Gemeinsame Workflows und Aufgaben im Zusammenhang mit Unified Manager

Active IQ Unified Manager 9.8

NetApp
January 31, 2025

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-98/health-checker/task-performing-corrective-action-for-storage-failover-interconnect-links-down.html on January 31, 2025. Always check docs.netapp.com for the latest.

Inhalt

Gemeinsame Workflows und Aufgaben im Zusammenhang mit Unified Manager . . . 1
Monitoring und Fehlerbehebung der Datenverfügbarkeit . . . 2
Behebung von Kapazitätsproblemen . . . 9
Verwalten von Systemzustandsschwellenwerten . . . 11
Verwalten von Zielen für die Cluster-Sicherheit . . . 17
Managen von Backup- und Restore-Vorgängen . . . 28
Verwalten von Skripten . . . 40
Verwalten und Überwachen von Gruppen . . . 43
Priorisieren von Storage-Objektereignissen mithilfe von Anmerkungen . . . 53
Was für ein Unified Manager-Wartungsfenster ist . . . 63
Verwalten von SAML-Authentifizierungseinstellungen . . . 65
Senden eines Unified Manager Support Bundle an den technischen Support . . . 72
Aufgaben und Informationen im Zusammenhang mit mehreren Workflows . . . 77

Gemeinsame Workflows und Aufgaben im Zusammenhang mit Unified Manager

Zu den geläufigsten administrativen Workflows und Aufgaben für Unified Manager gehört die Auswahl der zu überwachenden Storage-Cluster, die Diagnose von Bedingungen, die sich nachteilig auf die Datenverfügbarkeit, -Kapazität und -Sicherung auswirken, die Wiederherstellung verlorener Daten, die Konfiguration und das Management von Volumes sowie die Bündelung und das Senden von Diagnosedaten an den technischen Support (falls erforderlich).

Unified Manager gibt Storage-Administratoren die Möglichkeit, ein Dashboard anzuzeigen, die allgemeine Kapazität, Verfügbarkeit und den Sicherungsstatus der gemanagten Storage-Cluster zu bewerten und dann schnell spezielle Probleme zu identifizieren, zu lokalisieren, zu diagnostizieren und zu beheben.

Die wichtigsten Probleme im Zusammenhang mit einem Cluster, einer Storage Virtual Machine (SVM), einem Volume oder einem FlexGroup Volume, die die Storage-Kapazität oder Datenverfügbarkeit Ihrer gemanagten Storage-Objekte beeinträchtigen, werden in den Systemintegritätsdiagrammen und -Ereignissen auf der Dashboard-Seite angezeigt. Wenn kritische Probleme erkannt werden, enthält diese Seite Links zur Unterstützung geeigneter Workflows zur Fehlerbehebung.

Unified Manager kann auch in Workflows mit verwandten Management-Tools wie beispielsweise OnCommand Workflow Automation (WFA) integriert werden, um die direkte Konfiguration von Storage-Ressourcen zu unterstützen.

Allgemeine Workflows für die folgenden administrativen Aufgaben werden in diesem Dokument beschrieben:

- Diagnose und Management von Verfügbarkeitsproblemen

  Wenn ein Hardwarefehler oder Probleme bei der Konfiguration von Speicherressourcen die Anzeige von Datenverfügbarkeits-Ereignissen auf der Dashboard-Seite verursachen, können Storage-Administratoren den eingebetteten Links folgen, um Konnektivitätsinformationen über die betroffene Speicherressource anzuzeigen, Tipps zur Fehlerbehebung anzuzeigen und anderen Administratoren eine Problembehebung zuzuweisen.

- Konfiguration und Monitoring von Performance-Vorfällen

  Der Administrator kann die Performance der überwachten Storage-Systemressourcen überwachen und managen. Siehe "Einführung in das Active IQ Unified Manager Performance-Monitoring" Finden Sie weitere Informationen.

- Diagnose und Management von Kapazitätsproblemen bei Volumes

  Wenn Probleme mit der Speicherkapazität von Volumes auf der Seite Dashboard angezeigt werden, können Storage-Administratoren anhand der eingebetteten Links die aktuellen und historischen Trends bezüglich der Speicherkapazität des betroffenen Volumes anzeigen, Tipps zur Fehlerbehebung anzeigen und anderen Administratoren die Problembehebung zuweisen.

- Konfiguration, Monitoring und Diagnose von Problemen bei der Sicherungsbeziehung

  Nach dem Erstellen und Konfigurieren von Sicherungsbeziehungen können Storage-Administratoren mögliche Probleme im Zusammenhang mit Sicherungsbeziehungen, den aktuellen Zustand der Sicherungsbeziehungen, die aktuellen und historischen Sicherungsinformationen zu den betroffenen

Beziehungen sowie Hinweise zur Fehlerbehebung anzeigen. Siehe "Erstellen, Überwachen und Beheben von Sicherungsbeziehungen" Finden Sie weitere Informationen.

- Erstellen von Backup-Dateien und Wiederherstellen von Daten aus Backup-Dateien.
- Verknüpfen von Speicherobjekten mit Anmerkungen

  Durch Verknüpfen von Storage-Objekten mit Annotationen können Storage-Administratoren die Ereignisse, die zu den Storage-Objekten gehören, filtern und anzeigen, sodass Storage-Administratoren die mit den Ereignissen verbundenen Probleme priorisieren und lösen können.

- Verwendung VON REST-APIs zum Management der Cluster durch Anzeige der von Unified Manager erfassten Daten zu Systemzustand, Kapazität und Performance Siehe siehe "Erste Schritte mit Active IQ Unified Manager REST APIs" Finden Sie weitere Informationen.
- Senden eines Support Bundle an den technischen Support

  Storage-Administratoren können über die Wartungskonsole ein Support-Bundle abrufen und an den technischen Support senden. Support Bundles müssen an den technischen Support gesendet werden, wenn das Problem eine detailliertere Diagnose und Fehlerbehebung erfordert als eine AutoSupport Meldung.

Monitoring und Fehlerbehebung der Datenverfügbarkeit

Unified Manager überwacht die Zuverlässigkeit, mit der autorisierte Benutzer auf Ihre gespeicherten Daten zugreifen können, warnt Sie vor Bedingungen, die den Zugriff blockieren oder behindern, und ermöglicht Ihnen die Diagnose dieser Bedingungen.

Die Themen im Verfügbarkeits-Workflow in diesem Abschnitt beschreiben Beispiele, wie Storage-Administratoren mithilfe der Unified Manager Web-UI Hardware- und Software-Probleme lösen, diagnostizieren und zuweisen können, die sich negativ auf die Datenverfügbarkeit auswirken.

Scannen und Beheben von Verbindungsproblemen für Storage Failover Interconnect

Dieser Workflow bietet ein Beispiel dafür, wie Sie ausgefallene Storage Failover Interconnect-Verbindungsbedingungen suchen, bewerten und beheben können. In diesem Szenario suchen Sie als Administrator mit Unified Manager nach Storage-Failover-Risiken, bevor Sie ein ONTAP Version Upgrade auf den Nodes starten.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Falls während eines unterbrechungsfreien Upgrades die Verbindung zwischen Storage Failover und HA-Paar-Nodes ausfällt, schlägt das Upgrade fehl. Daher ist es üblich, dass der Administrator die Zuverlässigkeit des Storage Failover auf den Cluster-Nodes, die für das Upgrade benötigt werden, überwachen und bestätigen kann, bevor das Upgrade beginnt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**.
2. Wählen Sie auf der Seite * Event Management* Inventory die Option **Active Availability Events** aus.
3. Klicken Sie oben auf der Spalte **Event Management** Inventory Seite**Name** auf Und eingeben `*failover` Im Textfeld zur Begrenzung des Ereignisses auf Ereignisse mit Speicherausfallschutz.

   Es werden alle Ereignisse angezeigt, die in Bezug auf Storage-Failover-Bedingungen vergangen sind.

   In diesem Szenario zeigt der Unified Manager das Ereignis „`SStorage Failover Interconnect One" oder „More Links Down`“ im Bereich „Availability Incidents“ an.

4. Wenn ein oder mehrere Ereignisse im Zusammenhang mit dem Speicherausfallschutz auf der Seite **Ereignisverwaltung** Inventar angezeigt werden, führen Sie die folgenden Schritte aus:

   a. Klicken Sie auf den Link Event Title, um die Ereignisdetails für dieses Ereignis anzuzeigen.

      In diesem Beispiel klicken Sie auf den Ereignistitel “STorage Failover Interconnect One or More Links Down”.

   Die Seite Ereignisdetails für dieses Ereignis wird angezeigt.

   a. Auf der Seite **Event** Details können Sie eine oder mehrere der folgenden Aufgaben ausführen:
      - Überprüfen Sie die Fehlermeldung im Feld Ursache, und bewerten Sie das Problem. Durchführen von Korrekturmaßnahmen für Storage Failover Interconnect-Verbindungen als inaktiv
      - Weisen Sie das Ereignis einem Administrator zu. Ereignisse werden zugewiesen
      - Bestätigen Sie das Ereignis. Bestätigen und Beheben von Ereignissen

Durchführen von Korrekturmaßnahmen für Storage Failover Interconnect-Verbindungen als inaktiv

Wenn Sie die Seite Ereignisdetails eines Storage Failover-bezogenen Ereignisses anzeigen, können Sie die Zusammenfassungen der Seite überprüfen, um die Dringlichkeit des Ereignisses, die mögliche Ursache des Problems und eine mögliche Lösung des Problems festzustellen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

In diesem Beispielszenario enthält die Ereignisübersicht auf der Seite Ereignisdetails die folgenden Informationen über den Zustand der Verbindung zum Storage Failover Interconnect:

```
Event: Storage Failover Interconnect One or More Links Down

Summary

Severity: Warning
State: New
Impact Level: Risk
Impact Area: Availability
Source: aardvark
Source Type: Node
Acknowledged By:
Resolved By:
Assigned To:
Cause: At least one storage failover interconnected link
       between the nodes aardvark and bonobo is down.
       RDMA interconnect is up (Link0 up, Link1 down)
```

Die Beispielereignisinformationen zeigen an, dass eine Storage Failover Interconnect-Verbindung, Link1, zwischen HA-Paar-Nodes aardvark und bonobo ausgefallen ist, aber dass link0 zwischen Apple und Boy aktiv ist. Da eine Verbindung aktiv ist, funktioniert der Remote Dynamic Memory Access (RDMA) weiterhin und ein Storage Failover-Job kann weiterhin erfolgreich ausgeführt werden.

Um jedoch sicherzustellen, dass beide Links ausfallen und der Storage-Failover-Schutz vollständig deaktiviert ist, entscheiden Sie sich für eine weitere Diagnose des Fehlers von Link1.

Schritte

1. Auf der Seite **Event** Details können Sie auf den Link zu dem Ereignis klicken, das im Feld Quelle angegeben ist, um weitere Details zu anderen Ereignissen zu erhalten, die sich auf den Zustand der Verbindung zum Storage Failover Verbindungsabschaltung beziehen könnten.

   In diesem Beispiel ist die Quelle des Ereignisses der Node aardvark. Wenn Sie auf diesen Node-Namen klicken, werden auf der Registerkarte Nodes der Seite Cluster/Health Details die HA-Details für das betroffene HA-Paar, aardvark und bonobo, angezeigt und weitere Ereignisse, die kürzlich auf dem betroffenen HA-Paar aufgetreten sind, werden angezeigt.

2. Lesen Sie die **HA Details** für weitere Informationen über die Veranstaltung.

   In diesem Beispiel werden die relevanten Informationen in der Ereignistabelle angezeigt. Die Tabelle zeigt das Ereignis „`STorage Failover Connection One or More Link Down`“, die Zeit, zu der das Ereignis generiert wurde, und auch hier den Knoten, aus dem dieses Ereignis hervorgegangen ist.

Nachdem Sie fertig sind

Bitten Sie anhand der Standortinformationen des Node in den HA-Details eine physische Überprüfung und Reparatur des Storage Failover-Problems auf den betroffenen HA-Paar-Nodes oder führen Sie diese persönlich durch.

Lösung von Offline-Problemen des Volumes

Dieser Workflow bietet ein Beispiel dafür, wie Sie ein Offline-Ereignis eines Volumes bewerten und beheben können, das Unified Manager auf der Seite „Ereignismanagement-Bestand“ anzeigen kann. In diesem Szenario dienen Sie als Administrator, der Unified Manager zum Beheben von Fehlern bei einem oder mehreren Offline-Ereignissen des Volumes verwendet.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Volumes können aus verschiedenen Gründen offline gemeldet werden:

- Der SVM-Administrator hat das Volume absichtlich offline geschaltet.
- Der Hosting-Cluster-Node des Volumes ist ausgefallen und das Storage-Failover zu seinem HA-Paar-Partner ist ebenfalls ausgefallen.
- Das Volume, das die Storage Virtual Machine (SVM) hostet, wird angehalten, da der Node, der das Root-Volume dieser SVM hostet, ausgefallen ist.
- Das Hosting-Aggregat des Volumes ist aufgrund des gleichzeitigen Ausfalls von zwei RAID-Festplatten ausgefallen.

Mithilfe der Inventarseite für das Ereignismanagement und der Seiten „Cluster/Health“, „Storage VM/Health“ und „Volume/Health Details“ können Sie eine oder mehrere dieser Möglichkeiten bestätigen oder eliminieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**.
2. Wählen Sie auf der Seite * Event Management* Inventory die Option **Active Availability Events** aus.
3. Klicken Sie auf den Hypertext-Link, der für das Offlinevent Volume angezeigt wird.

   Die Seite Ereignisdetails für den Verfügbarkeitsereignis wird angezeigt.

4. Prüfen Sie auf dieser Seite die Hinweise, ob der SVM-Administrator das fragliche Volume offline geschaltet hat.
5. Auf der Seite **Event** Details können Sie die Informationen für eine oder mehrere der folgenden Aufgaben einsehen:
   - Überprüfen Sie die im Feld Ursache angezeigten Informationen, um eine mögliche Diagnoseführung zu erhalten.

     In diesem Beispiel werden Sie in den Informationen im Feld Ursache nur darüber informiert, dass das Volume offline ist.

   - Im Bereich „Notizen“ und „Updates“ werden alle Angaben darüber gemacht, dass der SVM-Administrator das fragliche Volume absichtlich offline geschaltet hat.
   - Klicken Sie auf die Quelle des Ereignisses, in diesem Fall auf das offline gemeldete Volume, um weitere Informationen zu diesem Volume zu erhalten. Durchführung von Korrekturmaßnahmen für Offline-Bedingungen des Volumes

- Weisen Sie das Ereignis einem Administrator zu. Ereignisse werden zugewiesen
- Bestätigen Sie das Ereignis oder markieren Sie es gegebenenfalls als erledigt. Bestätigen und Beheben von Ereignissen

Durchführung von Diagnoseaktionen für Offline-Bedingungen des Volumes

Nachdem Sie zur Seite Volume / Health Details eines gemeldeten Volumes navigieren, das offline sein soll, können Sie nach zusätzlichen Informationen suchen, die hilfreich sind, um die Offline-Bedingung des Volumens zu diagnostizieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Wenn das offline gemeldete Volume nicht absichtlich offline geschaltet wurde, ist das Volume aus verschiedenen Gründen offline.

Beginnend mit der Seite Volume / Health Details des Offline-Volumes können Sie zu anderen Seiten und Fenstern navigieren, um mögliche Ursachen zu bestätigen oder zu eliminieren:

Wahlmöglichkeiten

- Klicken Sie auf **Volume / Health** Details Seite Links, um festzustellen, ob das Volume offline ist, weil sein Host-Knoten ausgefallen ist und Storage Failover zu seinem HA-Paar-Partner hat auch fehlgeschlagen.

  Siehe Ermitteln, ob ein Offline-Zustand eines Volumes von einem Node nach unten verursacht wurde.

- Klicken Sie auf **Volume / Health** Detailseite Links, um festzustellen, ob das Volume offline ist und seine Host Storage Virtual Machine (SVM) angehalten wird, da der Node, der das Root-Volume dieser SVM hostet, nicht verfügbar ist.

  Siehe Ermitteln, ob ein Volume offline ist und die SVM angehalten wird, da ein Node ausfällt.

- Klicken Sie auf **Volumen / Gesundheit** Details Seite Links, um festzustellen, ob das Volumen ist offline wegen gebrochener Festplatten in seinem Host-Aggregat.

  Siehe Ermitteln, ob ein Volume aufgrund von defekten Festplatten in einem Aggregat offline ist.

Ermitteln, ob ein Volume offline ist, da sein Host-Node ausfällt

Mit der Unified Manager Web-UI lässt sich die Möglichkeit bestätigen oder ganz ausschließen, dass ein Volume offline ist, da der Host-Node ausfällt und das Storage Failover auf seinen HA-Paar-Partner nicht erfolgreich ist.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Um zu ermitteln, ob der Offlinezustand des Volumes durch einen Ausfall des Hosting-Node und eines nachfolgenden nicht erfolgreichen Storage-Failovers verursacht wird, führen Sie folgende Aktionen durch:

Schritte

1. Suchen und klicken Sie auf den Hypertext-Link, der unter SVM im Bereich **Related Devices** des Offline-Volume der Seite **Volume / Health** Details angezeigt wird.

   Auf der Seite Storage VM / Health Details werden Informationen zur SVM (Hosting Storage Virtual Machine) des Offline-Volumes angezeigt.

2. Suchen Sie im Bereich **Related Devices** der Seite **Storage VM / Health** Details den Hypertext-Link, der unter Volumes angezeigt wird, und klicken Sie auf diesen.

   In der Ansicht Systemzustand: Alle Volumes wird eine Tabelle mit Informationen zu allen Volumes angezeigt, die von der SVM gehostet werden.

3. Klicken Sie in der Spaltenüberschrift **Health: All Volumes** view State auf das Filtersymbol , Und wählen Sie dann die Option **Offline**.

   Es werden nur die SVM-Volumes im Offline-Zustand aufgeführt.

4. Klicken Sie in der Ansicht **Health: Alle Volumes** auf das Raster-Symbol , Und wählen Sie dann die Option **Cluster-Knoten**.

   Möglicherweise müssen Sie im Auswahlfeld Raster blättern, um die Option **Cluster Nodes** zu finden.

   Die Spalte Cluster Nodes wird dem Bestand der Volumes hinzugefügt und zeigt den Namen des Node an, der jedes Offline Volume hostet.

5. Suchen Sie in der Ansicht **Health: All Volumes** die Liste für das Offline-Volume und klicken Sie in der Spalte Cluster Node auf den Namen seines Hostknoten.

   Auf der Registerkarte Nodes auf der Seite Cluster / Health Details wird der Status des HA-Paar von Nodes angezeigt, zu dem der Hosting-Node gehört. Der Status des Hosting-Node und der Erfolg eines Cluster-Failover-Vorgangs wird in der Anzeige angezeigt.

Nachdem Sie fertig sind

Nachdem Sie bestätigt haben, dass der Offline-Zustand des Volume vorliegt, weil sein Host-Node ausgefallen ist und das Storage Failover zum HA-Paar-Partner fehlgeschlagen ist, wenden Sie sich an den entsprechenden Administrator oder Operator, um den heruntergeschilterten Node manuell neu zu starten und das Storage-Failover-Problem zu beheben.

Ermitteln, ob ein Volume offline ist und seine SVM angehalten ist, da ein Node ausfällt

Mit der Unified Manager Web-UI lässt sich die Möglichkeit bestätigen oder ganz vermeiden, dass ein Volume offline ist, da die SVM (Host Storage Virtual Machine) aufgrund des Node, der das Root-Volume dieser SVM hostet, angehalten wird.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Um zu ermitteln, ob die Offline-Bedingung des Volumes dazu führt, dass seine Host-SVM angehalten wird, da der Node, der das Root-Volume dieser SVM hostet, ausgefallen ist, führen Sie die folgenden Aktionen durch:

Schritte

1. Suchen Sie den Hypertext-Link, der unter der SVM im Bereich **Related Devices** des Offlinesdatentextes angezeigt wird, und klicken Sie auf die Seite **Volume / Health** Details.

   Auf der Seite Storage VM / Health Details wird der Status „`running`“ bzw. der Status „`stogedated`“ der Hosting-SVM angezeigt. Wenn der SVM-Status ausgeführt wird, wird die offline-Bedingung des Volumes nicht durch den Node verursacht, der das Root-Volume dieser SVM hostet, der ausgefallen ist.

2. Wenn der SVM-Status angehalten wird, klicken Sie auf **View SVMs**, um die Ursache des Anstoppens der Hosting-SVM zu ermitteln.
3. Klicken Sie in der Spaltenüberschrift **Health: All Storage VMs** viewSVM auf das Filtersymbol Geben Sie dann den Namen der angehalten SVM ein.

   Die Informationen für diese SVM sind in einer Tabelle dargestellt.

4. Klicken Sie in der Ansicht **Health: Alle Storage VMs** auf Und wählen Sie dann die Option **Root Volume** aus.

   Die Spalte „Root-Volume“ wird dem SVM-Inventar hinzugefügt und zeigt den Namen des Root-Volumes der angehalten SVM an.

5. Klicken Sie in der Spalte Root Volume auf den Namen des Root-Volumes, um die Seite **Storage VM / Health** Details für dieses Volume anzuzeigen.

   Wenn der Status des SVM-Root-Volumes (Online) lautet, wird die ursprüngliche Offline-Bedingung für das Volume nicht verursacht, da der Node, der das Root-Volume dieser SVM hostet, nicht verfügbar ist.

6. Wenn der Status des SVM-Root-Volumes (Offline) lautet, suchen und klicken Sie auf den Hypertext-Link, der unter Aggregat im Bereich **Related Devices** der Seite **Volume / Health** des SVM-Root-Volumes angezeigt wird.
7. Suchen und klicken Sie auf den Hypertext-Link, der unter Knoten im Bereich **Verwandte Geräte** der Seite * Aggregate / Health* Details des Aggregats angezeigt wird.

   Auf der Registerkarte Nodes auf der Seite Cluster/Integritätsdetails wird der Status des HA-Paars der Nodes angezeigt, dem der Hosting-Node des SVM-Root-Volumes angehört. Der Status des Knotens wird im Display angezeigt.

Nachdem Sie fertig sind

Nachdem Sie bestätigt haben, dass der Offline-Zustand des Volume durch den Offline-Zustand des Host-SVM verursacht wurde. Dies selbst wird durch den Node verursacht, der das Root-Volume der SVM hostet, der ausgefallen ist, wenden Sie sich an den entsprechenden Administrator oder Operator, um den ausgefallenen Node manuell neu zu starten.

Ermitteln, ob ein Volume aufgrund von defekten Festplatten in einem Aggregat offline ist

Sie können die Unified Manager Web-UI nutzen, um die Möglichkeit zu bestätigen oder zu beseitigen, dass ein Volume offline ist, da RAID-Festplattenprobleme sein Host-Aggregat offline geschaltet haben.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Um festzustellen, ob der Zustand des Volumes offline durch Probleme mit RAID-Festplatten verursacht wird, die das Hosting-Aggregat offline schalten, führen Sie die folgenden Schritte aus:

Schritte

1. Suchen Sie den Hypertext-Link, der unter Aggregate angezeigt wird, und klicken Sie auf der Seite **Volume / Health** Details im Bereich **Related Devices** auf.

   Auf der Seite Aggregate / Health Details wird der Online- oder Offline-Status des Hosting-Aggregats angezeigt. Wenn der Aggregatstatus online ist, sind Probleme mit der RAID-Festplatte nicht die Ursache dafür, dass das Volume offline ist.

2. Wenn der Aggregatstatus offline ist, klicken Sie auf **Disk Information** und suchen Sie in der Liste **Events** auf der Registerkarte **Disk Information** nach defekten Festplatten-Ereignissen.
3. Um die defekten Laufwerke weiter zu identifizieren, klicken Sie auf den Hypertext-Link, der unter Knoten im Bereich **Verwandte Geräte** angezeigt wird.

   Die Seite „Cluster/Health Details“ wird angezeigt.

4. Klicken Sie auf **Disks**, und wählen Sie dann im Bereich **Filter** * die Option **gebrochene** aus, um alle Festplatten im unterbrochenen Zustand anzuzeigen.

   Wenn die Laufwerke im Status „beschädigt“ den Offlinezustand des Host-Aggregats verursacht haben, wird der Name des Aggregats in der Spalte „Betroffener Aggregat“ angezeigt.

Nachdem Sie fertig sind

Nachdem Sie bestätigt haben, dass der Offlinezustand des Datenträgers durch defekte RAID-Laufwerke und das daraus resultierende Offline-Host-Aggregat verursacht wird, wenden Sie sich an den entsprechenden Administrator oder Operator, um die defekten Laufwerke manuell zu ersetzen und das Aggregat wieder online zu schalten.

Behebung von Kapazitätsproblemen

Dieser Workflow bietet ein Beispiel dafür, wie Sie ein Kapazitätsproblem lösen können. In diesem Szenario greifen Sie als Administrator oder Operator auf die Seite Unified ManagerDashboard zu, um zu sehen, ob eines der überwachten Speicherobjekte Kapazitätsprobleme haben. Sie möchten die mögliche Ursache und Lösung des Problems ermitteln.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Auf der Dashboard-Seite suchen Sie im Kapazitätsbereich unter der Dropdown-Liste Ereignisse ein Fehlerereignis „`Volume Space Full`“.

Schritte

1. Klicken Sie im Bereich **Kapazität** der Seite **Dashboard** auf den Namen des Fehlerereignisses Volume Space Full.

   Die Seite Ereignisdetails für den Fehler wird angezeigt.

2. Auf der Seite **Event** Details können Sie eine oder mehrere der folgenden Aufgaben ausführen:
   - Überprüfen Sie die Fehlermeldung im Feld Ursache, und klicken Sie auf die Vorschläge unter vorgeschlagene Korrekturmaßnahmen, um Beschreibungen möglicher Korrekturmaßnahmen zu prüfen. Durchführung von vorgeschlagenen Abhilfemaßnahmen für ein vollständiges Volumen
   - Klicken Sie im Feld Quelle auf den Objektnamen, in diesem Fall ein Volume, um Details zum Objekt anzuzeigen. Einzelheiten zu den Volumes
   - Suchen Sie nach Notizen, die zu diesem Event hinzugefügt wurden. Hinzufügen und Prüfen von Notizen zu einem Ereignis
   - Fügen Sie dem Ereignis eine Notiz hinzu. Hinzufügen und Prüfen von Notizen zu einem Ereignis
   - Das Ereignis einem anderen Benutzer zuweisen. Ereignisse werden zugewiesen
   - Bestätigen Sie das Ereignis. Bestätigen und Beheben von Ereignissen
   - Markieren Sie das Ereignis als erledigt. Bestätigen und Beheben von Ereignissen

Durchführung von vorgeschlagenen Abhilfemaßnahmen für ein vollständiges Volumen

Nachdem Sie ein Fehlerereignis „`Volume Space Full`“ erhalten haben, überprüfen Sie die vorgeschlagenen Korrekturmaßnahmen auf der Seite Ereignisdetails und entscheiden sich für eine der vorgeschlagenen Aktionen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Ein Benutzer mit einer beliebigen Rolle kann alle Aufgaben in diesem Workflow mit Unified Manager ausführen.

Über diese Aufgabe

In diesem Beispiel wurde ein Fehlerereignis „Volume Space Full“ auf der Seite „Unified ManagerEvent Management Inventory“ angezeigt und auf den Namen des Ereignisses geklickt.

Mögliche Abhilfemaßnahmen für ein komplettes Volume sind:

- Aktivieren von Autogrow, Deduplizierung oder Komprimierung auf dem Volume
- Ändern der Größe oder Verschieben des Volumes
- Löschen oder Verschieben von Daten vom Volume

Obwohl alle diese Aktionen entweder über ONTAP System Manager oder über die ONTAP CLI ausgeführt werden müssen, können Sie in Unified Manager Informationen finden, die Sie möglicherweise ermitteln müssen, welche Maßnahmen ergriffen werden sollen.

Schritte

1. Auf der Seite **Event** Details klicken Sie im Feld Quelle auf den Namen des Datenträgers, um Details zum betroffenen Volume anzuzeigen.
2. Klicken Sie auf der Seite **Volume / Health** Details auf **Konfiguration** und sehen Sie, dass die Deduplizierung und Komprimierung bereits auf dem Volume aktiviert sind.

   Sie entscheiden, die Größe des Volumes zu ändern.

3. Im Fensterbereich **Verwandte Geräte** klicken Sie auf den Namen des Hosting-Aggregats, um zu sehen, ob das Aggregat ein größeres Volumen aufnehmen kann.
4. Auf der Detailseite **Aggregate/Health** sehen Sie, dass das Aggregat, das das volle Volume hostet, über genügend freie Kapazität verfügt. Sie verwenden also den ONTAP System Manager, um die Größe des Volumes zu ändern und ihm mehr Kapazität zu geben.

Verwalten von Systemzustandsschwellenwerten

Sie können globale Statusschwellenwerte für alle Aggregate, Volumes und qtrees konfigurieren, um Verletzungen des Systemzustands zu verfolgen.

Welche Schwellenwerte für den Zustand von Storage-Kapazität sind

Ein Schwellenwert für die Storage-Kapazität ist der Punkt, an dem der Unified Manager Server Ereignisse generiert, um jedes Kapazitätsproblem im Zusammenhang mit Storage-Objekten zu melden. Sie können Benachrichtigungen so konfigurieren, dass sie benachrichtigt werden, wenn diese Ereignisse auftreten.

Die Schwellenwerte für den Zustand der Storage-Kapazität aller Aggregate, Volumes und qtrees sind auf die Standardwerte festgelegt. Sie können die Einstellungen je nach Bedarf für ein Objekt oder eine Gruppe von Objekten ändern.

Konfigurieren von globalen Schwellenwerteinstellungen für den Systemzustand

Sie können globale Statusschwellenwerte für Kapazität, Wachstum, Snapshot-Reserve, Quoten und Inodes konfigurieren, um die Aggregat-, Volume- und qtree-Größe effektiv zu überwachen. Sie können auch die Einstellungen für das Generieren von Ereignissen für das Überschreiten der Schwellenwerte für Verzögerungen bearbeiten.

Über diese Aufgabe

Globale Statusschwellenwerte gelten für alle Objekte, denen sie zugeordnet sind, z. B. Aggregate, Volumes

usw. Wenn die Schwellenwerte überschritten werden, wird ein Ereignis generiert und im Fall der Konfiguration von Meldungen eine Warnmeldung gesendet. Schwellenwertvorgaben sind auf empfohlene Werte festgelegt. Sie können sie aber ändern, um Ereignisse in Abständen zu generieren, um Ihre spezifischen Anforderungen zu erfüllen. Wenn Schwellenwerte geändert werden, werden Ereignisse im nächsten Überwachungszyklus generiert oder veraltet.

Auf globale Statusschwellenwerte kann im linken Navigationsmenü über den Abschnitt Ereignisschwellenwerte zugegriffen werden. Sie können Schwellwerteinstellungen für einzelne Objekte auch auf der Bestandsseite oder auf der Detailseite für das Objekt ändern.

Wahlmöglichkeiten

- Konfigurieren von globalen Integritätsschwellenwerten für das Aggregat

  Sie können die Statusschwellenwerte für Kapazität, Wachstum und Snapshot Kopien für alle Aggregate konfigurieren, damit bei Schwellenwertverletzungen eine Spur verfolgt wird.

- Konfigurieren von globalen Schwellenwerten für den Zustand des Volumes

  Sie können die Statusschwellenwerte für Kapazität, Snapshot Kopien, qtree Kontingente, Volume-Wachstum, Reserve überschreiben, Und Inodes für alle Volumes, um jede Schwellenverletzung zu verfolgen.

- Konfigurieren von globalen qtree-Zustandsschwellenwerten

  Sie können die Statusschwellenwerte für die Kapazität für alle qtrees bearbeiten, um Schwellenwertverletzungen nachzuverfolgen.

- Bearbeiten von Verzögerungszustands-Schwellenwerten für nicht verwaltete Schutzbeziehungen

  Sie können den prozentualen Anteil an Warn- oder Fehlerverzögerungen erhöhen oder reduzieren, sodass Ereignisse in Abständen erzeugt werden, die Ihren Anforderungen besser entsprechen.

Konfigurieren von globalen Integritätsschwellenwerten für das Aggregat

Sie können globale Statusschwellenwerte für alle Aggregate konfigurieren, um eine Schwellenwertverletzung zu verfolgen. Angemessene Ereignisse werden für Schwellenverletzungen generiert und Sie können auf dieser Grundlage vorbeugende Maßnahmen ergreifen. Sie können die globalen Werte basierend auf den Best-Practice-Einstellungen für Schwellenwerte konfigurieren, die für alle überwachten Aggregate gelten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Wenn Sie die Optionen global konfigurieren, werden die Standardwerte der Objekte geändert. Wenn jedoch die Standardwerte auf Objektebene geändert wurden, werden die globalen Werte nicht geändert.

Die Schwellenwertoptionen verfügen über Standardwerte für eine bessere Überwachung, Sie können diese jedoch an die Anforderungen Ihrer Umgebung anpassen.

Wenn Autogrow auf Volumes im Aggregat aktiviert ist, gilt die Kapazitätsschwellenwerte für die Aggregat basierend auf der durch Autogrow festgelegten maximalen Volume-Größe, nicht jedoch auf der ursprünglichen Volume-Größe.

Systemzustandsschwellenwerte gelten nicht für das Root-Aggregat des Nodes.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisschwellenwerte** > **Aggregat**.
2. Konfigurieren Sie die entsprechenden Schwellenwerte für Kapazität, Wachstum und Snapshot-Kopien.
3. Klicken Sie Auf **Speichern**.

Konfigurieren von globalen Schwellenwerten für den Zustand des Volumes

Sie können die globalen Schwellenwerte für den Zustand für alle Volumes konfigurieren, um eine Schwellenverletzung zu verfolgen. Geeignete Ereignisse werden zum Erreichen von Gesundheitsschwellenwerten generiert und anhand dieser Ereignisse können vorbeugende Maßnahmen ergriffen werden. Sie können die globalen Werte basierend auf den Best-Practice-Einstellungen für Schwellenwerte konfigurieren, die für alle überwachten Volumes gelten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die meisten Schwellenwertoptionen verfügen über Standardwerte für eine bessere Überwachung. Sie können die Werte jedoch entsprechend den Anforderungen Ihrer Umgebung ändern.

Beachten Sie, dass bei Aktivierung von Autogrow auf einem Volume die Kapazitätsschwellenwerte basierend auf der durch Autogrow festgelegten maximalen Volume-Größe gelten und nicht auf der ursprünglichen Volume-Größe basieren.

Der Standardwert von 1000 Snapshot Kopien ist nur für FlexVol Volumes anwendbar, wenn die ONTAP Version 9.4 oder höher ist, und auf FlexGroup Volumes, wenn ONTAP Version 9.8 und höher ist. Bei Clustern, die mit älteren Versionen der ONTAP Software installiert sind, beträgt die maximale Anzahl 250 Snapshot Kopien pro Volume. Bei diesen älteren Versionen interpretiert Unified Manager diese Nummer 1000 (und eine beliebige Zahl zwischen 1000 und 250) als 250. Das bedeutet, dass Sie weiterhin Ereignisse erhalten, wenn die Anzahl der Snapshot-Kopien 250 erreicht. Wenn Sie diesen Schwellenwert für diese älteren Versionen auf weniger als 250 setzen möchten, müssen Sie hier in der Ansicht Gesundheit: Alle Volumen oder auf der Seite Volume / Health Details den Schwellenwert auf 250 oder niedriger einstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisschwellenwerte** > **Lautstärke**.
2. Konfigurieren Sie die entsprechenden Schwellenwerte für Kapazität, Snapshot-Kopien, qtree-Kontingente, Volume-Wachstum und Inodes.
3. Klicken Sie Auf **Speichern**.

Konfigurieren von globalen qtree-Zustandsschwellenwerten

Sie können die globalen Schwellenwerte für den Systemzustand für alle qtrees konfigurieren, um Schwellenverletzungen zu verfolgen. Geeignete Ereignisse werden zum Erreichen von Gesundheitsschwellenwerten generiert und anhand dieser Ereignisse können vorbeugende Maßnahmen ergriffen werden. Sie können die globalen Werte anhand der Best Practice-Einstellungen für Schwellenwerte konfigurieren, die für alle überwachten qtrees gelten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die Schwellenwertoptionen verfügen über Standardwerte für eine bessere Überwachung, Sie können diese jedoch an die Anforderungen Ihrer Umgebung anpassen.

Ereignisse werden nur dann für einen qtree erzeugt, wenn ein qtree Kontingent oder eine Standard-Quote auf dem qtree festgelegt wurde. Ereignisse werden nicht generiert, wenn der in einem Benutzerkontingent oder Gruppenkontingent definierte Speicherplatz den Schwellenwert überschritten hat.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisschwellenwerte** > **qtree**.
2. Konfigurieren Sie die entsprechenden Kapazitätsschwellenwerte.
3. Klicken Sie Auf **Speichern**.

Konfigurieren von Verzögerungsschwellenwerten für nicht verwaltete Schutzbeziehungen

Sie können die Einstellungen für die globale Standard-Verzögerungswarnung und Fehlerzustandsschwellenwerte für nicht verwaltete Schutzbeziehungen bearbeiten, so dass Ereignisse in Abständen erzeugt werden, die Ihren Anforderungen entsprechen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die Verzögerungszeit darf nicht länger als das festgelegte Transferzeitintervall sein. Wenn der Transfer-Zeitplan beispielsweise stündlich ist, darf die Verzögerungszeit nicht mehr als eine Stunde sein. Der lag-Schwellenwert gibt einen Prozentsatz an, der die Verzögerungszeit nicht überschreiten darf. Mit dem Beispiel einer Stunde, wenn der lag-Schwellenwert als 150 % definiert ist, erhalten Sie ein Ereignis, wenn die Verzögerungszeit mehr als 1.5 Stunden beträgt.

Die in dieser Aufgabe beschriebenen Einstellungen werden global auf alle nicht verwalteten Schutzbeziehungen angewendet. Die Einstellungen können nicht nur auf eine nicht verwaltete Schutzbeziehung festgelegt und angewendet werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisschwellenwerte** > **Beziehung**.
2. Erhöhen oder verringern Sie je nach Bedarf den globalen Standard-Warn- oder Fehlerverzögerungsgrad.
3. Um die Auslösung eines Warn- oder Fehlerereignisses aus einem beliebigen Verzögerungsschwellenwert zu deaktivieren, deaktivieren Sie das Feld neben **enabled**.
4. Klicken Sie Auf **Speichern**.

Bearbeiten einzelner Zustandsschwellenwerte für das Aggregat

Sie können die Statusschwellenwerte für Aggregatskapazität, Wachstum und Snapshot Kopien eines oder mehrerer Aggregate bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnungen erzeugt und Sie erhalten Benachrichtigungen. Diese Benachrichtigungen helfen Ihnen, auf Basis des generierten Ereignisses vorbeugende Maßnahmen zu ergreifen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Basierend auf Änderungen an den Schwellenwerten werden Ereignisse im nächsten Überwachungszyklus generiert oder veraltet.

Wenn Autogrow auf Volumes im Aggregat aktiviert ist, gilt die Kapazitätsschwellenwerte für die Aggregat basierend auf der durch Autogrow festgelegten maximalen Volume-Größe, nicht jedoch auf der ursprünglichen Volume-Größe.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Aggregate**.
2. Wählen Sie in der Ansicht **Health: Alle Aggregate** einen oder mehrere Aggregate aus und klicken Sie dann auf **Schwellenwerte bearbeiten**.
3. Bearbeiten Sie im Dialogfeld **Aggregat Schwellenwerte bearbeiten** die Schwellenwerteinstellungen eines der folgenden Optionen: Kapazität, Wachstum oder Snapshot Kopien, indem Sie das entsprechende Kontrollkästchen aktivieren und dann die Einstellungen ändern.
4. Klicken Sie Auf **Speichern**.

Bearbeiten von Schwellenwerten für den Zustand einzelner Volumes

Sie können die Statusschwellenwerte für Volume-Kapazität, Wachstum, Kontingent und Speicherplatzreserve eines oder mehrerer Volumes bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnungen erzeugt und Sie erhalten Benachrichtigungen. Diese Benachrichtigungen helfen Ihnen, auf Basis des generierten Ereignisses vorbeugende Maßnahmen zu ergreifen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Basierend auf Änderungen an den Schwellenwerten werden Ereignisse im nächsten Überwachungszyklus generiert oder veraltet.

Beachten Sie, dass bei Aktivierung von Autogrow auf einem Volume die Kapazitätsschwellenwerte basierend auf der durch Autogrow festgelegten maximalen Volume-Größe gelten und nicht auf der ursprünglichen Volume-Größe basieren.

Der Standardwert von 1000 Snapshot Kopien ist nur für FlexVol Volumes anwendbar, wenn die ONTAP Version 9.4 oder höher ist, und auf FlexGroup Volumes, wenn ONTAP Version 9.8 und höher ist. Bei Clustern, die mit älteren Versionen der ONTAP Software installiert sind, beträgt die maximale Anzahl 250 Snapshot Kopien pro Volume. Bei diesen älteren Versionen interpretiert Unified Manager diese Nummer 1000 (und eine beliebige Zahl zwischen 1000 und 250) als 250. Das bedeutet, dass Sie weiterhin Ereignisse erhalten, wenn die Anzahl der Snapshot-Kopien 250 erreicht. Wenn Sie diesen Schwellenwert für diese älteren Versionen auf weniger als 250 setzen möchten, müssen Sie hier in der Ansicht Gesundheit: Alle Volumen oder auf der Seite Volume / Health Details den Schwellenwert auf 250 oder niedriger einstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie in der Ansicht **Health: Alle Volumes** ein oder mehrere Volumes aus und klicken Sie dann auf **Schwellenwerte bearbeiten**.
3. Bearbeiten Sie im Dialogfeld **Volume Schwellenwerte bearbeiten** die Schwellenwerteinstellungen eines der folgenden Werte: Kapazität, Snapshot-Kopien, qtree-Kontingent, Wachstum oder Inodes, indem Sie das entsprechende Kontrollkästchen aktivieren und dann die Einstellungen ändern.
4. Klicken Sie Auf **Speichern**.

Bearbeiten einzelner qtree-Statusschwellenwerte

Sie können die Statusschwellenwerte für qtree-Kapazität für eine oder mehrere qtrees bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnungen erzeugt und Sie erhalten Benachrichtigungen. Diese Benachrichtigungen helfen Ihnen, auf Basis des generierten Ereignisses vorbeugende Maßnahmen zu ergreifen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Basierend auf Änderungen an den Schwellenwerten werden Ereignisse im nächsten Überwachungszyklus generiert oder veraltet.

Schritte

1. Klicken Sie im linken Navigationsfenster auf **Storage** > **Qtrees**.
2. Wählen Sie in der Ansicht **Kapazität: Alle qtrees** eine oder mehrere qtrees aus und klicken Sie dann auf **Schwellenwerte bearbeiten**.
3. Ändern Sie im Dialogfeld **Qtree Schwellenwerte bearbeiten** die Kapazitätsschwellenwerte für den ausgewählten qtree oder qtrees und klicken Sie auf **Speichern**.

Auf der Seite Storage VM/Health Details können Sie auf der Registerkarte qtrees auch einzelne qtree-Schwellenwerte festlegen.

Verwalten von Zielen für die Cluster-Sicherheit

Unified Manager bietet ein Dashboard an, in dem die Sicherheit Ihrer ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes anhand der Empfehlungen ermittelt wird, die im *NetApp Security Hardening Guide for ONTAP 9* definiert wurden.

Ziel des Sicherheits-Dashboards ist es, Bereiche anzuzeigen, in denen die ONTAP Cluster nicht mit den von NetApp empfohlenen Richtlinien übereinstimmen, damit Sie die potenziellen Probleme beheben können. In den meisten Fällen werden Sie die Probleme mit dem ONTAP System Manager oder der ONTAP CLI beheben. Ihr Unternehmen befolgt möglicherweise nicht alle Empfehlungen, daher müssen Sie in einigen Fällen keine Änderungen vornehmen.

Detaillierte Empfehlungen und Entschließungen finden Sie im "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9" (TR-4569).

Zusätzlich zum Berichten des Sicherheitsstatus generiert Unified Manager auch Sicherheitsereignisse für alle Cluster oder SVMs mit Sicherheitsverletzungen. Sie können diese Probleme auf der Seite „Ereignismanagement-Bestand“ verfolgen und Warnmeldungen für diese Ereignisse so konfigurieren, dass Ihr Speicheradministrator benachrichtigt wird, wenn neue Sicherheitsereignisse auftreten.

Welche Sicherheitskriterien werden bewertet

Im Allgemeinen werden die Sicherheitskriterien für Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes im Vergleich zu den im „ *NetApp Security Hardening Guide for ONTAP 9*“ definierten Empfehlungen evaluiert.

