daten	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.
Unterstützung für Volumes, die aus Data ONTAP 7-Mode migriert wurden	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Nein
Möglichkeit zum Anpassen inaktiver Perioden in System Manager	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Nein
Aktivitätenverfolgung auf Volume-Ebene	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein
Vorgangsverfolgungsdaten in CSV herunterladen	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein
Aktivitätsverfolgung auf SVM-Ebene	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein
Zeitachse	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein
Nutzungsanalysen	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein
Option zum Aktivieren der Dateisystemanalyse standardmäßig	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein
Fortschrittsüberwachung für Initialisierungsscan	Ja.	Nein	Nein	Nein	Nein	Nein	Nein

Erfahren Sie mehr über die Dateisystemanalyse



Verwandte 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"

Aktivieren Sie die ONTAP Dateisystemanalyse

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

Ab ONTAP 9.17.1 ist File System Analytics (FSA) für Volumes auf neu erstellten SVMs in ONTAP -Clustern, die für NAS-Protokolle zugewiesen sind, standardmäßig aktiviert. FSA wird automatisch aktiviert, sobald ein Volume erstellt wird, und bietet sofortige Analysefunktionen ohne zusätzliche Konfiguration. Wenn Sie File System Analytics auf neuen Volumes nicht aktivieren möchten, müssen Sie "FSA auf neuen Volumes deaktivieren" vom SVM.

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.
- Die benötigte Zeit für die Aktivierung von Analysen hängt von der Größe und dem Inhalt des Volumes ab. System Manager zeigt den Fortschritt an und zeigt nach Abschluss Analysedaten an. Wenn Sie genauere Informationen über den Fortschritt des Initialisierungsscans benötigen, können Sie den Befehl ONTAP CLI verwenden `volume analytics show`.
  - Ab ONTAP 9.15.1 können Sie auf einem Node nur noch vier Initialisierungsscans gleichzeitig durchführen. Sie müssen warten, bis ein Scan abgeschlossen ist, bevor Sie einen neuen Scan starten. ONTAP erzwingt außerdem, dass genügend Speicherplatz auf dem Volume verfügbar ist, und zeigt eine Fehlermeldung an, wenn dies nicht der Fall ist. Stellen Sie sicher, dass mindestens 5 bis 8

Prozent des verfügbaren Speicherplatzes des Volumes frei sind. Wenn das Volume die automatische Größenanpassung aktiviert hat, berechnen Sie die verfügbare Größe basierend auf der maximalen Autogrow-Größe.

- 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.
- Erfahren Sie mehr über `volume analytics show` in der "ONTAP-Befehlsreferenz".

Aktivieren Sie die Dateisystemanalyse auf einem vorhandenen Volume

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

Beispiel 2. Schritt

System Manager

ONTAP 9.10.1 und höher	ONTAP 9.9.1 und ONTAP 9.8
1. Wählen Sie **Storage > Volumes**. 2. Wählen Sie das gewünschte Volumen aus. Wählen Sie im Menü für einzelne Volumes die Option **Dateisystem > Explorer** aus. 3. Wählen Sie **Enable Analytics** oder **Disable Analytics** aus.	1. Wählen Sie **Storage > Volumes**. 2. Wählen Sie das gewünschte Volume aus, und wählen Sie dann **Explorer**. 3. Wählen Sie **Enable Analytics** oder **Disable Analytics** aus.

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 präsentiert nach Abschluss Analysedaten. Wenn Sie genauere Informationen benötigen, können Sie den Befehl im Hintergrund ausführen. Verwenden Sie dazu die `-foreground false` und verwenden Sie dann 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.

Erfahren Sie mehr über `volume analytics on` in der "ONTAP-Befehlsreferenz".

Ändern Sie die Standardeinstellungen für die Dateisystemanalyse

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

Beispiel 3. Schritte

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 **Clustereinstellungen**.
2. Überprüfen Sie in den **Clustereinstellungen** die Registerkarte Dateisystemeinstellungen. Um die Einstellungen zu ändern, wählen Sie die Symbol.
3. Geben Sie im Feld „Aktivitätsverfolgung“ die Namen der SVMs ein, für die die Aktivitätsverfolgung standardmäßig aktiviert werden soll. Wenn Sie das Feld leer lassen, ist die Aktivitätsverfolgung auf allen SVMs deaktiviert.

