



Gemeinsame Workflows und Aufgaben im Zusammenhang mit Unified Manager

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

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	16
Managen von Backup- und Restore-Vorgängen	29
Verwalten von Skripten	47
Verwalten und Überwachen von Gruppen	50
Priorisieren von Storage-Objekt ereignissen mithilfe von Anmerkungen	59
Senden eines Support-Bundles über eine Web-UI und eine Wartungskonsole	68
Aufgaben und Informationen im Zusammenhang mit mehreren Workflows	76

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 Problembefehung 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 Problembefehung 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 Sicherheitsbeziehungen"](#) 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 ["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.

Was Sie brauchen

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

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 Seite **Event Management** Inventory 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 „Storage 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 Ereignisdetails können Sie eine oder mehrere der folgenden Aufgaben ausführen:
 - Überprüfen Sie die Fehlermeldung im Feld Ursache, und bewerten Sie das Problem.
 - Weisen Sie das Ereignis einem Administrator zu.
 - Bestätigen Sie das Ereignis.

Verwandte Informationen

["Seite mit den Veranstaltungsdetails"](#)

["Unified Manager Benutzer-Rollen und -Funktionen"](#)

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.

Was Sie brauchen

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

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 Beispielergebnisinformationen 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.

Bitte 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.

Verwandte Informationen

["Seite mit den Veranstaltungsdetails"](#)

["Unified Manager Benutzer-Rollen und -Funktionen"](#)

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.

Was Sie brauchen

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

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 Offlineevent 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.
- Weisen Sie das Ereignis einem Administrator zu.
- Bestätigen Sie das Ereignis oder markieren Sie es gegebenenfalls als erledigt.

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.

Was Sie brauchen

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

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-Volumens können Sie zu anderen Seiten und Fenstern navigieren, um mögliche Ursachen zu bestätigen oder zu eliminieren:

- 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](#)".

Verwandte Informationen

["Unified Manager Benutzer-Rollen und -Funktionen"](#)

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.

Was Sie brauchen

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

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.

- 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.

- 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.

- Klicken Sie in der Ansicht Systemzustand: 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.

- 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 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 heruntergeschilerten 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.

Was Sie brauchen


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

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

- 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 „stagedated“ 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** View SVM 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 Fensterbereich Verwandte Geräte der Seite Volume / Health Details 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 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.

Was Sie brauchen

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

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 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.

Was Sie brauchen

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

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.
 - Klicken Sie im Feld Quelle auf den Objektnamen, in diesem Fall ein Volume, um Details zum Objekt anzuzeigen.
 - Suchen Sie nach Notizen, die zu diesem Event hinzugefügt wurden.
 - Fügen Sie dem Ereignis eine Notiz hinzu.
 - Das Ereignis einem anderen Benutzer zuweisen.

- Bestätigen Sie das Ereignis.
- Markieren Sie das Ereignis als erledigt.

Verwandte Informationen

["Seite mit den Veranstaltungsdetails"](#)

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.

Was Sie brauchen

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.

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.

Verwandte Informationen

["Seite mit den Veranstaltungsdetails"](#)

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.

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 Schwellenwerteinstellungen für einzelne Objekte auch auf der Bestandsseite oder auf der Detailseite für das Objekt ändern.

- Weitere Informationen finden Sie unter ["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.

- Weitere Informationen finden Sie unter ["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.

- Weitere Informationen finden Sie unter ["Konfigurieren von globalen qtree-Zustandsschwellenwerten"](#).

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

- Weitere Informationen finden Sie unter ["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.

Was Sie brauchen

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

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**.

Verwandte Informationen

["Benutzer hinzufügen"](#)

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.

Was Sie brauchen

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

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 Volumes 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**.

Verwandte Informationen

["Benutzer hinzufügen"](#)

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.

Was Sie brauchen

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

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.

Was Sie brauchen

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

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**.

Verwandte Informationen

["Benutzer hinzufügen"](#)

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.

Was Sie brauchen

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

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**.

Verwandte Informationen

["Benutzer hinzufügen"](#)

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.

Was Sie brauchen

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

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 Volumes 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**.

Verwandte Informationen

["Benutzer hinzufügen"](#)

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.

Was Sie brauchen

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

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.

Siehe ["NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9"](#) (TR-4569) Detaillierte Empfehlungen und Lösungen.

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.

Weitere Informationen finden Sie unter ["Welche Sicherheitskriterien werden bewertet"](#).