Einige der Sicherheitsprüfungen umfassen:

- Gibt an, ob ein Cluster eine sichere Authentifizierungsmethode wie SAML verwendet
- Unabhängig davon, ob Peering-Cluster ihre Kommunikation verschlüsselt haben
- Gibt an, ob das Auditprotokoll auf einer Storage-VM aktiviert ist
- Ob Ihre Volumes eine Software- oder Hardwareverschlüsselung aktiviert haben

Ausführliche Informationen finden Sie in den Themen zu Compliance-Kategorien und im "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9" .

Auch Upgrade-Ereignisse, die von der Active IQ-Plattform gemeldet werden, gelten als Sicherheitsereignisse. Diese Ereignisse erkennen Probleme, wenn für die Lösung ein Upgrade der ONTAP Software, Node-Firmware oder Betriebssystemsoftware erforderlich ist (für Sicherheitsempfehlungen). Diese Ereignisse werden nicht im Fenster „Sicherheit“ angezeigt, sind aber auf der Seite „Ereignisverwaltung“ verfügbar.

Cluster-Compliance-Kategorien

In dieser Tabelle werden die Parameter für die Einhaltung der Cluster-Sicherheits-Compliance beschrieben, die von Unified Manager bewertet werden, die Empfehlung von NetApp und ob der Parameter sich auf die allgemeine Bestimmung des Clusters auswirkt, das eine Beschwerde ist oder nicht.

Die Verfügbarkeit nicht konformer SVMs auf einem Cluster wirkt sich auf den Compliance-Wert des Clusters aus. In einigen Fällen müssen Sie also möglicherweise ein Sicherheitsprobleme mit einer SVM beheben, bevor Ihre Cluster-Sicherheit konform erkannt wird.

Beachten Sie, dass nicht alle unten aufgeführten Parameter für alle Installationen angezeigt werden. Wenn Sie beispielsweise keine Peered Cluster haben oder AutoSupport auf einem Cluster deaktiviert haben, werden die Elemente Cluster Peering oder AutoSupport HTTPS Transport auf der UI-Seite nicht angezeigt.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
Globaler FIPS	Gibt an, ob der Compliance-Modus Global FIPS (Federal Information Processing Standard) 140-2 aktiviert oder deaktiviert ist. Wenn FIPS aktiviert ist, sind TLSv1 und SSLv3 deaktiviert und nur TLSv1.1 und TLSv1.2 zulässig.	Aktiviert	Ja.
Telnet	Gibt an, ob Telnet-Zugriff auf das System aktiviert oder deaktiviert ist. NetApp empfiehlt Secure Shell (SSH) für den sicheren Remote-Zugriff.	Deaktiviert	Ja.
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, z. B. Chiffren, die mit beginnen `*cbc`.	Nein	Ja.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
Anmelde-Banner	Zeigt an, ob das Anmeldebanner für Benutzer, die auf das System zugreifen, aktiviert oder deaktiviert ist.	Aktiviert	Ja.
Cluster-Peering	Gibt an, ob die Kommunikation zwischen Peering-Clustern verschlüsselt oder unverschlüsselt ist. Für diesen Parameter muss sowohl auf den Quell- als auch auf den Ziel-Clustern konfiguriert werden, damit er als konform betrachtet werden kann.	Verschlüsselt	Ja.
Network Time Protocol	Gibt an, ob das Cluster über einen oder mehrere konfigurierte NTP-Server verfügt. Aus Gründen der Redundanz und des besten Service empfiehlt NetApp, mindestens drei NTP-Server mit dem Cluster zu verknüpfen.	Konfiguriert	Ja.
OCSP	Gibt an, ob in ONTAP Anwendungen vorhanden sind, die nicht mit OCSP konfiguriert sind (Online Certificate Status Protocol) und daher keine Verschlüsselung der Kommunikation erfolgt. Die nicht kompatiblen Anwendungen werden aufgelistet.	Aktiviert	Nein
Remote Audit-Protokollierung	Gibt an, ob die Protokollweiterleitung (Syslog) verschlüsselt ist oder nicht verschlüsselt ist.	Verschlüsselt	Ja.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
AutoSupport HTTPS-Übertragung	Zeigt an, ob HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport Meldungen an den NetApp Support verwendet wird.	Aktiviert	Ja.
Standard-Admin-Benutzer	Gibt an, ob der standardmäßige Admin-Benutzer (integriert) aktiviert oder deaktiviert ist. NetApp empfiehlt, alle nicht benötigten integrierten Konten zu sperren (zu deaktivieren).	Deaktiviert	Ja.
SAML-Benutzer	Gibt an, ob SAML konfiguriert ist. Mit SAML können Sie Multi-Faktor-Authentifizierung (MFA) als Anmeldemethode für Single-Sign-On konfigurieren.	Keine Empfehlungen	Nein
Active Directory-Benutzer	Gibt an, ob Active Directory konfiguriert ist. Active Directory und LDAP sind die bevorzugten Authentifizierungsmechanismen für Benutzer, die auf Cluster zugreifen.	Keine Empfehlungen	Nein
LDAP-Benutzer	Gibt an, ob LDAP konfiguriert ist. Active Directory und LDAP sind die bevorzugten Authentifizierungsmechanismen für Benutzer, die Cluster über lokale Benutzer managen.	Keine Empfehlungen	Nein
Zertifikatbenutzer	Zeigt an, ob ein Zertifikatbenutzer zur Anmeldung beim Cluster konfiguriert ist.	Keine Empfehlungen	Nein

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
Lokale Benutzer	Zeigt an, ob lokale Benutzer für die Anmeldung am Cluster konfiguriert sind.	Keine Empfehlungen	Nein

SVM-Compliance-Kategorien

Diese Tabelle beschreibt die Compliance-Kriterien für die Storage Virtual Machine (SVM), die von Unified Manager bewertet werden, die NetApp Empfehlung und ob der Parameter sich auf die allgemeine Feststellung einer Beschwerde bzw. nicht auf eine Beschwerde des SVM auswirkt.

Parameter	Beschreibung	Empfehlung	Beeinträchtigt SVM-Compliance
Überwachungsprotokoll	Gibt an, ob die Überwachungsprotokollierung aktiviert oder deaktiviert ist.	Aktiviert	Ja.
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, z. B. Chiffren, die mit beginnen `cbc*`.	Nein	Ja.
Anmelde-Banner	Zeigt an, ob das Anmeldebanner für Benutzer, die auf SVMs im System zugreifen, aktiviert oder deaktiviert ist.	Aktiviert	Ja.
LDAP-Verschlüsselung	Gibt an, ob LDAP-Verschlüsselung aktiviert oder deaktiviert ist.	Aktiviert	Nein
NTLM-Authentifizierung	Gibt an, ob die NTLM-Authentifizierung aktiviert oder deaktiviert ist.	Aktiviert	Nein
LDAP Payload-Signatur	Gibt an, ob LDAP-Payload-Signatur aktiviert oder deaktiviert ist.	Aktiviert	Nein
CHAP-Einstellungen	Gibt an, ob CHAP aktiviert oder deaktiviert ist.	Aktiviert	Nein

Parameter	Beschreibung	Empfehlung	Beeinträchtigt SVM-Compliance
Kerberos V5	Gibt an, ob die Kerberos-V5-Authentifizierung aktiviert oder deaktiviert ist.	Aktiviert	Nein

Volume Compliance-Kategorien

Diese Tabelle beschreibt die Verschlüsselungsparameter des Volumes, die von Unified Manager geprüft werden, um zu ermitteln, ob die Daten auf Ihren Volumes vor dem Zugriff durch unbefugte Benutzer angemessen geschützt sind.

Zu beachten ist, dass die Verschlüsselungsparameter des Volumes keine Auswirkung haben, ob das Cluster oder die Storage-VM als konform betrachtet wird.

Parameter	Beschreibung
Softwareverschlüsselung	Zeigt die Anzahl der Volumes an, die mit Softwarelösungen für die NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) gesichert sind.
Hardware Verschlüsselt	Zeigt die Anzahl der Volumes an, die mit NSE-Hardwareverschlüsselung (NetApp Storage Encryption) gesichert sind.
Verschlüsselt für Software und Hardware	Zeigt die Anzahl der Volumes an, die sowohl durch Software- als auch durch Hardwareverschlüsselung geschützt sind.
Nicht Verschlüsselt	Zeigt die Anzahl der nicht verschlüsselten Volumes an.

Was bedeutet nicht, dass Compliance-Anforderungen erfüllt werden

Cluster und Storage Virtual Machines (SVMs) gelten als nicht kompatibel, wenn eine der untersuchten Sicherheitskriterien den im *NetApp Security Hardening Guide for ONTAP 9* definierten Empfehlungen entsprechen. Darüber hinaus gilt ein Cluster als nicht kompatibel, wenn eine SVM als nicht konform gekennzeichnet ist.

Die Statussymbole in den Sicherheitskarten haben in Bezug auf ihre Konformität die folgende Bedeutung:

- - Der Parameter ist wie empfohlen konfiguriert.
- - Der Parameter ist nicht wie empfohlen konfiguriert.
- - Entweder die Funktion ist auf dem Cluster nicht aktiviert oder der Parameter wurde nicht als empfohlen konfiguriert, aber dieser Parameter trägt nicht zur Compliance des Objekts bei.

Beachten Sie, dass der Volume-Verschlüsselungsstatus nicht dazu beiträgt, ob das Cluster oder die SVM als konform betrachtet werden.

Anzeigen des Sicherheitsstatus eines Clusters im hohen Level

Das Security Panel im Unified ManagerDashboard zeigt abhängig von der aktuellen Ansicht den allgemeinen Sicherheitsstatus aller Cluster oder für ein einzelnes Cluster an.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Je nachdem, ob Sie den Sicherheitsstatus für alle überwachten Cluster oder für einen einzelnen Cluster anzeigen möchten, wählen Sie **Alle Cluster** oder wählen Sie einen einzelnen Cluster aus dem Dropdown-Menü aus.
3. Öffnen Sie das Fenster **Sicherheit**, um den Gesamtstatus anzuzeigen.

   In diesem Fenster wird Folgendes angezeigt:

   - Eine Liste der Sicherheitsereignisse, die in den letzten 24 Stunden eingehen
   - Ein Link von jeder dieser Veranstaltungen zur Seite Veranstaltungsdetails
   - Ein Link, mit dem Sie alle aktiven Sicherheitsereignisse auf der Seite „Ereignisverwaltung“ anzeigen können
   - Cluster-Sicherheitsstatus (Anzahl an kompatiblen oder nicht kompatiblen Clustern)
   - Der SVM-Sicherheitsstatus (Anzahl an konformen oder nicht konformen SVMs)
   - Status der Volume-Verschlüsselung (Anzahl der verschlüsselten oder nicht verschlüsselten Volumes)
4. Klicken Sie auf den Rechtspfeil oben im Bedienfeld, um die Sicherheitsinformationen auf der Seite **Sicherheit** anzuzeigen.

Anzeigen des detaillierten Sicherheitsstatus für Cluster und SVMs

Die Seite Sicherheit zeigt den allgemeinen Sicherheitsstatus aller Cluster sowie einen detaillierten Sicherheitsstatus für einzelne Cluster an. Der detaillierte Cluster-Status umfasst Cluster-Compliance, SVM-Compliance und Volume-Verschlüsselung.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Je nachdem, ob Sie den Sicherheitsstatus für alle überwachten Cluster oder für einen einzelnen Cluster anzeigen möchten, wählen Sie **Alle Cluster** oder wählen Sie einen einzelnen Cluster aus dem Dropdown-Menü aus.
3. Klicken Sie im Fenster **Sicherheit** auf den Rechtspfeil.

   Auf der Seite Sicherheit werden die folgenden Informationen angezeigt:

   - Cluster-Sicherheitsstatus (Anzahl an kompatiblen oder nicht kompatiblen Clustern)
   - Der SVM-Sicherheitsstatus (Anzahl an konformen oder nicht konformen SVMs)
   - Status der Volume-Verschlüsselung (Anzahl der verschlüsselten oder nicht verschlüsselten Volumes)

- Die Cluster-Authentifizierungsmethoden, die in den einzelnen Clustern verwendet werden

4. Eine Anleitung, wie Sie alle Ihre Cluster, SVMs und Volumes mit den NetApp Sicherheitsempfehlungen konform gestalten, finden Sie im "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9" .

Anzeigen von Sicherheitsereignissen, für die möglicherweise Software- oder Firmware-Updates erforderlich sind

Es gibt bestimmte Sicherheitsereignisse, die einen Impact-Bereich von „`Upgrade`“ haben. Diese Ereignisse werden von der Active IQ Plattform gemeldet. Sie erkennen Probleme, wenn für die Lösung ein Upgrade der ONTAP Software, der Node-Firmware oder der Betriebssystemsoftware (für Sicherheitsempfehlungen) erforderlich ist.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Möglicherweise möchten Sie für einige dieser Probleme sofortige Korrekturmaßnahmen durchführen, während andere Probleme möglicherweise bis zur nächsten geplanten Wartung warten können. Sie können alle diese Ereignisse anzeigen und sie Benutzern zuweisen, die die Probleme lösen können. Außerdem können Sie anhand dieser Liste bestimmte Ereignisse für Sicherheitsaspekte identifizieren, über die Sie keine Benachrichtigung erhalten möchten, damit Sie diese Ereignisse deaktivieren können.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**.

   Standardmäßig werden alle aktiven (neuen und bestätigten) Ereignisse auf der Seite „Ereignismanagement-Bestand“ angezeigt.

2. Wählen Sie im Menü Ansicht die Option **Ereignisse aktualisieren** aus.

   Auf der Seite werden alle aktiven Sicherheitsereignisse für Upgrades angezeigt.

Anzeige des Managements der Benutzerauthentifizierung auf allen Clustern

Auf der Seite Sicherheit werden die Authentifizierungstypen angezeigt, die zur Authentifizierung von Benutzern in jedem Cluster verwendet werden, sowie die Anzahl der Benutzer, die mit jedem Typ auf das Cluster zugreifen. So können Sie überprüfen, ob die Benutzerauthentifizierung gemäß den Anforderungen Ihres Unternehmens sicher durchgeführt wird.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Wählen Sie oben im Dashboard im Dropdown-Menü * Alle Cluster* aus.
3. Klicken Sie im Fenster **Sicherheit** auf den rechten Pfeil, und die Seite **Sicherheit** wird angezeigt.
4. Zeigen Sie die **Cluster Authentication**-Karte an, um die Anzahl der Benutzer anzuzeigen, die mit jedem

Authentifizierungstyp auf das System zugreifen.

5. Zeigen Sie die **Cluster Security**-Karte an, um die Authentifizierungsmechanismen anzuzeigen, die zur Authentifizierung von Benutzern in jedem Cluster verwendet werden.

Ergebnisse

Wenn einige Benutzer über eine unsichere Methode auf das System zugreifen oder eine Methode verwenden, die von NetApp nicht empfohlen wird, können Sie die Methode deaktivieren.

Anzeigen des Verschlüsselungsstatus aller Volumes

Sie können eine Liste aller Volumes und ihren aktuellen Verschlüsselungsstatus anzeigen, um zu ermitteln, ob die Daten auf Ihren Volumes vor dem Zugriff durch nicht autorisierte Benutzer angemessen geschützt sind.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Auf ein Volume können folgende Verschlüsselungsarten angewendet werden:

- Software – Volumes, die mit Hilfe von NetApp Volume Encryption (NVE) oder NetApp Software-Verschlüsselungslösungen (NAE) gesichert werden.
- Hardware – Volumes, die mit der Hardware-Verschlüsselung von NetApp Storage Encryption (NSE) gesichert werden.
- Software- und Hardware-Volumes, die sowohl durch Software- als auch durch Hardware-Verschlüsselung geschützt sind.
- Keine - Volumen, die nicht verschlüsselt sind.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü **Ansicht** die Option **Gesundheit** > **Volumen-Verschlüsselung**
3. Sortieren Sie in der Ansicht **Health: Volumes Encryption** das Feld**Encryption Type**, oder verwenden Sie den Filter, um Volumes anzuzeigen, die einen bestimmten Verschlüsselungstyp haben, oder die nicht verschlüsselt sind (Verschlüsselungstyp von “None”).

Anzeigen aller aktiven Sicherheitsereignisse

Sie können alle aktiven Sicherheitsereignisse anzeigen und sie anschließend einem Benutzer zuweisen, der das Problem lösen kann. Wenn bestimmte Sicherheitsereignisse vorliegen, die Sie nicht empfangen möchten, kann Ihnen diese Liste helfen, die Ereignisse zu identifizieren, die Sie deaktivieren möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**.

   Standardmäßig werden neue und bestätigte Ereignisse auf der Seite „Ereignismanagement-Bestand“ angezeigt.

2. Wählen Sie im Menü Ansicht die Option **Aktive Sicherheitsereignisse** aus.

   Auf der Seite werden alle neuen und bestätigten Sicherheitsereignisse angezeigt, die in den letzten 7 Tagen generiert wurden.

Hinzufügen von Warnmeldungen für Sicherheitsereignisse

Sie können Benachrichtigungen für einzelne Sicherheitsereignisse so konfigurieren, wie es auch bei allen anderen Ereignissen, die Unified Manager empfangen hat. Wenn Sie außerdem alle Sicherheitsereignisse gleich behandeln und E-Mails an dieselbe Person senden möchten, können Sie eine einzelne Benachrichtigung erstellen, um Sie darüber zu informieren, wenn Sicherheitsereignisse ausgelöst werden.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Das folgende Beispiel zeigt, wie eine Warnung für das Sicherheitsereignis „`Telnet Protocol Enabled`“ erstellt wird. Dadurch wird eine Meldung ausgegeben, wenn ein Telnet-Zugriff für den Remote-Administratorzugriff auf das Cluster konfiguriert ist. Sie können diese Methode verwenden, um Warnungen für alle Sicherheitsereignisse zu erstellen.

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 den Cluster oder den Cluster aus, auf dem Sie diese Warnung aktivieren möchten.
5. Klicken Sie auf **Events** und führen Sie die folgenden Aktionen aus:
   a. Wählen Sie in der Liste Ereignis Severity die Option **Warnung** aus.
   b. Wählen Sie in der Liste passende Ereignisse die Option **Telnet-Protokoll aktiviert**.
6. Klicken Sie auf **Aktionen** und wählen Sie dann den Namen des Benutzers aus, der die Benachrichtigung per E-Mail im Feld * Diese Benutzer benachrichtigen* erhält.
7. Konfigurieren Sie alle anderen Optionen auf dieser Seite, um die Benachrichtigungshäufigkeit zu erhöhen, SNMP-Taps auszugeben und ein Skript auszuführen.
8. Klicken Sie Auf **Speichern**.

Bestimmte Sicherheitsereignisse deaktivieren

Standardmäßig sind alle Ereignisse aktiviert. Sie können bestimmte Ereignisse deaktivieren, um die Generierung von Benachrichtigungen für Ereignisse zu verhindern, die in Ihrer Umgebung nicht wichtig sind. Sie können Ereignisse aktivieren, die deaktiviert sind, wenn Sie den Empfang von Benachrichtigungen für sie fortsetzen möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Wenn Sie Ereignisse deaktivieren, werden die zuvor generierten Ereignisse im System als veraltet markiert und die für diese Ereignisse konfigurierten Warnmeldungen werden nicht ausgelöst. Wenn Sie deaktivierte Ereignisse aktivieren, werden die Benachrichtigungen für diese Ereignisse mit dem nächsten Überwachungszyklus generiert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Event-Setup**.
2. Deaktivieren oder aktivieren Sie auf der Seite * Event Setup* Ereignisse, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren von Ereignissen	a. Klicken Sie Auf **Deaktivieren**. b. Wählen Sie im Dialogfeld Ereignisse deaktivieren den Schweregrad * Warnung* aus. Dies ist die Kategorie für alle Sicherheitsereignisse. c. Wählen Sie in der Spalte Abpassende Ereignisse die zu deaktivierenden Sicherheitsereignisse aus, und klicken Sie dann auf den rechten Pfeil, um diese Ereignisse in die Spalte Ereignisse deaktivieren zu verschieben. d. Klicken Sie auf **Speichern und Schließen**. e. Stellen Sie sicher, dass die deaktivierten Ereignisse in der Listenansicht der Seite Event Setup angezeigt werden.
Aktivieren von Ereignissen	a. Aktivieren Sie in der Liste der deaktivierten Ereignisse das Kontrollkästchen für das Ereignis oder die Ereignisse, die Sie erneut aktivieren möchten. b. Klicken Sie Auf **Aktivieren**.

Sicherheitsereignisse

Sicherheitsereignisse ermöglichen Ihnen Informationen zum Sicherheitsstatus von ONTAP Clustern, Storage Virtual Machines (SVMs) und Volumes auf der Grundlage von Parametern, die im „ *NetApp Security Hardening Guide for ONTAP 9*“ definiert sind. Diese Ereignisse benachrichtigen Sie über potenzielle Probleme, sodass Sie den Schweregrad Ihrer Maßnahmen überprüfen und das Problem ggf. beheben können.

Sicherheitsereignisse werden nach Quelltyp gruppiert und enthalten den Ereignis- und Trap-Namen, den Impact-Level und den Schweregrad. Diese Ereignisse werden in den Ereigniskategorien für Cluster und Storage-VMs angezeigt.

Managen von Backup- und Restore-Vorgängen

Sie können Backups von Unified Manager erstellen und die Wiederherstellungsfunktion verwenden, um das Backup im Falle eines Systemausfalls oder Datenverlust auf dasselbe (lokales) System oder ein neues (Remote-) System wiederherzustellen.

Je nach Betriebssystem, auf dem Sie Unified Manager installiert haben, und basierend auf der Anzahl der zu verwaltenden Cluster und Nodes gibt es drei Backup- und Restore-Methoden:

Betriebssystem	Größe der Implementierung	Empfohlene Sicherungsmethode
VMware vSphere	Alle	VMware Snapshot der virtuellen Unified Manager Appliance
Red hat Enterprise Linux oder CentOS Linux	Klein	Unified Manager MySQL Datenbank-Dump
	Groß	NetApp Snapshot der Unified Manager Datenbank
Microsoft Windows	Alle	Unified Manager MySQL Datenbank-Dump

Diese verschiedenen Methoden werden in den folgenden Abschnitten beschrieben.

Backup- und Wiederherstellungsprozess für die virtuelle Appliance

Das Backup- und Restore-Modell für Unified Manager, wenn es auf einer virtuellen Appliance installiert ist, besteht darin, ein Image der gesamten virtuellen Applikation zu erfassen und wiederherzustellen.

Mit den folgenden Aufgaben können Sie ein Backup der virtuellen Appliance durchführen:

1. Schalten Sie die VM aus und erstellen Sie einen VMware Snapshot der virtuellen Unified Manager Appliance.
2. Erstellen Sie eine NetApp Snapshot Kopie auf dem Datenspeicher, um den VMware Snapshot zu erfassen.

Wenn der Datastore nicht auf einem System mit ONTAP-Software gehostet wird, befolgen Sie die Richtlinien des Storage-Anbieters, um ein Backup des VMware-Snapshots zu erstellen.

3. Replizierung der NetApp Snapshot Kopie (oder vergleichbarer Snapshot) in einem alternativen Storage
4. Löschen Sie den VMware Snapshot.

Sie sollten einen Backup-Zeitplan anhand dieser Aufgaben implementieren, um sicherzustellen, dass die virtuelle Unified Manager Appliance im Falle eines Problems geschützt ist.

Zum Wiederherstellen der VM können Sie den von Ihnen erstellten VMware Snapshot verwenden, um die VM auf den Point-in-Time-Zustand des Backups wiederherzustellen.

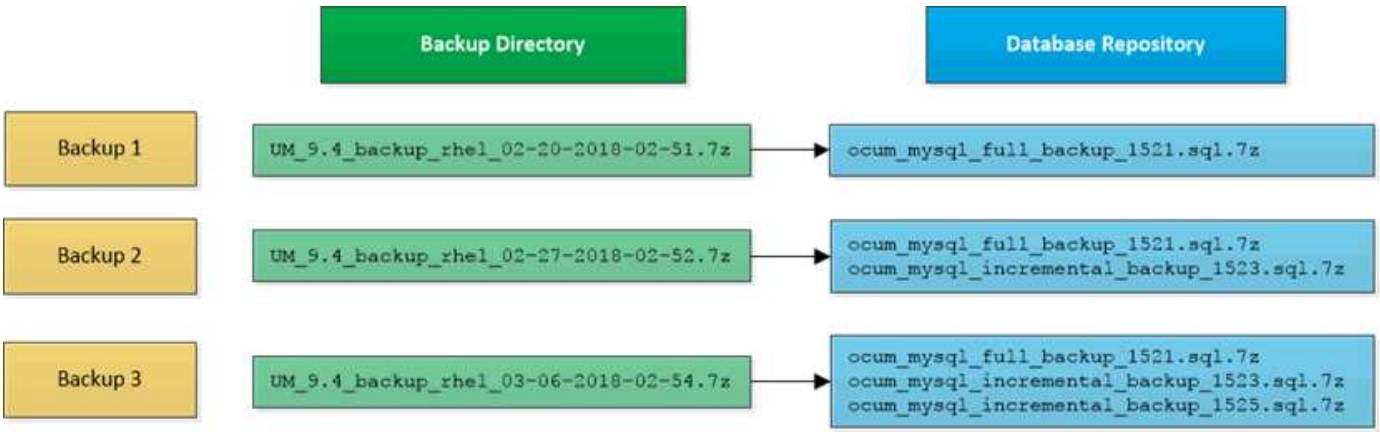
Sichern und Wiederherstellen mithilfe eines MySQL Datenbank-Dump

Ein MySQL Datenbank Dump Backup ist eine Kopie der Unified Manager-Datenbank und Konfigurationsdateien, die Sie im Falle eines Systemausfalls oder Datenverlust verwenden können. Sie können ein Backup so planen, dass es auf ein lokales Ziel oder auf ein Remote-Ziel geschrieben wird. Es wird dringend empfohlen, einen Remote-Standort außerhalb des Unified Manager Host-Systems zu definieren.

MySQL Datenbank Dump ist der Standard-Backup-Mechanismus, wenn Unified Manager auf einem Linux- und Windows-Server installiert ist. Bei Red hat Enterprise Linux oder CentOS Linux Systemen können Sie die Backup-Methode von NetApp Snapshot verwenden, wenn Unified Manager eine große Anzahl von Clustern und Knoten verwaltet oder wenn Ihre MySQL Backups mehrere Stunden in Anspruch nehmen.

Ein Datenbank-Dump-Backup besteht aus einer einzelnen Datei im Sicherungsverzeichnis und einer oder mehreren Dateien im Datenbank-Repository-Verzeichnis. Die Datei im Backup-Verzeichnis ist sehr klein, da sie nur einen Zeiger auf die Dateien enthält, die sich im Datenbank-Repository-Verzeichnis befinden und für die Wiederherstellung des Backups benötigt werden.

Beim ersten Generieren einer Datenbanksicherung wird im Backup-Verzeichnis eine einzelne Datei erstellt und im Datenbank-Repository-Verzeichnis eine vollständige Sicherungsdatei erstellt. Wenn Sie das nächste Mal ein Backup erstellen, wird im Backup-Verzeichnis eine einzelne Datei erstellt und im Datenbank-Repository-Verzeichnis eine inkrementelle Sicherungsdatei erstellt, die die Unterschiede zur vollständigen Backup-Datei enthält. Dieser Prozess wird bei der Erstellung zusätzlicher Backups bis zur Einstellung für maximale Aufbewahrung fortgesetzt, wie in der folgenden Abbildung dargestellt.



Benennen Sie die Sicherungsdateien in diesen beiden Verzeichnissen nicht um, oder entfernen Sie sie nicht. Bei einem späteren Wiederherstellungsvorgang schlägt dies fehl.

Wenn Sie Ihre Sicherungsdateien in das lokale System schreiben, sollten Sie einen Prozess starten, um die Backup-Dateien an einen Remote-Standort zu kopieren, damit sie verfügbar sind, falls Sie ein Systemproblem haben, das eine vollständige Wiederherstellung erfordert.

Vor Beginn eines Backup-Vorgangs führt Unified Manager eine Integritätsprüfung durch, um zu überprüfen, ob alle erforderlichen Backup-Dateien und Backup-Verzeichnisse vorhanden sind und beschreibbar sind. Außerdem wird überprüft, ob genügend Speicherplatz auf dem System vorhanden ist, um die Backup-Datei zu erstellen.

Beachten Sie, dass Sie ein Backup nur auf derselben Version von Unified Manager wiederherstellen können. Wenn Sie beispielsweise ein Backup auf Unified Manager 9.7 erstellt haben, kann das Backup nur auf Unified Manager 9.7 Systemen wiederhergestellt werden.

Konfigurieren des Ziels und Planen für Datenbank-Dump-Backups

Sie können die Backup-Einstellungen für die Backup-Dump-Datenbank von Unified Manager konfigurieren, um den Datenbank-Backup-Pfad, die Aufbewahrungsanzahl und den Backup-Zeitplan festzulegen. Sie können tägliche oder wöchentliche geplante Backups aktivieren. Standardmäßig werden geplante Backups deaktiviert, Sie sollten jedoch einen Backup-Zeitplan festlegen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen mindestens 150 GB Speicherplatz an dem Speicherort haben, den Sie als Backup-Pfad definieren.

  Es wird empfohlen, einen externen Standort zu verwenden, der sich außerhalb des Unified Manager-Hostsystems befindet.

- Wenn Unified Manager auf einem Linux-System installiert ist, stellen Sie sicher, dass der Benutzer „`jboss`“ über Schreibberechtigungen in das Backup-Verzeichnis verfügt.
- Sie sollten Backup-Vorgänge nicht so planen, dass sie unmittelbar nach dem Hinzufügen eines neuen Clusters ausgeführt werden, während Unified Manager historische Performance-Daten von 15 Tagen erfasst.

Über diese Aufgabe

Mehr Zeit wird bei der ersten Durchführung eines Backups als bei nachfolgenden Backups benötigt, da es sich bei dem ersten Backup um ein Vollbackup handelt. Ein vollständiges Backup kann über 1 GB dauern und kann drei bis vier Stunden dauern. Nachfolgende Backups sind inkrementell und erfordern weniger Zeit.

Wenn Sie feststellen, dass die Anzahl der inkrementellen Backup-Dateien für den von Ihnen für Backups zugewiesenen Platz zu groß wird, können Sie regelmäßig ein neues vollständiges Backup erstellen, um das alte vollständige Backup und alle untergeordneten inkrementellen Dateien zu ersetzen. Als weitere Option möchten Sie die NetApp Snapshot Backup-Methode nutzen, wenn Unified Manager auf einem Linux-System installiert ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Datenbank-Backup**.
2. Klicken Sie auf der Seite **Datenbank-Backup** auf **Backup-Einstellungen**.
3. Konfigurieren Sie die entsprechenden Werte für einen Backup-Pfad, eine Aufbewahrungsanzahl und einen Zeitplan.

   Der Standardwert für die Aufbewahrungsanzahl ist 10; Sie können 0 verwenden, um unbegrenzte Backups zu erstellen.

4. Wählen Sie die Schaltfläche **geplante tägliche** oder **geplante Woche** und geben Sie die Terminplandetails an.
5. Klicken Sie Auf **Anwenden**.

Ergebnisse

Backup-Dateien mit einem Datenbankdump werden auf Grundlage des Zeitplans erstellt. Die verfügbaren Sicherungsdateien finden Sie auf der Seite Datenbank-Backup.

Verwandte Informationen

"Wie man eine neue inkrementelle Backup-Kette innerhalb von Active IQ Unified Manager startet"

Was ist ein Datenbank-Restore

Bei einer Wiederherstellung einer MySQL Datenbank wird eine vorhandene Unified Manager Backup-Datei auf demselben oder einem anderen Unified Manager Server wiederhergestellt. Sie führen die Wiederherstellung über die Unified Manager-Wartungskonsole aus.

Wenn Sie einen Wiederherstellungsvorgang auf demselben (lokalen) System durchführen und die Sicherungsdateien alle lokal gespeichert sind, können Sie die Wiederherstellungsoption über den Standardspeicherort ausführen. Wenn Sie eine Wiederherstellung auf einem anderen Unified Manager-System (einem Remote-System) durchführen, müssen Sie die Sicherungsdatei oder Dateien vom sekundären Speicher auf die lokale Festplatte kopieren, bevor Sie die Wiederherstellungsoption ausführen.

Während des Wiederherstellungsprozesses werden Sie von Unified Manager abgemeldet. Sie können sich nach Abschluss der Wiederherstellung beim System anmelden.

Die Wiederherstellungsfunktion ist versionsspezifisch und plattformspezifisch. Sie können ein Unified Manager MySQL Backup nur auf derselben Version von Unified Manager wiederherstellen. Unified Manager unterstützt Backup und Restore in den folgenden Plattformszenarien:

- Backup der virtuellen Appliance auf Red hat Enterprise Linux oder CentOS
- Sicherung von Red hat oder CentOS Linux auf Red hat Enterprise Linux oder CentOS
- Windows Backup auf Windows

Wenn Sie das Backup-Image auf einem neuen Server wiederherstellen, müssen Sie nach Abschluss des Wiederherstellungsvorgangs ein neues HTTPS-Sicherheitszertifikat generieren und den Unified Manager-Server neu starten. Wenn Sie das Backup-Image auf einem neuen Server wiederherstellen müssen, müssen Sie auch SAML-Authentifizierungseinstellungen neu konfigurieren.

Alte Sicherungsdateien können nicht verwendet werden, um ein Image wiederherzustellen, nachdem Unified Manager auf eine neuere Softwareversion aktualisiert wurde. Um Speicherplatz zu sparen, werden alle alten Backupdateien außer der neuesten Datei beim Upgrade von Unified Manager automatisch entfernt.

Wiederherstellen einer Sicherung einer MySQL-Datenbank auf einem Linux-System

Im Falle eines Datenverlustes oder einer Beschädigung von Daten können Sie Unified Manager in den vorherigen stabilen Zustand bei minimalem Datenverlust wiederherstellen. Sie können die Unified Manager-Datenbank über die Unified Manager-Wartungskonsole auf einem lokalen oder entfernten Red hat Enterprise Linux- oder CentOS-System wiederherstellen.

Bevor Sie beginnen

- Sie müssen über die Stammbenutzeranmeldeinformationen für den Linux-Host verfügen, auf dem Unified Manager installiert ist.
- Sie müssen über eine Benutzer-ID und ein Passwort verfügen, um sich bei der Wartungskonsole des Unified Manager-Servers anzumelden.
- Sie müssen die Backup-Datei von Unified Manager und den Inhalt des Datenbank-Repository-Verzeichnisses auf das System kopiert haben, auf dem Sie den Wiederherstellungsvorgang ausführen möchten.

  Es wird empfohlen, die Sicherungsdatei in das Standardverzeichnis zu kopieren `/data/ocum-backup`. Die Datenbank-Repository-Dateien müssen in die kopiert werden `/database-dumps-repo` Unterverzeichnis unter dem `/ocum-backup` Verzeichnis.

- Die Sicherungsdateien müssen aus sein `.7z` Typ.

Über diese Aufgabe

Die Wiederherstellungsfunktion ist plattformspezifisch und versionsspezifisch. Sie können ein Unified Manager-Backup nur auf derselben Version von Unified Manager wiederherstellen. Sie können eine Sicherungsdatei für Linux oder eine Sicherungsdatei einer virtuellen Appliance auf einem Red hat Enterprise Linux oder CentOS System wiederherstellen.

Wenn der Name des Sicherungsordners ein Leerzeichen enthält, müssen Sie den absoluten Pfad oder den relativen Pfad in doppelte Anführungszeichen einschließen.

Schritte

1. Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager die UI nicht oder konfigurieren Sie nach Abschluss der Installation keine Cluster, Benutzer oder Authentifizierungseinstellungen. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.
2. Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domänennamen des Unified Manager-Systems her.
3. Melden Sie sich beim System mit dem Wartungs-Benutzer (umadmin) und dem Passwort an.
4. Geben Sie den Befehl ein `maintenance_console` Und drücken Sie die Eingabetaste.

5. Geben Sie in der Wartungskonsole **Hauptmenü** die Nummer für die Option **Backup Restore** ein.
6. Geben Sie die Nummer für die * MySQL-Sicherung wiederherstellen* ein.
7. Geben Sie bei entsprechender Aufforderung den absoluten Pfad der Sicherungsdatei ein.

```
Bundle to restore from: /data/ocum-
backup/UM_9.8.N151113.1348_backup_rhel_02-20-2020-04-45.7z
```

Nach Abschluss der Wiederherstellung können Sie sich bei Unified Manager einloggen.

Nachdem Sie fertig sind

Wenn der OnCommand Workflow Automation-Server nach der Wiederherstellung des Backups nicht funktioniert, führen Sie die folgenden Schritte aus:

1. Ändern Sie auf dem Workflow Automation Server die IP-Adresse des Unified Manager-Servers, um auf die neueste Maschine zu verweisen.
2. Setzen Sie auf dem Unified Manager-Server das Datenbankkennwort zurück, wenn die Erfassung in Schritt 1 fehlschlägt.

Wiederherstellen einer MySQL-Datenbank-Sicherung unter Windows

Bei Datenverlust oder Datenbeschädigung kann Unified Manager mit der Wiederherstellungsfunktion in den vorherigen stabilen Zustand bei minimalem Verlust wiederhergestellt werden. Sie können die Unified Manager MySQL-Datenbank mithilfe der Unified Manager-Wartungskonsole auf einem lokalen Windows-System oder einem Remote-Windows-System wiederherstellen.

Bevor Sie beginnen

- Sie müssen über Administratorrechte für Windows verfügen.
- Sie müssen die Backup-Datei von Unified Manager und den Inhalt des Datenbank-Repository-Verzeichnisses auf das System kopiert haben, auf dem Sie den Wiederherstellungsvorgang ausführen möchten.

  Es wird empfohlen, die Sicherungsdatei in das Standardverzeichnis zu kopieren `\ProgramData\NetApp\OnCommandAppData\ocum\backup`. Die Datenbank-Repository-Dateien müssen in die kopiert werden `\database_dumps_repo` Unterverzeichnis unter dem `\backup` Verzeichnis.

- Die Sicherungsdateien müssen aus sein `.7z` Typ.

Über diese Aufgabe

Die Wiederherstellungsfunktion ist plattformspezifisch und versionsspezifisch. Sie können ein Unified Manager MySQL Backup nur auf derselben Version von Unified Manager wiederherstellen. Ein Windows Backup kann nur auf einer Windows Plattform wiederhergestellt werden.

Wenn die Ordnernamen ein Leerzeichen enthalten, müssen Sie den absoluten Pfad oder den relativen Pfad der Sicherungsdatei in doppelten Anführungszeichen einschließen.

Schritte

1. Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager die UI nicht oder konfigurieren Sie nach Abschluss der Installation keine Cluster, Benutzer oder Authentifizierungseinstellungen. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.
2. Melden Sie sich mit den Administratoranmeldeinformationen beim Unified Manager-System an.
3. Starten Sie PowerShell als Windows-Administrator.
4. Geben Sie den Befehl ein `maintenance_console` Und drücken Sie die Eingabetaste.
5. Geben Sie in der Wartungskonsole **Hauptmenü** die Nummer für die Option **Backup Restore** ein.
6. Geben Sie die Nummer für die * MySQL-Sicherung wiederherstellen* ein.
7. Geben Sie bei entsprechender Aufforderung den absoluten Pfad der Sicherungsdatei ein.

   ```
   Bundle to restore from:
   \ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac
   kup_windows_02-20-2020-02-51.7z
   ```

   Nach Abschluss der Wiederherstellung können Sie sich bei Unified Manager einloggen.

Nachdem Sie fertig sind

Wenn der OnCommand Workflow Automation-Server nach der Wiederherstellung des Backups nicht funktioniert, führen Sie die folgenden Schritte aus:

1. Ändern Sie auf dem Workflow Automation Server die IP-Adresse des Unified Manager-Servers, um auf die neueste Maschine zu verweisen.
2. Setzen Sie auf dem Unified Manager-Server das Datenbankkennwort zurück, wenn die Erfassung in Schritt 1 fehlschlägt.

Backup und Restore mit NetApp Snapshots

Ein NetApp Snapshot Backup erstellt ein zeitpunktgenaues Image der Unified Manager Datenbank- und Konfigurationsdateien, mit denen eine Wiederherstellung im Falle eines Systemausfalls oder eines Datenverlusts möglich ist. Sie planen, ein Snapshot Backup regelmäßig auf ein Volume auf einem Ihrer ONTAP Cluster zu schreiben, sodass Sie immer eine aktuelle Kopie haben.

Diese Funktion ist nur verfügbar, wenn Unified Manager auf einem Red hat Enterprise Linux- oder CentOS Linux-Server installiert ist.

Snapshot Backups dauern sehr wenig Zeit, in der Regel nur ein paar Minuten, und die Unified Manager Datenbank ist innerhalb eines sehr kurzen Zeitrahmens gesperrt, sodass Ihre Installation nur sehr wenig unterbrochen wird. Das Image verbraucht nur wenig Storage und der Performance-Overhead ist minimal, da seit der letzten Snapshot Kopie nur Änderungen an Dateien aufgezeichnet werden. Da der Snapshot auf einem ONTAP Cluster erstellt wird, können Sie bei Bedarf mithilfe anderer NetApp Funktionen wie SnapMirror sekundäre Sicherungsfunktionen erstellen.

Vor Beginn eines Backup-Vorgangs führt Unified Manager eine Integritätsprüfung durch, um zu überprüfen, ob das Zielsystem verfügbar ist.

Beachten Sie, dass Sie ein Snapshot Backup nur auf derselben Version von Unified Manager wiederherstellen können. Wenn Sie beispielsweise ein Backup auf Unified Manager 9.8 erstellt haben, kann das Backup nur auf Unified Manager 9.8 Systemen wiederhergestellt werden.

Erstellung des Volumes, auf dem Backups gespeichert werden

Sie können das Volume erstellen, auf dem Snapshot Backups von ONTAP System Manager oder über die ONTAP CLI auf einem Ihrer ONTAP Cluster gespeichert werden.

Bevor Sie beginnen

Der Cluster, die Storage-VM und das Volume müssen folgende Anforderungen erfüllen:

- Cluster-Anforderungen:
  - ONTAP 9.3 oder höher muss installiert sein
  - Sie sollten sich in geographischer Nähe zum Unified Manager-Server befinden
  - Die Software kann zwar von Unified Manager überwacht werden, ist aber nicht erforderlich
- Storage-VM-Anforderungen:
  - CIFS/SMB- oder NFS-Services müssen aktiviert sein
  - Der Namensschalter und die Namenszuweisung müssen auf „`files`“ gesetzt werden.
  - NFSv4 muss auf dem NFS-Server und der NFSv4-iddomain aktiviert sein, die auf dem Client und der Storage-VM angegeben ist
  - Lokale Benutzer wurden erstellt, um den Client-seitigen Benutzern zu entsprechen
  - Stellen Sie sicher, dass alle Lese-/Schreibzugriff ausgewählt ist
  - Stellen Sie sicher, dass Superuser Access in der Exportrichtlinie auf „`any`“ eingestellt ist
- Volume-Anforderungen:
  - Das Volume sollte mindestens die doppelte Größe des Unified Manager/opt/netapp/Datenververzeichnisses haben

    Verwenden Sie den Befehl `du -sh /opt/netapp/data/` Um die aktuelle Größe zu überprüfen.
  - Der Sicherheitsstil muss auf UNIX festgelegt sein
  - Die lokale Snapshot-Richtlinie muss deaktiviert werden
  - Die automatische Volume-Größe sollte aktiviert sein
  - Das Performance-Service-Level sollte auf eine Richtlinie mit hohen IOPS-Werten und niedriger Latenz, wie z. B. „`Extreme`“, festgelegt werden.

Über diese Aufgabe

Detaillierte Schritte zur Erstellung des NFS-Volume finden Sie unter "So konfigurieren Sie NFSv4 in ONTAP 9" Und das "ONTAP 9 NFS Configuration Express Guide".

Festlegen des Zielorts für Snapshot-Backups

Sie konfigurieren den Zielspeicherort für Unified Manager Snapshot Backups auf einem Volume, das Sie bereits in einem der ONTAP Cluster konfiguriert haben. Sie definieren den Speicherort von der Unified Manager-Wartungskonsole aus.

Bevor Sie beginnen

- Sie müssen über die Stammbenutzeranmeldeinformationen für den Linux-Host verfügen, auf dem Unified Manager installiert ist.
- Sie müssen über eine Benutzer-ID und ein Passwort verfügen, um sich bei der Wartungskonsole des Unified Manager-Servers anzumelden.
- Sie müssen über die IP-Adresse für das Cluster-Management, den Namen der Storage-VM, den Namen des Volume und den Benutzernamen und das Kennwort des Speichersystems verfügen.
- Sie müssen das Volume auf den Unified Manager Host angehängt haben, und Sie müssen den Mount-Pfad aufweisen.