   Deaktivieren Sie das Kontrollkästchen **Auf neuen Speicher-VMs aktivieren**, um die Aktivitätsverfolgung auf neuen Speicher-VMs standardmäßig zu deaktivieren.

4. Geben Sie im Feld „Analyse“ die Namen der Speicher-VMs ein, für die die Kapazitätsanalyse standardmäßig aktiviert werden soll. Wenn Sie das Feld leer lassen, ist die Kapazitätsanalyse auf allen SVMs deaktiviert.

   Deaktivieren Sie das Kontrollkästchen **Auf neuen Speicher-VMs aktivieren**, um die Kapazitätsanalyse auf neuen Speicher-VMs standardmäßig zu deaktivieren.

5. Wählen Sie **Speichern**.

Einstellungen für Dateisystemanalysen auf einer SVM ändern

1. Wählen Sie die SVM aus, die Sie ändern möchten, und dann **Storage-VM-Einstellungen**.
2. Aktivieren oder deaktivieren Sie mithilfe der Schalter auf der Karte **Dateisystemanalyse** die Aktivitätsverfolgung und Kapazitätsanalyse für alle neuen Volumes auf der Speicher-VM.

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, um Kapazitätsanalysen und Aktivitätsverfolgung standardmäßig auf allen neu erstellten Volumes zu aktivieren:

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

   Erfahren Sie mehr über `vserver modify` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Zeigen Sie die ONTAP-Dateisystemaktivität mit FSA 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 Standardwert des Volumes von der CLI geändert wurde (durch Einstellung der `-atime-update` Option auf `false` mit dem `volume modify` Befehl), wird nur die zuletzt 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:

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

Verwandte Informationen

- "Volume-Änderung"

Aktivieren Sie die ONTAP-Aktivitätsverfolgung mit FSA

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. Ab ONTAP 9.11.1 bietet System Manager einen Zeitplan für die Aktivitätsverfolgung, in dem Sie bis zu fünf Minuten Daten zur Aktivitätsüberwachung nachschlagen 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 Aufzeichnung der Hotspot-Aktivitäten auf einem Volume oder einer SVM speichern und ungefähr alle fünf Sekunden kontinuierlich aktualisieren, während die Daten der letzten fünf Minuten beibehalten werden. Zeitachsendaten werden nur für Felder gespeichert, die auf der Seite sichtbar sind. Wenn Sie eine Tracking-Kategorie ausblenden oder scrollen, damit die Zeitleiste nicht mehr angezeigt wird, wird die Datenerfassung durch die Zeitleiste unterbrochen. Standardmäßig sind die Zeitleisten deaktiviert und werden automatisch deaktiviert, wenn Sie von der

Registerkarte „Vorgang“ wegnavigieren.

Aktivitäts-Tracking für ein einzelnes Volume aktivieren

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

Über diese Aufgabe

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

System Manager

Schritte

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

CLI

Schritte

1. Verfolgung Von Aktivitäten Aktivieren:

   ```
   volume activity-tracking on -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]
   ```

   Verwenden Sie `*`, um Activity Tracking für alle Volumes auf der angegebenen Speicher-VM zu aktivieren.

   Verwenden Sie `!` 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.

Aktivieren Sie ONTAP-Nutzungsanalysen mit FSA

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 ONTAP-Dateisystemaktivität anzeigen.

Ergreifen Sie Korrekturmaßnahmen basierend auf ONTAP-Analysen in FSA

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 asynchroner Funktion zum Löschen von Verzeichnissen mit geringer Latenz gelöscht. (Asynchrones Löschen von Verzeichnissen ist ab ONTAP 9.9.1 auch ohne aktivierte Analyse verfügbar.)

Ab ONTAP 9.10.1	In ONTAP 9.9.1
1. Wählen Sie **Speicher > Volumes** und wählen Sie den gewünschten Volumenamen aus. 2. Wählen Sie auf der Seite mit den einzelnen Volumes die Registerkarte **Dateisystem** und dann die Registerkarte **Explorer**. 3. Wählen Sie in der Ansicht **Explorer** das gewünschte Verzeichnis aus. 4. Zum Löschen bewegen Sie den Mauszeiger über eine Datei oder einen Ordner und das Löschen wird die Option angezeigt. Sie können jeweils nur ein Objekt löschen. Wenn Verzeichnisse und Dateien gelöscht werden, werden die neuen Speicherkapazitätswerte nicht sofort angezeigt.	1. Wählen Sie **Storage > Volumes**. 2. Wählen Sie das gewünschte Volume aus, und wählen Sie dann **Explorer**. 3. Wählen Sie in der Ansicht **Explorer** das gewünschte Verzeichnis aus. 4. Zum Löschen bewegen Sie den Mauszeiger über eine Datei oder einen Ordner und das Löschen wird die Option 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. Um Zieloptionen für ein Volume zu vergleichen, klicken Sie auf ⋮ das Volume und 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 ONTAP Dateisystemanalyse

Ab ONTAP 9.12.1 verfügt ONTAP über eine vordefinierte rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) mit der Bezeichnung `admin-no-fsa`. Die `admin-no-fsa` Rolle gewährt Privileges auf Administratorebene, verhindert jedoch, dass der Benutzer `files` in der ONTAP-CLI, der REST-API und in System Manager Vorgänge in Verbindung mit dem Endpunkt (z. B. Dateisystemanalysen) ausführt.

Weitere Informationen zur `admin-no-fsa` Rolle finden Sie unter 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 die RBAC-Berechtigungen für File System Analytics mithilfe von 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 die entsprechende "API-Endpunkte". In der folgenden Tabelle finden Sie primäre Pfade und sekundäre Pfade zum Konfigurieren von Zugriff oder Einschränkungen bei der Dateisystemanalyse.

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

   Sie können `/*/` anstelle einer UUID die Richtlinie für alle Volumes oder SVMs am Endpunkt festlegen.

   Wählen Sie die Zugriffsberechtigungen für jeden Endpunkt aus.

4. Wählen Sie **Speichern**.
5. Informationen zum Zuweisen der Rolle zu einem 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` Zum Kennwortschutz
   - `sysmgr` Für den System Manager-Zugriff

     ```
     vserver services web access create -vserver <svm-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 den Applikationstyp gilt für die ONTAP-REST-API und den 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"
- "Sicherheits-Login erstellen"

Überlegungen zur ONTAP 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 Sie eine deutliche Erhöhung der Latenz feststellen, lesen Sie die"NetApp Knowledge Base: Hohe oder schwankende Latenz nach dem Einschalten 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** des Systemmanagers oder mit dem CLI-Befehl verfolgen `volume analytics show`. Wenn ein Drosselungsereignis vorhanden ist, gibt ONTAP eine Benachrichtigung aus.

Wenn Sie File System Analytics auf einem Volume aktivieren, stellen Sie sicher, dass mindestens 5 bis 8 Prozent des verfügbaren Speicherplatzes des Volumes frei sind. Wenn das Volume die automatische Größenanpassung aktiviert hat, berechnen Sie die verfügbare Größe basierend auf der maximalen Autogrow-Größe. Ab ONTAP 9.15.1 zeigt ONTAP eine Fehlermeldung an, wenn beim Aktivieren der Dateisystemanalyse auf einem Volume nicht genügend Speicherplatz verfügbar ist.

Nach Abschluss des Scans wird die Dateisystemanalyse kontinuierlich in Echtzeit aktualisiert, wenn sich das Dateisystem ändert.

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 unterbrechen.

- 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

Erfahren Sie mehr über die ONTAP-EMS-Konfiguration

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 ONTAP 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 9.10.0 bis 9.7	Konfigurieren Sie nur SNMP-Trap-Hosts. Sie können ein anderes EMS-Ziel mit der ONTAP CLI konfigurieren. Siehe "Übersicht über die EMS-Konfiguration".

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. Erfahren Sie mehr über `event notification destination create` in der "ONTAP-Befehlsreferenz".