Schritte

1. Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domänennamen des Unified Manager-Systems her.
2. Melden Sie sich beim System mit dem Wartungs-Benutzer (umadmin) und dem Passwort an.
3. Geben Sie den Befehl ein `maintenance_console` Und drücken Sie die Eingabetaste.
4. Geben Sie in der Wartungskonsole **Hauptmenü** die Nummer für die Option **Backup Restore** ein.
5. Geben Sie die Nummer für * NetApp Snapshot Backup konfigurieren* ein.
6. Geben Sie die Nummer für **Konfiguration für NFS** ein.
7. Überprüfen Sie die Informationen, die Sie angeben müssen, und geben Sie dann die Nummer für **Backup Configuration Details** ein.
8. Um das Volume zu identifizieren, auf dem der Snapshot geschrieben werden soll, geben Sie die IP-Adresse der Cluster Management-Schnittstelle, den Namen der Storage VM, den Namen des Volumes, Benutzernamen und Passwort des Storage-Systems und den Mount-Pfad ein.
9. Überprüfen Sie diese Informationen, und geben Sie ein `y`.

   Das System führt die folgenden Aufgaben aus:

   - Stellt die Verbindung zum Cluster her
   - Stoppt alle Dienste
   - Erstellt ein neues Verzeichnis im Volume und kopiert die Konfigurationsdateien der Unified Manager Datenbank
   - Löscht die Dateien aus Unified Manager und erstellt eine Symlink zum neuen Datenbankverzeichnis
   - Startet alle Dienste neu
10. Beenden Sie die Wartungskonsole und starten Sie die Benutzeroberfläche von Unified Manager, um den Snapshot Backup-Zeitplan zu erstellen, sofern Sie dies noch nicht getan haben.

Definieren eines Zeitplans für Snapshot-Backups

Sie können den Zeitplan, auf dem Unified ManagerSnapshot Backups mithilfe der Benutzeroberfläche von Unified Manager erstellt werden, konfigurieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen die NetApp Snapshot Backup-Einstellungen von der Wartungskonsole konfiguriert haben, um das Ziel zu identifizieren, in dem die Snapshots erstellt werden.
- Sie sollten Backup-Vorgänge nicht so planen, dass sie unmittelbar nach dem Hinzufügen eines neuen Clusters ausgeführt werden, während Unified Manager historische Performance-Daten von 15 Tagen erfasst.

Über diese Aufgabe

Snapshot Backups werden in wenigen Minuten erstellt, und die Unified Manager Datenbank ist nur für wenige Sekunden gesperrt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Datenbank-Backup**.
2. Klicken Sie auf der Seite **Datenbank-Backup** auf **Backup-Einstellungen**.
3. Geben Sie im Feld * Retention Count* die maximale Anzahl an Snapshot Kopien ein, die Sie aufbewahren möchten.

   Der Standardwert für die Aufbewahrungsanzahl ist 10. Die maximale Anzahl Snapshot Kopien wird durch die Version der ONTAP Software auf dem Cluster bestimmt: 1020 für ONTAP 9.4 und höher und 250 für ONTAP 9.3 und früher. Sie können dieses Feld leer lassen, um den Maximalwert unabhängig von der ONTAP-Version zu implementieren.

4. Wählen Sie die Schaltfläche **geplante tägliche** oder **geplante Woche** und geben Sie die Terminplandetails an.
5. Klicken Sie Auf **Anwenden**.

Ergebnisse

Snapshot Backup-Dateien werden basierend auf dem Zeitplan erstellt. Die verfügbaren Sicherungsdateien finden Sie auf der Seite Datenbank-Backup.

Nachdem Sie fertig sind

Aufgrund der Bedeutung dieses Volumes und der Snapshots möchten Sie möglicherweise ein oder zwei Alarme für dieses Volume erstellen, sodass Sie bei einer der folgenden Aktionen benachrichtigt werden:

- Der Volumenspeicherplatz ist 90% voll. Verwenden Sie das Event **Volume Space Full**, um die Warnmeldung einzurichten.

  Sie können dem Volume mit ONTAP System Manager oder der ONTAP CLI Kapazität hinzufügen, sodass der Speicherplatz der Unified Manager-Datenbank nicht knapp wird.

- Die Anzahl der Snapshots erreicht fast die maximale Anzahl. Verwenden Sie das Ereignis **zu viele Snapshot Kopien** um die Warnung einzurichten.

Sie können ältere Schnappschüsse mit ONTAP System Manager oder der ONTAP CLI löschen, so dass immer Platz für neue Snapshot-Backups ist.

Auf der Seite „Alarmkonfiguration“ konfigurieren Sie Warnmeldungen.

Wiederherstellen eines Snapshot Backups

Im Falle eines Datenverlustes oder einer Beschädigung von Daten können Sie Unified Manager in den vorherigen stabilen Zustand bei minimalem Datenverlust wiederherstellen. Die Snapshot Datenbank von Unified Manager kann über die Unified Manager Wartungskonsole auf einem lokalen oder Remote Red hat Enterprise Linux oder CentOS System wiederhergestellt werden.

Bevor Sie beginnen

- Sie müssen über die Stammbenutzeranmeldeinformationen für den Linux-Host verfügen, auf dem Unified Manager installiert ist.
- Sie müssen über eine Benutzer-ID und ein Passwort verfügen, um sich bei der Wartungskonsole des Unified Manager-Servers anzumelden.

Über diese Aufgabe

Die Wiederherstellungsfunktion ist plattformspezifisch und versionsspezifisch. Sie können ein Unified Manager-Backup nur auf derselben Version von Unified Manager wiederherstellen.

Schritte

1. Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domänennamen des Unified Manager-Systems her.
2. Melden Sie sich beim System mit dem Wartungs-Benutzer (umadmin) und dem Passwort an.
3. Geben Sie den Befehl ein `maintenance_console` Und drücken Sie die Eingabetaste.
4. Geben Sie in der Wartungskonsole **Hauptmenü** die Nummer für die Option **Backup Restore** ein.
5. Geben Sie die Nummer für **Backup und Restore mit NetApp Snapshot** ein.

   Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager die UI nicht oder konfigurieren Sie nach Abschluss der Installation keine Cluster, Benutzer oder Authentifizierungseinstellungen. Geben Sie die Nummer für **Configure NetApp Snapshot Backup** ein und konfigurieren Sie die Snapshot Backup Einstellungen so, wie sie auf dem ursprünglichen System konfiguriert wurden.

6. Geben Sie die Nummer für **Restore mit NetApp Snapshot** ein.
7. Wählen Sie die Snapshot-Backup-Datei aus, die Sie wiederherstellen möchten, und drücken Sie die Eingabetaste.
8. Melden Sie sich nach Abschluss des Wiederherstellungsprozesses in der Benutzeroberfläche von Unified Manager an.

Nachdem Sie fertig sind

Wenn der OnCommand Workflow Automation-Server nach der Wiederherstellung des Backups nicht funktioniert, führen Sie die folgenden Schritte aus:

1. Ändern Sie auf dem Workflow Automation Server die IP-Adresse des Unified Manager-Servers, um auf die neueste Maschine zu verweisen.
2. Setzen Sie auf dem Unified Manager-Server das Datenbankkennwort zurück, wenn die Erfassung in Schritt 1 fehlschlägt.

Migration einer virtuellen Unified Manager Appliance zu einem Linux System

Sie können eine Backup-Dump-Datenbank von einer virtuellen Appliance in ein Red hat Enterprise Linux oder CentOS Linux System wiederherstellen, wenn Sie das Host-Betriebssystem ändern möchten, auf dem Unified Manager ausgeführt wird.

Bevor Sie beginnen

- Auf der virtuellen Appliance:
  - Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
  - Sie müssen den Namen des Unified Manager-Wartungsbenutzers für den Wiederherstellungsvorgang kennen.
- Auf dem Linux-System:
  - Sie müssen Unified Manager auf einem RHEL- oder CentOS-Server gemäß den Anweisungen im Installationshandbuch installiert haben.
  - Die Version von Unified Manager auf diesem Server muss mit der Version auf der virtuellen Appliance identisch sein, von der aus Sie die Sicherungsdatei verwenden.
  - Starten Sie die UI nicht oder konfigurieren Sie nach der Installation keine Cluster-, Benutzer- oder Authentifizierungseinstellungen auf dem Linux-System. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.
  - Sie müssen über die Stammbenutzeranmeldeinformationen für den Linux-Host verfügen.

Über diese Aufgabe

In diesen Schritten wird beschrieben, wie eine Sicherungsdatei auf der virtuellen Appliance erstellt, die Sicherungsdateien auf das Red hat Enterprise Linux oder CentOS System kopiert und dann die Datenbanksicherung auf das neue System wiederhergestellt wird.

Schritte

1. Klicken Sie auf der virtuellen Appliance auf **Verwaltung** > **Datenbank-Backup**.
2. Klicken Sie auf der Seite **Datenbank-Backup** auf **Backup-Einstellungen**.
3. Ändern Sie den Backuppfad in `/jail/support`.
4. Wählen Sie im Abschnitt Zeitplan die Option **planmäßig täglich** aus, und geben Sie einige Minuten nach der aktuellen Zeit ein, damit das Backup in Kürze erstellt wird.
5. Klicken Sie Auf **Anwenden**.
6. Warten Sie einige Stunden, bis das Backup erstellt wird.

   Ein vollständiges Backup kann über 1 GB betragen und kann drei bis vier Stunden in Anspruch nehmen.

7. Melden Sie sich als Root-Benutzer beim Linux-Host an, auf dem Unified Manager installiert ist, und

kopieren Sie die Sicherungsdateien von `/support` Auf der virtuellen Appliance mit SCP.`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .`

```
root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
```

Stellen Sie sicher, dass Sie den kopiert haben `.7z` Backup-Datei und alle `.7z` Repository-Dateien im `/database-dumps-repo` Unterverzeichnis.

8. Stellen Sie an der Eingabeaufforderung das Backup wieder her: `um backup restore -f /<backup_file_path>/<backup_file_name>`

```
um backup restore -f /UM_9.7.N151113.1348_backup_unix_02-12-2019-04-16.7z
```

9. Melden Sie sich nach Abschluss der Wiederherstellung bei der Web-UI von Unified Manager an.

Nachdem Sie fertig sind

Sie sollten die folgenden Aufgaben durchführen:

- Generieren Sie ein neues HTTPS-Sicherheitszertifikat, und starten Sie den Unified Manager-Server neu.
- Ändern Sie den Backuppfad auf die Standardeinstellung für Ihr Linux-System (`/data/ocum-backup`), oder zu einem neuen Weg Ihrer Wahl, weil es keine `/jail/support` Pfad auf dem Linux-System.
- Konfigurieren Sie beide Seiten Ihrer Workflow Automation Verbindung neu, falls WFA verwendet wird.
- Konfigurieren Sie SAML-Authentifizierungseinstellungen neu, wenn Sie SAML verwenden.

Nachdem Sie überprüft haben, dass alles auf Ihrem Linux-System wie erwartet ausgeführt wird, können Sie die virtuelle Unified Manager-Appliance herunterfahren und entfernen.

Verwalten von Skripten

Mithilfe von Skripten können mehrere Storage-Objekte in Unified Manager automatisch geändert oder aktualisiert werden. Das Skript ist einer Warnung zugeordnet. Wenn ein Ereignis eine Warnung auslöst, wird das Skript ausgeführt. Sie können benutzerdefinierte Skripts hochladen und deren Ausführung testen, wenn eine Warnung erzeugt wird.

Die Möglichkeit, Skripts in Unified Manager hochzuladen und sie auszuführen, ist standardmäßig aktiviert. Wenn Ihr Unternehmen diese Funktionalität aus Sicherheitsgründen nicht zulassen möchte, können Sie diese Funktion unter **Storage Management** > **Feature-Einstellungen** deaktivieren.

Funktionsweise von Skripten mit Warnmeldungen

Sie können eine Warnung mit Ihrem Skript verknüpfen, damit das Skript ausgeführt wird, wenn eine Warnung für ein Ereignis in Unified Manager ausgegeben wird. Sie können die Skripte verwenden, um Probleme mit Speicherobjekten zu lösen oder zu identifizieren, welche Speicherobjekte die Ereignisse generieren.

Wenn eine Warnung für ein Ereignis in Unified Manager generiert wird, wird eine Alarm-E-Mail an die angegebenen Empfänger gesendet. Wenn Sie einem Skript eine Warnung zugeordnet haben, wird das Skript ausgeführt. Die Details der Argumente, die an das Skript übergeben werden, können Sie aus der Alarm-E-Mail erhalten.

Das Skript verwendet die folgenden Argumente zur Ausführung:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Sie können die Argumente in Ihren Skripten verwenden, um verwandte Ereignisinformationen zu erfassen oder Speicherobjekte zu ändern.

Beispiel zum Abrufen von Argumenten aus Skripts

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

Wenn eine Warnung erzeugt wird, wird dieses Skript ausgeführt und die folgende Ausgabe angezeigt:

```
-eventID : 290
-eventSourceID : 4138
```

Skripte werden hinzugefügt

Im Unified Manager können Skripts hinzugefügt und die Skripte mit Warnmeldungen verknüpft werden. Diese Skripte werden automatisch ausgeführt, wenn eine Warnmeldung generiert wird, und ermöglichen es Ihnen, Informationen über Speicherobjekte zu erhalten, für die das Ereignis generiert wird.

Bevor Sie beginnen

- Sie müssen die Skripte erstellt und gespeichert haben, die Sie dem Unified Manager-Server hinzufügen möchten.
- Die unterstützten Dateiformate für Skripte sind Perl, Shell, PowerShell und `.bat` Dateien:

Plattform, auf der Unified Manager installiert ist	Unterstützte Sprachen
VMware	Perl- und Shell-Skripte
Linux	Perl- und Shell-Skripte

Windows	PowerShell, Perl und .bat Skripte

- Für Perl-Skripte muss Perl auf dem Unified Manager-Server installiert sein. Bei VMware-Installationen wird Perl 5 standardmäßig installiert und Skripte werden nur das unterstützen, was Perl 5 unterstützt. Wenn Perl nach Unified Manager installiert wurde, müssen Sie den Unified Manager-Server neu starten.
- Bei PowerShell Skripten muss auf dem Windows Server die entsprechende PowerShell Ausführungsrichtlinie festgelegt werden, damit die Skripte ausgeführt werden können.

Wenn Ihr Skript Protokolldateien erstellt, um den Fortschritt des Warnungsskripts zu verfolgen, müssen Sie sicherstellen, dass die Protokolldateien nicht überall im Unified Manager-Installationsordner erstellt werden.

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können benutzerdefinierte Skripts hochladen und Ereignisdetails zu der Meldung erfassen.

Wenn diese Funktion in der Benutzeroberfläche nicht angezeigt wird, liegt sie daran, dass die Funktion von Ihrem Administrator deaktiviert wurde. Bei Bedarf können Sie diese Funktion über **Speicherverwaltung** > **Funktionseinstellungen** aktivieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Scripts**.
2. Klicken Sie auf der Seite **Skripts** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Skript hinzufügen** auf **Durchsuchen**, um die Skriptdatei auszuwählen.
4. Geben Sie eine Beschreibung für das ausgewählte Skript ein.
5. Klicken Sie Auf **Hinzufügen**.

Skripte werden gelöscht

Sie können ein Skript aus Unified Manager löschen, wenn das Skript nicht mehr benötigt oder gültig ist.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Das Skript darf keiner Warnung zugeordnet werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Scripts**.
2. Wählen Sie auf der Seite **Skripts** das Skript aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang, indem Sie auf **Ja** klicken.

Skriptausführung wird getestet

Sie können überprüfen, ob Ihr Skript korrekt ausgeführt wird, wenn eine Warnung für ein Speicherobjekt generiert wird.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen ein Skript im unterstützten Dateiformat auf Unified Manager hochgeladen haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Scripts**.
2. Fügen Sie auf der Seite **Skripts** Ihr Testskript hinzu.
3. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Alarm-Setup**.
4. Führen Sie auf der Seite **Alarm Setup** eine der folgenden Aktionen durch:

An…	Tun Sie das…
Fügen Sie eine Meldung hinzu	a. Klicken Sie Auf **Hinzufügen**. b. Verknüpfen Sie im Abschnitt Aktionen den Alarm mit Ihrem Testskript.
Bearbeiten Sie eine Meldung	a. Wählen Sie einen Alarm aus, und klicken Sie dann auf **Bearbeiten**. b. Verknüpfen Sie im Abschnitt Aktionen den Alarm mit Ihrem Testskript.

5. Klicken Sie Auf **Speichern**.
6. Wählen Sie auf der Seite **Alarm Setup** die Warnmeldung aus, die Sie hinzugefügt oder geändert haben, und klicken Sie dann auf **Test**.

   Das Skript wird mit dem Argument „`-Test`“ ausgeführt, und eine Benachrichtigung wird an die E-Mail-Adressen gesendet, die beim Erstellen der Warnmeldung angegeben wurden.

Verwalten und Überwachen von Gruppen

Sie können Gruppen in Unified Manager erstellen, um Storage-Objekte zu managen.

Allgemeines zu Gruppen

Sie können Gruppen in Unified Manager erstellen, um Storage-Objekte zu managen. Wenn Sie die Konzepte zu Gruppen und die Art und Weise verstehen, wie Gruppenregeln das Hinzufügen von Speicherobjekten zu einer Gruppe ermöglichen, können Sie die Speicherobjekte in Ihrer Umgebung verwalten.

Was eine Gruppe ist

Eine Gruppe ist eine dynamische Sammlung heterogener Storage-Objekte (Cluster, SVMs oder Volumes). In Unified Manager können Sie Gruppen erstellen, um einfach eine Reihe von Storage-Objekten zu managen. Die Mitglieder einer Gruppe können sich je nach den Storage-Objekten ändern, die zu einem bestimmten Zeitpunkt von Unified Manager überwacht werden.

- Jede Gruppe hat einen eindeutigen Namen.
- Sie müssen für jede Gruppe mindestens eine Gruppenregel konfigurieren.
- Sie können einer Gruppe mehrere Gruppenregeln zuordnen.
- Jede Gruppe kann mehrere Typen von Storage-Objekten wie Clustern, SVMs oder Volumes enthalten.
- Speicherobjekte werden einer Gruppe dynamisch hinzugefügt, basierend auf dem Zeitpunkt, an dem eine Gruppenregel erstellt wurde oder wenn Unified Manager einen Überwachungszyklus abgeschlossen hat.
- Sie können gleichzeitig Aktionen auf alle Speicherobjekte einer Gruppe anwenden, z. B. Schwellenwerte für Volumes.

Funktionsweise von Gruppenregeln für Gruppen

Eine Gruppenregel ist ein Kriterium, das definiert wird, ob Storage-Objekte (Volumes, Cluster oder SVMs) in eine bestimmte Gruppe aufgenommen werden können. Sie können Bedingungsgruppen oder Bedingungen für das Definieren einer Gruppenregel für eine Gruppe verwenden.

- Sie müssen einer Gruppe eine Gruppenregel zuordnen.
- Sie müssen einen Objekttyp für eine Gruppenregel zuordnen. Einer Gruppenregel ist nur ein Objekttyp zugeordnet.
- Speicherobjekte werden nach jedem Überwachungszyklus oder beim Erstellen, Bearbeiten oder Löschen einer Regel aus der Gruppe hinzugefügt oder entfernt.
- Eine Gruppenregel kann eine oder mehrere Bedingungsgruppen haben, und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben.
- Speicherobjekte können basierend auf den von Ihnen erstellten Gruppenregeln mehreren Gruppen angehören.

Bestimmten Bedingungen

Sie können mehrere Bedingungsgruppen erstellen, und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben. Sie können alle definierten Bedingungsgruppen in einer Gruppenregel für Gruppen anwenden, um anzugeben, welche Speicherobjekte in der Gruppe enthalten sind.

Bedingungen innerhalb einer Bedingungsgruppe werden mit logischem UND ausgeführt. Alle Bedingungen in einer Bedingungsgruppe müssen erfüllt werden. Wenn Sie eine Gruppenregel erstellen oder ändern, wird eine Bedingung erstellt, die nur jene Speicherobjekte anwendet, auswählt und gruppiert, die alle Bedingungen in der Bedingungsgruppe erfüllen. Sie können mehrere Bedingungen innerhalb einer Bedingungsgruppe verwenden, wenn Sie den Umfang der Speicherobjekte einschränken möchten, die in eine Gruppe aufgenommen werden sollen.

Sie können mit Speicherobjekten Bedingungen erstellen, indem Sie die folgenden Operanden und den Operator verwenden und den erforderlichen Wert angeben.

Storage-Objekttyp	Anwendbare Operanden
Datenmenge	• Objektname • Der Name des Clusters • Name der SVM • Anmerkungen
SVM	• Objektname • Der Name des Clusters • Anmerkungen
Cluster	• Objektname • Anmerkungen

Wenn Sie Anmerkung als Operand für ein beliebiges Speicherobjekt auswählen, steht der Operator „`is`“ zur Verfügung. Für alle anderen Operanden können Sie entweder „`ist`“ oder „`enthält`“ als Operator auswählen.

- Operand

  Die Liste der Operanden in Unified Manager ändert sich basierend auf dem ausgewählten Objekttyp. Die Liste umfasst den Objektnamen, den Namen des Clusters, den Namen der SVM und die Anmerkungen, die Sie in Unified Manager definieren.

- Operator

  Die Liste der Operatoren ändert sich basierend auf dem ausgewählten Operand für eine Bedingung. Die in Unified Manager unterstützten Operatoren sind „`ist`“ und „`enthält`“.

  Wenn Sie den Operator „`is`“ auswählen, wird die Bedingung für die exakte Übereinstimmung des Operandwerts mit dem für den ausgewählten Operand angegebenen Wert ausgewertet.

  Wenn Sie den Operator „`contains`“ auswählen, wird die Bedingung anhand eines der folgenden Kriterien bewertet:

  - Der Operandwert ist eine exakte Übereinstimmung mit dem für den ausgewählten Operand angegebenen Wert
  - Der Operandwert enthält den für den ausgewählten Operand angegebenen Wert

- Wert

  Das Wertfeld ändert sich basierend auf dem ausgewählten Operand.

Beispiel einer Gruppenregel mit Bedingungen

Betrachten Sie eine Bedingungsgruppe für ein Volume mit den folgenden zwei Bedingungen:

- Name enthält „`vol`“
- SVM-Name: „`data_svm`“

Diese Bedingungsgruppe wählt alle Volumes aus, die „vol“ in ihren Namen enthalten und auf SVMs mit dem Namen „data_svm“ gehostet werden.

Bedingungsgruppen

Bedingungsgruppen werden mit logischem ODER ausgeführt und anschließend auf Speicherobjekte angewendet. Die Speicherobjekte müssen eine der Bedingungsgruppen erfüllen, die in eine Gruppe aufgenommen werden sollen. Die Speicherobjekte aller Bedingungsgruppen werden kombiniert. Sie können Bedingungsgruppen verwenden, um den Umfang von Speicherobjekten, die in eine Gruppe aufgenommen werden sollen, zu erhöhen.

Beispiel einer Gruppenregel mit Bedingungsgruppen

Es sollten zwei Bedingungsgruppen für ein Volume berücksichtigt werden, wobei jede Gruppe die folgenden beiden Bedingungen enthält:

- Bedingungsgruppe 1
  - Name enthält „vol“
  - SVM-Name ist „data_svm“ Condition Group 1 wählt alle Volumes aus, die „vol“ in ihren Namen enthalten und auf SVMs mit dem Namen „data_svm“ gehostet werden.
- Bedingungsgruppe 2
  - Name enthält „vol“
  - Der Anmerkungswert der Datenpriorität lautet „Critical“ Condition Group 2 wählt alle Volumes aus, die „vol“ in ihren Namen enthalten und die mit dem Wert der datenprioritären Annotation mit „Critical“ beschriftet werden.

Wenn eine Gruppenregel, die diese beiden Bedingungsgruppen enthält, auf Speicherobjekte angewendet wird, werden die folgenden Speicherobjekte zu einer ausgewählten Gruppe hinzugefügt:

- Alle Volumes mit „vol“ in ihren Namen, die auf der SVM mit dem Namen „data_svm“ gehostet werden.
- Alle Volumes, die „vol“ in ihren Namen enthalten und mit dem Anmerkungswert „kritisch“ der Datenpriorität versehen werden.

Funktionsweise von Gruppenaktionen auf Speicherobjekten

Eine Gruppenaktion ist ein Vorgang, der auf allen Speicherobjekten einer Gruppe ausgeführt wird. Sie können beispielsweise die Aktion für Volume-Schwellenwertgruppen konfigurieren, um gleichzeitig die Volume-Schwellenwerte aller Volumes in einer Gruppe zu ändern.

Gruppen unterstützen eindeutige Gruppen-Aktionstypen. Sie können eine Gruppe mit nur einem Aktionstyp für den Integritätsschwellenwert einer Volume-Gruppe haben. Sie können jedoch eine andere Art von Gruppenaktion konfigurieren, falls verfügbar, für dieselbe Gruppe. Der Rang einer Gruppenaktion bestimmt die Reihenfolge, in der die Aktion auf Speicherobjekte angewendet wird. Auf der Detailseite eines Speicherobjekts finden Sie Informationen darüber, welche Gruppenaktion auf das Speicherobjekt angewendet wird.

Beispiel für Aktionen eindeutiger Gruppen

Nehmen Sie sich ein Volume A an, das zu den Gruppen G1 und G2 gehört, und die folgenden Volume-Systemzustandsschwellenwerte werden für diese Gruppen konfiguriert:

- `Change_capacity_threshold` Gruppenaktion mit Rang 1 zur Konfiguration der Kapazität des Volumes
- `Change_snapshot_copies` Gruppenaktion mit Rang 2 zur Konfiguration der Snapshot-Kopien des Volumes

Der `Change_capacity_threshold` Gruppenaktionen haben immer Priorität über das `Change_snapshot_copies` Gruppenaktion und wird auf Volume A angewendet Wenn Unified Manager einen Überwachungszyklus abgeschlossen hat, werden die Systemzustandsereignisse bei Volume A anhand der neu beurteilt `Change_capacity_threshold` Gruppenaktion. Sie können keinen anderen Volume-Schwellenwerttyp für Gruppenaktion für G1- oder G2-Gruppe konfigurieren.

Hinzufügen von Gruppen

Gruppen können erstellt werden, um Cluster, Volumes und Storage Virtual Machines (SVMs) zu kombinieren und so das Management zu vereinfachen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können Gruppenregeln definieren, um Mitglieder aus der Gruppe hinzuzufügen oder zu entfernen und Gruppenaktionen für die Gruppe zu ändern.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppen** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Gruppe hinzufügen** einen Namen und eine Beschreibung für die Gruppe ein.
4. Klicken Sie Auf **Hinzufügen**.

Gruppen werden bearbeitet

Sie können den Namen und die Beschreibung einer Gruppe bearbeiten, die Sie in Unified Manager erstellt haben.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Wenn Sie eine Gruppe bearbeiten, um den Namen zu aktualisieren, müssen Sie einen eindeutigen Namen angeben; Sie können keinen vorhandenen Gruppennamen verwenden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppen** die Gruppe aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.

3. Ändern Sie im Dialogfeld **Gruppe bearbeiten** den Namen, die Beschreibung oder beides für die Gruppe.
4. Klicken Sie Auf **Speichern**.

Gruppen werden gelöscht

Sie können eine Gruppe aus Unified Manager löschen, wenn die Gruppe nicht mehr benötigt wird.

Bevor Sie beginnen

- Keines der Storage-Objekte (Cluster, SVMs, Volumes) muss einer beliebigen Gruppenregel zugeordnet sein, die der zu löschenden Gruppe zugeordnet ist.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppen** die Gruppe aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang, indem Sie auf **Ja** klicken.

   Durch das Löschen einer Gruppe werden die Gruppenaktionen, die der Gruppe zugeordnet sind, nicht gelöscht. Diese Gruppenaktionen werden jedoch nach dem Löschen der Gruppe aufgehoben.

Gruppenregeln werden hinzugefügt

Sie können Gruppenregeln für eine Gruppe erstellen, um der Gruppe dynamisch Storage-Objekte wie Volumes, Cluster oder Storage Virtual Machines (SVMs) hinzuzufügen. Sie müssen mindestens eine Bedingungsgruppe mit mindestens einer Bedingung konfigurieren, um eine Gruppenregel zu erstellen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Speicherobjekte, die aktuell überwacht werden, werden hinzugefügt, sobald die Gruppenregel erstellt wird. Neue Objekte werden erst nach Abschluss des Überwachungszyklus hinzugefügt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Gruppenregel hinzufügen** einen Namen für die Gruppenregel an.
4. Wählen Sie im Feld **Zielobjekttyp** den Typ des Speicherobjekts aus, das Sie gruppieren möchten.
5. Wählen Sie im Feld **Gruppe** die gewünschte Gruppe aus, für die Sie Gruppenregeln erstellen möchten.
6. Führen Sie im Abschnitt **Bedingungen** die folgenden Schritte aus, um eine Bedingung, eine

Bedingungsgruppe oder beide zu erstellen:

Zu erstellen	Tun Sie das…
Ein Zustand	a. Wählen Sie einen Operand aus der Liste der Operanden aus. b. Wählen Sie als Operator entweder **enthält** oder **IS** aus. c. Geben Sie einen Wert ein, oder wählen Sie einen Wert aus der Liste verfügbar aus.
Eine Bedingungsgruppe	a. Klicken Sie Auf **Bedingungsgruppe Hinzufügen** b. Wählen Sie einen Operand aus der Liste der Operanden aus. c. Wählen Sie als Operator entweder **enthält** oder **IS** aus. d. Geben Sie einen Wert ein, oder wählen Sie einen Wert aus der Liste verfügbar aus. e. Klicken Sie auf **Bedingung hinzufügen**, um bei Bedarf weitere Bedingungen zu erstellen, und wiederholen Sie die Schritte a bis d für jede Bedingung.

7. Klicken Sie Auf **Hinzufügen**.

Beispiel für das Erstellen einer Gruppenregel

Führen Sie im Dialogfeld Gruppenregel hinzufügen die folgenden Schritte aus, um eine Gruppenregel zu erstellen, einschließlich der Konfiguration einer Bedingung und dem Hinzufügen einer Bedingungsgruppe:

1. Geben Sie einen Namen für die Gruppenregel an.
2. Wählen Sie den Objekttyp als Storage Virtual Machine (SVM) aus.
3. Wählen Sie eine Gruppe aus der Gruppenliste aus.
4. Wählen Sie im Abschnitt Bedingungen als Operand **Objektname** aus.
5. Wählen Sie als Operator * enthält* aus.
6. Geben Sie den Wert als ein `svm_data`.
7. Klicken Sie auf **Bedingungsgruppe hinzufügen**.
8. Wählen Sie als Operand **Objektname** aus.
9. Wählen Sie als Operator * enthält* aus.
10. Geben Sie den Wert als ein `vol`.
11. Klicken Sie auf **Bedingung hinzufügen**.
12. Wiederholen Sie die Schritte 8 bis 10, indem Sie **Datenpriorität** als Operand in Schritt 8, **ist** als Operator in Schritt 9 und **kritisch** als Wert in Schritt 10 auswählen.

13. Klicken Sie auf **Hinzufügen**, um die Bedingung für die Gruppenregel zu erstellen.

Gruppenregeln werden bearbeitet

Sie können Gruppenregeln bearbeiten, um die Bedingungsgruppen und die Bedingungen innerhalb einer Bedingungsgruppe zu ändern, um Speicherobjekte zu oder aus einer bestimmten Gruppe hinzuzufügen oder zu entfernen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppenregeln** die Gruppenregel aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Gruppenregel bearbeiten** den Namen der Gruppenregel, den zugeordneten Gruppennamen, die Bedingungsgruppen und die Bedingungen, falls erforderlich.

   Sie können den Zielobjekttyp für eine Gruppenregel nicht ändern.

4. Klicken Sie Auf **Speichern**.

Gruppenregeln werden gelöscht

Sie können eine Gruppenregel aus Active IQ Unified Manager löschen, wenn die Gruppenregel nicht mehr erforderlich ist.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Wenn eine Gruppenregel gelöscht wird, werden die zugeordneten Speicherobjekte aus der Gruppe entfernt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppenregeln** die Gruppenregel aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang, indem Sie auf **Ja** klicken.

Gruppenaktionen werden hinzugefügt

Sie können Gruppenaktionen konfigurieren, die Sie auf Speicherobjekte in einer Gruppe anwenden möchten. Durch das Konfigurieren von Aktionen für eine Gruppe sparen Sie Zeit, da Sie diese Aktionen nicht einzeln zu jedem Objekt hinzufügen müssen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenaktionen** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld * Gruppenaktion* einen Namen und eine Beschreibung für die Aktion ein.
4. Wählen Sie im Menü **Gruppe** eine Gruppe aus, für die Sie die Aktion konfigurieren möchten.
5. Wählen Sie im Menü **Aktionstyp** einen Aktionstyp aus.

   Das Dialogfeld wird erweitert, sodass Sie den ausgewählten Aktionstyp mit den erforderlichen Parametern konfigurieren können.

6. Geben Sie die erforderlichen Werte für die erforderlichen Parameter ein, um eine Gruppenaktion zu konfigurieren.
7. Klicken Sie Auf **Hinzufügen**.

Gruppenaktionen werden bearbeitet

Sie können die Aktionsparameter der Gruppe bearbeiten, die Sie in Unified Manager konfiguriert haben, z. B. den Gruppenactionnamen, die Beschreibung, den zugeordneten Gruppennamen und die Parameter des Aktionstyps.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppenaktionen** die Gruppenaktion aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Gruppenaktion** den Gruppenaktionnamen, die Beschreibung, den zugeordneten Gruppennamen und die Parameter des Aktionstyps nach Bedarf.
4. Klicken Sie Auf **Speichern**.

Konfigurieren von Schwellenwerten für den Zustand von Volumes für Gruppen

Sie können Zustandsschwellenwerte für Volumes auf Gruppenebene für Kapazität, Snapshot Kopien, qtree Kontingente, Wachstum und Inodes konfigurieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Der Schwellenwerttyp für den Volume-Zustand der Gruppenaktion wird nur auf Volumes einer Gruppe angewendet.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenaktionen** auf **Hinzufügen**.
3. Geben Sie einen Namen und eine Beschreibung für die Gruppenaktion ein.
4. Wählen Sie aus dem Dropdown-Feld **Gruppe** eine Gruppe aus, für die Sie die Gruppenaktion konfigurieren möchten.
5. Wählen Sie als Schwellenwert für den Volumenzustand **Aktionstyp** aus.
6. Wählen Sie die Kategorie aus, für die Sie den Schwellenwert festlegen möchten.
7. Geben Sie die erforderlichen Werte für den Schwellenwert ein.
8. Klicken Sie Auf **Hinzufügen**.

Gruppenaktionen werden gelöscht

Sie können eine Gruppenaktion aus Unified Manager löschen, wenn die Gruppenaktion nicht mehr erforderlich ist.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Wenn Sie die Gruppenaktion für den Schwellenwert für den Systemzustand des Volumes löschen, werden globale Schwellenwerte auf die Speicherobjekte in dieser Gruppe angewendet. Zustandsschwellenwerte auf Objektebene, die für das Storage-Objekt festgelegt sind, werden nicht beeinträchtigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppenaktionen** die Gruppenaktion aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang, indem Sie auf **Ja** klicken.

Gruppenaktionen neu anordnen

Sie können die Reihenfolge der Gruppenaktionen ändern, die auf die Speicherobjekte in einer Gruppe angewendet werden sollen. Gruppenaktionen werden sequenziell auf Speicherobjekte basierend auf ihrer Rangfolge angewendet. Der niedrigste Rang wird der Gruppenaktion zugewiesen, die Sie zuletzt konfiguriert haben. Sie können den Rang der Gruppenaktion je nach Ihren Anforderungen ändern.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können entweder eine einzelne Zeile oder mehrere Zeilen auswählen und dann mehrere Drag-and-Drop-Vorgänge durchführen, um den Rang von Gruppenaktionen zu ändern. Sie müssen jedoch die Änderungen speichern, damit die Neupriorisierung im Raster Gruppenaktionen angezeigt wird.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenaktionen** auf **Neuordnung**.
3. Ziehen Sie im Dialogfeld **Gruppenaktionen neu anordnen** die Zeilen per Drag-and-Drop, um die Reihenfolge der Gruppenaktionen nach Bedarf neu anzuordnen.
4. Klicken Sie Auf **Speichern**.

Priorisieren von Storage-Objektereignissen mithilfe von Anmerkungen

Sie können Anmerkungsregeln für Storage-Objekte erstellen und anwenden, sodass Sie diese Objekte auf der Grundlage des Typs der verwendeten Annotation und ihrer Priorität identifizieren und filtern können.

Weitere Informationen zu Annotationen

Wenn Sie die Konzepte über Annotationen verstehen, können Sie Ereignisse aus dem Zusammenhang mit den Storage-Objekten in Ihrer Umgebung managen.

Welche Anmerkungen sind

Eine Anmerkung ist eine Textzeichenfolge (der Name), die einer anderen Textzeichenfolge (dem Wert) zugewiesen ist. Jedes Anmerkungsname-Wert-Paar kann mithilfe von Anmerkungsregeln dynamisch mit Speicherobjekten verknüpft werden. Wenn Sie Speicherobjekte mit vordefinierten Anmerkungen verknüpfen, können Sie die Ereignisse, die damit verbunden sind, filtern und anzeigen. Anmerkungen können auf Cluster, Volumes und Storage Virtual Machines (SVMs) angewendet werden.

Jeder Anmerkungsname kann mehrere Werte haben. Jedes Name-Wert-Paar kann über Regeln mit einem Storage-Objekt verknüpft werden.

Sie können beispielsweise eine Anmerkung mit dem Namen „`data-Center`“ mit den Werten „`Boston`“ und „`Canada`“ erstellen. Anschließend können Sie die Anmerkung „`data-Center`“ mit dem Wert „`Boston`“ auf Volume v1 anwenden. Wenn für jedes Ereignis auf einem Volume v1 eine Warnmeldung generiert wird, die mit „`data-Center`“ gekennzeichnet wird, weist die generierte E-Mail den Speicherort des Volume „`Boston`“ an. Auf diese Weise können Sie das Problem priorisieren und lösen.

Funktionieren von Anmerkungsregeln in Unified Manager

Eine Anmerkungsregel ist ein Kriterium, das definiert wird, um Storage-Objekte (Volumes, Cluster oder Storage Virtual Machines (SVMs)) zu beschriften. Sie können für das Definieren von Beschriftungsregeln entweder Bedingungsgruppen oder Bedingungen verwenden.

- Sie müssen eine Anmerkungsregel einer Anmerkung zuordnen.
- Sie müssen einen Objekttyp für eine Anmerkungsregel zuordnen. Für eine Anmerkungsregel kann nur ein Objekttyp zugeordnet werden.
- Unified Manager fügt nach jedem Überwachungszyklus oder bei dem Erstellen, Bearbeiten, Löschen oder Neuanordnen einer Regel Anmerkungen zu Storage-Objekten hinzu oder entfernt diese.
- Eine Anmerkungsregel kann eine oder mehrere Bedingungsgruppen haben, und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben.
- Speicherobjekte können mehrere Anmerkungen enthalten. Eine Anmerkungsregel für eine bestimmte Anmerkung kann auch unterschiedliche Anmerkungen in den Regelbedingungen verwenden, um bereits angekommenen Objekten eine weitere Anmerkung hinzuzufügen.

Bestimmten Bedingungen

Sie können mehrere Bedingungsgruppen erstellen, und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben. Sie können alle definierten Bedingungsgruppen in einer Anmerkungsregel einer Anmerkung anwenden, um Speicherobjekte zu beschriften.

Bedingungen innerhalb einer Bedingungsgruppe werden mit logischem UND ausgeführt. Alle Bedingungen in einer Bedingungsgruppe müssen erfüllt werden. Wenn Sie eine Anmerkungsregel erstellen oder ändern, wird eine Bedingung erstellt, die nur jene Speicherobjekte anwendet, auswählt und mit denen sie alle Bedingungen in der Bedingungsgruppe erfüllen. Sie können mehrere Bedingungen innerhalb einer Bedingungsgruppe verwenden, wenn Sie den Umfang der zu kommendenden Speicherobjekte einschränken möchten.

Sie können mit Speicherobjekten Bedingungen erstellen, indem Sie die folgenden Operanden und den Operator verwenden und den erforderlichen Wert angeben.

Storage-Objekttyp	Anwendbare Operanden
Datenmenge	• Objektname • Der Name des Clusters • Name der SVM • Anmerkungen
SVM	• Objektname • Der Name des Clusters • Anmerkungen
Cluster	• Objektname • Anmerkungen

Wenn Sie Anmerkung als Operand für ein beliebiges Speicherobjekt auswählen, steht der Operator „`is`“ zur

Verfügung. Für alle anderen Operanden können Sie entweder „ist“ oder „enthält“ als Operator auswählen. Wenn Sie den Operator „is“ auswählen, wird die Bedingung für eine exakte Übereinstimmung des Operandwerts mit dem für den ausgewählten Operand angegebenen Wert ausgewertet. Wenn Sie den Operator „contains“ auswählen, wird die Bedingung anhand eines der folgenden Kriterien bewertet:

- Der Operandwert ist eine exakte Übereinstimmung mit dem Wert des ausgewählten Operanden.
- Der Operandwert enthält den für den ausgewählten Operand angegebenen Wert.

Beispiel einer Anmerkungsregel mit Bedingungen

Betrachten Sie eine Anmerkungsregel mit einer Bedingungsgruppe für ein Volumen mit den folgenden beiden Bedingungen:

- Name enthält „vol“
- SVM-Name: „data_svm“

Diese Anmerkungsregel bezeichnet alle Volumes, die „vol“ in ihren Namen enthalten und auf SVMs mit dem Namen „data_svm“ mit der ausgewählten Annotation und dem Anmerkungstyp gehostet werden.

Bedingungsgruppen

Bedingungsgruppen werden mit logischem ODER ausgeführt und anschließend auf Speicherobjekte angewendet. Die Speicherobjekte müssen die Anforderungen einer der Bedingungsgruppen erfüllen, die mit Anmerkungen versehen werden sollen. Die Speicherobjekte, die den Bedingungen aller Bedingungsgruppen entsprechen, werden mit Anmerkungen versehen. Mithilfe von Bedingungsgruppen kann der Umfang der zu kommendenden Speicherobjekte erhöht werden.

Beispiel einer Anmerkungsregel mit Bedingungsgruppen

Berücksichtigen Sie eine Anmerkungsregel mit zwei Bedingungsgruppen für ein Volume; jede Gruppe enthält die folgenden zwei Bedingungen:

- Bedingungsgruppe 1
  - Name enthält „vol“
  - SVM-Name lautet „data_svm“. Diese Bedingungsgruppe bezeichnet alle Volumes, die „vol“ in ihren Namen enthalten und auf SVMs mit dem Namen „data_svm“ gehostet werden.
- Bedingungsgruppe 2
  - Name enthält „vol“
  - Der Anmerkungswert der Datenpriorität lautet „kritisch“. Diese Bedingungsgruppe bezeichnet alle Volumes, die „vol“ in ihren Namen enthalten und die mit dem Wert für die datenprioritäre Annotation mit „kritisch“ beschriftet werden.

Wenn eine Anmerkungsregel, die diese beiden Bedingungsgruppen enthält, auf Speicherobjekte angewendet wird, werden die folgenden Speicherobjekte kommentiert:

- Alle Volumes mit „vol“ in ihren Namen, die auf der SVM mit dem Namen „data_svm“ gehostet werden.
- Alle Volumes, die „vol“ in ihren Namen enthalten und mit dem Wert für Annotation mit Datenpriorität als „kritisch“ beschriftet werden.

Beschreibung der vordefinierten Anmerkungswerte

Data-Priority ist eine vordefinierte Anmerkung mit den Werten Mission Critical, High und Low. Mit diesen Werten können Sie Storage-Objekte anhand der Priorität der enthaltenen Daten annotieren. Sie können die vordefinierten Anmerkungswerte nicht bearbeiten oder löschen.

- **Datenpriorität:unternehmenskritisch**

  Diese Annotation wird auf Storage-Objekte angewendet, die geschäftskritische Daten enthalten. Objekte mit Produktionsapplikationen können beispielsweise als unternehmenskritisch angesehen werden.

- **Datenpriorität:hoch**

  Diese Annotation wird auf Storage-Objekte angewendet, die Daten mit hoher Priorität enthalten. Objekte, die Business-Applikationen hosten, gelten beispielsweise als hohe Priorität.

- **Datenpriorität:Niedrig**

  Diese Annotation wird auf Storage-Objekte angewendet, die Daten mit niedriger Priorität enthalten. Beispielsweise sind Objekte, die sich auf sekundärem Storage befinden, wie z. B. Ziele für Backups und Spiegelungen, von geringer Priorität.

Anmerkungen werden dynamisch hinzugefügt

Beim Erstellen benutzerdefinierter Annotationen ordnet Unified Manager Cluster, Storage Virtual Machines (SVMs) und Volumes anhand von Regeln dynamisch den Annotationen zu. Diese Regeln weisen die Anmerkungen automatisch den Speicherobjekten zu.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Klicken Sie auf der Seite **Anmerkungen** auf **Anmerkung hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkung hinzufügen** einen Namen und eine Beschreibung für die Anmerkung ein.
4. Optional: Klicken Sie im Abschnitt **Anmerkungswerte** auf **Hinzufügen**, um der Anmerkung Werte hinzuzufügen.
5. Klicken Sie Auf **Speichern**.