Schritte

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

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

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

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

Webhook (Ab 9.10.1)	• Webhook-URL • Clientauthentifizierung (wählen Sie diese Option, um ein Clientzertifikat anzugeben)

Erstellen Sie einen neuen EMS-Ereignisbenachrichtigungs-Filter

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

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮, und klicken Sie dann auf **Ereignisziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisfilter** aus.
4. Klicken Sie Auf + Add .
5. Geben Sie einen Namen an, und wählen Sie aus, ob Regeln aus einem vorhandenen Ereignisfilter kopiert oder neue Regeln hinzugefügt werden sollen.
6. Führen Sie je nach Ihrer Wahl die folgenden Schritte aus:

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

Bearbeiten Sie ein EMS-Ereignisbenachrichtigungs-Ziel

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

Schritte

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

Verwandte Informationen

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

Konfigurieren Sie EMS-Ereignisbenachrichtigungen mit der CLI

ONTAP EMS-Konfigurationsworkflow

Sie müssen wichtige EMS-Ereignisbenachrichtigungen so konfigurieren, dass sie entweder als E-Mail gesendet, an einen Syslog-Server weitergeleitet, an einen SNMP

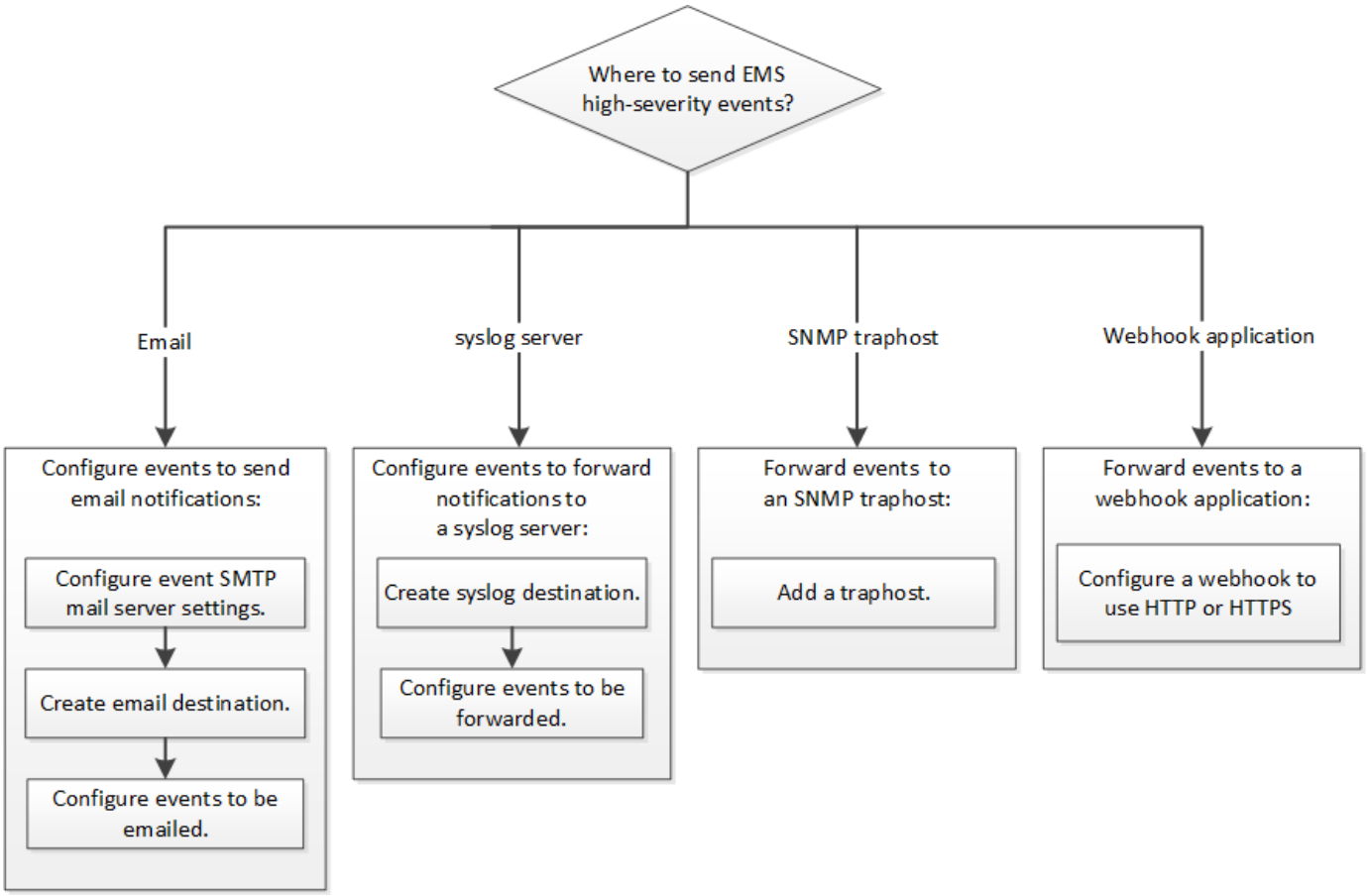
traphost weitergeleitet oder an eine Webhook-Anwendung weitergeleitet werden. Auf diese Weise können Sie Systemstörungen vermeiden, indem Sie Korrekturmaßnahmen rechtzeitig ergreifen.

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 ONTAP EMS-Ereignisse, um E-Mail-Benachrichtigungen zu senden

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.

Bevor Sie beginnen

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
   ```

   Erfahren Sie mehr über `event config modify` in der "ONTAP-Befehlsreferenz".

2. E-Mail-Ziel für Ereignisbenachrichtigungen erstellen:

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

   Erfahren Sie mehr über `event notification destination create` in der "ONTAP-Befehlsreferenz".

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

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

   Erfahren Sie mehr über `event notification create` in der "ONTAP-Befehlsreferenz".

Konfigurieren Sie wichtige ONTAP EMS-Ereignisse, um Benachrichtigungen an einen Syslog-Server weiterzuleiten

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.

Bevor Sie beginnen

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 den angegeben wird `syslog-transport`, überprüft ONTAP die Identität des Zielhosts durch Validierung seines Zertifikats. Der Standardwert ist `udp-unencrypted`.

`syslog-port`

Der Standardwertparameter `syslog-port` hängt von der Einstellung für den `syslog-transport` Parameter ab. Wenn `syslog-transport` auf `tcp-encrypted`, gesetzt ist, `syslog-port` hat den Standardwert 6514.

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 folgende Werte angegeben werden für `syslog-transport`:

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

     Das Standardprotokoll ist `udp-unencrypted`.

   Erfahren Sie mehr über `event notification destination create` in der "ONTAP-Befehlsreferenz".

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

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

ems

Erfahren Sie mehr über `event notification create` in der "ONTAP-Befehlsreferenz".

Konfigurieren Sie ONTAP SNMP-Traphosts für den Empfang von Ereignisbenachrichtigungen

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

Bevor Sie beginnen

- 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 ONTAP-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. "Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTP"Die Konfigurationsdetails finden Sie unter.

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. "Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS"Die Konfigurationsdetails finden Sie unter.

HTTPS mit gegenseitiger Authentifizierung

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

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`, um die Ereignisse zu empfangen:

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

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

   Erfahren Sie mehr über `event notification destination create` in der "ONTAP-Befehlsreferenz".

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

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

Erfahren Sie mehr über `event notification create` in der "ONTAP-Befehlsreferenz".

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 das `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 `important-events` Filter mit dem neuen `restapi-ems` Ziel verknüpft:

   ```
   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 der Aufgabe aus"Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS", um das Serverzertifikat zu installieren, 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 das `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 `important-events` Filter mit dem neuen `restapi-ems` Ziel verknüpft:

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

Verwandte Informationen

- "Sicherheitszertifikat installieren"

Aktualisieren der veralteten EMS-Ereigniszuordnung

Erfahren Sie mehr über die ONTAP EMS-Ereigniszuordnungsmodelle

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

Beginnend mit ONTAP 9.0, ist die beste Praxis für ONTAP EMS-Ereigniszielzuordnung, das skalierbarere Ereignisfiltermodell `event filter` `event notification` `event notification destination` zu verwenden, in dem Musterabgleich auf mehreren Feldern erfolgt, mit den, und Befehlssätzen.

Wenn Ihre EMS-Zuordnung mit den veralteten Befehlen konfiguriert ist, sollten Sie Ihre Zuordnung aktualisieren, um die `event filter` `event notification` `event notification destination` Befehlssätze , und zu verwenden. Erfahren Sie mehr über `event` in der "ONTAP-Befehlsreferenz".

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 `event destination create` Befehl erstellt.