Hinzufügen von Werten zu Beschriftungen

Sie können Annotationen Werte hinzufügen und Speicherobjekte anschließend einem bestimmten Namenwertpaar der Anmerkung zuordnen. Durch das Hinzufügen von Werten zu Annotationen können Sie Storage-Objekte effizienter managen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können vordefinierten Anmerkungen keine Werte hinzufügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Wählen Sie auf der Seite **Anmerkungen** die Anmerkung aus, zu der Sie einen Wert hinzufügen möchten, und klicken Sie dann im Abschnitt **Werte** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkungswert** einen Wert für die Anmerkung an.

   Der von Ihnen angegebene Wert muss für die ausgewählte Anmerkung eindeutig sein.

4. Klicken Sie Auf **Hinzufügen**.

Anmerkungen werden gelöscht

Sie können benutzerdefinierte Anmerkungen und ihre Werte löschen, wenn sie nicht mehr benötigt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Die Anmerkungswerte dürfen nicht in anderen Anmerkungen oder Gruppenregeln verwendet werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungen** die zu löschende Anmerkung aus.

   Die Details der ausgewählten Anmerkung werden angezeigt.

3. Klicken Sie auf **Aktionen** > **Löschen**, um die ausgewählte Anmerkung und ihren Wert zu löschen.
4. Klicken Sie im Dialogfeld Warnung auf **Ja**, um den Löschvorgang zu bestätigen.

Anzeigen der Anmerkungsliste und der Details

Sie können eine Liste mit Anmerkungen anzeigen, die zu Clustern, Volumes und Storage Virtual Machines (SVMs) dynamisch zugeordnet werden. Sie können auch Details wie die Beschreibung anzeigen, erstellt von, erstellt Datum, Werte, Regeln, Und die mit der Anmerkung verknüpften Objekte.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungen** auf den Anmerkungsnamen, um die zugehörigen Details

anzuzeigen.

Löschen von Werten aus Anmerkungen

Sie können Werte löschen, die mit benutzerdefinierten Anmerkungen verknüpft sind, wenn dieser Wert nicht mehr für die Anmerkung gilt.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Der Anmerkungswert darf keiner Anmerkungsregel oder Gruppenregeln zugeordnet werden.

Über diese Aufgabe

Werte können nicht aus vordefinierten Anmerkungen gelöscht werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Wählen Sie in der Anmerkungsliste auf der Registerkarte **Anmerkungen** die Anmerkung aus, aus der Sie einen Wert löschen möchten.
3. Wählen Sie im Bereich **Werte** der Registerkarte **Anmerkungen** den Wert aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.
4. Klicken Sie im Dialogfeld **Warnung** auf **Ja**.

   Der Wert wird gelöscht und nicht mehr in der Liste der Werte für die ausgewählte Anmerkung angezeigt.

Anmerkungsregeln werden erstellt

Zudem können Anmerkungsregeln erstellt werden, die in Unified Manager verwendet werden, um Storage-Objekte wie Volumes, Cluster oder Storage Virtual Machines (SVMs) dynamisch anzunotieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Aktuell überwachte Storage-Objekte werden kommentiert, sobald die Anmerkungsregel erstellt wurde. Neue Objekte werden erst nach Abschluss des Überwachungszyklus mit Anmerkungen versehen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungsregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkungsregel hinzufügen** einen Namen für die Anmerkungsregel an.
4. Wählen Sie im Feld **Zielobjekttyp** den Typ des Speicherobjekts aus, das Sie mit Anmerkungen versehen möchten.

5. Wählen Sie in den Feldern **Anmerkung anwenden** den Anmerkungs- und Anmerkungswert aus, den Sie verwenden möchten.
6. Führen Sie im Abschnitt **Bedingungen** die entsprechende Aktion aus, um eine Bedingung, eine Bedingungsgruppe oder beide zu erstellen:

Zu erstellen…	Tun Sie das…
Ein Zustand	a. Wählen Sie einen Operand aus der Liste der Operanden aus. b. Wählen Sie als Operator entweder **enthält** oder **IS** aus. c. Geben Sie einen Wert ein, oder wählen Sie einen Wert aus der Liste verfügbar aus.
Eine Bedingungsgruppe	a. Klicken Sie Auf **Bedingungsgruppe Hinzufügen**. b. Wählen Sie einen Operand aus der Liste der Operanden aus. c. Wählen Sie als Operator entweder **enthält** oder **IS** aus. d. Geben Sie einen Wert ein, oder wählen Sie einen Wert aus der Liste verfügbar aus. e. Klicken Sie auf **Bedingung hinzufügen**, um bei Bedarf weitere Bedingungen zu erstellen, und wiederholen Sie die Schritte a bis d für jede Bedingung.

7. Klicken Sie Auf **Hinzufügen**.

Beispiel für das Erstellen einer Anmerkungsregel

Führen Sie im Dialogfeld Anmerkungsregel hinzufügen die folgenden Schritte aus, um eine Anmerkungsregel zu erstellen, einschließlich der Konfiguration einer Bedingung und des Hinzufügens einer Bedingungsgruppe:

1. Geben Sie einen Namen für die Anmerkungsregel an.
2. Wählen Sie den Zielobjekttyp als Storage Virtual Machine (SVM) aus.
3. Wählen Sie eine Anmerkung aus der Liste der Anmerkungen aus, und geben Sie einen Wert an.
4. Wählen Sie im Abschnitt Bedingungen als Operand **Objektname** aus.
5. Wählen Sie als Operator * enthält* aus.
6. Geben Sie den Wert als ein `svm_data`.
7. Klicken Sie auf **Bedingungsgruppe hinzufügen**.
8. Wählen Sie als Operand **Objektname** aus.
9. Wählen Sie als Operator * enthält* aus.
10. Geben Sie den Wert als ein `vol`.
11. Klicken Sie auf **Bedingung hinzufügen**.

12. Wiederholen Sie die Schritte 8 bis 10, indem Sie **Datenpriorität** als Operand in Schritt 8, **ist** als Operator in Schritt 9 und **unternehmenskritisch** als Wert in Schritt 10 auswählen.
13. Klicken Sie Auf **Hinzufügen**.

Anmerkungen manuell zu einzelnen Speicherobjekten hinzufügen

Ausgewählte Volumes, Cluster und SVMs lassen sich manuell und ohne Verwendung von Annotationsregeln beschriften. Sie können ein einzelnes Storage-Objekt oder mehrere Storage-Objekte mit Anmerkungen versehen und die erforderliche Kombination aus Name-Wert-Paaren für die Annotation angeben.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Navigieren Sie zu den Storage-Objekten, die Anmerkungen machen sollen:

So fügen Sie Kommentare hinzu:	Tun Sie das…
Cluster	a. Klicken Sie Auf **Storage** > **Cluster**. b. Wählen Sie ein oder mehrere Cluster aus.
Volumes	a. Klicken Sie Auf **Storage** > **Volumes**. b. Wählen Sie ein oder mehrere Volumes aus.
SVMs	a. Klicken Sie auf **Storage** > **SVMs**. b. Wählen Sie eine oder mehrere SVMs aus.

2. Klicken Sie auf **Annotate** und wählen Sie ein Name-Wert-Paar aus.
3. Klicken Sie Auf **Anwenden**.

Anmerkungsregeln werden bearbeitet

Sie können Anmerkungsregeln bearbeiten, um die Bedingungsgruppen und -Bedingungen innerhalb der Bedingungsgruppe zu ändern, um Anmerkungen zu Speicherobjekten hinzuzufügen oder sie aus ihnen zu entfernen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Anmerkungen werden vom Speicherobjekt distanziert, wenn Sie die zugehörigen Anmerkungsregeln bearbeiten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungsregeln** die Anmerkungsregel aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Aktionen** > **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Anmerkungsregel bearbeiten** den Regelnamen, den Anmerkungsnamen und den Wert, die Bedingungsgruppen und die Bedingungen nach Bedarf.

   Sie können den Zielobjekttyp für eine Anmerkungsregel nicht ändern.

4. Klicken Sie Auf **Speichern**.

Konfigurieren von Bedingungen für Anmerkungsregeln

Sie können eine oder mehrere Bedingungen konfigurieren, um Anmerkungsregeln zu erstellen, die Unified Manager für die Speicherobjekte anwendet. Die Speicherobjekte, die die Anmerkungsregel erfüllen, werden mit dem in der Regel angegebenen Wert versehen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungsregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkungsregel hinzufügen** einen Namen für die Regel ein.
4. Wählen Sie einen Objekttyp aus der Liste Zielobjekttyp aus, und wählen Sie dann einen Anmerkungsnamen und einen Wert aus der Liste aus.
5. Wählen Sie im Abschnitt **Bedingungen** des Dialogfelds einen Operanden und einen Operator aus der Liste aus und geben Sie einen Bedingungswert ein, oder klicken Sie auf **Bedingung hinzufügen**, um eine neue Bedingung zu erstellen.
6. Klicken Sie auf **Speichern und Hinzufügen**.

Beispiel für die Konfiguration einer Bedingung für eine Anmerkungsregel

Es empfiehlt sich eine Bedingung für den Objekttyp „SVM“, bei der der Objektname „`svm_Data`“ enthält.

Führen Sie die folgenden Schritte im Dialogfeld Anmerkungsregel hinzufügen durch, um die Bedingung zu konfigurieren:

1. Geben Sie einen Namen für die Anmerkungsregel ein.
2. Wählen Sie den Zielobjekttyp als SVM aus.
3. Wählen Sie eine Anmerkung aus der Liste der Anmerkungen und einen Wert aus.
4. Wählen Sie im Feld **Bedingungen** als Operand **Objektname** aus.
5. Wählen Sie als Operator * enthält* aus.
6. Geben Sie den Wert als ein `svm_data`.

7. Klicken Sie Auf **Hinzufügen**.

Anmerkungsregeln werden gelöscht

Anmerkungsregeln können Sie aus Active IQ Unified Manager löschen, wenn die Regeln nicht mehr benötigt werden.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Wenn Sie eine Anmerkungsregel löschen, wird die Anmerkung getrennt und aus den Speicherobjekten entfernt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungsregeln** die Anmerkungsregel aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie im Dialogfeld **Warnung** auf **Ja**, um den Löschvorgang zu bestätigen.

Anmerkungsregeln neu anordnen

Sie können die Reihenfolge ändern, in der Unified Manager Anmerkungsregeln auf Storage-Objekte anwendet. Anmerkungsregeln werden sequenziell auf Storage-Objekte basierend auf ihrer Rangfolge angewendet. Wenn Sie eine Anmerkungsregel konfigurieren, ist der Rang am wenigsten. Sie können den Rang der Anmerkungsregel jedoch je nach Ihren Anforderungen ändern.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können entweder eine einzelne oder mehrere Zeilen auswählen und viele Drag-and-Drop-Vorgänge durchführen, um den Rang der Anmerkungsregeln zu ändern. Sie müssen jedoch die Änderungen speichern, damit die Neupriorisierung auf der Registerkarte Anmerkungsregeln angezeigt werden kann.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungsregeln** auf **Neuordnung**.
3. Ziehen Sie im Dialogfeld **Anmerkungsregel neu anordnen** einzelne oder mehrere Zeilen per Drag-and-Drop, um die Reihenfolge der Anmerkungsregeln neu anzuordnen.
4. Klicken Sie Auf **Speichern**.

   Sie müssen die Änderungen speichern, damit die Neuordnung angezeigt werden kann.

Was für ein Unified Manager-Wartungsfenster ist

Sie definieren ein Unified Manager Wartungsfenster, um Ereignisse und Warnmeldungen für einen bestimmten Zeitraum zu unterdrücken, wenn Sie für eine Cluster-Wartung geplant haben und keine unerwünschte Benachrichtigungen erhalten möchten.

Wenn das Wartungsfenster beginnt, wird ein Ereignis „`Object Maintenance Window Started`“ auf der Seite „Event Management Inventory“ veröffentlicht. Dieses Ereignis wird automatisch veraltet, wenn das Wartungsfenster endet.

Während eines Wartungsfensters werden die Ereignisse, die sich auf alle Objekte im Cluster beziehen, weiterhin generiert, jedoch nicht in einer UI-Seite angezeigt und für diese Ereignisse werden keine Meldungen oder andere Arten von Benachrichtigungen gesendet. Sie können jedoch die Ereignisse anzeigen, die während eines Wartungsfensters für alle Speicherobjekte generiert wurden, indem Sie auf der Seite „Ereignismanagement-Bestand“ eine der Optionen „Ansicht“ auswählen.

Sie können ein Wartungsfenster für die Zukunft planen, die Start- und Endzeit für ein geplantes Wartungsfenster ändern und ein Wartungsfenster abbrechen.

Planen eines Wartungsfensters zum Deaktivieren der Cluster-Ereignisbenachrichtigungen

Wenn Sie z. B. vor einer geplanten Ausfallzeit für ein Cluster stehen, um ein Cluster zu aktualisieren oder einen der Nodes zu verschieben, können Sie die Ereignisse und Warnungen unterdrücken, die normalerweise während dieses Zeitfensters generiert werden würden, indem Sie ein Unified Manager Wartungsfenster planen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Während eines Wartungsfensters werden die Ereignisse, die mit allen Objekten auf dem Cluster zusammenhängen, weiterhin generiert, jedoch nicht auf der Ereignisseite angezeigt und für diese Ereignisse werden keine Meldungen oder andere Arten von Benachrichtigungen gesendet.

Die Zeit, die Sie für das Wartungsfenster eingeben, basiert auf der Zeit im Unified Manager-Server.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Cluster-Setup**.
2. Wählen Sie in der Spalte **Wartungsmodus** für den Cluster die Schieberegler-Schaltfläche aus, und verschieben Sie sie nach rechts.

   Das Kalenderfenster wird angezeigt.

3. Wählen Sie das Start- und Enddatum und die Uhrzeit für das Wartungsfenster aus und klicken Sie auf **Anwenden**.

   Neben dem Schieberegler wird die Meldung „`Scheduled`“ angezeigt.

Ergebnisse

Wenn die Startzeit erreicht ist, wechselt das Cluster in den Wartungsmodus und ein Ereignis „`Object Maintenance Window gestartet`“ wird generiert.

Ändern oder Abbrechen eines geplanten Wartungsfensters

Wenn Sie ein Wartungsfenster von Unified Manager für die Zukunft konfiguriert haben, können Sie die Start- und Endzeit ändern oder das Wartungsfenster nicht mehr ausführen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Das Abbrechen eines derzeit ausgeführten Wartungsfensters ist hilfreich, wenn Sie die Cluster-Wartung vor dem Ende des geplanten Wartungsfensters abgeschlossen haben und Sie möchten Ereignisse und Warnmeldungen vom Cluster erneut empfangen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Cluster-Setup**.
2. In der Spalte **Wartungsmodus** für den Cluster:

Ihr Ziel ist	Führen Sie diesen Schritt aus…
Ändern Sie den Zeitrahmen für ein geplantes Wartungsfenster	a. Klicken Sie neben dem Schieberegler auf den Text „`Scheduled`“. b. Ändern Sie das Start- und/oder Enddatum und die Uhrzeit, und klicken Sie auf **Anwenden**.
Verlängern Sie die Länge eines aktiven Wartungsfensters	a. Klicken Sie auf den Text „`Active`“ neben der Schieberegler-Schaltfläche. b. Ändern Sie das Enddatum und die Endzeit, und klicken Sie auf **Anwenden**.
Abbrechen eines geplanten Wartungsfensters	Wählen Sie die Schieberegler-Taste, und verschieben Sie sie nach links.
Abbrechen eines aktiven Wartungsfensters	Wählen Sie die Schieberegler-Taste, und verschieben Sie sie nach links.

Anzeigen von Ereignissen, die während eines Wartungsfensters aufgetreten sind

Bei Bedarf können Sie die Ereignisse anzeigen, die während eines Unified Manager-Wartungsfensters für alle Storage-Objekte generiert wurden. Die meisten Ereignisse

werden nach Abschluss des Wartungsfensters im Status „veraltet“ angezeigt und alle Systemressourcen werden gesichert und ausgeführt.

Bevor Sie beginnen

Mindestens ein Wartungsfenster muss abgeschlossen sein, bevor Ereignisse verfügbar sind.

Über diese Aufgabe

Ereignisse, die während eines Wartungsfensters aufgetreten sind, werden standardmäßig nicht auf der Seite „Inventar der Ereignisverwaltung“ angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Events**.

   Standardmäßig werden alle aktiven (neuen und bestätigten) Ereignisse auf der Seite „Ereignismanagement-Bestand“ angezeigt.

2. Wählen Sie im Fensterbereich **Ansicht** die Option **Alle Ereignisse, die während der Wartung generiert wurden**.

   Die Liste der Ereignisse, die in den letzten 7 Tagen aus allen Wartungsfenster und aus allen Clustern ausgelöst wurden, wird angezeigt.

3. Wenn mehrere Wartungsfenster für einen einzelnen Cluster vorhanden waren, können Sie auf das Kalendersymbol **ausgelöste Zeit** klicken und den Zeitraum für die Wartungsfenster-Ereignisse auswählen, die Sie interessieren.

Verwalten von SAML-Authentifizierungseinstellungen

Nachdem Sie die Remote-Authentifizierungseinstellungen konfiguriert haben, können Sie die SAML-Authentifizierung (Security Assertion Markup Language) aktivieren, sodass Remote-Benutzer von einem sicheren Identitäts-Provider (IdP) authentifiziert werden, bevor sie auf die Unified Manager Web-UI zugreifen können.

Beachten Sie, dass nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager haben, nachdem die SAML-Authentifizierung aktiviert wurde. Lokale Benutzer und Wartungbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Wartungskonsole zugreifen.

Anforderungen an Identitätsanbieter

Wenn Sie Unified Manager für die Verwendung eines Identitäts-Providers (IdP) konfigurieren, um die SAML-Authentifizierung für alle Remote-Benutzer durchzuführen, müssen Sie einige erforderliche Konfigurationseinstellungen beachten, damit die Verbindung zu Unified Manager erfolgreich hergestellt wird.

Sie müssen die Unified Manager-URI und die Metadaten im IdP-Server eingeben. Sie können diese Informationen von der Seite Unified ManagerSAML Authentication kopieren. Unified Manager gilt im SAML-Standard (Security Assertion Markup Language) als Service Provider (SP).

Unterstützte Verschlüsselungsstandards

- Advanced Encryption Standard (AES): AES-128 und AES-256
- Sicherer Hash-Algorithmus (SHA): SHA-1 und SHA-256

Validierte Identitätsanbieter

- Shibboleth
- Active Directory Federation Services (ADFS)

ADFS-Konfigurationsanforderungen

- Sie müssen drei Antragsregeln in der folgenden Reihenfolge definieren, die erforderlich sind, damit Unified Manager ADFS SAML-Antworten für diesen Vertrauenseintrag der Treuhandgesellschaft analysieren kann.

Forderungsregel	Wert
SAM-Account-Name	Name-ID
SAM-Account-Name	Urne:oid:0.9.2342.19200300.100.1.1
Token-Gruppen — Unqualifizierter Name	Urne:oid:1.3.6.1.4.1.5923.1.5.1.1

- Sie müssen die Authentifizierungsmethode auf „`Forms Authentication`“ setzen, oder Benutzer erhalten möglicherweise einen Fehler beim Abmelden von Unified Manager. Führen Sie hierzu folgende Schritte aus:
  a. Öffnen Sie die ADFS-Verwaltungskonsole.
  b. Klicken Sie in der linken Strukturansicht auf den Ordner Authentication Policies.
  c. Klicken Sie unter Aktionen auf der rechten Seite auf Globale primäre Authentifizierungsrichtlinie bearbeiten.
  d. Setzen Sie die Intranet-Authentifizierungsmethode auf „`Forms Authentication`“ anstatt auf die Standardauthentifizierung „`Windows Authentication`“.
- In einigen Fällen wird die Anmeldung über das IdP abgelehnt, wenn das Unified Manager-Sicherheitszertifikat CA-signiert ist. Es gibt zwei Problemumgehungen zur Lösung dieses Problems:
  - Befolgen Sie die Anweisungen im Link, um die Widerrufs-Prüfung auf dem ADFS-Server für verkettete CA-Zertifikat zugeordnete abhängige Partei zu deaktivieren:

    "Deaktivieren Sie die Überprüfung der Widerruferstellung pro Vertrauen der Vertrauensgruppe"

  - Der CA-Server befindet sich im ADFS-Server, um die Zertifiktanforderung des Unified Manager-Servers zu signieren.

Sonstige Konfigurationsanforderungen

- Die Unified Manager-Taktskew ist auf 5 Minuten eingestellt, sodass der Zeitunterschied zwischen dem IdP-Server und dem Unified Manager-Server nicht mehr als 5 Minuten betragen kann oder die Authentifizierung fehlschlägt.

Aktivieren der SAML-Authentifizierung

Sie können die SAML-Authentifizierung (Security Assertion Markup Language) aktivieren, sodass Remote-Benutzer von einem Secure Identity Provider (IdP) authentifiziert werden, bevor sie auf die Web-UI von Unified Manager zugreifen können.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung konfiguriert und bestätigt haben, dass sie erfolgreich ist.
- Sie müssen mindestens einen Remote-Benutzer oder eine Remote-Gruppe mit der Rolle „Anwendungsadministrator“ erstellt haben.
- Der Identitäts-Provider (IdP) muss von Unified Manager unterstützt und konfiguriert werden.
- Sie müssen über die IdP-URL und die Metadaten verfügen.
- Sie müssen Zugriff auf den IdP-Server haben.

Über diese Aufgabe

Nachdem Sie die SAML-Authentifizierung von Unified Manager aktiviert haben, können Benutzer erst dann auf die grafische Benutzeroberfläche zugreifen, wenn das IdP mit den Hostinformationen des Unified Manager-Servers konfiguriert wurde. Daher müssen Sie darauf vorbereitet sein, beide Teile der Verbindung abzuschließen, bevor Sie mit dem Konfigurationsprozess beginnen. Das IdP kann vor oder nach der Konfiguration von Unified Manager konfiguriert werden.

Nach Aktivierung der SAML-Authentifizierung haben nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager. Lokale Benutzer und Wartungbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Wartungskonsole, die Unified Manager-Befehle oder Zapis zugreifen.

Unified Manager wird automatisch neu gestartet, nachdem Sie die SAML-Konfiguration auf dieser Seite abgeschlossen haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **SAML Authentifizierung**.
2. Aktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.

   Die Felder, die zum Konfigurieren der IdP-Verbindung erforderlich sind, werden angezeigt.

3. Geben Sie die IdP-URI und die IdP-Metadaten ein, die erforderlich sind, um den Unified Manager-Server mit dem IdP-Server zu verbinden.

   Wenn der IdP-Server direkt über den Unified Manager-Server erreichbar ist, können Sie nach Eingabe der IdP-URI auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um das Feld IdP-Metadaten automatisch zu füllen.

4. Kopieren Sie den Unified Manager-Host-Metadaten-URI, oder speichern Sie die Host-Metadaten in eine XML-Textdatei.

   Sie können den IdP-Server derzeit mit diesen Informationen konfigurieren.

5. Klicken Sie Auf **Speichern**.

Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

6. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.

Ergebnisse

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldedaten auf der Anmeldeseite IdP statt auf der Anmeldeseite von Unified Manager ein.

Nachdem Sie fertig sind

Wenn noch nicht abgeschlossen ist, greifen Sie auf Ihr IdP zu, und geben Sie den URI und die Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

Wenn Sie ADFS als Identitäts-Provider verwenden, wird die Unified Manager-GUI nicht das ADFS-Timeout-Timeout erfüllt und funktioniert weiter, bis das Timeout der Unified Manager-Sitzung erreicht ist. Sie können das Timeout der GUI-Sitzung ändern, indem Sie auf **Allgemein** > **Feature-Einstellungen** > **Inaktivität Timeout** klicken.

Ändern des Identitäts-Providers, der für die SAML-Authentifizierung verwendet wird

Sie können den Identitäts-Provider (IdP), den Unified Manager zur Authentifizierung von Remote-Benutzern verwendet, ändern.

Bevor Sie beginnen

- Sie müssen über die IdP-URL und die Metadaten verfügen.
- Sie müssen Zugriff auf die IdP haben.

Über diese Aufgabe

Der neue IdP kann vor oder nach der Konfiguration von Unified Manager konfiguriert werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **SAML Authentifizierung**.
2. Geben Sie die neue IdP-URI und die IdP-Metadaten ein, die erforderlich sind, um den Unified Manager-Server mit dem IdP zu verbinden.

   Wenn der IdP direkt über den Unified Manager-Server aufgerufen werden kann, können Sie nach Eingabe der IdP-URL auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um das Feld IdP-Metadaten automatisch auszufüllen.

3. Kopieren Sie den Unified Manager-Metadaten-URI oder speichern Sie die Metadaten in eine XML-Textdatei.
4. Klicken Sie Auf **Konfiguration Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration ändern möchten.

5. Klicken Sie auf **OK**.

Nachdem Sie fertig sind

Greifen Sie auf den neuen IdP zu, und geben Sie die URI und die Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

Wenn die autorisierten Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldeinformationen auf der neuen Anmeldeseite für IdP anstelle der alten Anmeldeseite ein.

SAML-Authentifizierungseinstellungen werden nach Änderung des Unified Manager-Sicherheitszertifikats aktualisiert

Jede Änderung am HTTPS-Sicherheitszertifikat, das auf dem Unified Manager-Server installiert ist, erfordert, dass Sie die Einstellungen für die SAML-Authentifizierung aktualisieren. Das Zertifikat wird aktualisiert, wenn Sie das Hostsystem umbenennen, eine neue IP-Adresse für das Hostsystem zuweisen oder das Sicherheitszertifikat für das System manuell ändern.

Über diese Aufgabe

Nach der Änderung des Sicherheitszertifikats und dem Neustart des Unified Manager-Servers funktioniert die SAML-Authentifizierung nicht, und Benutzer können nicht auf die grafische Benutzeroberfläche von Unified Manager zugreifen. Sie müssen die SAML-Authentifizierungseinstellungen sowohl auf dem IdP-Server als auch auf dem Unified Manager-Server aktualisieren, um den Zugriff auf die Benutzeroberfläche wieder zu aktivieren.

Schritte

1. Melden Sie sich bei der Wartungskonsole an.
2. Geben Sie im **Hauptmenü** die Nummer für die Option **SAML-Authentifizierung deaktivieren** ein.

   Es wird eine Meldung angezeigt, die bestätigt, dass die SAML-Authentifizierung deaktiviert und Unified Manager neu gestartet werden soll.

3. Starten Sie die Unified Manager-Benutzeroberfläche mit der aktualisierten FQDN- oder IP-Adresse, akzeptieren Sie das aktualisierte Serverzertifikat in Ihrem Browser und melden Sie sich mit den Anmeldeinformationen für den Wartungsbenutzer an.
4. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML Authentication** aus und konfigurieren Sie die IdP-Verbindung.
5. Kopieren Sie den Unified Manager-Host-Metadaten-URI, oder speichern Sie die Host-Metadaten in eine XML-Textdatei.
6. Klicken Sie Auf **Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

7. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.
8. Greifen Sie auf Ihren IdP-Server zu, und geben Sie die URI und die Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

Identitäts-Provider	Konfigurationsschritte
ADFS	a. Löschen Sie den vorhandenen Vertrauenseintrag der Vertrauensantragenden Partei in der ADFS-Management-GUI. b. Fügen Sie mit dem einen neuen Vertrauenseintrag einer Vertrauensbasis hinzu `saml_sp_metadata.xml` Über den aktualisierten Unified Manager-Server aus. c. Definieren Sie die drei Forderungsregeln, die für Unified Manager erforderlich sind, um ADFS SAML-Antworten für diesen Vertrauenseintrag der Vertrauensbasis zu analysieren. d. Starten Sie den ADFS Windows-Dienst neu.
Shibboleth	a. Aktualisieren Sie den neuen FQDN des Unified Manager-Servers in das `attribute-filter.xml` Und `relying-party.xml` Dateien: b. Starten Sie den Apache Tomcat Webserver neu und warten Sie, bis Port 8005 online ist.

9. Melden Sie sich bei Unified Manager an und stellen Sie sicher, dass die SAML-Authentifizierung über Ihr IdP wie erwartet funktioniert.

Deaktivieren der SAML-Authentifizierung

Sie können die SAML-Authentifizierung deaktivieren, wenn Sie die Authentifizierung von Remote-Benutzern über einen sicheren Identitäts-Provider (IdP) beenden möchten, bevor sie sich in der Web-UI von Unified Manager anmelden können. Wenn die SAML-Authentifizierung deaktiviert ist, führen die konfigurierten Verzeichnisdienstanbieter wie Active Directory oder LDAP eine Anmeldeauthentifizierung durch.

Über diese Aufgabe

Nachdem Sie die SAML-Authentifizierung deaktiviert haben, können lokale Benutzer und Wartungbenutzer zusätzlich zu konfigurierten Remote-Benutzern auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML-Authentifizierung auch über die Unified Manager-Wartungskonsole deaktivieren, wenn Sie keinen Zugriff auf die grafische Benutzeroberfläche haben.

Unified Manager wird automatisch neu gestartet, nachdem die SAML-Authentifizierung deaktiviert ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **SAML Authentifizierung**.
2. Deaktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.

3. Klicken Sie Auf **Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

4. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.

Ergebnisse

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldedaten auf der Anmeldeseite von Unified Manager anstelle der IdP-Anmeldeseite ein.

Nachdem Sie fertig sind

Greifen Sie auf Ihren IdP zu und löschen Sie die URI und die Metadaten des Unified Manager-Servers.

Deaktivieren der SAML-Authentifizierung über die Wartungskonsole

Wenn kein Zugriff auf die Unified Manager GUI besteht, müssen Sie möglicherweise die SAML-Authentifizierung von der Wartungskonsole aus deaktivieren. Dies kann bei einer Fehlkonfiguration oder bei nicht zugänglichem IdP auftreten.

Bevor Sie beginnen

Sie müssen als Wartungbenutzer Zugriff auf die Wartungskonsole haben.

Über diese Aufgabe

Wenn die SAML-Authentifizierung deaktiviert ist, führen die konfigurierten Verzeichnisdienstanbieter wie Active Directory oder LDAP eine Anmeldeauthentifizierung durch. Lokale Benutzer und Wartungbenutzer können zusätzlich zu konfigurierten Remote-Benutzern auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML-Authentifizierung auch über die Seite Setup/Authentifizierung in der UI deaktivieren.

Unified Manager wird automatisch neu gestartet, nachdem die SAML-Authentifizierung deaktiviert ist.

Schritte

1. Melden Sie sich bei der Wartungskonsole an.
2. Geben Sie im **Hauptmenü** die Nummer für die Option **SAML-Authentifizierung deaktivieren** ein.

   Es wird eine Meldung angezeigt, die bestätigt, dass die SAML-Authentifizierung deaktiviert und Unified Manager neu gestartet werden soll.

3. Geben Sie **y** ein, und drücken Sie dann die Eingabetaste, und Unified Manager wird neu gestartet.

Ergebnisse

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldedaten auf der Anmeldeseite von Unified Manager anstelle der IdP-Anmeldeseite ein.

Nachdem Sie fertig sind

Greifen Sie bei Bedarf auf Ihr IdP zu, und löschen Sie die URL und Metadaten des Unified Manager-Servers.

Senden eines Unified Manager Support Bundle an den technischen Support

In diesem Workflow erfahren Sie, wie Sie über die Unified Manager Wartungskonsole ein Support Bundle generieren, abrufen und an den technischen Support senden. Sie sollten ein Support-Bundle senden, wenn das Problem, das Sie haben, detailliertere Diagnose und Fehlerbehebung erfordert als eine AutoSupport-Meldung.

Über diese Aufgabe

Unified Manager speichert maximal zwei generierte Support-Bundles gleichzeitig.

Weitere Informationen über die Wartungskonsole finden Sie im "Active IQ Unified Manager wird konfiguriert".

Zugriff auf die Wartungskonsole

Wenn die Benutzeroberfläche von Unified Manager nicht ausgeführt wird oder Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Wartungskonsole zugreifen, um Ihr Unified Manager System zu verwalten.

Bevor Sie beginnen

Sie müssen Unified Manager installiert und konfiguriert haben.

Über diese Aufgabe

Nach 15 Minuten Inaktivität meldet die Wartungskonsole sie aus.

> Wenn Sie auf VMware installiert sind und sich bereits über die VMware-Konsole als Wartungsbenutzer angemeldet haben, können Sie sich nicht gleichzeitig mit Secure Shell anmelden.

Schritte

1. Führen Sie die folgenden Schritte aus, um auf die Wartungskonsole zuzugreifen:

Auf diesem Betriebssystem…	Führen Sie die folgenden Schritte aus…
VMware	a. Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domänennamen der virtuellen Unified Manager-Appliance her. b. Melden Sie sich mit Ihrem Wartungs-Benutzernamen und -Passwort an der Wartungskonsole an.
Linux	a. Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domänennamen des Unified Manager-Systems her. b. Melden Sie sich beim System mit dem Wartungs-Benutzer (umadmin) und dem Passwort an. c. Geben Sie den Befehl ein `maintenance_console` Und drücken Sie die Eingabetaste.
Windows	a. Melden Sie sich mit den Administratoranmeldeinformationen beim Unified Manager-System an. b. Starten Sie PowerShell als Windows-Administrator. c. Geben Sie den Befehl ein `maintenance_console` Und drücken Sie die Eingabetaste.

Das Menü der Unified Manager-Wartungskonsole wird angezeigt.

Erstellen und Hochladen eines Supportpakets

Sie können ein Support-Paket mit Diagnoseinformationen erstellen, damit Sie es an den technischen Support senden können, um Hilfe zur Fehlerbehebung zu erhalten. Wenn Ihr Unified Manager Server ab Unified Manager 9.8 mit dem Internet verbunden ist, können Sie das Support Bundle über die Wartungskonsole auch auf NetApp hochladen.

Bevor Sie beginnen

Sie müssen als Wartungbenutzer Zugriff auf die Wartungskonsole haben.

Über diese Aufgabe

Da einige Arten von Support-Daten große Mengen von Cluster-Ressourcen verwenden oder sehr viel Zeit in Anspruch nehmen können, können Sie bei Auswahl des vollständigen Support-Pakets Datentypen angeben, die ein- oder ausschließen sollen, um die Größe des Support-Pakets zu verringern. Sie haben auch die Möglichkeit, ein einfaches Support-Bundle zu erstellen, das nur 30 Tage Protokolle und

Konfigurationsdatenbanken enthält - es schließt Performancedaten, Erfassungsdateien und Server Heap Dump aus.

Unified Manager speichert nur die zwei zuletzt erstellten Support Bundles. Ältere Supportpakete werden aus dem System gelöscht.

Schritte

1. Wählen Sie in der Wartungskonsole **Hauptmenü** die Option **Support/Diagnose**.
2. Wählen Sie * Light Support Bundle erzeugen* oder **Support Bundle generieren** abhängig von der Detailebene aus, die Sie im Support Bundle haben möchten.
3. Wenn Sie das vollständige Support-Paket auswählen, wählen Sie die folgenden Datentypen aus, die im Support-Bundle enthalten oder ausschließen sollen:

   - **Datenbankauszug**

     Ein Dump der MySQL Server Datenbank.

   - **Haufendump**

     Ein Snapshot des Status der wichtigsten Unified Manager Serverprozesse. Diese Option ist standardmäßig deaktiviert und sollte nur ausgewählt werden, wenn sie vom Kundendienst angefordert wird.

   - **Aufnahmeaufzeichnungen**

     Eine Aufzeichnung der gesamten Kommunikation zwischen Unified Manager und den überwachten Clustern.

   Wenn Sie die Auswahl aller Datentypen aufheben, wird das Support-Paket immer noch mit anderen Unified Manager-Daten generiert.

4. Typ `g`, Und drücken Sie dann die Eingabetaste, um das Supportpaket zu generieren.

   Da es sich bei der Generierung eines Support-Bundles um einen speicherintensiven Vorgang handelt, werden Sie aufgefordert zu überprüfen, ob Sie das Support-Bundle derzeit sicher erstellen möchten.

5. Typ `y`, Und drücken Sie dann die Eingabetaste, um das Supportpaket zu generieren.

   Wenn Sie das Support-Bundle derzeit nicht generieren möchten, geben Sie ein `n`, Und drücken Sie dann die Eingabetaste.

6. Wenn Sie Datenbank-Dump-Dateien in das vollständige Support-Bundle aufgenommen haben, werden Sie aufgefordert, den Zeitraum anzugeben, für den Performance-Statistiken enthalten sein sollen. Das Einführen von Performance-Statistiken kann viel Zeit und Speicherplatz beanspruchen, sodass Sie auch eine Dump-Datenbank ohne inklusive der Performance-Statistiken erstellen können:

   a. Geben Sie das Startdatum im Format YYYYMMDD ein.

      Geben Sie beispielsweise ein `20210101` Für den 1. Januar 2021. Eingabe `n` Wenn Sie nicht möchten, dass Performance-Statistiken aufgenommen werden sollen.

   b. Geben Sie die Anzahl der Tage der einzuführenden Statistiken ab 12 Uhr ein Am angegebenen Startdatum.

Sie können eine Zahl zwischen 1 und 10 eingeben.

Wenn Sie Performance-Statistiken vorhalten, zeigt das System den Zeitraum an, für den Performance-Statistiken erfasst werden sollen.

7. Nach Erstellung des Support Bundles werden Sie gefragt, ob Sie es nach NetApp hochladen möchten. Typ `y`, Und drücken Sie dann die Eingabetaste.

   Sie werden aufgefordert, Ihre Support-Case-Nummer einzugeben.

8. Wenn Sie bereits eine Case-Nummer haben, geben Sie die Nummer ein, und drücken Sie die Eingabetaste. Anderenfalls drücken Sie einfach die Eingabetaste.

   Das Support Bundle wird auf NetApp hochgeladen.

Nachdem Sie fertig sind

Wenn Ihr Unified Manager-Server nicht mit dem Internet verbunden ist oder Sie das Support-Paket aus einem anderen Grund nicht hochladen können, können Sie es abrufen und manuell senden. Sie können den Client mit einem SFTP-Client oder unter Verwendung von UNIX- oder Linux-CLI-Befehlen abrufen. Unter Windows-Installationen können Sie Remote Desktop (RDP) verwenden, um das Supportpaket abzurufen.

Das generierte Supportpaket befindet sich im `/support` Verzeichnis auf VMware Systemen, in `/opt/netapp/data/support/` Auf Linux-Systemen und in `ProgramData\NetApp\OnCommandAppData\ocum\support` Auf Windows-Systemen.

Abrufen des Support-Pakets über einen Windows-Client

Als Windows-Benutzer können Sie ein Tool herunterladen und installieren, um das Support-Paket von Ihrem Unified Manager-Server abzurufen. Sie können das Support Bundle an den technischen Support senden, um eine detailliertere Diagnose eines Problems zu erhalten. FileZilla oder WinSCP sind Beispiele für Werkzeuge, die Sie verwenden können.

Bevor Sie beginnen

Sie müssen der Wartungbenutzer sein, um diese Aufgabe ausführen zu können.

Sie müssen ein Werkzeug verwenden, das SCP oder SFTP unterstützt.

Schritte

1. Laden Sie ein Tool herunter und installieren Sie es, um das Support Bundle abzurufen.
2. Öffnen Sie das Werkzeug.
3. Stellen Sie über SFTP eine Verbindung mit dem Unified Manager-Managementserver her.

   Das Werkzeug zeigt den Inhalt des an `/support` Verzeichnis und Sie können alle bestehenden Support Bundles anzeigen.

4. Wählen Sie das Zielverzeichnis für das Supportpaket aus, das Sie kopieren möchten.
5. Wählen Sie das Supportpaket aus, das Sie kopieren möchten, und kopieren Sie die Datei vom Unified

Manager-Server auf Ihr lokales System.

Verwandte Informationen

"Filezilla - https://filezilla-project.org/"

"WinSCP - http://winscp.net"

Abrufen des Support-Pakets über einen UNIX oder Linux Client

Wenn Sie UNIX- oder Linux-Benutzer sind, können Sie das Support Bundle über Ihre vApp abrufen, indem Sie die Befehlszeilenschnittstelle (CLI) auf Ihrem Linux-Client-Server verwenden. Sie können das Supportpaket entweder mit SCP oder SFTP abrufen.

Bevor Sie beginnen

Sie müssen der Wartungbenutzer sein, um diese Aufgabe ausführen zu können.

Sie müssen ein Support-Bundle mit der Wartungskonsole generiert haben und den Support-Bundle-Namen haben.

Schritte

1. Greifen Sie über Telnet oder die Konsole auf die CLI über Ihren Linux-Client-Server zu.
2. Auf das zugreifen `/support` Verzeichnis.
3. Rufen Sie das Support Bundle ab und kopieren Sie es mit dem folgenden Befehl in das lokale Verzeichnis:

Sie verwenden…	Verwenden Sie dann den folgenden Befehl…
SCP	`scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`
SFTP	`sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`

   Der Name des Support-Pakets wird Ihnen bereitgestellt, wenn Sie es mit der Wartungskonsole erstellen.

4. Geben Sie das Wartungs-Benutzerpasswort ein.

Beispiele

Im folgenden Beispiel wird SCP verwendet, um das Supportpaket abzurufen:

```
        $ scp admin@10.10.12.69:/support/support_bundle_20160216_145359.7z
.
Password: <maintenance_user_password>
support_bundle_20160216_145359.7z   100%  119MB  11.9MB/s   00:10
```

Im folgenden Beispiel wird SFTP zum Abrufen des Supportpakets verwendet:

```
        $ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .
Password: <maintenance_user_password>
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

Senden eines Support Bundle an den technischen Support

Wenn ein Problem detailliertere Diagnose- und Fehlerbehebungsinformationen erfordert als eine AutoSupport Meldung, können Sie ein Support Bundle an den technischen Support senden.

Bevor Sie beginnen

Sie müssen Zugriff auf das Support-Bundle haben, um es an den technischen Support zu senden.

Sie müssen über die technische Support-Website eine Case-Nummer generiert haben.

Schritte

1. Loggen Sie sich auf der NetApp Support Site ein.
2. Laden Sie die Datei hoch.

   "Wie zum Hochladen einer Datei auf NetApp"

Aufgaben und Informationen im Zusammenhang mit mehreren Workflows

Einige Aufgaben und Referenztexte, die Ihnen helfen, einen Workflow zu verstehen und abzuschließen, sind für viele Workflows in Unified Manager üblich. Dazu gehören das Hinzufügen und Prüfen von Notizen zu einem Ereignis, das Zuweisen eines Ereignisses, das Erkennen und Beheben von Ereignissen sowie Details zu Volumes, Storage Virtual Machines (SVMs), Aggregaten, Und so weiter.

Hinzufügen und Überprüfen von Notizen zu einem Ereignis

Während Sie Ereignisse ansprechen, können Sie Informationen darüber hinzufügen, wie das Problem behoben wird, indem Sie den Bereich Hinweise und Aktualisierungen auf der Seite Ereignisdetails verwenden. Mit diesen Informationen kann ein anderer Benutzer aktiviert werden, der dem Ereignis zugewiesen ist. Sie können auch Informationen anzeigen, die vom Benutzer hinzugefügt wurden, der ein Ereignis zuletzt adressiert hat, basierend auf dem letzten Zeitstempel.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Events**.
2. Klicken Sie auf der Seite **Event Management** Inventory auf das Ereignis, für das Sie die ereignisbezogenen Informationen hinzufügen möchten.
3. Fügen Sie auf der Seite **Event** Details die erforderlichen Informationen im Bereich **Hinweise und Updates** ein.
4. Klicken Sie Auf **Post**.

Zuweisen von Ereignissen zu bestimmten Benutzern

Sie können nicht zugewiesene Ereignisse selbst oder anderen Benutzern, einschließlich Remote-Benutzern, zuweisen. Sie können zugewiesene Ereignisse bei Bedarf einem anderen Benutzer zuweisen. Wenn z. B. häufig Probleme an einem Storage-Objekt auftreten, können Sie den Benutzer, der das Objekt verwaltet, die Ereignisse für diese Probleme zuweisen.

Bevor Sie beginnen

- Der Name und die E-Mail-ID des Benutzers müssen korrekt konfiguriert sein.
- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**.
2. Wählen Sie auf der Seite **Event Management** Inventory ein oder mehrere Ereignisse aus, die Sie zuweisen möchten.
3. Ordnen Sie das Ereignis zu, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie das Ereignis zuweisen möchten…	Dann tun Sie das…
Sich Selbst.	Klicken Sie Auf **Zuweisen Zu** > **Mich**.

Wenn Sie das Ereignis zuweisen möchten…	Dann tun Sie das…
Einem anderen Benutzer	a. Klicken Sie auf **Zuweisen zu** > **anderer Benutzer**. b. Geben Sie im Dialogfeld Eigentümer zuweisen den Benutzernamen ein, oder wählen Sie einen Benutzer aus der Dropdown-Liste aus. c. Klicken Sie Auf **Zuweisen**. Der Benutzer erhält eine E-Mail-Benachrichtigung. Wenn Sie keinen Benutzernamen eingeben oder einen Benutzer aus der Dropdown-Liste auswählen und auf **Zuweisen** klicken, bleibt die Zuweisung des Ereignisses aufgehoben.

Bestätigen und Beheben von Ereignissen

Sie sollten ein Ereignis bestätigen, bevor Sie mit der Bearbeitung des Problems beginnen, das das Ereignis verursacht hat, damit Sie keine wiederholten Warnmeldungen erhalten. Nachdem Sie die Korrekturmaßnahme für ein bestimmtes Ereignis durchgeführt haben, sollten Sie das Ereignis als gelöst markieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Sie können mehrere Ereignisse gleichzeitig bestätigen und beheben.

Sie können keine Informationsereignisse bestätigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**.
2. Führen Sie in der Ereignisliste die folgenden Aktionen durch, um die Ereignisse zu bestätigen:

Ihr Ziel ist	Tun Sie das…
Bestätigen Sie ein einzelnes Ereignis und markieren Sie es als gelöst	a. Klicken Sie auf den Ereignisnamen. b. Bestimmen Sie auf der Seite Ereignisdetails die Ursache des Ereignisses. c. Klicken Sie Auf **Bestätigen**. d. Ergreifen Sie geeignete Korrekturmaßnahmen. e. Klicken Sie Auf **Als Gelöst Markieren**.
Bestätigen und markieren Sie mehrere Ereignisse als erledigt	a. Bestimmen Sie die Ursache der Ereignisse auf der entsprechenden Seite „Ereignisdetails“. b. Wählen Sie die Ereignisse aus. c. Klicken Sie Auf **Bestätigen**. d. Ergreifen Sie geeignete Korrekturmaßnahmen. e. Klicken Sie Auf **Als Gelöst Markieren**.

Nachdem das Ereignis als erledigt markiert wurde, wird das Ereignis in die Liste aufgelöster Ereignisse verschoben.

3. Fügen Sie im Bereich **Notizen und Updates** eine Notiz hinzu, wie Sie das Ereignis angesprochen haben, und klicken Sie dann auf **Post**.

Seite mit den Veranstaltungsdetails

Auf der Seite Ereignisdetails können Sie die Details eines ausgewählten Ereignisses anzeigen, z. B. den Schweregrad des Ereignisses, den Aufprallwert, den Aufprallbereich und die Ereignisquelle. Weitere Informationen zu möglichen Korrekturmaßnahmen können Sie zur Behebung des Problems einsehen.

- **Name Des Events**

  Der Name des Ereignisses und die Zeit, zu der das Ereignis zuletzt gesehen wurde.

  Bei Ereignissen ohne Leistungseinfall, während sich das Ereignis im Status „Neu“ oder „bestätigt“ befindet, sind die zuletzt erkannten Informationen nicht bekannt und daher verborgen.

- **Veranstaltungsbeschreibung**

  Eine kurze Beschreibung der Veranstaltung.

  In manchen Fällen wird in der Ereignisbeschreibung ein Grund für das ausgelöste Ereignis angegeben.

- **Komponente in Konflikt**

  Für dynamische Performance-Ereignisse werden in diesem Abschnitt Symbole angezeigt, die die logischen und physischen Komponenten des Clusters darstellen. Wenn eine Komponente einen Konflikt hat, ist ihr Symbol eingekreist und rot markiert.

  Siehe Cluster-Komponenten und warum sie über Konflikte verfügen können Für eine Beschreibung der

hier angezeigten Komponenten.

Die Abschnitte Ereignisinformationen, Systemdiagnose und vorgeschlagene Maßnahmen werden in anderen Themen beschrieben.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Notizen-Symbol**

  Ermöglicht Ihnen das Hinzufügen oder Aktualisieren von Notizen zum Ereignis und die Überprüfung aller von anderen Benutzern verbleibenden Notizen.

Aktionen Menü

- **Mir zuweisen**

  Weist Ihnen das Ereignis zu.

- **Anderen zuweisen**

  Öffnet das Dialogfeld „Eigentümer zuweisen“, in dem Sie das Ereignis anderen Benutzern zuweisen oder neu zuweisen können.

  Wenn Sie einem Benutzer ein Ereignis zuweisen, werden der Benutzername und die Uhrzeit, zu der das Ereignis zugewiesen wurde, in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt.

  Sie können auch die Zuweisung von Ereignissen aufheben, indem Sie das Feld Eigentumsrechte leer lassen.

- * Quittieren*

  Bestätigt die ausgewählten Ereignisse, damit Sie keine Wiederholungsbenachrichtigungen erhalten.

  Wenn Sie ein Ereignis bestätigen, werden Ihr Benutzername und die Zeit, zu der Sie das Ereignis bestätigt haben, in der Ereignisliste (bestätigt von) für die ausgewählten Ereignisse hinzugefügt. Wenn Sie ein Ereignis bestätigen, übernehmen Sie die Verantwortung für die Verwaltung dieses Ereignisses.

- **Als Gelöst Markieren**

  Ermöglicht Ihnen die Änderung des Ereignisstatus in „gelöst“.

  Wenn Sie ein Ereignis auflösen, werden Ihr Benutzername und die Zeit, zu der Sie das Ereignis aufgelöst haben, in der Ereignisliste (aufgelöst von) für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie Korrekturmaßnahmen für das Ereignis ergriffen haben, müssen Sie das Ereignis als gelöst markieren.

- **Alarm Hinzufügen**

  Zeigt das Dialogfeld Alarm hinzufügen an, in dem Sie eine Warnung für das ausgewählte Ereignis hinzufügen können.

Das wird im Abschnitt „Ereignisinformationen“ angezeigt

Über den Abschnitt „Ereignisinformationen“ auf der Seite „Ereignisdetails“ können Sie Details zu einem ausgewählten Ereignis anzeigen, z. B. den Schweregrad des Ereignisses, den Aufprallgrad, den Wirkungsbereich und die Ereignisquelle.

Felder, die nicht auf den Ereignistyp anwendbar sind, werden ausgeblendet. Sie können folgende Veranstaltungsdetails anzeigen:

- **Ereignis Trigger Zeit**

  Die Zeit, zu der das Ereignis generiert wurde.

- **Bundesland**

  Der Ereignisstatus: Neu, bestätigt, aufgelöst oder veraltet.

- **Veraltete Ursache**

  Die Aktionen, durch die das Ereignis veraltet war, z. B. wurde das Problem behoben.

- **Veranstaltungsdauer**

  Bei aktiven (neuen und bestätigten) Ereignissen handelt es sich um die Zeit zwischen der Erkennung und der Zeit, zu der das Ereignis zuletzt analysiert wurde. Bei veralteten Ereignissen ist dies die Zeit zwischen der Erkennung und dem Zeitpunkt, zu dem das Ereignis gelöst wurde.

  Dieses Feld wird für alle Performanceereignisse und für andere Ereignistypen angezeigt, nachdem sie aufgelöst oder veraltet sind.

- **Zuletzt Gesehen**

  Datum und Uhrzeit, zu der das Ereignis zuletzt als aktiv angesehen wurde.

  Bei Performanceereignissen kann dieser Wert höher sein als die Ereignis-Trigger-Zeit, da dieses Feld nach jeder neuen Sammlung von Performancedaten aktualisiert wird, solange das Ereignis aktiv ist. Bei anderen Arten von Ereignissen, wenn sich der Status Neu oder bestätigt befindet, wird dieser Inhalt nicht aktualisiert und das Feld wird daher ausgeblendet.

- **Severity**

  Der Schweregrad des Ereignisses: Kritisch (), Fehler (), Warnung (), und Informationen ().

- **Impact Level**

  Die Auswirkungen auf das Ereignis: Vorfall, Risiko, Ereignis oder Upgrade.

- **Aufprallbereich**

  Der Ereigniswirkungsbereich: Verfügbarkeit, Kapazität, Performance, Schutz, Konfiguration, Oder Sicherheit.

- **Quelle**

  Der Name des Objekts, auf dem das Ereignis aufgetreten ist.

Wenn sich die Details zu einem Ereignis für eine Shared QoS-Richtlinie anzeigen lassen, werden in diesem Feld bis zu drei Workload-Objekte aufgeführt, die die meisten IOPS oder MB/s verbrauchen.

Sie können auf den Link des Quellnamens klicken, um die Seite mit den Angaben zu Systemzustand oder Performance für das Objekt anzuzeigen.

- **Quellanmerkungen**

  Zeigt den Anmerkungsnamen und -Wert für das Objekt an, dem das Ereignis zugeordnet ist.

  Dieses Feld wird nur für Systemzustandsereignisse in Clustern, SVMs und Volumes angezeigt.

- **Quellgruppen**

  Zeigt die Namen aller Gruppen an, deren Mitglied das betroffene Objekt ist.

  Dieses Feld wird nur für Systemzustandsereignisse in Clustern, SVMs und Volumes angezeigt.

- **Quelltyp**

  Den Objekttyp (z. B. SVM, Volume oder Qtree), mit dem das Ereignis verknüpft ist.

- * Auf Cluster*

  Der Name des Clusters, an dem das Ereignis aufgetreten ist.

  Sie können auf den Cluster-Link klicken, um die Seite mit den Angaben zu Systemzustand und Performance für das Cluster anzuzeigen.

- **Betroffene Objekte Zählen**

  Die Anzahl der vom Ereignis betroffenen Objekte.

  Sie können auf den Objektlink klicken, um die Bestandsseite anzuzeigen, die mit den Objekten ausgefüllt wird, die aktuell von diesem Ereignis betroffen sind.

  Dieses Feld wird nur für Performanceereignisse angezeigt.

- * Betroffene Volumen*

  Die Anzahl der Volumes, die von diesem Ereignis betroffen sind.

  Dieses Feld wird nur für Performance-Ereignisse auf Nodes oder Aggregaten angezeigt.

- * Ausgelöste Richtlinie*

  Der Name der Schwellenwertrichtlinie, die das Ereignis ausgegeben hat.

  Sie können den Mauszeiger über den Richtliniennamen bewegen, um Details zur Schwellenwertrichtlinie anzuzeigen. Für anpassungsfähige QoS-Richtlinien werden die definierte Richtlinie, die Blockgröße und der Zuweisungstyp (zugewiesener Speicherplatz oder genutzter Speicherplatz) angezeigt.

  Dieses Feld wird nur für Performanceereignisse angezeigt.

- **Regel-Id**

Bei Active IQ-Plattformereignissen ist dies die Anzahl der Regel, die zur Generierung des Ereignisses ausgelöst wurde.

- * Bestätigt durch*

  Der Name der Person, die das Ereignis bestätigt hat und die Zeit, zu der das Ereignis bestätigt wurde.

- * Gelöst von*

  Der Name der Person, die das Ereignis gelöst hat, und die Zeit, zu der das Ereignis gelöst wurde.

- * Zugewiesen zu*

  Der Name der Person, die der Arbeit an dem Ereignis zugeordnet ist.

- **Warnmeldungseinstellungen**

  Die folgenden Informationen über Meldungen werden angezeigt:

  - Wenn dem ausgewählten Ereignis keine Warnmeldungen zugeordnet sind, wird ein Link **Alarm hinzufügen** angezeigt.

    Sie können das Dialogfeld Alarm hinzufügen öffnen, indem Sie auf den Link klicken.

  - Wenn dem ausgewählten Ereignis eine Warnung zugeordnet ist, wird der Alarmname angezeigt.

    Sie können das Dialogfeld Alarm bearbeiten öffnen, indem Sie auf den Link klicken.

  - Wenn dem ausgewählten Ereignis mehr als eine Warnung zugeordnet ist, wird die Anzahl der Warnmeldungen angezeigt.

    Sie können die Seite „Alarmkonfiguration“ öffnen, indem Sie auf den Link klicken, um weitere Details zu diesen Warnmeldungen anzuzeigen.

  Deaktivierte Warnmeldungen werden nicht angezeigt.

- **Letzte Benachrichtigung Gesendet**

  Das Datum und die Uhrzeit, zu der die letzte Benachrichtigung gesendet wurde.

- **Senden nach**

  Der Mechanismus, der zum Senden der Alarmierung verwendet wurde: E-Mail oder SNMP-Trap.

- **Vorheriger Skriptlauf**

  Der Name des Skripts, das beim Generieren der Warnmeldung ausgeführt wurde.

Anzeigen des Abschnitts Systemdiagnose

Im Abschnitt Systemdiagnose der Seite Ereignisdetails finden Sie Informationen, die Ihnen bei der Diagnose von Problemen helfen können, die möglicherweise für das Ereignis verantwortlich waren.

Dieser Bereich wird nur für bestimmte Ereignisse angezeigt.

Einige Performanceereignisse bieten Diagramme, die für das Ereignis relevant sind, das ausgelöst wurde. Dies beinhaltet in der Regel ein IOPS- oder MB/s-Diagramm und ein Latenzdiagramm für die vorherigen zehn Tage. Nach Absprache sehen Sie, welche Storage-Komponenten die Latenz am meisten beeinträchtigen oder von der Latenz beeinträchtigt werden, wenn das Ereignis aktiv ist.

Für dynamische Performance-Ereignisse werden die folgenden Diagramme angezeigt:

- Workload-Latenz: Zeigt den Verlauf der Latenz für die Top-Opfer, -Bully oder -Hai-Workloads bei den zu versagenden Komponenten an.
- Workload-Aktivität: Zeigt Details zur Workload-Nutzung der Cluster-Komponente an, die durch Konflikte verursacht wird.
- Resource Activity: Zeigt historische Performance-Statistiken für eine Clusterkomponente an, die mit einem Konflikt in der Cluster-Komponente Konflikt ist.

Andere Diagramme werden angezeigt, wenn einige Clusterkomponenten mit einem Konflikt zu belegen sind.

Andere Ereignisse liefern eine kurze Beschreibung der Analysetyp, die das System auf dem Storage-Objekt durchführt. In manchen Fällen gibt es eine oder mehrere Zeilen; eine für jede analysierte Komponente, für systemdefinierte Performance-Richtlinien, die mehrere Performance-Zähler analysieren. In diesem Szenario wird neben der Diagnose ein grünes oder rotes Symbol angezeigt, um anzugeben, ob ein Problem in dieser speziellen Diagnose gefunden wurde oder nicht.

Der Abschnitt „Empfohlene Maßnahmen“ wird angezeigt

Der Abschnitt „Empfohlene Maßnahmen“ auf der Seite „Veranstaltungsdetails“ enthält mögliche Gründe für das Ereignis und schlägt einige Maßnahmen vor, damit Sie versuchen können, das Ereignis selbst zu lösen. Die vorgeschlagenen Maßnahmen werden auf Grundlage der Art des Ereignisses oder des Schwellenwerts, die nicht eingehalten wurden, angepasst.

Dieser Bereich wird nur für bestimmte Ereignistypen angezeigt.

In einigen Fällen gibt es **Hilfe** Links auf der Seite, die zusätzliche Informationen für viele empfohlene Aktionen, einschließlich Anweisungen für die Durchführung einer bestimmten Aktion. Einige der Aktionen können die Verwendung von Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI-Befehlen oder einer Kombination dieser Tools umfassen.

Die hier vorgeschlagenen Maßnahmen sollten Sie nur als Anleitung zur Lösung dieses Ereignisses betrachten. Die Maßnahmen, die Sie zur Lösung dieses Ereignisses ergreifen, sollten auf dem Kontext Ihrer Umgebung beruhen.

Wenn Sie das Objekt und das Ereignis genauer analysieren möchten, klicken Sie auf die Schaltfläche **Workload analysieren**, um die Seite Workload Analysis anzuzeigen.

Es gibt bestimmte Ereignisse, die Unified Manager sorgfältig diagnostizieren und eine einzige Lösung anbieten kann. Wenn verfügbar, werden diese Auflösungen mit der Schaltfläche **Fix IT** angezeigt. Klicken Sie auf diese Schaltfläche, damit Unified Manager das Problem, das das Ereignis verursacht, behebt.

Bei Ereignissen der Active IQ Plattform kann dieser Abschnitt einen Link zu einem NetApp Knowledgebase Artikel enthalten, sofern verfügbar, der das Problem und mögliche Lösungen beschreibt. In Sites ohne externen Netzwerkzugriff wird lokal eine PDF-Datei des Knowledgebase-Artikels geöffnet. Die PDF-Datei ist Teil der Regeldatei, die Sie manuell in die Unified Manager-Instanz herunterladen.

Beschreibung der Ereignistypen

Jedes Ereignis ist mit einem Schweregrad verknüpft, der Ihnen dabei hilft, die Ereignisse zu priorisieren, die eine unmittelbare Korrekturmaßnahme erfordern.

- * Kritisch*

  Ein Problem, das zu einer Serviceunterbrechung führen kann, wenn keine Korrekturmaßnahmen sofort ergriffen werden.

  Performance-kritische Ereignisse werden nur von benutzerdefinierten Schwellenwerten gesendet.

- **Fehler**

  Die Event-Quelle befindet sich noch in einer Performance. Zur Vermeidung von Serviceunterbrechungen sind jedoch Korrekturmaßnahmen erforderlich.

- **Warnung**

  Bei der Event-Quelle kommt es zu einem Vorfall, den Sie beachten sollten, oder ein Performance-Zähler für ein Cluster-Objekt liegt außerhalb des normalen Bereichs und sollte überwacht werden, um sicherzustellen, dass der kritische Schweregrad nicht erreicht wurde. Ereignisse dieses Schweregrades führen nicht zu einer Serviceunterbrechung und unmittelbare Korrekturmaßnahmen sind möglicherweise nicht erforderlich.

  Ereignisse mit Performance-Warnmeldungen werden von benutzerdefinierten, systemdefinierten oder dynamischen Schwellenwerten gesendet.

- **Information**

  Das Ereignis tritt auf, wenn ein neues Objekt erkannt wird oder wenn eine Benutzeraktion durchgeführt wird. Beispiel: Wenn ein Storage-Objekt gelöscht wird oder wenn Konfigurationsänderungen vorliegen, wird das Ereignis mit dem Schweregrad „Informationen“ generiert.

  Informationsereignisse werden direkt von ONTAP gesendet, wenn eine Konfigurationsänderung erkannt wird.

Beschreibung der Level der Ereignisauswirkungen

Jedes Ereignis ist mit einer Folgenabstufe (Vorfall, Risiko, Ereignis oder Upgrade) verbunden, die Ihnen dabei hilft, Ereignisse zu priorisieren, die umgehend Korrekturmaßnahmen erfordern.

- **Vorfall**

  Ein Vorfall ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster keine Daten mehr für den Client bereitstellt, und nicht mehr genügend Speicherplatz zum Speichern von Daten vorhanden ist. Ereignisse mit Auswirkungen auf den Vorfall sind am schwersten. Um Serviceunterbrechungen zu vermeiden, sollten sofortige Korrekturmaßnahmen ergriffen werden.

- **Risiko**

  Ein Risiko ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster nicht mehr Daten für den Client bereitstellt, und nicht mehr genügend Speicherplatz zum Speichern von Daten vorhanden ist.

Ereignisse mit Risikoeinwirkung können zu Serviceunterbrechungen führen. Möglicherweise ist eine Korrekturmaßnahme erforderlich.

- **Veranstaltung**

  Ein Ereignis ist eine Statusänderung von Storage-Objekten und ihren Attributen. Ereignisse mit Auswirkungen auf das Ereignis dienen zur Information und erfordern keine Korrekturmaßnahmen.

- **Upgrade**

  Upgrade-Ereignisse sind ein bestimmter Ereignistyp, der von der Active IQ Plattform gemeldet wird. Diese Ereignisse erkennen Probleme, wenn für die Lösung ein Upgrade der ONTAP Software, Node-Firmware oder Betriebssystemsoftware erforderlich ist (für Sicherheitsempfehlungen). Möglicherweise möchten Sie für einige dieser Probleme sofortige Korrekturmaßnahmen durchführen, während andere Probleme möglicherweise bis zur nächsten geplanten Wartung warten können.

Beschreibung der Bereiche für Ereignisauswirkungen

Ereignisse werden in sechs Auswirkungsbereiche unterteilt (Verfügbarkeit, Kapazität, Konfiguration, Performance, Schutz, Und Sicherheit) damit Sie sich auf die Arten von Ereignissen konzentrieren können, für die Sie verantwortlich sind.

- **Verfügbarkeit**

  Verfügbarkeitsereignisse melden Sie, wenn ein Storage-Objekt offline geschaltet wird, wenn ein Protokollservice ausfällt, ein Problem mit dem Storage Failover auftritt oder wenn ein Problem mit der Hardware auftritt.

- * Kapazität*

  Kapazitätsereignisse benachrichtigen Sie, wenn sich Ihre Aggregate, Volumes, LUNs oder Namespaces nähern oder einen Größenschwellenwert erreicht haben oder die Wachstumsrate für Ihre Umgebung ungewöhnlich ist.

- **Konfiguration**

  Konfigurationsereignisse informieren Sie über die Erkennung, das Löschen, das Hinzufügen, das Entfernen oder Umbenennen Ihrer Storage-Objekte. Konfigurationsereignisse haben eine Auswirkung auf das Ereignis und einen Schweregrad der Informationen.

- **Leistung**

  Bei Performance-Ereignissen werden Sie über Ressourcen, Konfigurationen oder Aktivitätsbedingungen auf dem Cluster informiert, die negative Auswirkungen auf die Geschwindigkeit der Eingabe oder den Abruf von Daten-Storage für Ihre überwachten Storage-Objekte haben können.

- **Schutz**

  Schutzereignisse benachrichtigen Sie über Vorfälle oder Risiken im Zusammenhang mit SnapMirror Beziehungen, Probleme mit Zielkapazität, Probleme mit SnapVault Beziehungen oder Probleme mit Sicherungsaufgaben. Alle ONTAP Objekte (insbesondere Aggregate, Volumes und SVMs), die sekundäre Volumes und Sicherungsbeziehungen hosten, werden im Bereich der Sicherungsauswirkungen kategorisiert.

- **Sicherheit**

  Sicherheitsereignisse informieren Sie darüber, wie sicher Ihre ONTAP-Cluster, Storage Virtual Machines (SVMs) und Volumes auf den in definierten Parametern basieren "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9".

  Darüber hinaus umfasst dieser Bereich Upgrade-Ereignisse, die von der Active IQ-Plattform gemeldet werden.

Cluster-Komponenten und warum sie über Konflikte verfügen können

Sie können Probleme mit der Cluster-Performance identifizieren, wenn ein Konflikt zwischen einer Cluster-Komponente besteht. Die Performance der Workloads, die die Komponente nutzen, verlangsamen sich und ihre Reaktionszeit (Latenz) für Client-Anforderungen steigt. Dadurch wird ein Ereignis in Unified Manager ausgelöst.

Eine Komponente, die einen Konflikt verursacht, kann nicht auf einer optimalen Ebene ausgeführt werden. Die Performance ist gesunken, und die Performance anderer Cluster-Komponenten und Workloads, sogenannten *Opfern*, hat möglicherweise eine höhere Latenz zur Verfügung. Um die Konflikte einer Komponente zu beseitigen, müssen Sie ihre Workloads verringern oder die Fähigkeit erhöhen, mehr Arbeit zu erledigen, damit die Performance wieder auf das normale Niveau kommt. Da Unified Manager die Workload-Performance in fünf-Minuten-Intervallen erfasst und analysiert, wird nur erkannt, wenn eine Cluster-Komponente konsistent überlastet ist. Vorübergehende Überlastungsspitzen, die nur für eine kurze Dauer innerhalb des fünfminütigen Intervalls dauern, werden nicht erkannt.

Beispielsweise könnte ein Storage-Aggregat unter Konflikt stehen, da ein oder mehrere Workloads darauf konkurrierende, dass ihre I/O-Anfragen erfüllt werden. Andere Workloads auf dem Aggregat können beeinträchtigt werden, was zu einer Abnahme der Performance führt. Um die Aktivitätsmenge auf dem Aggregat zu verringern, können verschiedene Schritte durchgeführt werden, beispielsweise zum Verschieben von einem oder mehreren Workloads auf ein weniger ausgelastete Aggregat oder Node, um die allgemeinen Workload-Anforderungen des aktuellen Aggregats zu verringern. Bei einer QoS-Richtliniengruppe können Sie das Durchsatzlimit anpassen oder Workloads in eine andere Richtliniengruppe verschieben, sodass die Workloads nicht mehr gedrosselt werden.

Unified Manager überwacht die folgenden Cluster-Komponenten, um bei Engpässen eine Warnung zu erhalten:

- **Netzwerk**

  Zeigt die Wartezeit von I/O-Anfragen durch die externen Netzwerkprotokolle auf dem Cluster an. Die Wartezeit beträgt bis zum Abschluss von „`Transfer ready`“-Transaktionen, bevor das Cluster auf eine I/O-Anforderung reagieren kann. Wenn die Netzwerkkomponente stark betroffen ist, bedeutet dies, dass hohe Wartezeiten auf der Protokollebene die Latenz eines oder mehrerer Workloads beeinflussen.

- * Netzwerkverarbeitung*

  Repräsentiert die Softwarekomponente in dem Cluster, die mit I/O-Verarbeitung zwischen Protokollebene und Cluster beteiligt ist Der Knoten, der die Netzwerkverarbeitung verarbeitet, hat sich seit dem Erkennen des Ereignisses möglicherweise geändert. Wenn die Netzwerkverarbeitungskomponente einen Konflikt verursacht, bedeutet dies, dass eine hohe Auslastung des Node zur Netzwerkverarbeitung die Latenz eines oder mehrerer Workloads beeinträchtigt.

  Wenn Sie in einer aktiv/aktiv-Konfiguration ein All-SAN-Array-Cluster verwenden, wird der Wert für die

Netzwerklatenz für beide Nodes angezeigt, sodass Sie überprüfen können, ob die Nodes die Last gleichmäßig teilen.

- **QoS-Limit max.**

  Steht für den maximalen Durchsatz (Spitzenwert) der dem Workload zugewiesenen Richtliniengruppe für Storage Quality of Service (QoS). Wenn die Richtliniengruppe Konflikte hat, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch das festgelegte Durchsatzlimit gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- * QoS Limit Min.*

  Zeigt die Latenz einem Workload an, der durch die dem anderen Workload zugewiesene Mindestmenge für den QoS-Durchsatz (erwartet) verursacht wird. Wenn das QoS-Minimum für bestimmte Workloads den Großteil der Bandbreite verwendet, um den versprochenen Durchsatz zu gewährleisten, werden andere Workloads gedrosselt und es wird mehr Latenz erreicht.

- * Cluster Interconnect*

  Stellt die Kabel und Adapter dar, mit denen die physischen Nodes des Clustern verbunden sind. Wenn die Cluster-Interconnect-Komponente einen Konflikt verursacht, bedeutet dies hohe Wartezeiten bei I/O-Anfragen am Cluster Interconnect, die sich auf die Latenz eines oder mehrerer Workloads auswirken.

- **Datenverarbeitung**

  Zeigt die Softwarekomponente in dem Cluster an, die mit I/O-Verarbeitung zwischen dem Cluster und dem Storage-Aggregat, das den Workload enthält. Der Node, der die Datenverarbeitung verarbeitet, hat sich seit dem Erkennen des Ereignisses geändert. Wenn die Datenverarbeitungkomponente einen Konflikt verursacht, bedeutet dies, dass eine hohe Auslastung am Datenverarbeitungs-Node die Latenz eines oder mehrerer Workloads beeinträchtigt.

- **Volume-Aktivierung**

  Stellt den Prozess dar, der die Nutzung aller aktiven Volumes verfolgt. In großen Umgebungen, in denen mehr als 1000 Volumes aktiv sind, verfolgt dieser Prozess, wie viele kritische Volumes gleichzeitig auf Ressourcen über den Node zugreifen müssen. Wenn die Anzahl gleichzeitiger aktiver Volumes den empfohlenen maximalen Schwellenwert überschreitet, kommt es bei einigen der nicht kritischen Volumes zu einer Latenz, die hier angegeben wurde.

- **MetroCluster Ressourcen**

  Repräsentiert die MetroCluster-Ressourcen, einschließlich NVRAM und Interswitch Links (ISLs), die zur Spiegelung von Daten zwischen Clustern in einer MetroCluster Konfiguration verwendet werden. Wenn die MetroCluster Komponente Konflikte verursacht, bedeutet dies einen hohen Schreibdurchsatz von Workloads auf dem lokalen Cluster oder ein Link-Systemzustandsproblem Auswirkungen auf die Latenz einer oder mehrerer Workloads auf dem lokalen Cluster. Wenn das Cluster nicht in einer MetroCluster-Konfiguration befindet, wird dieses Symbol nicht angezeigt.

- **Aggregate oder SSD Aggregate Ops**

  Repräsentiert das Storage-Aggregat, auf dem die Workloads ausgeführt werden Wenn die Aggregat-Komponente Konflikte verursacht, bedeutet dies, dass eine hohe Auslastung des Aggregats sich auf die Latenz eines oder mehrerer Workloads auswirkt. Ein Aggregat besteht aus allen HDDs oder einer Kombination aus HDDs und SSDs (einem Flash Pool Aggregat) oder einer Kombination aus HDDs und einem Cloud Tier (einem FabricPool Aggregat). Ein „`SSD Aggregat`“ besteht aus allen SSDs (ein All-

Flash-Aggregat) oder einer Kombination aus SSDs und einer Cloud Tier (ein FabricPool Aggregat).

- **Cloud-Latenz**

  Stellt die Softwarekomponente in dem Cluster dar, die mit I/O-Verarbeitung zwischen dem Cluster und dem Cloud-Tier beschäftigt ist, auf dem Benutzerdaten gespeichert werden Wenn die Komponente für die Cloud-Latenz aufgrund von Konflikten vorliegen, bedeutet dies, dass sich ein großer Anteil der in der Cloud-Ebene gehosteten Lesevorgänge auf die Latenz eines oder mehrerer Workloads auswirkt.

- **Sync SnapMirror**

  Repräsentiert die Software-Komponente in dem Cluster, die mit der Replizierung von Benutzerdaten vom primären Volume auf das sekundäre Volume in einer SnapMirror Synchronous-Beziehung beteiligt ist Wenn die synchrone SnapMirror Komponente Konflikte verursacht, bedeutet dies, dass die Aktivitäten des synchronen Betriebs von SnapMirror sich auf die Latenz eines oder mehrerer Workloads auswirken.

Hinzufügen von Meldungen

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

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 Skript “Test”, und der Benutzer muss alle 15 Minuten benachrichtigt werden

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

1. Klicken Sie auf **Name** und geben Sie ein `HealthTest` Im Feld **Alarmname**.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
   a. Eingabe `abc` Im Feld **Name enthält** werden die Volumes angezeigt, deren Name „`abc`“ enthält.
   b. Wählen Sie **<<All Volumes whose name contains 'abc'>>** aus dem Bereich Verfügbare Ressourcen und in den Bereich Ausgewählte Ressourcen verschieben.
   c. Klicken Sie auf **Ausschließe**, und geben Sie ein `xyz` Klicken Sie im Feld **Name enthält** auf **Hinzufügen**.

3. Klicken Sie auf **Events** und wählen Sie im Feld Ereignis Severity * die Option **kritisch** aus.
4. Wählen Sie im Bereich passende Ereignisse die Option * Alle kritischen Ereignisse* aus, und verschieben Sie sie in den Bereich Ausgewählte Ereignisse.
5. Klicken Sie auf **Aktionen** und geben Sie ein `sample@domain.com` Im Feld „Diese Benutzer benachrichtigen“.
6. Wählen Sie **alle 15 Minuten**, um den Benutzer alle 15 Minuten zu benachrichtigen.

   Sie können eine Warnung konfigurieren, um wiederholt Benachrichtigungen an die Empfänger für eine bestimmte Zeit zu senden. Legen Sie fest, zu welchem Zeitpunkt die Ereignisbenachrichtigung für die Warnmeldung aktiv ist.
7. Wählen Sie im Menü Skript zum Ausführen auswählen die Option **Test**-Skript aus.
8. Klicken Sie Auf **Speichern**.

Seite „Volume/Health Details“

Auf der Seite Volume/Health Details können Sie ausführliche Informationen zu einem ausgewählten Volume anzeigen, z. B. Kapazität, Storage-Effizienz, Konfiguration, Sicherung, Kommentare und erzeugte Ereignisse. Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für dieses Volume anzeigen.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für das ausgewählte Volume ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Ermöglicht die Navigation zur Seite Volume-/Performance-Details.

- **Aktionen**
  - Alarm Hinzufügen

    Ermöglicht das Hinzufügen einer Warnmeldung zum ausgewählten Volume.
  - Schwellenwerte Bearbeiten

    Ermöglicht das Ändern der Schwellenwerteinstellungen für das ausgewählte Volume.
  - Anmerkungen Hinzufügen

    Ermöglicht Ihnen, das ausgewählte Volume mit Anmerkungen zu versehen.
  - Sichern

    Ermöglicht die Erstellung von SnapMirror oder SnapVault Beziehungen für das ausgewählte Volume.
  - Beziehung

    Ermöglicht Ihnen die Ausführung folgender Sicherungsbeziehungsvorgänge:

- Bearbeiten

  Öffnet das Dialogfeld „Beziehung bearbeiten“, in dem Sie vorhandene SnapMirror Richtlinien, Zeitpläne und maximale Übertragungsraten für eine vorhandene Sicherungsbeziehung ändern können.

- Abbrechen

  Bricht Transfers ab, die für eine ausgewählte Beziehung in Bearbeitung sind. Optional können Sie den Checkpoint beim Neustart für andere Transfers als den Basistransfer entfernen. Sie können den Kontrollpunkt für einen Basistransfer nicht entfernen.

- Stilllegen

  Zeitweilige Aktualisierungen für eine ausgewählte Beziehung werden vorübergehend deaktiviert. Transfers, die bereits in Bearbeitung sind, müssen vor der Stilllegung abgeschlossen werden.

- Pause

  Bricht die Beziehung zwischen Quell- und Zielvolumen ab und ändert das Ziel in ein Lese-Schreib-Volume.

- Entfernen

  Löscht dauerhaft die Beziehung zwischen der ausgewählten Quelle und dem ausgewählten Ziel. Die Volumes werden nicht zerstört und die Snapshot-Kopien auf den Volumes werden nicht entfernt. Dieser Vorgang kann nicht rückgängig gemacht werden.

- Fortsetzen

  Ermöglicht geplante Transfers für eine stillgelegte Beziehung. Beim nächsten geplanten Transferintervall wird ein Neustart-Checkpoint verwendet, falls vorhanden.

- Neu Synchronisieren

  Ermöglicht Ihnen die Neusynchronisierung einer zuvor unterbrochenen Beziehung.

- Initialisierung/Aktualisierung

  Ermöglicht Ihnen, eine erste Basistransfer für eine neue Schutzbeziehung durchzuführen oder eine manuelle Aktualisierung durchzuführen, wenn die Beziehung bereits initialisiert ist.

- Reverse Resync

  Ermöglicht Ihnen die Wiederherstellung einer zuvor unterbrochenen Schutzbeziehung, indem Sie die Funktion von Quelle und Ziel umkehren, indem Sie der Quelle eine Kopie des ursprünglichen Ziels machen. Der Inhalt der Quelle wird durch den Inhalt des Ziels überschrieben, und alle Daten, die neuer als die Daten der gemeinsamen Snapshot Kopie sind, werden gelöscht.

◦ Wiederherstellen

Ermöglicht Ihnen die Wiederherstellung von Daten von einem Volume auf einem anderen Volume.

Die Schaltfläche „Wiederherstellen“ und die Schaltflächen zum Beziehungsvorgang stehen für Volumes, die sich in synchronen Schutzbeziehungen befinden, nicht zur Verfügung.

- **View Volumes**

  Ermöglicht Ihnen die Navigation zur Ansicht „Systemzustand: Alle Volumes“.

Registerkarte „Kapazität“

Auf der Registerkarte Kapazität werden Details zum ausgewählten Volume angezeigt, z. B. seine physische Kapazität, logische Kapazität, Schwellwerte, Kontingentkapazität und Informationen über jede beliebige Volume-Verschiebung:

- **Kapazität Physisch**

  Detaillierte Informationen zur physischen Kapazität des Volumes:

  - Snapshot-Überlauf

    Zeigt den Speicherplatz an, der von den Snapshot Kopien verbraucht wird.

  - Verwendet

    Zeigt den Speicherplatz an, der von Daten im Volume verwendet wird.

  - Warnung

    Zeigt an, dass der Speicherplatz im Volume fast voll ist. Wird diese Schwelle nicht erreicht, wird das Ereignis „Space Fast Full“ generiert.

  - Fehler

    Zeigt an, dass der Speicherplatz im Volume voll ist. Wird dieser Schwellenwert nicht erreicht, wird das Ereignis „Space Full“ generiert.

  - Nicht Nutzbar

    Zeigt an, dass der risikobehaftete Speicherplatz des Thin Provisioning Volume generiert wird und dass der Speicherplatz im Thin Provisioning Volume aufgrund von Kapazitätsproblemen im Aggregat gefährdet ist. Die nicht nutzbare Kapazität wird nur für Volumes angezeigt, die über Thin Provisioning bereitgestellt wurden.

  - Datendiagramm

    Zeigt die Gesamtkapazität und die genutzte Datenkapazität des Volume an.

    Wenn Autogrow aktiviert ist, wird im Datendiagramm der verfügbare Speicherplatz im Aggregat angezeigt. Das Datendiagramm zeigt den effektiven Speicherplatz, der von Daten auf dem Volume genutzt werden kann. Dies kann einer der folgenden Werte sein:

    - Tatsächliche Datenkapazität des Volumes für die folgenden Bedingungen:
      - Autogrow ist deaktiviert.
      - Das autogrow-fähige Volume hat die maximale Größe erreicht.
      - Autogrow-aktivierte Volumes mit Thick Provisioning können nicht weiter wachsen.
    - Datenkapazität des Volumes unter Berücksichtigung der maximalen Volume-Größe (für Volumes mit Thin Provisioning und für Thick Provisioning Volumes, wenn das Aggregat über genügend Platz

für das Volume verfügt, um die maximale Größe zu erreichen)

- Datenkapazität des Volumes nach Berücksichtigung der nächsten möglichen Autogrow Größe (für Thick Provisioning Volumes, die einen Autogrow-Prozentwert haben)

◦ Diagramm Snapshot Kopien

Dieses Diagramm wird nur angezeigt, wenn die verwendete Snapshot-Kapazität oder die Snapshot-Reserve nicht null ist.

Beide Diagramme zeigen die Kapazität an, um die die Snapshot-Kapazität die Snapshot-Reserve überschreitet, wenn die verwendete Snapshot-Kapazität die Snapshot-Reserve überschreitet.

- **Kapazität Logisch**

Zeigt die logischen Platzeigenschaften des Volumes an. Der logische Speicherplatz gibt die tatsächliche Größe der auf Festplatte gespeicherten Daten an, ohne dabei die Einsparungen durch die ONTAP Storage-Effizienztechnologien zu verwenden.

◦ Bericht Zu Logischem Speicherplatz

Zeigt an, ob für das Volume ein Bericht über den logischen Speicherplatz konfiguriert ist. Der Wert kann aktiviert, deaktiviert oder nicht zutreffend sein. „`not anwendbare`“ wird für Volumes auf älteren ONTAP-Versionen oder auf Volumes angezeigt, die kein logisches Speicherplatz-Reporting unterstützen.

◦ Verwendet

Zeigt die Menge des logischen Speicherplatzes an, der von Daten im Volume verwendet wird, und den Prozentsatz des logischen Speicherplatzes, der basierend auf der Gesamtkapazität genutzt wird.

◦ Durchsetzung Des Logischen Speicherplatzes

Zeigt an, ob die Durchsetzung des logischen Speicherplatzes für über Thin Provisioning bereitgestellte Volumes konfiguriert ist. Bei Einstellung auf aktiviert kann die verwendete logische Größe des Volumes nicht größer sein als die aktuell eingestellte physische Volume-Größe.

- **Autogrow**

Zeigt an, ob das Volumen automatisch wächst, wenn es nicht mehr genügend Speicherplatz hat.

- * Raumgarantie*

Zeigt die FlexVol-Lautstärkeregelung an, wenn ein Volume freie Blöcke aus einem Aggregat entfernt. Diese Blöcke sind dann garantiert für Schreibvorgänge auf Dateien im Volume verfügbar. Die Speicherplatzgarantie kann auf eine der folgenden gesetzt werden:

◦ Keine

Es wurde keine Speicherplatzzusage für das Volume konfiguriert.

◦ Datei

Die vollständige Größe von dünn geschriebenen Dateien (zum Beispiel LUNs) ist garantiert.

◦ Datenmenge

Die volle Größe des Volumens wird garantiert.

- Teilweise

  Das FlexCache-Volume reserviert basierend auf seiner Größe Speicherplatz. Wenn die Größe des FlexCache-Volumes 100 MB oder mehr ist, ist die Mindestplatzgarantie standardmäßig auf 100 MB gesetzt. Wenn die Größe des FlexCache-Volumes weniger als 100 MB ist, wird die Mindestplatzgarantie auf die Größe des FlexCache-Volumes gesetzt. Wenn die Größe des FlexCache-Volumes später erhöht wird, wird die Mindestplatzgarantie nicht erhöht.

Die Speicherplatzzusage ist ein Teil, wenn es sich um ein Volume vom Typ Data-Cache handelt.

- **Details (Physisch)**

  Zeigt die physischen Merkmale des Volumes an.

- **Gesamtkapazität**

  Zeigt die gesamte physische Kapazität im Volume an.

- **Datenkapazität**

  Zeigt den vom Volume genutzten physischen Speicherplatz (genutzte Kapazität) und die Menge an verfügbarem (freier Kapazität) physischen Speicherplatz im Volume an. Diese Werte werden auch als Prozentsatz der gesamten physischen Kapazität angezeigt.

  Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, wird die vom Volume verwendete Menge an Speicherplatz (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht verwendet werden kann (nicht nutzbare Kapazität), da die Kapazität des Aggregats angezeigt wird.

- **Snapshot Reserve**

  Zeigt die Menge an Speicherplatz an, der von den Snapshot Kopien verwendet (genutzte Kapazität) und die Menge an Speicherplatz, die für Snapshot Kopien verfügbar ist (freie Kapazität) im Volume an. Diese Werte werden auch als Prozentsatz der gesamten Snapshot-Reserve angezeigt.

  Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, dann wird die Menge an Speicherplatz, der von den Snapshot Kopien verwendet wird (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht für die Erstellung von Snapshot Kopien verwendet werden kann (nicht nutzbare Kapazität). Aufgrund von Aggregat-Kapazitätsproblemen wird angezeigt.

- **Volumenschwellwerte**

  Zeigt die folgenden Schwellenwerte für die Volume-Kapazität an:

  - Nahezu Vollständig. Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Volumen fast voll ist.

  - Vollständiger Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Volume voll ist.

- **Weitere Details**
  - Autogrow Maximalgröße

    Zeigt die maximale Größe an, bis die Lautstärke automatisch erweitert werden kann. Der Standardwert ist 120 % der Volume-Größe bei der Erstellung. Dieses Feld wird nur angezeigt, wenn Autogrow für das Volume aktiviert ist.