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

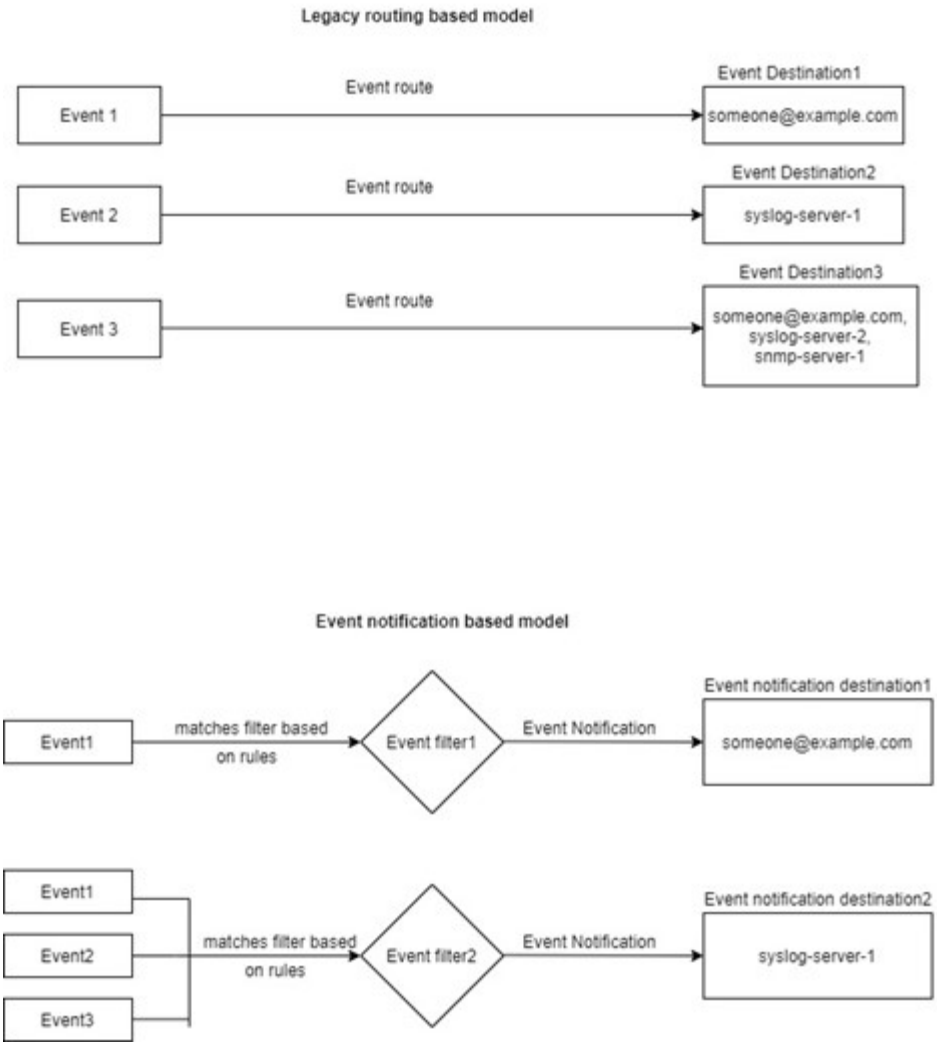
Im veralteten Modell werden EMS-Ereignisse über den `event route add-destinations` Befehl individuell einem Ziel zugeordnet.

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

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

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

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



Aktualisieren Sie die ONTAP-EMS-Ereigniszuordnung von veralteten Befehlen

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

Schritte

1. Führen Sie mit dem `event destination show` Befehl alle Event-Ziele im System auf.

```
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 zugeordnet werden `event route show -destinations <destination name>`, mit dem Befehl.

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

3. Erstellen Sie ein entsprechendes `event filter`, das alle diese Teilmengen von Ereignissen enthält. Wenn Sie beispielsweise nur die `raid.aggr.*` -Ereignisse einbeziehen möchten, verwenden Sie `message-name` beim Erstellen des Filters einen Platzhalter für den Parameter. Sie können auch Filter für einzelne Ereignisse erstellen.

   Erfahren Sie mehr über `event filter` in der "ONTAP-Befehlsreferenz".

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 eines `event notification destination` für jeden `event destination` Endpunkt (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.
```

Erfahren Sie mehr über `event notification destination` und `event destination` in der "ONTAP-Befehlsreferenz".

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 alle `event destination`, die eine `event route` Zuordnung haben.

> Ereignisse, die an SNMP-Ziele weitergeleitet werden `snmp-traphost`, sollten dem Ziel für die Ereignisbenachrichtigung zugeordnet werden. 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?: -
```