  - Der Qtree Kontingent Verplante Kapazität

    Zeigt den Speicherplatz an, der in den Quoten reserviert wurde.

  - Qtree-Kontingent Überbeansprucht Kapazität

    Zeigt die Menge an Speicherplatz an, die verwendet werden kann, bevor das System das überverplante Ereignis des Volume Qtree-Kontingents generiert.

  - Fraktionale Reserve

    Steuert die Größe der Überschreibungsreserve. Standardmäßig ist die fraktionale Reserve auf 100 festgelegt und gibt an, dass 100 Prozent des erforderlichen reservierten Speicherplatzes reserviert werden, damit die Objekte für Überschreibungen vollständig gesichert sind. Wenn die fraktionale Reserve weniger als 100 Prozent beträgt, wird der reservierte Speicherplatz für alle platzreservierten Dateien in diesem Volume auf den Prozentsatz der fraktionalen Reserve reduziert.

  - Tägliche Snapshot Wachstumsrate

    Zeigt die Änderung an (in Prozent oder in KB, MB, GB usw.), die alle 24 Stunden in den Snapshot Kopien des ausgewählten Volumes stattfindet.

  - Snapshot Tage voll belegt

    Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor der für die Snapshot Kopien im Volume reservierte Speicherplatz den angegebenen Schwellenwert erreicht.

    Das Feld „Snapshot Days to Full“ zeigt einen nicht anwendbaren Wert an, wenn das Wachstum der Snapshot-Kopien im Volume null oder negativ ist oder wenn es keine Daten zur Berechnung der Wachstumsrate gibt.

  - Snapshot Automatisch Löschen

    Gibt an, ob Snapshot Kopien automatisch in freien Speicherplatz gelöscht werden, wenn ein Schreibvorgang auf ein Volume aufgrund von fehlendem Speicherplatz im Aggregat ausfällt.

  - Snapshots

    Zeigt Informationen über die Snapshot-Kopien im Volume an.

    Die Anzahl der Snapshot Kopien auf dem Volume wird als Link angezeigt. Wenn Sie auf den Link klicken, werden die Snapshot Kopien in dem Dialogfeld Volume geöffnet, in dem Details zu den Snapshot Kopien angezeigt werden.

Die Anzahl der Snapshot Kopien wird etwa jede Stunde aktualisiert. Die Liste der Snapshot-Kopien wird jedoch zu dem Zeitpunkt aktualisiert, zu dem Sie auf das Symbol klicken. Dies kann zu einem Unterschied zwischen der in der Topologie angezeigten Anzahl der Snapshot Kopien und der Anzahl der aufgelisteten Snapshot Kopien führen, wenn Sie auf das Symbol klicken.

- **Volume Move**

  Zeigt den Status der aktuellen oder der letzten Volume-Verschiebung an, die am Volume durchgeführt wurde, und weitere Details an, z. B. die aktuelle Phase der Verschiebung eines Volumes – im Gange ist, das Quellaggregat, das Zielaggregat, die Startzeit, die Endzeit, Und die geschätzte Endzeit.

  Zeigt außerdem die Anzahl der Vorgänge zum Verschieben von Volumes an, die auf dem ausgewählten Volume ausgeführt werden. Weitere Informationen über die Vorgänge zum Verschieben von Volumes erhalten Sie, indem Sie auf den Link **Protokoll zum Verschieben von Volumes** klicken.

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration werden Details zum ausgewählten Volume angezeigt, z. B. Richtlinie für den Export, RAID-Typ, Kapazität und Storage-Effizienz-Funktionen des Volumes:

- **Übersicht**
  - Vollständiger Name

    Zeigt den vollständigen Namen des Volumes an.

  - Aggregate

    Zeigt den Namen des Aggregats, auf dem sich das Volume befindet, oder die Anzahl der Aggregate an, auf denen sich das FlexGroup Volume befindet.

  - Tiering-Richtlinie

    Zeigt die Tiering-Richtlinie für das Volume an; wenn das Volume auf einem FabricPool-fähigen Aggregat implementiert wird. Die Richtlinie kann „Keine“, „nur Snapshot“, „Backup“, „automatisch“ oder „Alle“ lauten.

  - Storage VM

    Zeigt den Namen der SVM an, die das Volume enthält.

  - Verbindungspfad

    Zeigt den Status des Pfads an, der aktiv oder inaktiv sein kann. Der Pfad in der SVM, auf den das Volume angehängt ist, wird ebenfalls angezeigt. Sie können auf den Link **Verlauf** klicken, um die letzten fünf Änderungen am Verbindungspfad anzuzeigen.

  - Exportrichtlinie

    Zeigt den Namen der Exportrichtlinie an, die für das Volume erstellt wurde. Über den Link können Sie Details zu den Exportrichtlinien, den Authentifizierungsprotokollen und den aktivierten Zugriff auf die Volumes anzeigen, die zu der SVM gehören.

  - Stil

    Zeigt den Volumenstil an. Der Volume-Stil kann FlexVol oder FlexGroup sein.

  - Typ

    Zeigt den Typ des ausgewählten Volumens an. Der Volume-Typ kann Lese-/Schreibvorgänge,

Lastverteilung, Datensicherung, Daten-Cache oder temporär sein.

- RAID-Typ

  Zeigt den RAID-Typ des ausgewählten Volumes an. Der RAID-Typ kann RAID0, RAID4, RAID-DP oder RAID-TEC sein.

  > Es können mehrere RAID-Typen für FlexGroup Volumes angezeigt werden, da sich die zusammengehörigen Volumes für FlexGroups auf Aggregaten unterschiedlicher Typen sein können.

- SnapLock-Typ

  Zeigt den SnapLock-Typ des Aggregats an, der das Volume enthält.

- SnapLock Expiry

  Zeigt das Ablaufdatum des SnapLock-Volume an.

- * Kapazität*
  - Thin Provisioning

    Zeigt an, ob Thin Provisioning für das Volume konfiguriert ist.

  - Autogrow

    Zeigt an, ob das flexible Volume automatisch innerhalb eines Aggregats wächst.

  - Snapshot Automatisch Löschen

    Gibt an, ob Snapshot Kopien automatisch in freien Speicherplatz gelöscht werden, wenn ein Schreibvorgang auf ein Volume aufgrund von fehlendem Speicherplatz im Aggregat ausfällt.

  - Kontingente

    Gibt an, ob die Quoten für das Volume aktiviert sind.

- * Effizienz*
  - Komprimierung

    Gibt an, ob die Komprimierung aktiviert oder deaktiviert ist.

  - Deduplizierung

    Gibt an, ob die Deduplizierung aktiviert oder deaktiviert ist.

  - Deduplizierungsmodus

    Gibt an, ob der auf einem Volume aktivierte Deduplizierungsvorgang ein manueller, geplanter oder richtlinienbasierter Vorgang ist. Wenn der Modus auf „geplant“ eingestellt ist, wird der Betriebsplan angezeigt, und wenn der Modus auf eine Richtlinie festgelegt ist, wird der Richtlinienname angezeigt.

  - Deduplizierungsart

    Gibt den Typ des Deduplizierungsvorgangs an, der auf dem Volume ausgeführt wird. Wenn das

Volume eine SnapVault-Beziehung hat, wird als SnapVault angezeigt. Für jedes andere Volumen wird der Typ als normal angezeigt.

- Storage-Effizienzrichtlinie

  Gibt den Namen der Storage-Effizienzrichtlinie an, die diesem Volume durch Unified Manager zugewiesen wurde. Diese Richtlinie steuert die Komprimierungs- und Deduplizierungseinstellungen.

- **Schutz**
  - Snapshots

    Gibt an, ob die automatischen Snapshot Kopien aktiviert oder deaktiviert sind.

Registerkarte „Schutz“

Auf der Registerkarte Schutz werden Sicherungsdetails zum ausgewählten Volume angezeigt, z. B. Verzögerungsinformationen, Beziehungstyp und Topologie der Beziehung.

- **Zusammenfassung**

  Zeigt die Eigenschaften von SnapMirror- und SnapVault-Beziehungen für ein ausgewähltes Volume an. Für einen anderen Beziehungstyp wird nur die Eigenschaft Beziehungstyp angezeigt. Wenn ein primäres Volume ausgewählt wird, werden nur die Richtlinie für verwaltete und lokale Snapshot-Kopien angezeigt. Für SnapMirror und SnapVault Beziehungen werden folgende Eigenschaften angezeigt:

  - Quell-Volume

    Zeigt den Namen der Quelle des ausgewählten Volumes an, wenn das ausgewählte Volume ein Ziel ist.

  - Verzögerungsstatus

    Zeigt den Status der Update- oder Transferverzögerungen für eine Schutzbeziehung an. Der Status kann „Fehler“, „Warnung“ oder „kritisch“ sein.

    Der lag-Status gilt nicht für synchrone Beziehungen.

  - Verzögerungsdauer

    Zeigt die Zeit an, mit der die Daten auf dem Spiegel hinter der Quelle liegen.

  - Letzte Erfolgreiche Aktualisierung

    Zeigt Datum und Uhrzeit der letzten erfolgreichen Schutzaktualisierung an.

    Die letzte erfolgreiche Aktualisierung gilt nicht für synchrone Beziehungen.

  - Storage Service-Mitglied

    Zeigt entweder Ja oder Nein an, um anzugeben, ob das Volume zu einem Storage-Service gehört und von diesem gemanagt wird.

  - Versionsflexible Replizierung

    Zeigt entweder Ja, Ja mit Sicherungsoption oder Keine an. Ja zeigt an, dass die SnapMirror

Replizierung möglich ist, auch wenn auf Quell- und Ziel-Volumes unterschiedliche Versionen der ONTAP Software ausgeführt werden. Ja, mit der Backup-Option bezeichnet die Implementierung von SnapMirror Sicherung mit der Möglichkeit, mehrere Versionen von Backup-Kopien auf dem Zielsystem aufzubewahren. Keine gibt an, dass die Version Flexible Replikation nicht aktiviert ist.

- Beziehungsfähigkeit

  Zeigt die ONTAP-Funktionen an, die für die Sicherungsbeziehung verfügbar sind.

- Protection Service

  Zeigt den Namen des Schutzdienstes an, wenn die Beziehung von einer Schutzpartneranwendung verwaltet wird.

- Beziehungstyp

  Zeigt alle Beziehungstypen an, einschließlich Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync, Und Synchronisierung.

- Beziehungsstatus

  Zeigt den Status der SnapMirror oder SnapVault Beziehung an. Der Staat kann ohne Initialisierung, SnapMirrored oder Abbruch erfolgen. Wenn ein Quell-Volume ausgewählt ist, ist der Beziehungsstatus nicht zutreffend und wird nicht angezeigt.

- Übertragungsstatus

  Zeigt den Übertragungsstatus der Schutzbeziehung an. Der Übertragungsstatus kann einer der folgenden Werte sein:

  - Wird Abgebrochen

    SnapMirror-Transfers sind aktiviert; ein Vorgang, bei dem der Transfer abgebrochen wird, während das Checkpoint entfernt wird.

  - Prüfen

    Das Zielvolumen wird einer Diagnose-Prüfung unterzogen und es wird keine Übertragung durchgeführt.

  - Abschließen

    SnapMirror Transfers sind aktiviert. Das Volume befindet sich derzeit in der Phase nach dem Transfer für inkrementelle SnapVault Transfers.

  - Leerlauf

    Transfers sind aktiviert, und es wird keine Übertragung durchgeführt.

  - Synchronisiert

    Die Daten in den beiden Volumes in der synchronen Beziehung werden synchronisiert.

  - Out-of-Sync

    Die Daten im Ziel-Volume werden nicht mit dem Quell-Volume synchronisiert.

- Vorbereitung

  SnapMirror Transfers sind aktiviert. Das Volume befindet sich derzeit in der Phase vor der Übertragung für inkrementelle SnapVault Transfers.

- Warteschlange

  SnapMirror Transfers sind aktiviert. Es werden keine Transfers durchgeführt.

- Stillgelegt

  SnapMirror Transfers sind deaktiviert. Es wird keine Übertragung durchgeführt.

- Wird Stillgelegt

  Ein SnapMirror Transfer läuft. Zusätzliche Transfers sind deaktiviert.

- Übertragung

  SnapMirror Transfers sind aktiviert, und ein Transfer läuft.

- Übergang

  Der asynchrone Datentransfer aus dem Quell- zum Ziel-Volume ist abgeschlossen, und der Übergang zum synchronen Betrieb wurde gestartet.

- Warten

  Ein SnapMirror Transfer wurde initiiert, aber einige zugehörige Aufgaben warten darauf, in die Warteschlange verschoben zu werden.

◦ Max. Übertragungsrate

Zeigt die maximale Übertragungsrate für die Beziehung an. Die maximale Übertragungsrate kann ein numerischer Wert in Kilobyte pro Sekunde (Kbit/s), Megabyte pro Sekunde (Mbit/s), Gigabyte pro Sekunde (Gbit/s) oder Terabyte pro Sekunde (Tbit/s) sein. Wenn kein Limit angezeigt wird, ist die Basistransfer zwischen Beziehungen unbegrenzt.

◦ SnapMirror Richtlinie

Zeigt die Schutzrichtlinie für das Volume an. DPDefault gibt die standardmäßige Richtlinie für den Schutz der asynchronen Spiegelung an, XDPDefault gibt die standardmäßige asynchrone Vault-Richtlinie an, und DPSyncStandard gibt die standardmäßige asynchrone MirrorVault-Richtlinie an. StrictSync gibt die standardmäßige Richtlinie für den synchronen strengen Schutz an, und Sync gibt die standardmäßige synchrone Richtlinie an. Sie können auf den Richtliniennamen klicken, um die mit dieser Richtlinie verknüpften Details anzuzeigen, einschließlich der folgenden Informationen:

- Übertragungspriorität
- Einstellung der Zugriffszeit ignorieren
- Limit für Versuche
- Kommentare
- SnapMirror-Labels
- Aufbewahrungseinstellungen

        - Tatsächliche Snapshot Kopien
        - Bewahren Sie Snapshot Kopien auf
        - Schwellenwert für Warnung bei Aufbewahrung
        - Snapshot-Kopien ohne Aufbewahrungseinstellungen in einer kaskadierenden SnapVault-Beziehung, wobei die Quelle ein Datensicherungs-Volume (DP) ist, gilt nur die Regel „`sm_created`“.
    - Zeitplan Aktualisieren

      Zeigt den SnapMirror Zeitplan an, der der Beziehung zugewiesen ist. Wenn Sie den Cursor über das Informationssymbol positionieren, werden die Terminplandetails angezeigt.

    - Lokale Snapshot-Richtlinie

      Zeigt die Snapshot Kopie-Richtlinie für das Volume an. Die Richtlinie ist Standard, Keine oder ein beliebiger Name, der einer benutzerdefinierten Richtlinie zugewiesen wurde.

- **Ausblick**

  Zeigt die Schutztopologie des ausgewählten Volumes an. Die Topologie enthält grafische Darstellungen aller Volumes, die sich auf das ausgewählte Volume beziehen. Das ausgewählte Volumen wird durch einen dunkelgrauen Rahmen angezeigt, und Linien zwischen Volumes in der Topologie geben den Schutzbeziehungstyp an. Die Richtung der Beziehungen in der Topologie wird von links nach rechts angezeigt, wobei die Quelle jeder Beziehung auf der linken Seite und das Ziel auf der rechten Seite.

  Zweifett gedruckte Zeilen geben eine asynchrone Spiegelbeziehung an. Eine einzelne, fett gedruckte Zeile gibt eine asynchrone Vault-Beziehung an, doppelte Einzelzeilen geben eine asynchrone MirrorVault-Beziehung an, und eine fettgedruckte Zeile und eine nicht fettgedruckte Zeile gibt eine synchrone Beziehung an. Die folgende Tabelle gibt an, ob die synchrone Beziehung StrictSync oder Sync ist.

  Durch Klicken mit der rechten Maustaste auf ein Volume wird ein Menü angezeigt, aus dem Sie entweder das Volume schützen oder Daten darauf wiederherstellen können. Mit der rechten Maustaste auf eine Beziehung klicken wird ein Menü angezeigt, aus dem Sie entweder bearbeiten, abbrechen, stilllegen, brechen, entfernen, Oder nehmen Sie eine Beziehung wieder auf.

  Die Menüs werden in den folgenden Fällen nicht angezeigt:

    - Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
    - Wenn sich das Volume in einer synchronen Schutzbeziehung befindet
    - Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung vorliegt und das Ziel-Cluster noch nicht erkannt wurde, wird durch Klicken auf ein anderes Volume in der Topologie Informationen für das entsprechende Volume ausgewählt und angezeigt. Ein Fragezeichen ( ) In der linken oberen Ecke eines Volumens gibt an, dass entweder das Volumen fehlt oder es noch nicht entdeckt wurde. Sie können außerdem angeben, dass Kapazitätsinformationen nicht vorhanden sind. Wenn Sie den Mauszeiger über das Fragezeichen positionieren, werden weitere Informationen angezeigt, einschließlich Vorschläge für Korrekturmaßnahmen.

  In der Topologie werden Informationen zur Volume-Kapazität, Verzögerung, Snapshot-Kopien und zum letzten erfolgreichen Datentransfer angezeigt, wenn sie einer von mehreren gängigen Topologievorlagen entspricht. Wenn eine Topologie keiner dieser Vorlagen entspricht, werden Informationen zur Volume-Verzögerung und zum letzten erfolgreichen Datentransfer in einer Beziehungstabelle unter der Topologie angezeigt. In diesem Fall gibt die markierte Zeile in der Tabelle das ausgewählte Volume an, und in der Topologieansicht zeigen fettgedruckte Linien mit einem blauen Punkt die Beziehung zwischen dem

ausgewählten Volume und seinem Quellvolumen an.

Topologieansichten umfassen folgende Informationen:

- Kapazität

  Zeigt die Gesamtkapazität des Volumes an. Wenn Sie den Cursor auf ein Volumen in der Topologie positionieren, werden im Dialogfeld Aktuelle Schwellenwerteinstellungen die aktuellen Warn- und kritischen Schwellwerte für dieses Volume angezeigt. Sie können die Schwellenwerteinstellungen auch bearbeiten, indem Sie im Dialogfeld Aktuelle Schwellenwerteinstellungen auf den Link **Schwellenwerte bearbeiten** klicken. Wenn Sie das Kontrollkästchen **Kapazität** deaktivieren, werden alle Kapazitätsinformationen für alle Volumes in der Topologie ausgeblendet.

- Verzögerung

  Zeigt die Verzögerungsdauer und den Verzögerungsstatus der eingehenden Schutzbeziehungen an. Wenn Sie das Kontrollkästchen **lag** deaktivieren, werden alle lag-Informationen für alle Volumes in der Topologie ausgeblendet. Wenn das Kontrollkästchen **lag** gedimmt ist, werden die Verzögerungsinformationen für das ausgewählte Volume in der Beziehungstabelle unter der Topologie sowie die lag-Informationen für alle zugehörigen Volumes angezeigt.

- Snapshot

  Zeigt die Anzahl der für ein Volume verfügbaren Snapshot Kopien an. Wenn Sie das Kontrollkästchen **Snapshot** deaktivieren, werden alle Snapshot Kopie-Informationen für alle Volumes in der Topologie ausgeblendet. Klicken auf das Symbol für die Snapshot Kopie ( ) Zeigt die Liste der Snapshot Kopien für ein Volume an. Die Anzahl der Snapshot Kopien neben dem Symbol wird ungefähr jede Stunde aktualisiert. Die Liste der Snapshot-Kopien wird jedoch beim Klicken auf das Symbol aktualisiert. Dies kann zu einem Unterschied zwischen der in der Topologie angezeigten Anzahl der Snapshot Kopien und der Anzahl der aufgelisteten Snapshot Kopien führen, wenn Sie auf das Symbol klicken.

- Letzte Erfolgreiche Übertragung

  Zeigt den Betrag, die Dauer, die Zeit und das Datum der letzten erfolgreichen Datenübertragung an. Wenn das Kontrollkästchen **Letzter erfolgreicher Transfer** abgeblendet ist, werden die letzten erfolgreichen Übertragungsinformationen für das ausgewählte Volume in der Beziehungstabelle unter der Topologie sowie die letzten erfolgreichen Übertragungsinformationen für alle zugehörigen Volumes angezeigt.

  - **Geschichte**

    Zeigt die Historie der eingehenden SnapMirror- und SnapVault-Sicherungsbeziehungen für das ausgewählte Volume in einem Diagramm an. Es sind drei Verlaufsdiagramme verfügbar: Die Dauer des eingehenden Beziehungsverzögerungsablaufs, die Dauer der eingehenden Beziehungstransfers und die Größe der eingehenden Beziehung, die übertragen wurde. Die Verlaufsdaten werden nur angezeigt, wenn Sie ein Zielvolume auswählen. Wenn Sie ein primäres Volume auswählen, sind die Diagramme leer und die Meldung `No data found` Wird angezeigt.

    Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Historische Grafiken können Ihnen bei der Identifizierung von Trends helfen: Wenn zum Beispiel große Datenmengen zur gleichen Zeit des Tages oder der Woche übertragen werden oder wenn der lag-Warn- oder lag-Fehlerschwellenwert konsistent verletzt wird, können Sie geeignete Maßnahmen ergreifen. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

Sicherungsverlauf-Diagramme zeigen die folgenden Informationen an:

- **Beziehungsdauer**

  Anzeige von Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Anzeige von Tagen, Monaten oder Jahren auf der horizontalen Achse (x), abhängig vom ausgewählten Zeitraum. Der obere Wert auf der Y-Achse gibt die maximale Verzögerungsdauer an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. In der orangefarbenen Linie im Diagramm wird der lag-Fehlerschwellenwert angezeigt, während die horizontale gelbe Linie den lag-Warnungsschwellenwert darstellt. Wenn Sie den Mauszeiger über diese Zeilen positionieren, wird die Schwellenwerteinstellung angezeigt. Die waagerechte blaue Linie zeigt die Verzögerungsdauer an. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen interessanten Bereich positionieren.

- **Dauer Der Beziehungsübertragung**

  Anzeige von Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Anzeige von Tagen, Monaten oder Jahren auf der horizontalen Achse (x), abhängig vom ausgewählten Zeitraum. Der obere Wert auf der Y-Achse gibt die maximale Übertragungsdauer an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den Bereich von Interesse positionieren.

  Dieses Diagramm ist nicht für Volumes verfügbar, die sich in synchronen Sicherungsbeziehungen befinden.

- **Beziehung Übertragen Größe**

  Zeigt Bytes, Kilobyte, Megabyte usw. auf der vertikalen Achse (y) je nach Übertragungsgröße an und zeigt Tage, Monate oder Jahre auf der horizontalen Achse (x) je nach ausgewähltem Zeitraum an. Der obere Wert auf der Y-Achse gibt die maximale Übertragungsgröße an, die im auf der x-Achse angezeigten Zeitraum erreicht wurde. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen interessanten Bereich positionieren.

  Dieses Diagramm ist nicht für Volumes verfügbar, die sich in synchronen Sicherungsbeziehungen befinden.

Historienbereich

Im Bereich Verlauf werden Diagramme angezeigt, die Informationen über die Kapazität und die Platzreservierungen des ausgewählten Volumes enthalten. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

Diagramme sind möglicherweise leer und die Meldung `No data found` Wird angezeigt, wenn die Daten oder der Status des Volumes über einen Zeitraum hinweg unverändert bleiben.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Verlaufsdiagramme können Ihnen dabei helfen, Trends zu erkennen - wenn beispielsweise die Volumennutzung den Schwellenwert „nahezu voll“ konsistent überschreitet, können Sie entsprechende Maßnahmen ergreifen.

Verlaufsdiagramme zeigen folgende Informationen an:

- **Verwendete Volume-Kapazität**

Zeigt die verwendete Kapazität im Volume und den Trend in der Art und Weise an, wie die Volume-Kapazität basierend auf dem Nutzungsverlauf verwendet wird, als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende zu „Volume Used Capacity“ klicken, wird die Zeile des Diagramms „Volume Used Capacity“ ausgeblendet.

- **Verwendete Volume-Kapazität vs Gesamt**

  Zeigt den Trend der Volume-Kapazität basierend auf dem Nutzungsverlauf sowie der verwendeten Kapazität, der Gesamtkapazität und den Details der Speicherersparnis durch Deduplizierung und Komprimierung an. Dies sind Liniendiagramme in Byte, Kilobyte, Megabyte, Und so weiter, auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „verwendete Trend-Kapazität“ klicken, wird das Diagramm „verwendete Trendkapazität“ ausgeblendet.

- **Verwendete Volume-Kapazität (%)**

  Zeigt die verwendete Kapazität im Volumen und den Trend in der Art und Weise an, wie die Volume-Kapazität basierend auf dem Nutzungsverlauf, als Liniendiagramme, in Prozent, auf der vertikalen (y) Achse verwendet wird. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende zu „Volume Used Capacity“ klicken, wird die Zeile des Diagramms „Volume Used Capacity“ ausgeblendet.

- **Verwendete Snapshot-Kapazität (%)**

  Zeigt den Schwellenwert für die Snapshot-Reserve und die Snapshot-Warnung als Liniendiagramme und die von den Snapshot Kopien verwendete Kapazität als Diagramm in Prozent auf der vertikalen Achse (y) an. Der Snapshot-Überlauf ist mit verschiedenen Farben dargestellt. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende der Snapshot Reserve klicken, wird die Grafik der Snapshot Reserve ausgeblendet.

Ereignisliste

In der Ereignisliste werden Details zu neuen und bestätigten Ereignissen angezeigt:

- **Severity**

  Zeigt den Schweregrad des Ereignisses an.

- **Veranstaltung**

  Zeigt den Ereignisnamen an.

- **Auslösezeit**

  Zeigt die Zeit an, die seit der Erzeugung des Ereignisses verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, zu dem das Ereignis generiert wurde.

Bereich „Verwandte Anmerkungen“

Im Bereich Verwandte Anmerkungen können Sie Anmerkungsdetails anzeigen, die mit dem ausgewählten Volume verknüpft sind. Die Details umfassen den Anmerkungsnamen und die Anmerkungswerte, die auf das Volumen angewendet werden. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie SVMs, Aggregate, qtrees, LUNs und Snapshot Kopien anzeigen und navigieren, die mit dem Volume zusammenhängen:

- **Storage Virtual Machine**

  Zeigt die Kapazität und den Integritätsstatus der SVM an, die das ausgewählte Volume enthält.

- * Aggregat*

  Zeigt die Kapazität und den Integritätsstatus des Aggregats an, das das ausgewählte Volume enthält. Für FlexGroup Volumes wird die Anzahl der Aggregate aufgelistet, die die FlexGroup umfassen.

- **Volumen im Aggregat**

  Zeigt die Anzahl und Kapazität aller Volumes an, die zum übergeordneten Aggregat des ausgewählten Volumes gehören. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt. Wenn beispielsweise ein Aggregat zehn Volumes enthält, von denen fünf den Warnstatus und die übrigen fünf den kritischen Status anzeigen, ist der angezeigte Status kritisch. Diese Komponente wird für FlexGroup-Volumes nicht angezeigt.

- **Qtrees**

  Zeigt die Anzahl der vom ausgewählten Volume enthaltenen qtrees sowie die Kapazität von qtrees mit Kontingent an, die das ausgewählte Volume enthält. Die Kapazität der qtrees mit Kontingent wird in Bezug auf die Volume-Datenkapazität angezeigt. Auf der Grundlage des höchsten Schweregrades wird auch der Integritätsstatus der qtrees angezeigt. Wenn ein Volume beispielsweise zehn qtrees, fünf mit Warnstatus und die verbleibenden fünf mit kritischem Status aufweist, ist der angezeigte Status kritisch.

- **NFS-Freigaben**

  Zeigt die Anzahl und den Status der NFS-Freigaben an, die mit dem Volume verknüpft sind.

- **SMB-Freigaben**

  Zeigt die Anzahl und den Status der SMB/CIFS-Freigaben an.

- **LUNs**

  Zeigt die Anzahl und Gesamtgröße aller LUNs im ausgewählten Volume an. Auf der Grundlage des höchsten Schweregrades wird außerdem der Systemzustand der LUNs angezeigt.

- **Benutzer- und Gruppenquoten**

  Zeigt die Anzahl und den Status der Quoten für Benutzer und Benutzergruppen im Zusammenhang mit dem Volume und seinen qtrees an.

- **FlexClone Volumes**

  Zeigt die Anzahl und Kapazität aller geklonten Volumes des ausgewählten Volumes an. Anzahl und Kapazität werden nur angezeigt, wenn das ausgewählte Volume geklonte Volumes enthält.

- **Parent Volume**

  Zeigt den Namen und die Kapazität des übergeordneten Volume eines ausgewählten FlexClone Volume an. Das übergeordnete Volume wird nur angezeigt, wenn das ausgewählte Volume ein FlexClone Volume ist.

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ können Sie die Liste der Gruppen anzeigen, die dem ausgewählten Volume zugeordnet sind.

Bereich „Verwandte Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnmeldungen anzeigen, die für das ausgewählte Volume erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Storage VM / Health Details Seite

Sie können auf der Seite Storage VM / Health Details ausführliche Informationen zur ausgewählten SVM anzeigen, z. B. Systemzustand, Kapazität, Konfiguration, Datenrichtlinien, logische Schnittstellen (LIFs), LUNs, qtrees sowie Benutzer- und Gruppenkontingente. Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für die SVM anzeigen.

Es können nur Data SVMs überwacht werden.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für die ausgewählte SVM ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Ermöglicht Ihnen die Navigation zur Seite Storage VM / Performance Details.

- **Aktionen**
  - Alarm Hinzufügen

    Hiermit können Sie eine Warnung zur ausgewählten SVM hinzufügen.

  - Anmerkungen Hinzufügen

Ermöglicht Ihnen, die ausgewählte SVM zu kommentieren.

- **View Storage VMs**

  Ermöglicht Ihnen die Navigation zur Ansicht „Systemzustand: Alle Storage VMs“.

Registerkarte Systemzustand

Auf der Registerkarte Systemzustand werden detaillierte Informationen zur Datenverfügbarkeit, Datenkapazität und Sicherung verschiedener Objekte wie Volumes, Aggregate, NAS LIFs, SAN LIFs, LUNs, angezeigt. Protokolle, Services, NFS-Freigaben und CIFS-Freigaben.

Sie können auf das Diagramm eines Objekts klicken, um die gefilterte Liste der Objekte anzuzeigen. Beispielsweise können Sie auf das Diagramm für die Volume-Kapazität klicken, das Warnungen anzeigt, um die Liste der Volumes mit Kapazitätsproblemen mit dem Schweregrad „Warnung“ anzuzeigen.

- **Verfügbarkeitsprobleme**

  Zeigt als Diagramm die Gesamtzahl der Objekte an, einschließlich Objekten mit Verfügbarkeitsproblemen und Objekten, die keine Probleme mit der Verfügbarkeit haben. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Verfügbarkeitsproblemen, die sich auf die Verfügbarkeit von Daten in der SVM auswirken oder bereits davon betroffen sein können. Beispielsweise werden Informationen zu den NAS-LIFs und den SAN-LIFs angezeigt, die ausgefallen sind und die Volumes offline sind.

  Zudem können Sie Informationen zu den aktuell ausgeführten Protokollen und Services sowie zur Anzahl und dem Status von NFS- und CIFS-Freigaben anzeigen.

- **Kapazitätsprobleme**

  Zeigt als Diagramm die Gesamtzahl der Objekte an, einschließlich Objekten mit Kapazitätsproblemen und Objekten, die keine Kapazitätsprobleme haben. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die nachfolgende Grafik liefert Details zu Kapazitätsproblemen, die sich auf die Kapazität der Daten der SVM auswirken oder bereits beeinträchtigen können. Beispielsweise werden Informationen zu Aggregaten angezeigt, die mit hoher Wahrscheinlichkeit die festgelegten Schwellenwerte überschreiten.

- **Schutzprobleme**

  Er bietet eine schnelle Übersicht über den Schutz der SVM, indem die Gesamtzahl der Beziehungen, einschließlich Beziehungen mit Schutzproblemen und Beziehungen, bei denen keine Sicherungsprobleme auftreten, als Diagramm angezeigt werden. Wenn nicht geschützte Volumes vorhanden sind, führt ein Klick auf den Link zur Ansicht „Systemzustand: Alle Volumes“, in der eine gefilterte Liste der ungeschützten Volumes auf der SVM angezeigt werden kann. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Durch Klicken auf ein Diagramm gelangen Sie zur Beziehungsansicht „Alle Beziehungen“, in der Sie eine gefilterte Liste mit Details zu den Schutzbeziehungen anzeigen können. Die nachfolgenden Informationen enthalten Details zu Sicherungsproblemen, die sich auf den Schutz der Daten in der SVM auswirken oder bereits beeinträchtigen können. Beispielsweise werden Informationen über Volumes angezeigt, die eine Snapshot Kopie-Reserve haben, die fast voll ist, oder über Probleme mit der SnapMirror Beziehungs-Verzögerung.

  Wenn die ausgewählte SVM eine Repository-SVM ist, wird der Schutzbereich nicht angezeigt.

Registerkarte „Kapazität“

Auf der Registerkarte Kapazität werden ausführliche Informationen zur Datenkapazität der ausgewählten SVM angezeigt.

Folgende Informationen werden für eine SVM mit FlexVol-Volume oder FlexGroup-Volume angezeigt:

- * Kapazität*

  Im Kapazitätsbereich werden Details zur verwendeten und verfügbaren Kapazität angezeigt, die aus allen Volumes zugewiesen sind:

  - Gesamtkapazität

    Zeigt die Gesamtkapazität der SVM an.

  - Verwendet

    Zeigt den Speicherplatz an, der von Daten in den Volumes verwendet wird, die zur SVM gehören.

  - Garantiert Verfügbar

    Zeigt den garantierten verfügbaren Speicherplatz für Daten an, die für Volumes in der SVM verfügbar sind.

  - Nicht Garantiert

    Zeigt den verfügbaren Speicherplatz für Daten an, die in der SVM für Thin Provisioning Volumes zugewiesen sind.

- **Volumen mit Kapazitätsproblemen**

  Die Liste der Volumes mit Kapazitätsproblemen zeigt in tabellarischer Form Details zu den Volumes mit Kapazitätsproblemen an:

  - Status

    Zeigt an, dass das Volumen ein kapazitätsbezogenes Problem mit einem angezeigten Schweregrad hat.

    Sie können den Mauszeiger über den Status bewegen, um weitere Informationen zu dem kapazitätsbezogenen Ereignis oder den für das Volume generierten Ereignissen anzuzeigen.

    Wenn der Status des Volumes durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen wurde, und die Ursache des Ereignisses anzeigen. Sie können die Schaltfläche **Details anzeigen** verwenden, um weitere Informationen über die Veranstaltung anzuzeigen.

    Wenn der Status des Volumes durch mehrere Ereignisse desselben Schweregrades bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

Ein Volume kann mehrere Ereignisse desselben Schweregrades oder unterschiedlicher Schweregrade aufweisen. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Volume zwei Ereignisse mit Schweregraden für Fehler und Warnung enthält, wird nur der Schweregrad Fehler angezeigt.

- Datenmenge

  Zeigt den Namen des Volumes an.

- Genutzte Datenkapazität

  Zeigt als Diagramm Informationen zur Auslastung der Volume-Kapazität (in Prozent) an.

- Tage voll

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor das Volume die volle Kapazität erreicht.

- Thin Provisioning

  Zeigt an, ob die Platzgarantie für das ausgewählte Volume festgelegt ist. Gültige Werte sind Ja und Nein

- Aggregate

  Zeigt für FlexVol Volumes den Namen des Aggregats an, das das Volume enthält. Für FlexGroup-Volumes zeigt die Anzahl der Aggregate an, die in der FlexGroup verwendet werden.

Registerkarte Konfiguration

Auf der Registerkarte Configuration werden Konfigurationsdetails zu der ausgewählten SVM, z. B. deren Cluster, das Root-Volume, der zugehörige Volume-Typ (FlexVol-Volumes) und die auf der SVM erstellten Richtlinien angezeigt:

- **Übersicht**
  - Cluster

    Zeigt den Namen des Clusters an, zu dem die SVM gehört.

  - Zulässiger Volume-Typ

    Zeigt den Typ der Volumes an, die in der SVM erstellt werden können. Der Typ kann FlexVol oder FlexVol/FlexGroup sein.

  - Root-Volume

    Zeigt den Namen des Root-Volumes der SVM an.

  - Zulässige Protokolle

    Zeigt den Typ der Protokolle an, die für die SVM konfiguriert werden können. Außerdem gibt an, ob ein Protokoll aktiv ist (), unten (), oder ist nicht konfiguriert ().

- **Datennetzwerkschnittstellen**

- NAS

  Zeigt die Anzahl der NAS-Schnittstellen an, die der SVM zugeordnet sind. Außerdem gibt an, ob die Schnittstellen aktiv sind (Oder runter ().

- San

  Zeigt die Anzahl der SAN-Schnittstellen an, die der SVM zugeordnet sind. Außerdem gibt an, ob die Schnittstellen aktiv sind (Oder runter ().

- FC-NVMe

  Zeigt die Anzahl der FC-NVMe-Schnittstellen an, die der SVM zugeordnet sind. Außerdem gibt an, ob die Schnittstellen aktiv sind (Oder runter ().

- **Management-Netzwerk-Schnittstellen**
  - Gesteigerte

    Zeigt die Anzahl der Managementschnittstellen an, die der SVM zugeordnet sind. Außerdem gibt an, ob die Management-Schnittstellen aktiv sind (Oder runter ().

- **Richtlinien**
  - Snapshots

    Zeigt den Namen der Snapshot-Richtlinie an, die auf der SVM erstellt wurde.

  - Exportrichtlinien

    Zeigt entweder den Namen der Exportrichtlinie an, wenn eine einzelne Richtlinie erstellt wird, oder zeigt die Anzahl der Exportrichtlinien an, wenn mehrere Richtlinien erstellt werden.

- **Services**
  - Typ

    Zeigt den Service-Typ an, der für die SVM konfiguriert ist. Der Typ kann Domain Name System (DNS) oder Network Information Service (NIS) sein.

  - Bundesland

    Zeigt den Status des Dienstes an, der aktiv sein kann (), Down (), oder nicht konfiguriert ().

  - Domain-Name

    Zeigt die vollständig qualifizierten Domänennamen (FQDNs) des DNS-Servers für die DNS-Dienste oder NIS-Server für die NIS-Dienste an. Wenn der NIS-Server aktiviert ist, wird der aktive FQDN des NIS-Servers angezeigt. Wenn der NIS-Server deaktiviert ist, wird die Liste aller FQDNs angezeigt.

  - IP-Adresse

    Zeigt die IP-Adressen des DNS- oder NIS-Servers an. Wenn der NIS-Server aktiviert ist, wird die aktive IP-Adresse des NIS-Servers angezeigt. Wenn der NIS-Server deaktiviert ist, wird die Liste aller IP-Adressen angezeigt.

Registerkarte Netzwerkschnittstellen

Auf der Registerkarte Netzwerkschnittstellen werden Details zu den Datennetzwerkschnittstellen (LIFs) angezeigt, die auf der ausgewählten SVM erstellt wurden:

- **Netzwerkschnittstelle**

  Zeigt den Namen der Schnittstelle an, die auf der ausgewählten SVM erstellt wurde.

- **Betriebsstatus**

  Zeigt den Betriebsstatus der Schnittstelle an, die aktiv sein kann ( ), Down (Oder Unbekannt ( ). Der Betriebsstatus einer Schnittstelle wird durch den Status ihrer physischen Ports bestimmt.

- **Verwaltungsstatus**

  Zeigt den Administrationsstatus der Schnittstelle an. Dieser kann aktiv sein ( ), Down (Oder Unbekannt ( ). Der Administrationsstatus einer Schnittstelle wird vom Storage-Administrator gesteuert, um Änderungen an der Konfiguration oder zu Wartungszwecken vorzunehmen. Der Administrationsstatus kann sich vom Betriebsstatus unterscheiden. Wenn jedoch der Administrationsstatus einer Schnittstelle „Inaktiv“ lautet, ist der Betriebsstatus standardmäßig „Inaktiv“.

- **IP-Adresse / WWPN**

  Zeigt die IP-Adresse für Ethernet-Schnittstellen und den World Wide Port Name (WWPN) für FC LIFs an.

- **Protokolle**

  Zeigt die Liste der für die Schnittstelle angegebenen Datenprotokolle an, z. B. CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe und FlexCache.

- * Rolle*

  Zeigt die Schnittstellenrolle an. Die Rollen können Daten oder Management sein.

- * Home Port*

  Zeigt den physischen Port an, dem die Schnittstelle ursprünglich zugeordnet war.

- **Aktueller Port**

  Zeigt den physischen Port an, dem die Schnittstelle derzeit zugeordnet ist. Wenn die Schnittstelle migriert wird, unterscheidet sich der aktuelle Port möglicherweise vom Home Port.

- **Portsatz**

  Zeigt den Port-Satz an, dem die Schnittstelle zugeordnet ist.

- **Failover-Richtlinie**

  Zeigt die Failover-Richtlinie an, die für die Schnittstelle konfiguriert ist. Für NFS-, CIFS- und FlexCache-Schnittstellen ist die standardmäßige Failover-Richtlinie Next verfügbar. Failover-Richtlinie gilt nicht für FC- und iSCSI-Schnittstellen.

- **Routing-Gruppen**

Zeigt den Namen der Routinggruppe an. Sie können weitere Informationen zu den Routen und dem Ziel-Gateway anzeigen, indem Sie auf den Namen der Routinggruppe klicken.

Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt. Daher wird für diese Cluster eine leere Spalte angezeigt.

- **Failover-Gruppe**

  Zeigt den Namen der Failover-Gruppe an.

Registerkarte „qtrees“

Auf der Registerkarte qtrees werden Details zu qtrees und ihren Kontingenten angezeigt. Sie können auf die Schaltfläche **Schwellenwerte bearbeiten** klicken, wenn Sie die gesundheitlichen Schwellenwerte für qtree-Kapazität für eine oder mehrere qtrees bearbeiten möchten.

Verwenden Sie die Schaltfläche **Exportieren**, um einen kommagetrennten Wert zu erstellen (`.csv`) Datei mit den Details aller überwachten qtrees. Beim Export in eine CSV-Datei können Sie wahlweise einen qtrees-Bericht für die aktuelle SVM, für alle SVMs im aktuellen Cluster oder alle SVMs für alle Cluster in Ihrem Datacenter erstellen. In der exportierten CSV-Datei werden einige zusätzliche Felder „qtrees“ angezeigt.

- **Status**

  Zeigt den aktuellen Status des qtree an. Der Status kann kritisch sein (), Fehler (), Warnung (Oder normal ().

  Sie können den Mauszeiger über das Statussymbol bewegen, um weitere Informationen zu dem für den qtree generierten Ereignis oder Ereignissen anzuzeigen.

  Wenn der Status des qtree durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Sie können **Details anzeigen** verwenden, um weitere Informationen über die Veranstaltung anzuzeigen.

  Wenn der Status des qtree durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch **Alle Ereignisse anzeigen** verwenden, um die Liste der generierten Ereignisse anzuzeigen.

  > Ein qtree kann mehrere Ereignisse des gleichen Schweregrads oder unterschiedlicher Schweregrade aufweisen. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn ein qtree z. B. zwei Ereignisse mit Schweregraden für Fehler und Warnung hat, wird nur der Schweregrad „Fehler“ angezeigt.

- **Qtree**

  Zeigt den Namen des qtree an.

- * Cluster*

  Zeigt den Namen des Clusters an, der den qtree enthält. Wird nur in der exportierten CSV-Datei angezeigt.

- **Storage Virtual Machine**

  Zeigt den Namen der Storage Virtual Machine (SVM) an, die den qtree enthält. Wird nur in der exportierten CSV-Datei angezeigt.

- **Lautstärke**

  Zeigt den Namen des Volume an, das den qtree enthält.

  Sie können den Zeiger über den Volume-Namen verschieben, um weitere Informationen zum Volume anzuzeigen.

- **Quota Set**

  Gibt an, ob ein Kontingent aktiviert oder auf dem qtree deaktiviert ist.

- **Quotentyp**

  Gibt an, ob das Kontingent für einen Benutzer, eine Benutzergruppe oder einen qtree ist. Wird nur in der exportierten CSV-Datei angezeigt.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Für jeden Benutzer und jede Benutzergruppe werden mehrere Zeilen angezeigt. Wenn der Kontingenttyp qtree ist oder nicht festgelegt ist, ist die Spalte leer. Wird nur in der exportierten CSV-Datei angezeigt.

- **Verwendete Festplatte %**

  Zeigt den Prozentsatz des verwendeten Festplattenspeichers an. Wenn ein Festplattenlimit festgelegt ist, basiert dieser Wert auf dem Festplattenlimit. Wenn das Kontingent ohne Festplattenlimit festgelegt wird, basiert der Wert auf dem Volume-Datenraum. Wenn das Kontingent nicht festgelegt ist oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört, wird „`not anwendbare`“ auf der Grid-Seite angezeigt und das Feld in den CSV-Exportredaten leer ist.

- **Festplatten-Hard-Limit**

  Zeigt die maximale Menge an Festplattenspeicher an, die für den qtree zugewiesen ist. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht wird und keine weiteren Festplattenschreibvorgänge mehr zulässig sind. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein Festplattenlimit gesetzt wird, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört.

- **Soft Limit Für Festplatten**

  Zeigt die Menge an Festplattenspeicher an, die dem qtree zugewiesen ist, bevor ein Warnereignis generiert wird. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein Disk-Softlimit gesetzt wird, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört. Standardmäßig ist diese Spalte ausgeblendet.

- **Datenträgerschwellenwert**

  Zeigt den Schwellenwert an, der für den Festplattenspeicher festgelegt wurde. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein

Festplattenschwellenwert eingestellt ist, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im qtree verwendeten Dateien an. Wenn das harte Limit für die Datei festgelegt ist, basiert dieser Wert auf dem harten Limit der Datei. Es wird kein Wert angezeigt, wenn das Kontingent ohne harte Dateibegrenzung festgelegt ist. Wenn das Kontingent nicht festgelegt ist oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört, wird „`not anwendbare`“ auf der Grid-Seite angezeigt und das Feld in den CSV-Exportredaten leer ist.

- **Harte Dateibegrenzung**

  Zeigt das endgültige Limit für die Anzahl der Dateien an, die auf den qtrees zulässig sind. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne eine feste Dateibegrenzung festgelegt wird, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört.

- **Soft Limit Für Dateien**

  Zeigt den Softlimit für die Anzahl der Dateien an, die auf qtrees zulässig sind. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein Datei-Softlimit gesetzt wird, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört. Standardmäßig ist diese Spalte ausgeblendet.

Registerkarte „Benutzer- und Gruppenkontingente“

Zeigt Details zu den Quoten für Benutzer und Benutzergruppen für die ausgewählte SVM an. Sie können Informationen wie den Status des Kontingents, den Namen des Benutzers oder der Benutzergruppe, die auf den Festplatten und Dateien festgelegten Soft- und Hard-Limits, den Speicherplatz und die Anzahl der verwendeten Dateien sowie den Schwellenwert für die Festplatte anzeigen. Sie können auch die E-Mail-Adresse ändern, die einem Benutzer oder einer Benutzergruppe zugeordnet ist.

- **Schaltfläche 'Email-Adresse bearbeiten'**

  Öffnet das Dialogfeld E-Mail-Adresse bearbeiten, in dem die aktuelle E-Mail-Adresse des ausgewählten Benutzers oder der ausgewählten Benutzergruppe angezeigt wird. Sie können die E-Mail-Adresse ändern. Wenn das Feld**E-Mail-Adresse bearbeiten** leer ist, wird die Standardregel verwendet, um eine E-Mail-Adresse für den ausgewählten Benutzer oder die ausgewählte Benutzergruppe zu generieren.

  Wenn mehrere Benutzer das gleiche Kontingent haben, werden die Namen der Benutzer als kommagetrennte Werte angezeigt. Außerdem wird die Standardregel nicht verwendet, um die E-Mail-Adresse zu generieren; Sie müssen daher die erforderliche E-Mail-Adresse angeben, damit Benachrichtigungen gesendet werden können.

- **Schaltfläche E-Mail-Regeln konfigurieren**

  Mit dieser Option können Sie Regeln erstellen oder ändern, um eine E-Mail-Adresse für die auf der SVM konfigurierten Benutzer- oder Benutzergruppen-Quoten zu generieren. Bei einer Quota-Verletzung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

- **Status**

  Zeigt den aktuellen Status des Kontingents an. Der Status kann kritisch sein (), Warnung (Oder normal ().

Sie können den Zeiger über das Statussymbol verschieben, um weitere Informationen über das Ereignis oder die Ereignisse anzuzeigen, die für das Kontingent generiert wurden.

Wenn der Status des Kontingents durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugeordnet ist, und die Ursache des Ereignisses anzeigen. Sie können **Details anzeigen** verwenden, um weitere Informationen über die Veranstaltung anzuzeigen.

Wenn der Status des Kontingents durch mehrere Ereignisse desselben Schweregrades bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum angezeigt, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch **Alle Ereignisse anzeigen** verwenden, um die Liste der generierten Ereignisse anzuzeigen.

Eine Quote kann mehrere Ereignisse desselben Schweregrades oder unterschiedlicher Schweregrade haben. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Kontingent zwei Ereignisse mit Schweregraden für Fehler und Warnung enthält, wird nur der Schweregrad „Fehler“ angezeigt.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Wenn mehrere Benutzer das gleiche Kontingent haben, werden die Namen der Benutzer als kommagetrennte Werte angezeigt.

  Der Wert wird als „`Unbekannt`“ angezeigt, wenn ONTAP aufgrund von SECD-Fehlern keinen gültigen Benutzernamen liefert.

- **Typ**

  Gibt an, ob das Kontingent für einen Benutzer oder eine Benutzergruppe gilt.

- **Volumen oder Qtree**

  Zeigt den Namen des Volume oder qtree an, auf dem das Benutzer- oder Benutzergruppenkontingent angegeben ist.

  Sie können den Mauszeiger über den Namen des Volume oder qtree bewegen, um weitere Informationen zum Volume oder qtree anzuzeigen.

- **Verwendete Festplatte %**

  Zeigt den Prozentsatz des verwendeten Festplattenspeichers an. Der Wert wird als „`not anwendbares`“ angezeigt, wenn das Kontingent ohne Festplattenlimit festgelegt wird.

- **Festplatten-Hard-Limit**

  Zeigt den maximalen Speicherplatz an, der dem Kontingent zugewiesen ist. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht wird und keine weiteren Festplattenschreibvorgänge mehr zulässig sind. Der Wert wird als „`Unlimited`“ angezeigt, wenn das Kontingent ohne Festplattenlimit festgelegt wird.

- **Soft Limit Für Festplatten**

  Zeigt die Menge an Festplattenspeicher an, die für das Kontingent zugewiesen ist, bevor ein Warnereignis

generiert wird. Der Wert wird als „Unlimited“ angezeigt, wenn das Kontingent ohne Laufwerk-Softlimit festgelegt wird. Standardmäßig ist diese Spalte ausgeblendet.

- **Datenträgerschwellenwert**

  Zeigt den Schwellenwert an, der für den Festplattenspeicher festgelegt wurde. Der Wert wird als „Unlimited“ angezeigt, wenn das Kontingent ohne Datenträgerschwellenwert eingestellt ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im qtree verwendeten Dateien an. Der Wert wird als „not anwendbares“ angezeigt, wenn das Kontingent ohne harte Dateibegrenzung festgelegt ist.

- **Harte Dateibegrenzung**

  Zeigt das harte Limit für die Anzahl der Dateien an, die auf dem Kontingent zulässig sind. Der Wert wird als „Unlimited“ angezeigt, wenn das Kontingent ohne hartes Dateilimit festgelegt wird.

- **Soft Limit Für Dateien**

  Zeigt das Softlimit für die Anzahl der Dateien an, die auf dem Kontingent zulässig sind. Der Wert wird als „Unlimited“ angezeigt, wenn das Kontingent ohne DateiSoftlimit festgelegt wird. Standardmäßig ist diese Spalte ausgeblendet.

- **E-Mail-Adresse**

  Zeigt die E-Mail-Adresse des Benutzers oder der Benutzergruppe an, an die Benachrichtigungen gesendet werden, wenn eine Verletzung der Quoten vorhanden ist.

Registerkarte NFS Shares

Auf der Registerkarte NFS-Shares werden Informationen über NFS Shares angezeigt, z. B. sein Status, der dem Volume zugeordnete Pfad (FlexGroup Volumes oder FlexVol Volumes), die Zugriffsebenen von Clients auf die NFS-Shares und die für die exportierten Volumes definierte Exportrichtlinie. NFS-Freigaben werden unter folgenden Bedingungen nicht angezeigt: Wenn das Volume nicht gemountet wurde oder wenn die mit der Exportrichtlinie für das Volume verknüpften Protokolle keine NFS-Freigaben enthalten.

- **Status**

  Zeigt den aktuellen Status der NFS-Freigaben an. Der Status kann „Fehler“ sein ( ) Oder normal ( ).

- **Verbindungspfad**

  Zeigt den Pfad an, auf den das Volume angehängt ist. Wird auf einen qtree eine explizite NFS Exportrichtlinie angewendet, zeigt die Spalte den Pfad des Volume an, über das auf den qtree zugegriffen werden kann.

- **Verbindungspfad Aktiv**

  Zeigt an, ob der Pfad für den Zugriff auf das bereitgestellte Volume aktiv oder inaktiv ist.

- **Volumen oder Qtree**

  Zeigt den Namen des Volumes oder qtree an, auf das die NFS-Exportrichtlinie angewendet wird. Wenn

eine NFS-Exportrichtlinie auf einen qtree im Volume angewendet wird, werden in der Spalte sowohl die Namen des Volume als auch der qtree angezeigt.

Sie können auf den Link klicken, um Details zum Objekt auf der entsprechenden Detailseite anzuzeigen. Wenn es sich bei dem Objekt um einen qtree handelt, werden sowohl für den qtree als auch für das Volume Links angezeigt.

- **Volume-Status**

  Zeigt den Status des Volumes an, das exportiert wird. Der Status kann Offline, Online, eingeschränkt oder gemischt sein.

  - Offline

    Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

  - Online

    Lese- und Schreibzugriff auf das Volume ist zulässig.

  - Eingeschränkt

    Begrenzte Vorgänge, wie etwa die Paritätsrekonstruktion, sind zulässig, der Datenzugriff jedoch nicht.

  - Gemischt

    Die Komponenten eines FlexGroup-Volumes sind nicht alle im selben Zustand.

- **Sicherheitsstil**

  Zeigt die Zugriffsberechtigung für die exportierten Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder gemischt sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume haben UNIX Berechtigungen.

  - Virtualisierung

    Dateien und Verzeichnisse im Volume weisen einen einheitlichen Sicherheitsstil auf.

  - NTFS (CIFS-Clients)

    Dateien und Verzeichnisse im Volume haben Windows NTFS-Berechtigungen.

  - Gemischt

    Dateien und Verzeichnisse auf dem Volume können entweder UNIX Berechtigungen oder Windows NTFS Berechtigungen haben.

- **UNIX-Erlaubnis**

  Zeigt die UNIX-Berechtigungsbits in einem Oktal-String-Format an, das für die exportierten Volumes festgelegt ist. Es ähnelt den Berechtigungsbits im UNIX-Stil.

- **Exportrichtlinie**

Zeigt die Regeln an, die die Zugriffsberechtigung für exportierte Volumes definieren. Sie können auf den Link klicken, um Details zu den Regeln anzuzeigen, die mit der Exportrichtlinie verknüpft sind, z. B. die Authentifizierungsprotokolle und die Zugriffsberechtigung.

Registerkarte „SMB-Freigaben“

Zeigt Informationen zu den SMB-Freigaben auf der ausgewählten SVM an. Sie können Informationen anzeigen, wie z. B. den Status der SMB-Freigabe, den Share-Namen, den mit der SVM verknüpften Pfad, den Status des Verbindungspfads der Freigabe, das Objekt enthält, den Status des enthaltenden Volumes, die Sicherheitsdaten der Freigabe und die für die Freigabe definierten Exportrichtlinien. Sie können auch festlegen, ob ein äquivalenter NFS-Pfad für die SMB-Freigabe vorhanden ist.

Freigaben in Ordnern werden auf der Registerkarte SMB-Freigaben nicht angezeigt.

- **Befehlsschaltfläche Benutzerzuordnung anzeigen**

  Öffnet das Dialogfeld Benutzerzuordnung.

  Sie können sich die Details der Benutzerzuordnung für die SVM anzeigen lassen.

- **ACL-Befehlstaste anzeigen**

  Öffnet das Dialogfeld „Zugriffskontrolle“ für die Freigabe.

  Sie können Benutzer- und Berechtigungsdetails für die ausgewählte Freigabe anzeigen.

- **Status**

  Zeigt den aktuellen Status der Freigabe an. Der Status kann Normal ( ) Oder Fehler ( ).

- **Name Der Weitergabe**

  Zeigt den Namen der SMB-Freigabe an.

- **Pfad**

  Zeigt den Verbindungspfad an, auf dem die Freigabe erstellt wird.

- **Verbindungspfad Aktiv**

  Zeigt an, ob der Pfad für den Zugriff auf die Freigabe aktiv oder inaktiv ist.

- **Objekt**

  Zeigt den Namen des enthaltenden Objekts an, zu dem die Freigabe gehört. Das zugehörige Objekt kann ein Volume oder ein qtree sein.

  Durch Klicken auf den Link können Sie auf der entsprechenden Detailseite Details über das zugehörige Objekt anzeigen. Wenn es sich bei dem enthaltenen Objekt um einen qtree handelt, werden sowohl für qtree als auch für das Volume Links angezeigt.

- **Volume-Status**

  Zeigt den Status des Volumes an, das exportiert wird. Der Status kann Offline, Online, eingeschränkt oder gemischt sein.

- Offline

  Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

- Online

  Lese- und Schreibzugriff auf das Volume ist zulässig.

- Eingeschränkt

  Begrenzte Vorgänge, wie etwa die Paritätsrekonstruktion, sind zulässig, der Datenzugriff jedoch nicht.

- Gemischt

  Die Komponenten eines FlexGroup-Volumes sind nicht alle im selben Zustand.

- **Sicherheit**

  Zeigt die Zugriffsberechtigung für die exportierten Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder gemischt sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume haben UNIX Berechtigungen.

  - Virtualisierung

    Dateien und Verzeichnisse im Volume weisen einen einheitlichen Sicherheitsstil auf.

  - NTFS (CIFS-Clients)

    Dateien und Verzeichnisse im Volume haben Windows NTFS-Berechtigungen.

  - Gemischt

    Dateien und Verzeichnisse auf dem Volume können entweder UNIX Berechtigungen oder Windows NTFS Berechtigungen haben.

- **Exportrichtlinie**

  Zeigt den Namen der Exportrichtlinie an, die für die Freigabe gilt. Wenn keine Exportrichtlinie für die SVM angegeben ist, wird der Wert als nicht aktiviert angezeigt.

  Sie können auf den Link klicken, um Details zu den Regeln anzuzeigen, die der Exportrichtlinie zugeordnet sind, z. B. Zugriffsprotokolle und Berechtigungen. Die Verknüpfung ist deaktiviert, wenn die Exportrichtlinie für die ausgewählte SVM deaktiviert ist.

- **NFS-Äquivalent**

  Gibt an, ob ein Äquivalent zu NFS für die Freigabe vorhanden ist.

REGISTERKARTE „SAN“

Zeigt Details zu LUNs, Initiatorgruppen und Initiatoren für die ausgewählte SVM an. Standardmäßig wird die Ansicht LUNs angezeigt. Sie können Details zu den Initiatorgruppen auf der Registerkarte Initiatorgruppen und

Details zu Initiatoren auf der Registerkarte Initiatoren anzeigen.

- **LUNs-Registerkarte**

  Zeigt Details zu den LUNs an, die zur ausgewählten SVM gehören. Sie können Informationen anzeigen, wie z. B. den LUN-Namen, den LUN-Zustand (online oder offline), den Namen des Filesystems (Volume oder qtree), das die LUN enthält, den Typ des Host-Betriebssystems, die Gesamtkapazität und die Seriennummer der LUN. Die Spalte LUN Performance enthält einen Link zur Seite LUN/Performance Details.

  Sie können auch anzeigen, ob Thin Provisioning auf der LUN aktiviert ist und ob die LUN einer Initiatorgruppe zugeordnet ist. Wenn er einem Initiator zugeordnet ist, können Sie die Initiatorgruppen und Initiatoren anzeigen, die der ausgewählten LUN zugeordnet sind.

- **Registerkarte Initiatorgruppen**

  Zeigt Details zu Initiatorgruppen an. Sie können Details anzeigen, z. B. den Namen der Initiatorgruppe, den Zugriffsstatus, den Typ des Host-Betriebssystems, das von allen Initiatoren in der Gruppe verwendet wird, und das unterstützte Protokoll. Wenn Sie in der Spalte Zugriffsstatus auf den Link klicken, können Sie den aktuellen Zugriffsstatus der Initiatorgruppe anzeigen.

  - **Normal**

    Die Initiatorgruppe ist mit mehreren Zugriffspfaden verbunden.

  - * Einzelner Pfad*

    Die Initiatorgruppe ist mit einem einzelnen Zugriffspfad verbunden.

  - **Keine Pfade**

    Es ist kein Zugriffspfad mit der Initiatorgruppe verbunden.

  Sie können anzeigen, ob Initiatorgruppen über einen Port-Satz allen Schnittstellen oder spezifischen Schnittstellen zugeordnet sind. Wenn Sie in der Spalte zugeordnete Schnittstellen auf den Link Zählen klicken, werden entweder alle Schnittstellen angezeigt oder bestimmte Schnittstellen für einen Port-Satz werden angezeigt. Schnittstellen, die über das Zielportal zugeordnet sind, werden nicht angezeigt. Es wird die Gesamtzahl der Initiatoren und LUNs angezeigt, die einer Initiatorgruppe zugeordnet sind.

Sie können auch die LUNs und Initiatoren anzeigen, die der ausgewählten Initiatorgruppe zugeordnet sind.

- **Registerkarte Initiatoren**

  Zeigt den Namen und Typ des Initiators und die Gesamtzahl der Initiatorgruppen an, die diesem Initiator für die ausgewählte SVM zugeordnet sind.

  Sie können auch die LUNs und Initiatorgruppen anzeigen, die der ausgewählten Initiatorgruppe zugeordnet sind.

Bereich „Verwandte Anmerkungen“

Im Fensterbereich Verwandte Anmerkungen können Sie die mit der ausgewählten SVM verknüpften Anmerkungsdetails anzeigen. Details umfassen den Anmerkungsnamen und die auf die SVM angewandten Anmerkungswerte. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie Cluster, Aggregate und Volumes anzeigen, die mit der SVM in Verbindung stehen:

- * Cluster*

  Zeigt den Integritätsstatus des Clusters an, zu dem die SVM gehört.

- **Aggregate**

  Zeigt die Anzahl der Aggregate an, die zur ausgewählten SVM gehören. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt. Wenn eine SVM z. B. zehn Aggregate enthält, von denen fünf den Warnstatus und die verbleibenden fünf den kritischen Status anzeigen, ist der angezeigte Status „kritisch“.

- * Zugewiesene Aggregate*

  Zeigt die Anzahl der Aggregate an, die einer SVM zugewiesen sind. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt.

- **Bände**

  Zeigt die Anzahl und Kapazität der Volumes an, die zur ausgewählten SVM gehören. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt. In der SVM sind FlexGroup Volumes vorhanden, auch die Zählung FlexGroups. FlexGroup-Komponenten sind darin nicht enthalten.

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ können Sie eine Liste der Gruppen anzeigen, die der ausgewählten SVM zugeordnet sind.

Bereich „Verwandte Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnmeldungen anzeigen, die für die ausgewählte SVM erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link **Alarm hinzufügen** klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Namen der Warnmeldung klicken.

„Cluster/Systemzustand“-Details

Auf der Seite „Cluster/Systemzustand“ finden Sie ausführliche Informationen über ein ausgewähltes Cluster, z. B. Angaben zu Systemzustand, Kapazität und Konfiguration. Sie können auch Informationen zu Netzwerkschnittstellen (LIFs), Nodes, Festplatten, zugehörigen Geräten und zugehörigen Warnmeldungen für das Cluster anzeigen.

Der Status neben dem Cluster-Namen, z. B. (gut), stellt den Kommunikationsstatus dar, ob Unified Manager mit dem Cluster kommunizieren kann. Er stellt nicht den Failover-Status oder den Gesamtstatus des Clusters dar.

Befehlsschaltflächen

Mit den Schaltflächen des Befehls können Sie die folgenden Aufgaben für das ausgewählte Cluster ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Ermöglicht Ihnen die Navigation zur Seite „Cluster/Performance Details“.

- **Aktionen**

  - Alarm hinzufügen: Öffnet das Dialogfeld Alarm hinzufügen, in dem Sie dem ausgewählten Cluster eine Warnung hinzufügen können.
  - Erneut entdecken: Initiiert eine manuelle Aktualisierung des Clusters, sodass Unified Manager die neuesten Änderungen am Cluster erkennen kann.

    Bei Kombination von Unified Manager mit OnCommand Workflow Automation erfasst der Wiederauffindungvorgang ggf. auch zwischengespeicherte Daten von WFA.

  Nachdem der Vorgang zur erneuten Erkennung initiiert wurde, wird ein Link zu den zugehörigen Jobdetails angezeigt, um die Nachverfolgung des Jobstatus zu ermöglichen.

  - Anmerkungen: Ermöglicht es Ihnen, das ausgewählte Cluster zu kommentieren.

- **Cluster Anzeigen**

  Ermöglicht die Navigation in der Ansicht „Health: All Clusters“.

Registerkarte Systemzustand

Zeigt detaillierte Informationen zur Datenverfügbarkeit und zu Kapazitätsproblemen der verschiedenen Cluster-Objekte wie Nodes, SVMs und Aggregate an. Verfügbarkeitsprobleme hängen von der Datenserverfunktion der Cluster-Objekte ab. Kapazitätsprobleme stehen im Zusammenhang mit der Datenspeicherfunktion der Cluster-Objekte.

Sie können auf das Diagramm eines Objekts klicken, um eine gefilterte Liste der Objekte anzuzeigen. Beispielsweise können Sie auf das SVM-Kapazitätsdiagramm klicken, in dem Warnungen angezeigt werden, um eine gefilterte Liste der SVMs anzuzeigen. Diese Liste enthält SVMs mit Volumes oder qtrees, deren Kapazitätsprobleme mit einem Schweregrad von Warnung auftreten. Sie können auch auf das Diagramm „SVMs Verfügbarkeit“ klicken, in dem Warnungen angezeigt werden, um die Liste der SVMs mit Verfügbarkeitsproblemen und einem Schweregrad „Warnung“ anzuzeigen.

- **Verfügbarkeitsprobleme**

  Grafische Darstellung der Gesamtzahl an Objekten, einschließlich Objekten mit Verfügbarkeitsproblemen und Objekten, bei denen keine Probleme mit der Verfügbarkeit auftreten Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Verfügbarkeitsproblemen, die sich auf die Verfügbarkeit von Daten im Cluster auswirken oder bereits davon betroffen sein können. Beispielsweise werden Informationen über Festplatten-Shelfs angezeigt, die ausgefallen sind und Aggregate, die offline sind.

Die für das SFO-Balkendiagramm angezeigten Daten basieren auf dem HA-Status der Nodes. Die für alle anderen Balkendiagramme angezeigten Daten werden auf Grundlage der generierten Ereignisse berechnet.

- **Kapazitätsprobleme**

  Grafische Darstellung der Gesamtzahl an Objekten, einschließlich Objekten mit Kapazitätsproblemen und Objekten, die keine Kapazitätsprobleme haben. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Kapazitätsproblemen, die sich auf die Kapazität von Daten im Cluster auswirken oder bereits sie beeinträchtigen können. Beispielsweise werden Informationen zu Aggregaten angezeigt, die mit hoher Wahrscheinlichkeit die festgelegten Schwellenwerte überschreiten.

Registerkarte „Kapazität“

Zeigt detaillierte Informationen zur Kapazität des ausgewählten Clusters an.

- * Kapazität*

  Zeigt das Datenkapazitätsdiagramm zu der genutzten Kapazität und der verfügbaren Kapazität aus allen zugewiesenen Aggregaten an:

  - Genutzter Logischer Speicherplatz

    Die tatsächliche Größe der Daten, die auf allen Aggregaten auf diesem Cluster gespeichert werden, ohne dabei die Einsparungen durch die ONTAP Storage-Effizienztechnologien zu verwenden.

  - Verwendet

    Die physische Kapazität, die von Daten auf allen Aggregaten verwendet wird. Dies schließt nicht die Kapazität ein, die für Parität, richtige Dimensionierung und Reservierung verwendet wird.

  - Verfügbar

    Zeigt die für Daten verfügbare Kapazität an.

  - Ersatzteile

    Zeigt die verfügbare Speicherkapazität für die Speicherung aller freien Festplatten an.

  - Provisioniert

    Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

- **Details**

  Zeigt detaillierte Informationen zur verwendeten und verfügbaren Kapazität an.

  - Gesamtkapazität

    Zeigt die Gesamtkapazität des Clusters an. Dies schließt nicht die Kapazität ein, die Parität zugewiesen ist.

  - Verwendet

    Zeigt die Kapazität an, die von Daten verwendet wird. Dies schließt nicht die Kapazität ein, die für Parität, richtige Dimensionierung und Reservierung verwendet wird.

  - Verfügbar

Zeigt die für Daten verfügbare Kapazität an.

- Provisioniert

  Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

- Ersatzteile

  Zeigt die verfügbare Speicherkapazität für die Speicherung aller freien Festplatten an.

- * Cloud Tier*

  Zeigt die insgesamt genutzte Cloud-Tier-Kapazität und die Kapazität der einzelnen verbundenen Cloud-Tiers für FabricPool-fähige Aggregate im Cluster an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

- **Physische Kapazität Breakout nach Disk-Typ**

  Im Bereich physische Kapazität Breakout nach Festplattentyp werden ausführliche Informationen zur Festplattenkapazität der verschiedenen Festplattentypen im Cluster angezeigt. Durch Klicken auf den Festplattentyp werden weitere Informationen zum Festplattentyp auf der Registerkarte Laufwerke angezeigt.

  - Nutzbare Gesamtkapazität –

    Zeigt die verfügbare Kapazität und freie Kapazität der Datenfestplatten an.

  - HDD

    Grafische Darstellung der verwendeten Kapazität und der verfügbaren Kapazität aller Festplatten im Cluster. Die gestrichelte Linie stellt die freie Kapazität der Datenfestplatten dar.

  - Flash
    - SSD-Daten

      Grafische Darstellung der verwendeten Kapazität und der verfügbaren Kapazität der SSD-Datenfestplatten im Cluster

    - SSD Cache

      Zeigt grafisch die speicherbare Kapazität der SSD-Cache-Laufwerke im Cluster an.

    - SSD Spare

      Grafische Darstellung der freien Kapazität der SSD-, Daten- und Cache-Festplatten im Cluster

  - Nicht Zugewiesene Festplatten

    Zeigt die Anzahl der nicht zugewiesenen Festplatten im Cluster an.

- **Aggregate mit Kapazitätsprobleme Liste**

  Zeigt Details zur verwendeten Kapazität und zur verfügbaren Kapazität der Aggregate mit Kapazitätsproblemen in Tabellenform an.

- Status

  Zeigt an, dass das Aggregat ein kapazitätsbezogenes Problem mit einem bestimmten Schweregrad hat.

  Sie können den Zeiger auf den Status verschieben, um weitere Informationen zu dem für das Aggregat generierten Ereignis oder Ereignissen anzuzeigen.

  Wenn der Status des Aggregats durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen wurde, und die Ursache des Ereignisses anzeigen. Sie können auf die Schaltfläche **Details anzeigen** klicken, um weitere Informationen über die Veranstaltung anzuzeigen.

  Wenn der Status des Aggregats durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen angezeigt, z. B. Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst werden, und der Name des Administrators, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

  > Ein Aggregat kann mehrere kapazitätsbezogene Ereignisse vom gleichen Schweregrad oder verschiedene Schweregrade aufweisen. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Aggregat zwei Ereignisse mit dem Schweregrad „Fehler“ und „kritisch“ hat, wird nur der Schweregrad „kritisch“ angezeigt.

- Aggregat

  Zeigt den Namen des Aggregats an.

- Genutzte Datenkapazität

  Grafische Anzeige von Informationen zur Kapazitätsauslastung des Aggregats (in Prozent)

- Tage voll

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor die volle Kapazität des Aggregats erreicht ist.

Registerkarte Konfiguration

Zeigt Details zum ausgewählten Cluster an, z. B. IP-Adresse, Seriennummer, Kontakt und Standort:

- **Cluster Übersicht**
  - Managementoberfläche

    Zeigt die Cluster-Management-LIF an, die Unified Manager zum Herstellen einer Verbindung mit dem Cluster verwendet. Der Betriebsstatus der Schnittstelle wird ebenfalls angezeigt.

  - Host-Name oder IP-Adresse

    Zeigt den FQDN, den Kurznamen oder die IP-Adresse der Clusterverwaltungs-LIF an, die Unified Manager zur Verbindung mit dem Cluster verwendet.

- FQDN

  Zeigt den vollständig qualifizierten Domänennamen (FQDN) des Clusters an.

- Betriebssystemversion

  Zeigt die ONTAP-Version an, die das Cluster ausführt. Wenn im Cluster die Nodes unterschiedliche Versionen von ONTAP ausführen, wird die früheste ONTAP-Version angezeigt.

- Seriennummer

  Zeigt die Seriennummer des Clusters an.

- Kontakt

  Zeigt Details zum Administrator an, an den Sie bei Cluster-Problemen wenden sollten.

- Standort

  Zeigt den Speicherort des Clusters an.

- Persönlichkeit

  Gibt an, ob es sich um ein für All-SAN-Arrays konfiguriertes Cluster handelt.

- **Remote Cluster Übersicht**

  Enthält Details zum Remote-Cluster in einer MetroCluster-Konfiguration. Diese Informationen werden nur für MetroCluster-Konfigurationen angezeigt.

  - Cluster

    Zeigt den Namen des Remote-Clusters an. Sie können auf den Cluster-Namen klicken, um zur Detailseite des Clusters zu navigieren.

  - Host-Name oder IP-Adresse

    Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Remote-Clusters an.

  - Seriennummer

    Zeigt die Seriennummer des Remote-Clusters an.

  - Standort

    Zeigt den Speicherort des Remote-Clusters an.

- **MetroCluster Übersicht**

  Bietet Details zum lokalen Cluster in einer MetroCluster Konfiguration. Diese Informationen werden nur für MetroCluster-Konfigurationen angezeigt.

  - Typ

    Zeigt an, ob es sich bei dem MetroCluster-Typ um zwei oder vier Nodes handelt.

◦ Konfiguration

Zeigt die MetroCluster-Konfiguration an, die die folgenden Werte aufweisen kann:

- Stretch-Konfiguration mit SAS-Kabeln
- Stretch-Konfiguration mit FC-SAS Bridge
- Fabric-Konfiguration mit FC Switches

Bei einem MetroCluster mit vier Nodes wird nur eine Fabric-Konfiguration mit FC-Switches unterstützt.

+

◦ Automatisiertes ungeplantes Switchover (AUSO)

Zeigt an, ob das automatisierte ungeplante Switchover für das lokale Cluster aktiviert ist. Standardmäßig ist AUSO für alle Cluster in einer MetroCluster-Konfiguration mit zwei Knoten in Unified Manager aktiviert. Sie können die AUSO-Einstellung über die Befehlszeilenschnittstelle ändern.

- **Knoten**
  - ◦ Gesteigerte

    Zeigt die Anzahl der Knoten an, die aktiv sind (Oder runter ( ) Im Cluster.

  - ◦ Betriebssystemversionen

    Zeigt die ONTAP-Versionen, die die Nodes ausführen, sowie die Anzahl der Nodes, auf denen eine bestimmte Version von ONTAP ausgeführt wird. Beispielsweise gibt 9.6 (2), 9.3 (1) an, dass zwei Nodes ONTAP 9.6 ausführen und auf einem Node ONTAP 9.3 ausgeführt wird.
- **Storage Virtual Machines**
  - ◦ Gesteigerte

    Zeigt die Anzahl der SVMs an, die aktiv sind (Oder runter ( ) Im Cluster.
- **Netzwerkschnittstellen**
  - ◦ Gesteigerte

    Zeigt die Anzahl der nicht-Daten-LIFs an, die in der aktiv sind (Oder runter ( ) Im Cluster.

  - ◦ Cluster-Management-Schnittstellen

    Zeigt die Anzahl der Cluster-Management-LIFs an.

  - ◦ Node-Management-Schnittstellen

    Zeigt die Anzahl der LIFs für das Node-Management an.

  - ◦ Cluster-Schnittstellen

    Zeigt die Anzahl der Cluster-LIFs an.

  - ◦ Intercluster-Schnittstellen

Zeigt die Anzahl der Intercluster-LIFs an.

- **Protokolle**
  - Datenprotokolle

    Zeigt die Liste der lizenzierten Datenprotokolle an, die für den Cluster aktiviert sind. Datenprotokolle sind iSCSI, CIFS, NFS, NVMe und FC/FCoE.

- **Cloud-Tiers**

  In sind die Namen der Cloud-Tiers aufgeführt, mit denen dieses Cluster verbunden ist. Außerdem werden die Typen (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage oder StorageGRID) und die Status der Cloud-Tiers (verfügbar oder nicht verfügbar) aufgelistet.

Registerkarte MetroCluster-Konnektivität

Zeigt die Probleme und den Konnektivitätsstatus der Clusterkomponenten der MetroCluster Konfiguration an. Ein Cluster wird in einem roten Feld angezeigt, wenn der Disaster-Recovery-Partner des Clusters Probleme hat.

Die Registerkarte MetroCluster-Konnektivität wird nur für Cluster angezeigt, die sich in einer MetroCluster-Konfiguration befinden.

Sie können zur Detailseite eines Remote-Clusters navigieren, indem Sie auf den Namen des Remote-Clusters klicken. Sie können die Details der Komponenten auch anzeigen, indem Sie auf den Zähllink einer Komponente klicken. Wenn Sie beispielsweise auf den Zähllink des Node im Cluster klicken, wird auf der Detailseite des Clusters die Registerkarte Node angezeigt. Wenn Sie auf den Link Zählen der Festplatten im Remote-Cluster klicken, wird die Registerkarte Festplatte auf der Detailseite des Remote-Clusters angezeigt.

Beim Verwalten einer MetroCluster Konfiguration mit acht Nodes wird durch Klicken auf den Zähllink der Komponente Platten-Shelfs nur die lokalen Shelfs des Standard-HA-Paars angezeigt. Es gibt auch keine Möglichkeit, die lokalen Shelfs auf dem anderen HA-Paar anzuzeigen.

Sie können den Mauszeiger über die Komponenten bewegen, um bei jedem Problem die Details und den Konnektivitätsstatus der Cluster anzuzeigen. Außerdem werden weitere Informationen zu dem für das Problem erzeugten Ereignis oder Ereignissen angezeigt.

Wenn der Status des Verbindungsproblem zwischen den Komponenten durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugeordnet ist, und die Ursache des Ereignisses anzeigen. Die Schaltfläche Details anzeigen enthält weitere Informationen zum Ereignis.

Wenn der Status des Verbindungsproblem zwischen den Komponenten durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum bei Auslösung der Ereignisse und dem Namen des Administrators angezeigt, dem das Ereignis zugeordnet ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

Registerkarte „MetroCluster-Replikation“

Zeigt den Status der Daten an, die repliziert werden. Sie können die Registerkarte MetroCluster-Replikation verwenden, um die Datensicherung durch synchrones Spiegeln der Daten mit den bereits Peering-Clustern zu gewährleisten. Ein Cluster wird in einem roten Feld angezeigt, wenn der Disaster-Recovery-Partner des Clusters Probleme hat.

Die Registerkarte MetroCluster-Replikation wird nur für Cluster angezeigt, die sich in einer MetroCluster-Konfiguration befinden.

In einer MetroCluster-Umgebung können Sie diese Registerkarte verwenden, um die logischen Verbindungen und Peering des lokalen Clusters mit dem Remote-Cluster zu überprüfen. Sie können die objektive Darstellung der Cluster-Komponenten mit ihren logischen Verbindungen anzeigen. Dadurch werden Probleme identifiziert, die bei der Spiegelung von Metadaten und Daten auftreten können.

Auf der Registerkarte MetroCluster-Replikation bietet das lokale Cluster eine detaillierte grafische Darstellung des ausgewählten Clusters. MetroCluster-Partner bezieht sich auf das Remote-Cluster.

Registerkarte Netzwerkschnittstellen

Zeigt Details zu allen nicht-Daten-LIFs an, die auf dem ausgewählten Cluster erstellt wurden.

- **Netzwerkschnittstelle**

  Zeigt den Namen der logischen Schnittstelle an, die im ausgewählten Cluster erstellt wird.

- **Betriebsstatus**

  Zeigt den Betriebsstatus der Schnittstelle an, die aktiv sein kann ( ), Down (Oder Unbekannt ( ). Der Betriebsstatus einer Netzwerkschnittstelle wird durch den Status ihrer physischen Ports bestimmt.

- **Verwaltungsstatus**

  Zeigt den Administrationsstatus der Schnittstelle an. Dieser kann aktiv sein ( ), Down (Oder Unbekannt ( ). Sie können den Administrationsstatus einer Schnittstelle steuern, wenn Sie Änderungen an der Konfiguration oder während der Wartung vornehmen. Der Administrationsstatus kann sich vom Betriebsstatus unterscheiden. Wenn jedoch der Administrationsstatus eines LIF „Inaktiv“ lautet, ist der Betriebsstatus standardmäßig „Inaktiv“.

- **IP-Adresse**

  Zeigt die IP-Adresse der Schnittstelle an.

- * Rolle*

  Zeigt die Rolle der Schnittstelle an. Mögliche Rollen sind Cluster-Management-LIFs, Node-Management-LIFs, Cluster-LIFs und Intercluster-LIFs.

- * Home Port*

  Zeigt den physischen Port an, dem die Schnittstelle ursprünglich zugeordnet war.

- **Aktueller Port**

  Zeigt den physischen Port an, dem die Schnittstelle derzeit zugeordnet ist. Nach der LIF-Migration kann

sich der aktuelle Port vom Home Port unterscheiden.

- **Failover-Richtlinie**

  Zeigt die Failover-Richtlinie an, die für die Schnittstelle konfiguriert ist.

- **Routing-Gruppen**

  Zeigt den Namen der Routinggruppe an. Sie können weitere Informationen zu den Routen und dem Ziel-Gateway anzeigen, indem Sie auf den Namen der Routinggruppe klicken.

  Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt. Daher wird für diese Cluster eine leere Spalte angezeigt.

- **Failover-Gruppe**

  Zeigt den Namen der Failover-Gruppe an.

Registerkarte Knoten

Zeigt Informationen zu Nodes im ausgewählten Cluster an. Sie können ausführliche Informationen zu HA-Paaren, Festplatten-Shelfs und Ports anzeigen:

- **HA Details**

  Stellt eine bildliche Darstellung des HA-Status und des Integritätsstatus der Nodes im HA-Paar bereit. Der Integritätsstatus des Node wird durch die folgenden Farben angezeigt:

  - **Grün**

    Der Node befindet sich in einem Betriebszustand.

  - **Gelb**

    Der Node hat den Partner-Node übernommen oder der Node weist einige Umgebungsprobleme auf.

  - * Rot*

    Der Node ist ausgefallen.

  Sie können Informationen zur Verfügbarkeit des HA-Paars anzeigen und erforderliche Maßnahmen ergreifen, um Risiken zu vermeiden. Im Fall eines möglichen Übernahmevorgangs wird beispielsweise die folgende Meldung angezeigt: `Storage failover possible`.

Sie können eine Liste der Ereignisse anzeigen, die zum HA-Paar und seiner Umgebung betreffen, z. B. Lüfter, Netzteile, NVRAM-Batterie, Flash-Karten, Serviceprozessor und Verbindung von Festplatten-Shelfs: Sie können auch die Uhrzeit anzeigen, zu der die Ereignisse ausgelöst wurden.

Sie können weitere Informationen zu Nodes anzeigen, z. B. die Modellnummer und die Seriennummer.

Bei Single-Node-Clustern können Sie auch Details zu den Nodes anzeigen.

- **Platten-Shelves**

  Zeigt Informationen über die Festplatten-Shelfs im HA-Paar an.

Sie können auch Ereignisse anzeigen, die für die Festplatten-Shelfs und die Umgebungskomponenten generiert wurden, sowie die Zeit, zu der die Ereignisse ausgelöst wurden.

- **Regal-ID**

  Zeigt die ID des Shelf an, in dem sich die Festplatte befindet.

- **Komponentenstatus**

  Zeigt Umgebungsdetails der Festplatten-Shelfs an, z. B. Netzteile, Lüfter, Temperatursensor, aktuelle Sensoren, Festplattenkonnektivität. Und Spannungssensoren. Die Umgebungsdetails werden als Symbole in den folgenden Farben angezeigt:

  - **Grün**

    Die Umgebungskomponenten funktionieren ordnungsgemäß.

  - **Grau**

    Für die Umgebungskomponenten sind keine Daten verfügbar.

  - * Rot*

    Einige Umgebungskomponenten sind nicht verfügbar.

- **Bundesland**

  Zeigt den Status des Festplatten-Shelf an. Mögliche Status sind Offline, Online, kein Status, Initialisierung erforderlich, fehlt, Und Unbekannt.

- **Modell**

  Zeigt die Modellnummer des Festplatten-Shelf an.

- **Lokales Festplatten-Shelf**

  Gibt an, ob sich das Festplatten-Shelf auf dem lokalen Cluster oder dem Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

- * Unique ID*

  Zeigt die eindeutige ID des Festplatten-Shelf an.

- **Firmware-Version**

  Zeigt die Firmware-Version des Festplatten-Shelf an.

- **Ports**

Zeigt Informationen zu den zugehörigen FC-, FCoE- und Ethernet-Ports an. Sie können Details zu den Ports und den zugehörigen LIFs anzeigen, indem Sie auf die Port-Symbole klicken.

Sie können auch die für die Ports generierten Ereignisse anzeigen.

Sie können folgende Portdetails anzeigen:

- Port-ID

  Zeigt den Namen des Ports an. Die Port-Namen können beispielsweise E0M, e0a und e0b sein.

- Rolle

  Zeigt die Rolle des Ports an. Mögliche Rollen sind Cluster, Data, Intercluster, Node-Management und Undefined.

- Typ

  Zeigt das Protokoll der physischen Schicht an, das für den Port verwendet wird. Mögliche Typen sind Ethernet, Fibre Channel und FCoE.

- WWPN

  Zeigt den WWPN (World Wide Port Name) des Ports an.

- Firmware-Version

  Zeigt die Firmware-Version des FC/FCoE-Ports an.

- Status

  Zeigt den aktuellen Status des Ports an. Mögliche Status sind „up“, „Down“, „Link Not Connected“ oder „Unbekannt“ ( ).

Sie können die portbezogenen Ereignisse in der Ereignisliste anzeigen. Sie können auch die zugehörigen LIF-Details anzeigen, z. B. LIF-Name, Betriebsstatus, IP-Adresse oder WWPN, Protokolle, den Namen der zu dieser LIF gehörenden SVM, den aktuellen Port, die Failover-Richtlinie und die Failover-Gruppe.

Registerkarte „Festplatten“

Zeigt Details zu den Festplatten im ausgewählten Cluster an. Sie können Festplatten-bezogene Informationen wie die Anzahl der verwendeten Festplatten, Ersatzfestplatten, fehlerhafte Festplatten und nicht zugewiesene Laufwerke anzeigen. Sie können auch weitere Details anzeigen, z. B. den Festplattennamen, den Festplattentyp und den Besitzer-Node der Festplatte.

- **Disk Pool Zusammenfassung**

  Zeigt die Anzahl der Laufwerke an, die nach effektiven Typen (FCAL, SAS, SATA, MSATA, SSD, NVMe SSD, SSD CAP, Array LUN und VMDISK) und der Zustand der Festplatten. Sie können auch andere Details anzeigen, wie z. B. die Anzahl der Aggregate, gemeinsam genutzte Festplatten, Ersatzfestplatten, fehlerhafte Festplatten, nicht zugewiesene Festplatten, Und nicht unterstützten Festplatten. Wenn Sie auf den Link zur Anzahl der effektiven Festplattentypen klicken, werden Festplatten mit dem ausgewählten Status und dem effektiven Typ angezeigt. Wenn Sie beispielsweise auf den Zähllink für den Festplattenstatus „beschädigt“ und „effektiver Typ SAS“ klicken, werden alle Festplatten mit dem Festplattenstatus „beschädigt“ und „effektiver Typ „SAS“ angezeigt.

- **Datenträger**

  Zeigt den Namen der Festplatte an.

- **RAID-Gruppen**

Zeigt den Namen der RAID-Gruppe an.

- **Owner Node**

  Zeigt den Namen des Node an, zu dem die Festplatte gehört. Wenn die Festplatte nicht zugewiesen ist, wird in dieser Spalte kein Wert angezeigt.

- **Bundesland**

  Zeigt den Status der Festplatte an: Aggregate, Shared, Spare, broken, Unassigned, Nicht unterstützt oder Unbekannt. Standardmäßig wird diese Spalte sortiert, um die Status in der folgenden Reihenfolge anzuzeigen: Gebrochen, nicht zugewiesen, nicht unterstützt, Spare, Aggregat, Und Shared IT.

- **Lokaler Datenträger**

  Zeigt entweder Ja oder Nein an, um anzugeben, ob sich das Laufwerk im lokalen Cluster oder im Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

- **Position**

  Zeigt die Position des Laufwerks basierend auf seinem Container-Typ an, z. B. Kopieren, Daten oder Parität. Standardmäßig ist diese Spalte ausgeblendet.

- **Betroffene Aggregate**

  Zeigt die Anzahl der Aggregate an, die aufgrund der ausgefallenen Festplatte betroffen sind. Sie können den Mauszeiger über den Zähllink verschieben, um die betroffenen Aggregate anzuzeigen. Klicken Sie dann auf den Aggregatnamen, um Details zum Aggregat anzuzeigen. Sie können auch auf die Aggregatanzahl klicken, um die Liste der betroffenen Aggregate in der Ansicht „Systemzustand: Alle Aggregate“ anzuzeigen.

  In dieser Spalte wird für die folgenden Fälle kein Wert angezeigt:

  - Für fehlerhafte Festplatten, wenn ein Cluster mit solchen Festplatten zu Unified Manager hinzugefügt wird
  - Wenn keine ausgefallenen Festplatten vorhanden sind

- **Speicherpool**

  Zeigt den Namen des Speicherpools an, zu dem die SSD gehört. Sie können den Zeiger über den Speicherpool verschieben, um Details des Speicherpools anzuzeigen.

- **Speicherbare Kapazität**

  Zeigt die verfügbare Festplattenkapazität an.

- **Rohkapazität**

  Zeigt die Kapazität der unformatierten RAW-Festplatte vor der richtigen Dimensionierung und RAID-Konfiguration an. Standardmäßig ist diese Spalte ausgeblendet.

- **Typ**

  Zeigt die Festplattentypen an, z. B. ATA, SATA, FCAL oder VMDISK.

- * Effektiver Typ*

Zeigt den von ONTAP zugewiesenen Festplattentyp an.

Bestimmte ONTAP-Festplattentypen werden als gleichbedeutend mit dem Erstellen und Hinzufügen zu Aggregaten und mit Ersatzmanagement angesehen. ONTAP weist jedem Festplattentyp einen effektiven Festplattentyp zu.

- **Spare Blocks Verbraucht %**

  Zeigt in Prozent die Spare-Blöcke an, die in der SSD-Festplatte verbraucht werden. Diese Spalte ist bei anderen Festplatten als SSD-Festplatten leer.

- **Bewertete Lebensdauer %**

  Zeigt prozentual eine Schätzung der verwendeten SSD-Lebensdauer an, basierend auf der tatsächlichen SSD-Nutzung und der Vorhersage der SSD-Lebensdauer des Herstellers. Ein Wert größer als 99 zeigt an, dass die geschätzte Haltbarkeit verbraucht wurde, weist aber möglicherweise nicht auf einen SSD-Ausfall hin. Wenn der Wert unbekannt ist, wird die Platte weggelassen.

- **Firmware**

  Zeigt die Firmware-Version der Festplatte an.

- **U/MIN**

  Zeigt die Umdrehungen pro Minute (U/min) der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

- **Modell**

  Zeigt die Modellnummer der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

- * Anbieter*

  Zeigt den Namen des Festplattenanbieters an. Standardmäßig ist diese Spalte ausgeblendet.

- **Regal-ID**

  Zeigt die ID des Shelf an, in dem sich die Festplatte befindet.

- **Bucht**

  Zeigt die ID des Einschubschachts an, in dem sich die Festplatte befindet.

Bereich „Verwandte Anmerkungen“

Hiermit können Sie die mit dem ausgewählten Cluster verknüpften Anmerkungsdetails anzeigen. Die Details umfassen den Anmerkungsnamen und die auf das Cluster angewandten Anmerkungswerte. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Mit dieser Option können Sie Gerätedetails anzeigen, die mit dem ausgewählten Cluster verknüpft sind.

Zu den Details gehören Eigenschaften des mit dem Cluster verbundenen Geräts, wie z. B. Gerätetyp, Größe, Anzahl und Integritätsstatus. Sie können auf den Zähllink klicken, um weitere Analysen zu diesem Gerät

durchzuführen.

Mithilfe des Teilfensters MetroCluster können Sie Anzahl und auch Details zum Remote MetroCluster Partner sowie zu den zugehörigen Cluster-Komponenten wie Nodes, Aggregaten und SVMs abrufen. Das Teilfenster „MetroCluster Partner“ wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

Im Bereich „Verwandte Geräte“ können Sie die Nodes, SVMs und Aggregate anzeigen und navigieren, die mit dem Cluster in Verbindung stehen:

- **MetroCluster Partner**

  Zeigt den Integritätsstatus des MetroCluster Partners an. Über den Link „count“ können Sie weitere Informationen über Zustand und Kapazität der Cluster-Komponenten abrufen.

- **Knoten**

  Zeigt die Anzahl, die Kapazität und den Systemzustand der Nodes an, die zum ausgewählten Cluster gehören. Kapazität gibt die nutzbare Gesamtkapazität über die verfügbare Kapazität an.

- **Storage Virtual Machines**

  Zeigt die Anzahl der SVMs an, die zum ausgewählten Cluster gehören.

- **Aggregate**

  Zeigt die Anzahl, Kapazität und den Systemzustand der Aggregate an, die zum ausgewählten Cluster gehören.

Bereich „Verwandte Gruppen“

Mit können Sie die Liste der Gruppen anzeigen, die den ausgewählten Cluster enthalten.

Bereich „Verwandte Warnungen“

Im Teilfenster „Related Alerts“ können Sie die Liste der Meldungen für das ausgewählte Cluster anzeigen. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Registerkarte „Aggregate/Health Details“

Mithilfe der Seite „Aggregat/Systemzustand“ werden ausführliche Informationen über das ausgewählte Aggregat angezeigt, beispielsweise Kapazität, Festplatteninformationen, Konfigurationsdetails und erzeugte Ereignisse. Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für das Aggregat anzeigen.

Befehlsschaltflächen

> Bei der Überwachung eines FabricPool-fähigen Aggregats gelten die überzugesund auf dieser Seite überzuschichtenden Werte nur für die lokale Kapazität oder das Performance-Tier. Der auf dem Cloud-Tier verfügbare Speicherplatz wird nicht in den überengagierten Werten dargestellt. Ebenso gelten die Werte für die Aggregatschwellenwerte nur für die lokale Performance-Tier.

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für das ausgewählte Aggregat ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Ermöglicht Ihnen die Navigation zur Seite „Aggregat-/Performance-Details“.

- **Aktionen**
  - Alarm Hinzufügen

    Ermöglicht Ihnen das Hinzufügen einer Warnung zum ausgewählten Aggregat.

  - Schwellenwerte Bearbeiten

    Ermöglicht Ihnen das Ändern der Schwellenwerteinstellungen für das ausgewählte Aggregat.

- **Aggregate Anzeigen**

  Ermöglicht Ihnen die Navigation zur Ansicht „Systemzustand: Alle Aggregate“.

Registerkarte „Kapazität“

Auf der Registerkarte Kapazität werden ausführliche Informationen zum ausgewählten Aggregat, z. B. Kapazität, Schwellenwerte und tägliche Wachstumsrate, angezeigt.

Standardmäßig werden Kapazitätsereignisse nicht für die Root-Aggregate generiert. Darüber hinaus gelten die von Unified Manager verwendeten Schwellenwertwerte nicht für die Root-Aggregate der Nodes. Nur ein Mitarbeiter des technischen Supports kann die Einstellungen für diese zu erstellenden Ereignisse ändern. Wenn die Einstellungen von einem Mitarbeiter des technischen Supports geändert werden, werden die Schwellenwerte auf das Root-Aggregat des Nodes angewendet.

- * Kapazität*

  Zeigt das Datenkapazitätsdiagramm und das Diagramm Snapshot Kopien an, in dem Kapazitätsdetails zum Aggregat angezeigt werden:

  - Genutzter Logischer Speicherplatz

    Die tatsächliche Größe der im Aggregat gespeicherten Daten, ohne dabei die Einsparungen durch die ONTAP Storage-Effizienztechnologien zu verwenden.

  - Verwendet

    Die von Daten im Aggregat genutzte physische Kapazität

  - Überengagiert

    Wenn der Speicherplatz im Aggregat zu hoch belegt ist, wird im Diagramm ein Flag mit dem überbelegten Betrag angezeigt.

  - Warnung

    Zeigt eine gepunktete Linie an der Stelle an, an der der Warnschwellenwert eingestellt ist; Bedeutung der Speicherplatz im Aggregat ist fast voll. Wird diese Schwelle nicht erreicht, wird das Ereignis „Space Fast Full“ generiert.

  - Fehler

Zeigt eine solide Zeile an dem Ort an, an dem der Fehlerschwellenwert festgelegt ist; bedeutet, dass der Speicherplatz im Aggregat voll ist. Wird dieser Schwellenwert nicht erreicht, wird das Ereignis „Space Full“ generiert.

◦ Diagramm Snapshot Kopien

Dieses Diagramm wird nur angezeigt, wenn die verwendete Snapshot-Kapazität oder die Snapshot-Reserve nicht null ist.

Beide Diagramme zeigen die Kapazität an, in der die Snapshot-Kapazität die Snapshot-Reserve überschreitet, wenn die genutzte Snapshot-Kapazität die Snapshot-Reserve überschreitet.

- * Cloud Tier*

  Zeigt den Speicherplatz an, der für Daten im Cloud-Tier für FabricPool-fähige Aggregate verwendet wird. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

  Wenn die Cloud-Ebene zu einem anderen Cloud-Provider (die “mMirror Tier”) gespiegelt wird, werden hier beide Cloud-Tiers angezeigt.

- **Details**

  Zeigt detaillierte Informationen zur Kapazität an.

  ◦ Gesamtkapazität

  Zeigt die Gesamtkapazität im Aggregat an.

  ◦ Datenkapazität

  Zeigt den vom Aggregat (genutzte Kapazität) verwendeten Speicherplatz und die Menge des verfügbaren Speicherplatzes im Aggregat an (freie Kapazität).

  ◦ Snapshot-Reserve

  Zeigt die verwendete und freie Snapshot Kapazität des Aggregats an.

  ◦ Überzuviel Kapazität

  Zeigt die Überbelegung des Aggregats an. Aufgrund einer Überbelegung von Aggregaten bieten Sie mehr Storage, als tatsächlich in einem bestimmten Aggregat verfügbar ist, sofern nicht alle Storage-Ressourcen derzeit verwendet werden. Bei Nutzung von Thin Provisioning kann die Gesamtgröße der Volumes im Aggregat die Gesamtkapazität des Aggregats überschreiten.

  Wenn Sie Ihr Aggregat zu hoch ansetzen, müssen Sie den verfügbaren Speicherplatz sorgfältig überwachen und Storage nach Bedarf hinzufügen, um Schreibfehler aufgrund von unzureichendem Speicherplatz zu vermeiden.

  ◦ Cloud-Tier

  Zeigt den Speicherplatz an, der für Daten im Cloud-Tier für FabricPool-fähige Aggregate verwendet wird. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein. Wenn der Cloud-Tier zu einem anderen Cloud-Provider (der Spiegeltier) gespiegelt wird, werden hier beide Cloud-Tiers angezeigt

  ◦ Cache-Speicherplatz Insgesamt

Zeigt den gesamten Speicherplatz der Solid State-Laufwerke (SSDs) bzw. Zuweisungseinheiten an, die einem Flash Pool Aggregat hinzugefügt werden. Wenn Sie Flash Pool für ein Aggregat aktiviert, aber keine SSDs hinzugefügt haben, wird der Cache-Speicherplatz als 0 KB angezeigt.

Dieses Feld ist ausgeblendet, wenn Flash Pool für ein Aggregat deaktiviert ist.

- Schwellenwerte Für Aggregate

  Zeigt die folgenden Kapazitätsschwellenwerte für das Aggregat an:

  - Nahezu Vollständig. Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Aggregat fast voll ist.

  - Vollständiger Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Aggregat voll ist.

  - Nahezu Überbeanspruchung Des Schwellenwerts

    Gibt den Prozentsatz an, mit dem ein Aggregat fast überbelegt ist.

  - Überbeanspruchung Des Schwellenwerts

    Gibt den Prozentsatz an, zu dem ein Aggregat überengagiert ist.

- Weitere Details: Tägliche Wachstumsrate

  Zeigt den im Aggregat verwendeten Festplattenspeicher an, wenn die Änderungsrate zwischen den letzten beiden Proben 24 Stunden andauert.

  Wenn ein Aggregat beispielsweise 10 GB Festplattenspeicher bei 2:00 Uhr und 12 GB bei 6:00 Uhr nutzt, beträgt die tägliche Wachstumsrate (GB) für dieses Aggregat 2 GB.

- Volume-Verschiebung

  Zeigt die Anzahl der aktuell laufenden Volume-Move-Vorgänge an:

  - Volumes Aus

    Zeigt die Anzahl und Kapazität der Volumes an, die aus dem Aggregat verschoben werden.

  Über den Link können Sie weitere Details anzeigen, beispielsweise den Volume-Namen, die Aggregate, zu denen das Volume verschoben wird, den Status der Verschiebung eines Volumes und die geschätzte Endzeit.

  - Volumes In

    Zeigt die Anzahl und die verbleibende Kapazität der Volumes an, die in das Aggregat verschoben werden.

Über den Link können Sie weitere Details anzeigen, beispielsweise den Volume-Namen, das Aggregat, aus dem das Volume verschoben wird, den Status der Verschiebung des Volumes und die geschätzte Endzeit.

- Geschätzte genutzte Kapazität nach der Verschiebung eines Volumes

  Zeigt den geschätzten belegten Speicherplatz (in Prozent und in KB, MB, GB usw.) im Aggregat an, nachdem die Verschiebevorgänge des Volumes abgeschlossen sind.

- **Kapazitätsüberblick - Volumen**

  Zeigt Diagramme an, die Informationen zur Kapazität der Volumes im Aggregat enthalten sind. Es wird die Menge an Speicherplatz angezeigt, die vom Volume (genutzte Kapazität) und die Menge des verfügbaren Speicherplatzes (freie Kapazität) im Volume verwendet wird. Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, wird die vom Volume verwendete Menge an Speicherplatz (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht verwendet werden kann (nicht nutzbare Kapazität), da die Kapazität des Aggregats angezeigt wird.

  Sie können das anzuangezeigte Diagramm in den Dropdown-Listen auswählen. Sie können die im Diagramm angezeigten Daten sortieren, um Details wie die genutzte Größe, die bereitgestellte Größe, die verfügbare Kapazität, die schnellste tägliche Wachstumsrate und die langsamste Wachstumsrate anzuzeigen. Sie können die Daten auf Grundlage der Storage Virtual Machines (SVMs) filtern, die die Volumes im Aggregat enthalten. Sie können auch Details zu Volumes anzeigen, die über Thin Provisioning bereitgestellt wurden. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den Bereich von Interesse positionieren. Standardmäßig werden im Diagramm die Top 30 der gefilterten Volumes im Aggregat angezeigt.

Registerkarte „Festplatteninformationen“

Zeigt detaillierte Informationen zu den Festplatten im ausgewählten Aggregat an, einschließlich RAID-Typ und -Größe sowie Typ der im Aggregat verwendeten Festplatten. Auf der Registerkarte werden auch die RAID-Gruppen und die verwendeten Festplatten (z. B. SAS, ATA, FCAL, SSD oder VMDISK) grafisch dargestellt. Weitere Informationen, wie z. B. der Schacht, das Shelf und die Drehgeschwindigkeit der Festplatte, können Sie mit dem Cursor über die Parity-Festplatten und die Daten-Festplatten anzeigen.

- * Daten*

  Grafische Anzeige von Details zu dedizierten Datenträgern, freigegebenen Datenträgern oder beidem. Wenn die Datenfestplatten freigegebene Laufwerke enthalten, werden grafische Details der freigegebenen Laufwerke angezeigt. Wenn die Datenfestplatten dedizierte Laufwerke und freigegebene Festplatten enthalten, werden grafische Details sowohl der dedizierten Datenlaufwerke als auch der freigegebenen Datenträger angezeigt.

  - **RAID-Details**

    RAID-Details werden nur für dedizierte Festplatten angezeigt.

    - Typ

      Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

    - Gruppengröße

      Zeigt die maximale Anzahl an Laufwerken an, die in der RAID-Gruppe zulässig sind.

    - Gruppen

      Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

- **Verwendete Festplatten**
  - Effektiver Typ

    Zeigt die Typen der Datenfestplatten an (z. B. ATA, SATA, FCAL, SSD, Oder VMDISK) im Aggregat.

  - Datenfestplatten

    Zeigt die Anzahl und Kapazität der Datenfestplatten an, die einem Aggregat zugewiesen sind. Details zur Datenfestplatte werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Festplatten enthält.

  - Parity-Festplatten

    Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat zugewiesen werden. Details zur Parity-Festplatte werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Festplatten enthält.

  - Gemeinsame Festplatten

    Zeigt die Anzahl und Kapazität der freigegebenen Datenfestplatten an, die einem Aggregat zugewiesen sind. Details zu gemeinsam genutzten Festplatten werden nur angezeigt, wenn das Aggregat freigegebene Festplatten enthält.

- **Ersatzfestplatten**

  Zeigt den effektiven Typ, die Nummer und die Kapazität der Ersatzfestplatten an, die für den Knoten im ausgewählten Aggregat verfügbar sind.

  Bei einem Failover eines Aggregats an den Partner-Node zeigt Unified Manager nicht alle freien Festplatten an, die mit dem Aggregat kompatibel sind.

- **SSD Cache**

  Enthält Details zu dedizierten Cache-SSD-Festplatten und Shared Cache SSD-Festplatten.

  Für die dedizierten Cache-SSD-Festplatten werden folgende Details angezeigt:

  - **RAID-Details**
    - Typ

      Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

    - Gruppengröße

      Zeigt die maximale Anzahl an Laufwerken an, die in der RAID-Gruppe zulässig sind.

    - Gruppen

      Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

  - **Verwendete Festplatten**
    - Effektiver Typ

Gibt an, dass die Festplatten, die für den Cache im Aggregat verwendet werden, vom Typ SSD sind.

- Datenfestplatten

  Zeigt die Anzahl und Kapazität der Datenfestplatten an, die einem Aggregat für den Cache zugewiesen werden.

- Parity-Festplatten

  Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat für den Cache zugewiesen werden.

◦ **Ersatzfestplatten**

Zeigt den effektiven Typ, die Nummer und die Kapazität der Ersatzfestplatten an, die für den Knoten im ausgewählten Aggregat für den Cache verfügbar sind.

Bei einem Failover eines Aggregats an den Partner-Node zeigt Unified Manager nicht alle freien Festplatten an, die mit dem Aggregat kompatibel sind.

Enthält die folgenden Details für den gemeinsamen Cache:

◦ **Speicherpool**

Zeigt den Namen des Speicherpools an. Sie können den Zeiger über den Speicherpool-Namen verschieben, um folgende Details anzuzeigen:

- Status

  Zeigt den Status des Speicherpools an, der gesund oder ungesund sein kann.

- Gesamtzuweisungen

  Zeigt die Gesamtzuordnungseinheiten und die Größe im Speicherpool an.

- Größe Der Zuordnungseinheit

  Zeigt den minimalen Speicherplatz im Speicherpool an, der einem Aggregat zugewiesen werden kann.

- Festplatten

  Zeigt die Anzahl der Laufwerke an, die zum Erstellen des Speicherpools verwendet werden. Wenn die Anzahl der Laufwerke in der Spalte „Speicherpool“ und die Anzahl der Festplatten, die auf der Registerkarte „Laufwerksinformationen“ für diesen Speicherpool angezeigt werden, nicht übereinstimmen, zeigt dies an, dass eine oder mehrere Festplatten beschädigt sind und der Speicherpool ungesund ist.

- Zuweisung Verwendet

  Zeigt Anzahl und Größe der von den Aggregaten verwendeten Zuordnungseinheiten an. Sie können auf den Aggregatnamen klicken, um Details zum Aggregat anzuzeigen.

- Verfügbare Zuweisung

Zeigt die Anzahl und Größe der für die Nodes verfügbaren Zuweisungseinheiten an. Sie können auf den Node-Namen klicken, um weitere Details zum Aggregat anzuzeigen.

- **Zugewiesener Cache**

  Zeigt die Größe der vom Aggregat verwendeten Zuordnungseinheiten an.

- **Zuordnungseinheiten**

  Zeigt die Anzahl der vom Aggregat verwendeten Zuordnungseinheiten an.

- **Festplatten**

  Zeigt die Anzahl der Festplatten im Speicherpool an.

- **Details**
  - Storage-Pool

    Zeigt die Anzahl der Speicherpools an.

  - Gesamtgröße

    Zeigt die Gesamtgröße der Speicherpools an.

- * Cloud Tier*

  Zeigt den Namen der Cloud-Tier an, sofern Sie ein FabricPool-fähiges Aggregat konfiguriert haben und den insgesamt verwendeten Speicherplatz anzeigt. Wenn der Cloud-Tier zu einem anderen Cloud-Provider (der Spiegeltier) gespiegelt wird, werden hier die Details für beide Cloud-Tiers angezeigt

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration werden Details zum ausgewählten Aggregat angezeigt, z. B. hinsichtlich seines Cluster-Nodes, des Blocktyps, des RAID-Typs, der RAID-Größe und der Anzahl der RAID-Gruppen:

- **Übersicht**
  - Knoten

    Zeigt den Namen des Node an, der das ausgewählte Aggregat enthält.

  - Blocktyp

    Zeigt das Blockformat des Aggregats an: Entweder 32-Bit oder 64-Bit.

  - RAID-Typ

    Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP, RAID-TEC oder gemischtes RAID).

  - RAID-Größe

    Zeigt die Größe der RAID-Gruppe an.

  - RAID-Gruppen

    Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

- SnapLock-Typ

  Zeigt den SnapLock-Typ des Aggregats an.

- * Cloud Tier*

  Wenn es sich um ein FabricPool-fähiges Aggregat handelt, werden die Details für die Cloud-Tier angezeigt. Einige Felder sind je nach Speicheranbieter unterschiedlich. Wenn die Cloud-Ebene zu einem anderen Cloud-Provider (die “mMirror Tier”) gespiegelt wird, werden hier beide Cloud-Tiers angezeigt.

  - Anbieter

    Zeigt den Namen des Storage-Providers an, z. B. StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud, Google Cloud Storage oder Alibaba Cloud Object Storage.

  - Name

    Zeigt den Namen des Cloud-Tiers an, als er von ONTAP erstellt wurde.

  - Server

    Zeigt den FQDN der Cloud-Tier an.

  - Port

    Der Port, der für die Kommunikation mit dem Cloud-Provider verwendet wird.

  - Auf Schlüssel oder Konto zugreifen

    Zeigt den Zugriffsschlüssel oder das Konto für die Cloud-Tier an.

  - Containername

    Zeigt den Bucket- oder Container-Namen des Cloud-Tiers an.

  - SSL

    Zeigt an, ob die SSL-Verschlüsselung für die Cloud-Ebene aktiviert ist.

Historienbereich

Im Bereich Verlauf werden Diagramme angezeigt, die Informationen über die Kapazität des ausgewählten Aggregats enthalten. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Verlaufsdiagramme können Ihnen bei der Identifizierung von Trends helfen: Wenn beispielsweise die Aggregatnutzung konsistent den Schwellenwert „nahezu voll“ überschreitet, können Sie die entsprechenden Maßnahmen ergreifen.

Verlaufsdiagramme zeigen folgende Informationen an:

- **Verwendete Aggregatskapazität (%)**

Zeigt die verwendete Kapazität im Aggregat und den Trend in der Art und Weise an, wie die aggregierte Kapazität basierend auf dem Nutzungsverlauf als Liniendiagramme in Prozentsätzen auf der vertikalen (y) Achse verwendet wird. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Kapazität verwendet“ klicken, wird die Diagramm-Zeile mit der verwendeten Kapazität ausgeblendet.

- **Verwendete Aggregatskapazität vs Gesamtkapazität**

  Zeigt den Trend in der Verwendung der Aggregatskapazität basierend auf dem Nutzungsverlauf sowie der verwendeten Kapazität und der Gesamtkapazität als Liniendiagramme in Byte, Kilobyte, Megabyte, Und so weiter, auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „verwendete Trend-Kapazität“ klicken, wird das Diagramm „verwendete Trendkapazität“ ausgeblendet.

- **Verwendete Aggregatskapazität (%) gegenüber dem Einsatz (%)**

  Zeigt den Trend an, wie die aggregierte Kapazität basierend auf dem Nutzungsverlauf verwendet wird, sowie den belegten Speicherplatz als Liniendiagramme in Prozent auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Space engagierte“ klicken, wird die Zeile „Space engagierte“ ausgeblendet.

Ereignisliste

In der Ereignisliste werden Details zu neuen und bestätigten Ereignissen angezeigt:

- **Severity**

  Zeigt den Schweregrad des Ereignisses an.

- **Veranstaltung**

  Zeigt den Ereignisnamen an.

- **Auslösezeit**

  Zeigt die Zeit an, die seit der Erzeugung des Ereignisses verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel für den Zeitpunkt angezeigt, zu dem das Ereignis generiert wurde.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie den Clusterknoten, Volumes und Festplatten anzeigen, die mit dem Aggregat in Verbindung stehen:

- **Knoten**

  Zeigt die Kapazität und den Integritätsstatus des Node an, der das Aggregat enthält. Kapazität gibt die nutzbare Gesamtkapazität über die verfügbare Kapazität an.

- **Aggregate im Knoten**

  Zeigt die Anzahl und Kapazität aller Aggregate im Cluster-Node an, der das ausgewählte Aggregat enthält. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt. Wenn z. B. ein Cluster-Node zehn Aggregate enthält, von denen fünf den Warnstatus und die verbleibenden fünf den kritischen Status anzeigen, ist der angezeigte Status „kritisch“.

- **Bände**

  Zeigt die Anzahl und Kapazität der FlexVol Volumes und FlexGroup Volumes im Aggregat an. Die Anzahl umfasst keine FlexGroup-Komponenten. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt.

- **Ressourcen-Pool**

  Zeigt die mit dem Aggregat verbundenen Ressourcen-Pools an.

- **Festplatten**

  Zeigt die Anzahl der Festplatten im ausgewählten Aggregat an.

Bereich „Verwandte Warnungen“

Im Bereich „Related Alerts“ können Sie die Liste der Warnmeldungen anzeigen, die für das ausgewählte Aggregat erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Benutzer hinzufügen

Sie können lokale Benutzer oder Datenbankbenutzer über die Seite Benutzer hinzufügen. Sie können auch Remote-Benutzer oder -Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Sie können diesen Benutzern Rollen zuweisen. Anhand der Berechtigungen der Rollen können Benutzer Storage-Objekte und -Daten mit Unified Manager managen oder die Daten in einer Datenbank anzeigen.

Bevor Sie beginnen

- Sie müssen über die Anwendungsadministratorrolle verfügen.
- Um einen Remote-Benutzer oder eine Remotegruppe hinzuzufügen, müssen Sie die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsserver konfiguriert haben.
- Wenn Sie die SAML-Authentifizierung so konfigurieren möchten, dass ein Identitäts-Provider (IdP) Benutzer authentifiziert, die auf die grafische Schnittstelle zugreifen, stellen Sie sicher, dass diese Benutzer als „`remote`“-Benutzer definiert sind.

  Der Zugriff auf die Benutzeroberfläche ist Benutzern vom Typ „`local`“ oder „`maintBuße`“ nicht erlaubt, wenn die SAML-Authentifizierung aktiviert ist.

Über diese Aufgabe

Wenn Sie eine Gruppe aus Windows Active Directory hinzufügen, können sich alle direkten Mitglieder und geschachtelten Untergruppen bei Unified Manager authentifizieren, es sei denn, geschachtelte Untergruppen sind deaktiviert. Wenn Sie eine Gruppe von OpenLDAP oder anderen Authentifizierungsdiensten hinzufügen, können sich nur die direkten Mitglieder dieser Gruppe bei Unified Manager authentifizieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Klicken Sie auf der Seite **Users** auf **Add**.
3. Wählen Sie im Dialogfeld **Benutzer hinzufügen** den Benutzertyp aus, den Sie hinzufügen möchten, und geben Sie die erforderlichen Informationen ein.

   Wenn Sie die erforderlichen Benutzerinformationen eingeben, müssen Sie eine E-Mail-Adresse angeben, die für diesen Benutzer eindeutig ist. Sie müssen vermeiden, E-Mail-Adressen anzugeben, die von mehreren Benutzern gemeinsam verwendet werden.

4. Klicken Sie Auf **Hinzufügen**.

Erstellen eines Datenbankbenutzers

Um eine Verbindung zwischen Workflow Automation und Unified Manager zu unterstützen oder auf Datenbankansichten zuzugreifen, müssen Sie in der Weboberfläche von Unified Manager zunächst einen Datenbankbenutzer mit dem Integrations-Schema oder dem Berichtschema erstellen.

Bevor Sie beginnen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Über diese Aufgabe

Datenbankbenutzer ermöglichen die Integration in Workflow Automation und den Zugriff auf Berichtsspezifische Datenbankansichten. Datenbankbenutzer haben keinen Zugriff auf die Unified Manager Web-UI oder die Wartungskonsole und können keine API-Aufrufe ausführen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Klicken Sie auf der Seite **Benutzer** auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld **Benutzer hinzufügen** in der Dropdown-Liste **Typ** die Option **Datenbankbenutzer** aus.
4. Geben Sie einen Namen und ein Kennwort für den Datenbankbenutzer ein.
5. Wählen Sie in der Dropdown-Liste **Rolle** die entsprechende Rolle aus.

Ihr Unternehmen	Wählen Sie diese Rolle aus
Verbindung von Unified Manager mit Workflow Automation	Integrationsschema

Ihr Unternehmen	Wählen Sie diese Rolle aus
Zugriff auf Berichtsdaten und andere Datenbankansichten	Berichtschema

6. Klicken Sie Auf **Hinzufügen**.

Definitionen von Benutzerrollen

Der Wartungsbenutzer oder der Anwendungsadministrator weist jedem Benutzer eine Rolle zu. Jede Rolle enthält bestimmte Berechtigungen. Der Umfang der Aktivitäten, die Sie in Unified Manager ausführen können, hängt von der Ihnen zugewiesenen Rolle ab und welchen Berechtigungen die Rolle enthält.

Unified Manager enthält die folgenden vordefinierten Benutzerrollen:

- **Betreiber**

  Anzeige von Storage-Systeminformationen und anderen von Unified Manager erfassten Daten, einschließlich Verläufe und Kapazitätstrends Mit dieser Rolle kann der Speicherbetreiber Notizen zu den Ereignissen anzeigen, zuweisen, bestätigen, auflösen und hinzufügen.

- * Storage Administrator*

  Konfiguration von Storage-Managementvorgängen in Unified Manager Diese Rolle ermöglicht es dem Storage-Administrator, Schwellenwerte zu konfigurieren und Alarme sowie andere für das Storage-Management spezifische Optionen und Richtlinien zu erstellen.

- **Anwendungsadministrator**

  Konfiguriert Einstellungen, die in keinem Zusammenhang mit dem Storage-Management stehen. Diese Rolle ermöglicht das Management von Benutzern, Sicherheitszertifikaten, Datenbankzugriff und Verwaltungsoptionen, einschließlich Authentifizierung, SMTP, Networking und AutoSupport.

  Wenn Unified Manager auf Linux-Systemen installiert wird, heißt der erste Benutzer mit der Anwendungsadministratorrolle automatisch „`umadmin`“.

- **Integrationsschema**

  Diese Rolle bietet schreibgeschützten Zugriff auf Unified Manager Datenbankansichten für die Integration von Unified Manager mit OnCommand Workflow Automation (WFA).

- **Schema Melden**

  Diese Rolle ermöglicht einen schreibgeschützten Zugriff auf Reporting und andere Datenbankansichten direkt aus der Unified Manager Datenbank. Folgende Datenbanken stehen zur Verfügung:

  - netapp_Modell_Ansicht
  - netapp_Performance
  - Okum
  - Ocum_Report

- Ocum_Report_birt
- opm
- Skalemonitor

Definitionen der Benutzertypen

Ein Benutzertyp gibt die Art des Kontos an, das der Benutzer besitzt und umfasst Remote-Benutzer, Remote-Gruppen, lokale Benutzer, Datenbankbenutzer und Wartungbenutzer. Jeder dieser Typen hat seine eigene Rolle, die von einem Benutzer mit der Rolle „Administrator“ zugewiesen wird.

Unified Manager-Benutzertypen sind wie folgt:

- **Benutzer der Wartung**

  Erstellt während der Erstkonfiguration von Unified Manager. Der Wartungsbenutzer erstellt dann weitere Benutzer und weist Rollen zu. Der Benutzer der Wartung ist außerdem der einzige Benutzer, der Zugriff auf die Wartungskonsole hat. Wenn Unified Manager auf einem Red hat Enterprise Linux- oder CentOS-System installiert ist, erhält der Wartungbenutzer den Benutzernamen „`umadmin`.“.

- **Lokaler Benutzer**

  Greift auf die Unified Manager-Benutzeroberfläche zu und führt Funktionen basierend auf der Rolle durch, die der Wartungsbenutzer oder ein Benutzer mit der Anwendungsadministratorrolle angegeben hat.

- **Remote-Gruppe**

  Eine Gruppe von Benutzern, die mit den auf dem Authentifizierungsserver gespeicherten Anmeldeinformationen auf die Benutzeroberfläche von Unified Manager zugreifen. Der Name dieses Kontos muss mit dem Namen einer auf dem Authentifizierungsserver gespeicherten Gruppe übereinstimmen. Allen Benutzern innerhalb der Remote-Gruppe wird über ihre individuellen Benutzeranmeldeinformationen der Zugriff auf die Unified Manager-Benutzeroberfläche gewährt. Remote-Gruppen können Funktionen entsprechend ihren zugewiesenen Rollen ausführen.

- **Remote-Benutzer**

  Greift über die auf den Authentifizierungsserver gespeicherten Anmeldeinformationen auf die Unified Manager-UI zu. Ein Remote-Benutzer führt Funktionen basierend auf der Rolle aus, die der Wartungsbenutzer oder ein Benutzer mit der Anwendungsadministratorrolle angegeben hat.

- **Datenbankbenutzer**

  Hat schreibgeschützten Zugriff auf Daten in der Unified Manager-Datenbank, hat keinen Zugriff auf die Unified Manager-Webschnittstelle oder die Wartungskonsole und kann keine API-Aufrufe ausführen.

Unified Manager Benutzer-Rollen und -Funktionen

Anhand der Ihnen zugewiesenen Benutzerrolle können Sie festlegen, welche Vorgänge Sie in Unified Manager ausführen können.

In der folgenden Tabelle sind die Funktionen aufgeführt, die die einzelnen Benutzerrollen ausführen können:

Funktion	Operator	Storage-Administrator	Applikationsadministrator	Integrationsschema	Berichtschema
Anzeigen von Speichersysteminformationen	•	•	•	•	•
Andere Daten wie Verläufe und Kapazitätstrends anzeigen	•	•	•	•	•
Ereignisse anzeigen, zuweisen und lösen	•	•	•		
Anzeigen von Storage-Serviceobjekten, z. B. SVM-Zuordnungen und Ressourcenpools	•	•	•		
Anzeigen von Schwellenwertrichtlinien	•	•	•		
Management von Storage-Serviceobjekten wie SVM-Zuordnungen und Ressourcenpools		•	•		
Definieren von Warnmeldungen		•	•		
Optionen für das Storage Management managen		•	•		

Funktion	Operator	Storage-Administrator	Applikationsadministrator	Integrationsschema	Berichtschema
Storage Management-Richtlinien managen		•	•		
Benutzer managen			•		
Management von Verwaltungsoptionen			•		
Definieren Sie Schwellenwertrichtlinien			•		
Datenbankzugriff managen			•		
Managen Sie die Integration in WFA und erhalten Sie Zugriff auf die Datenbankansichten				•	
Planen und Speichern von Berichten		•	•		
Führen Sie „`Fix IT`“-Vorgänge aus Management Actions aus		•	•		
Schreibgeschützter Zugriff auf Datenbankansichten					•

Erstellen eines HTTPS-Sicherheitszertifikats

Sie können aus mehreren Gründen ein neues HTTPS-Sicherheitszertifikat generieren, z.

B. wenn Sie mit einer anderen Zertifizierungsstelle signieren möchten oder wenn das aktuelle Sicherheitszertifikat abgelaufen ist. Das neue Zertifikat ersetzt das vorhandene Zertifikat.

Bevor Sie beginnen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Über diese Aufgabe

Wenn Sie keinen Zugriff auf die Web-UI von Unified Manager haben, können Sie mithilfe der Wartungskonsole das HTTPS-Zertifikat mit den gleichen Werten neu generieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikat erneut erstellen**.

   Das Dialogfeld „HTTPS-Zertifikat neu erstellen“ wird angezeigt.

3. Wählen Sie je nach Erstellung des Zertifikats eine der folgenden Optionen aus:

Ihr Ziel ist	Tun Sie das…
Generieren Sie das Zertifikat mit den aktuellen Werten neu	Klicken Sie auf die Option **regenerieren mit aktuellen Zertifikatattributen**.

Ihr Ziel ist	Tun Sie das…
Generieren Sie das Zertifikat mithilfe anderer Werte	Klicken Sie auf die Option **Aktuellen Zertifikatattributen aktualisieren**. Die Felder allgemeiner Name und Alternative Namen verwenden die Werte aus dem vorhandenen Zertifikat, wenn Sie keine neuen Werte eingeben. Die anderen Felder benötigen keine Werte, aber Sie können Werte eingeben, z. B. für Stadt, Bundesland und Land, wenn diese Werte in das Zertifikat eingetragen werden sollen. Sie können das Kontrollkästchen „`lokale Identifizierungsdaten ausschließen (z. B. localhost)`“ aktivieren, wenn Sie die lokalen Identifizierungsdaten aus dem Feld Alternative Namen im Zertifikat entfernen möchten. Wenn dieses Kontrollkästchen aktiviert ist, werden nur die Daten verwendet, die Sie in das Feld Alternative Namen eingeben. Wenn das Zertifikat leer gelassen wird, hat das resultierende Zertifikat überhaupt kein Feld alternativer Namen.

4. Klicken Sie auf **Ja**, um das Zertifikat erneut zu generieren.
5. Starten Sie den Unified Manager-Server neu, damit das neue Zertifikat wirksam wird.

Nachdem Sie fertig sind

Überprüfen Sie die neuen Zertifikatinformationen, indem Sie das HTTPS-Zertifikat anzeigen.

Unterstützte CLI-Befehle von Unified Manager

Als Storage-Administrator führen Sie mit den CLI-Befehlen Abfragen für die Storage-Objekte durch, z. B. für Cluster, Aggregate, Volumes, Qtrees und LUNs. Sie können die CLI-Befehle verwenden, um die interne Datenbank von Unified Manager und die ONTAP-Datenbank abzufragen. Sie können auch CLI-Befehle in Skripten verwenden, die zu Beginn oder am Ende eines Vorgangs ausgeführt oder ausgeführt werden, wenn eine Meldung ausgelöst wird.

Allen Befehlen muss der Befehl vorangestellt sein `um cli login` Und einen gültigen Benutzernamen und ein gültiges Passwort für die Authentifizierung.

CLI-Befehl	Beschreibung	Ausgabe
`um cli login -u <username> [-p <password>]`	Melden Sie sich bei der CLI an. Wegen der Auswirkungen auf die Sicherheit sollten Sie nur den Benutzernamen nach der Option „ `-U` “ eingeben. Wenn Sie auf diese Weise verwendet werden, werden Sie zur Eingabe des Passworts aufgefordert, und das Passwort wird nicht in der Historie oder Prozesstabelle erfasst. Die Sitzung läuft nach drei Stunden ab dem Zeitpunkt der Anmeldung ab. Danach muss sich der Benutzer erneut anmelden.	Zeigt die entsprechende Meldung an.
`um cli logout`	Melden Sie sich über die CLI ab.	Zeigt die entsprechende Meldung an.
`um help`	Zeigt alle Unterbefehle der ersten Ebene an.	Zeigt alle Unterbefehle der ersten Ebene an.
`um run cmd [ -t <timeout> ] <cluster> <command>`	Die einfachste Methode, einen Befehl auf einem oder mehreren Hosts auszuführen. Hauptsächlich wird verwendet für Alert Scripting um ONTAP zu erhalten oder eine Operation durchzuführen. Das optionale Argument für die Zeitüberschreitung setzt eine maximale Zeitgrenze (in Sekunden), damit der Befehl auf dem Client ausgeführt werden kann. Der Standardwert ist 0 (ewig warten).	Nach Erhalt bei ONTAP.
`um run query <sql command>`	Führt eine SQL-Abfrage aus. Es sind nur Abfragen erlaubt, die aus der Datenbank gelesen werden. Aktualisierungsvorgänge, Einfügevorgänge oder Löschvorgänge werden nicht unterstützt.	Die Ergebnisse werden in tabellarischer Form angezeigt. Wenn ein leerer Satz zurückgegeben wird, oder wenn ein Syntaxfehler oder eine fehlerhafte Anforderung vorliegt, wird die entsprechende Fehlermeldung angezeigt.

CLI-Befehl	Beschreibung	Ausgabe
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Fügt der Liste der gemanagten Speichersysteme eine Datenquelle hinzu. Eine Datenquelle beschreibt, wie Verbindungen zu Speichersystemen hergestellt werden. Beim Hinzufügen einer Datenquelle müssen die Optionen -U (Benutzername) und -P (Passwort) angegeben werden. Die Option -t (Protocol) gibt das Protokoll an, das zur Kommunikation mit dem Cluster verwendet wird (http oder https). Wenn das Protokoll nicht angegeben wird, werden beide Protokolle versucht, die Option -p (Port) gibt den Port an, der zur Kommunikation mit dem Cluster verwendet wird. Wenn der Port nicht angegeben wird, wird versucht, den Standardwert des entsprechenden Protokolls zu verwenden. Dieser Befehl kann nur vom Storage-Admin ausgeführt werden.	Fordert den Benutzer auf, das Zertifikat anzunehmen, und druckt die entsprechende Meldung.
`um datasource list [ <datasource-id>]`	Zeigt die Datenquellen für verwaltete Speichersysteme an.	Zeigt die folgenden Werte im Tabellenformat an: `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message.`
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	Ändert eine oder mehrere Datenquellenoptionen. Kann nur vom Storage-Administrator ausgeführt werden.	Zeigt die entsprechende Meldung an.
`um datasource remove <datasource-id>`	Entfernt die Datenquelle (Cluster) aus Unified Manager.	Zeigt die entsprechende Meldung an.
`um option list [ <option> .. ]`	Listet alle Optionen auf, die Sie mit konfigurieren können `set` Befehl.	Zeigt die folgenden Werte im Tabellenformat an: `Name, Value, Default Value, and Requires Restart.`

CLI-Befehl	Beschreibung	Ausgabe
`um option set <option-name>=<option-value> [ <option-name>=<option-value> ... ]`	Legt eine oder mehrere Optionen fest. Der Befehl kann nur vom Storage-Admin ausgeführt werden.	Zeigt die entsprechende Meldung an.
`um version`	Zeigt die Softwareversion von Unified Manager an.	`Version ("9.6")`
`um lun list [-q] [ -ObjectType <object-id>]`	Führt die LUNs nach dem Filtern auf das angegebene Objekt auf. -q ist für alle Befehle geeignet, keine Kopfzeile anzuzeigen. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, Oder svm. Beispiel: `um lun list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Mit dem Befehl werden alle LUNs im Cluster mit der ID 1 aufgeführt.	Zeigt die folgenden Werte im Tabellenformat an: `ID and LUN path`.
`um svm list [-q] [ -ObjectType <object-id>]`	Führt die Storage-VMs nach dem Filtern nach dem angegebenen Objekt auf. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, Oder svm. Beispiel: `um svm list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Storage VMs innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an: `Name and Cluster ID`.
`um qtree list [-q] [ -ObjectType <object-id>]`	Führt die qtrees nach dem Filtern auf dem angegebenen Objekt auf. -q ist für alle Befehle geeignet, keine Kopfzeile anzuzeigen. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, Oder svm. Beispiel: `um qtree list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Mit dem Befehl werden alle qtrees im Cluster mit der ID 1 aufgelistet.	Zeigt die folgenden Werte im Tabellenformat an: `Qtree ID and Qtree Name`.

CLI-Befehl	Beschreibung	Ausgabe
`um disk list [-q] [-ObjectType <object-id>]`	Listet die Festplatten nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node oder Cluster sein. Beispiel: `um disk list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Festplatten im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `ObjectType and object-id.`
`um cluster list [-q] [-ObjectType <object-id>]`	Listet die Cluster nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster, lun, sein Qtree, Volume, Kontingent oder svm. Beispiel:`um cluster list -aggr 1` In diesem Beispiel ist "-aggr" der objectType und "1" die objectId. Der Befehl listet das Cluster auf, zu dem das Aggregat mit der ID 1 gehört.	Zeigt die folgenden Werte im Tabellenformat an: `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.`
`um cluster node list [-q] [-ObjectType <object-id>]`	Führt die Cluster-Nodes nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node oder Cluster sein. Beispiel: `um cluster node list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Nodes im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Name and Cluster ID.`
`um volume list [-q] [-ObjectType <object-id>]`	Listet die Volumes nach dem Filtern auf dem angegebenen Objekt auf. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, svm oder Aggregat: Beispiel: `um volume list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Volumes im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Volume ID and Volume Name.`

CLI-Befehl	Beschreibung	Ausgabe
`um quota user list [-q] [-ObjectType <object-id>]`	Listet die Quota-Benutzer nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann qtree, Cluster, Volume, Kontingent oder svm sein. Beispiel: `um quota user list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Kontingentbenutzer innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `ID, Name, SID and Email.`
`um aggr list [-q] [-ObjectType <object-id>]`	Führt die Aggregate nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster oder Volume sein. Beispiel: `um aggr list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Aggregate innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Aggr ID, and Aggr Name.`
`um event ack <event-ids>`	Bestätigt ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event resolve <event-ids>`	Löst ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event assign -u <username> <event-id>`	Weist einem Benutzer ein Ereignis zu.	Zeigt die entsprechende Meldung an.
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Listet die vom System oder Benutzer generierten Ereignisse auf. Filtern von Ereignissen nach Quelle, Status und IDs	Zeigt die folgenden Werte im Tabellenformat an `Source, Source type, Name, Severity, State, User and Timestamp.`
`um backup restore -f <backup_file_path_and_name>`	Stellt eine Sicherung einer MySQL-Datenbank mithilfe von .7z-Dateien wieder her.	Zeigt die entsprechende Meldung an.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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