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

Weitere Informationen finden Sie unter Compliance-Kategorien und im ["NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9"](#) Ausführliche Informationen finden Sie unter.



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.

Weitere Informationen finden Sie unter ["Verwalten von Zielen für die Cluster-Sicherheit"](#).

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 *cbc beginnen.	Nein	Ja.
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.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
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.
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.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
SAML-Benutzer	Gibt an, ob SAML konfiguriert ist. Mit SAML können Sie Multi-Faktor-Authentifizierung (MFA) als Anmeldemethode für Single-Sign-On konfigurieren.	Nein	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.	Nein	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.	Nein	Nein
Zertifikatbenutzer	Zeigt an, ob ein Zertifikatbenutzer zur Anmeldung beim Cluster konfiguriert ist.	Nein	Nein
Lokale Benutzer	Zeigt an, ob lokale Benutzer für die Anmeldung am Cluster konfiguriert sind.	Nein	Nein
Remote Shell	Zeigt an, ob RSH aktiviert ist. Aus Sicherheitsgründen sollte RSH deaktiviert werden. Vorzugsweise ist Secure Shell (SSH) für sicheren Remote-Zugriff.	Deaktiviert	Ja.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
MD5 wird verwendet	Zeigt an, ob ONTAP-Benutzerkonten die weniger sichere MD5-Hash-Funktion verwenden. Die MD5-Hashed-Benutzerkonten-Migration auf die sicherere kryptografische Hash-Funktion wie SHA-512 wird bevorzugt.	Nein	Ja.
Zertifikatsaussteller Typ	Gibt den Typ des verwendeten digitalen Zertifikats an.	CA-signiert	Nein

Compliance-Kategorien für Storage-VMs

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 <code>cbc*</code> .	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

Parameter	Beschreibung	Empfehlung	Beeinträchtigt SVM-Compliance
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
Kerberos V5	Gibt an, ob die Kerberos-V5-Authentifizierung aktiviert oder deaktiviert ist.	Aktiviert	Nein
NIS-Authentifizierung	Gibt an, ob die Verwendung der NIS-Authentifizierung konfiguriert ist.	Deaktiviert	Nein
FPolicy Status aktiv	Zeigt an, ob FPolicy erstellt wird oder nicht.	Ja.	Nein
SMB-Verschlüsselung aktiviert	Gibt an, ob SMB -Signing & Sealing nicht aktiviert ist.	Ja.	Nein
SMB-Signatur aktiviert	Gibt an, ob SMB -Signing nicht aktiviert ist.	Ja.	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.

Parameter	Beschreibung
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 für Cluster und Storage VMs

Active IQ Unified Manager ermöglicht Ihnen, den Sicherheitsstatus der Storage-Objekte in Ihrer Umgebung von verschiedenen Punkten der Schnittstelle aus anzuzeigen. Sie können Informationen und Berichte auf der Basis definierter Parameter erfassen und analysieren und verdächtige Verhaltensweisen oder nicht autorisierte Systemänderungen auf den überwachten Clustern und Storage-VMs erkennen.

Informationen zu den Sicherheitsempfehlungen finden Sie im ["NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9"](#)

Anzeigen des Sicherheitsstatus auf Objektebene auf der Sicherheitsseite

Als Systemadministrator können Sie die Seite **Sicherheit** verwenden, um einen Überblick über die Sicherheitskraft Ihrer ONTAP Cluster und Storage VMs auf Datacenter- und Standortebene zu erhalten. Die unterstützten Objekte sind Cluster, Storage VMs und Volumes. Führen Sie hierzu folgende Schritte aus:

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. Die Seite Sicherheit wird angezeigt.

Klicken Sie auf die Balkendiagramme, -Zählungen und *View Reports* Über Links gelangen Sie zur Seite **Volumes**, **Cluster** oder **Storage VMs**, auf der Sie die entsprechenden Details anzeigen oder Berichte erstellen können.

Auf der Seite Sicherheit werden die folgenden Felder angezeigt:

- **Cluster Compliance:** Der Sicherheitsstatus (Anzahl der Cluster, die konform sind oder nicht kompatibel sind) aller Cluster in einem Rechenzentrum
- **Storage VM Compliance:** Der Sicherheitsstatus (Anzahl der konformen oder nicht konformen Storage VMs) für alle Storage VMs in Ihrem Datacenter
- **Volume Encryption:** Der Volume-Verschlüsselungsstatus (Anzahl der verschlüsselten oder nicht verschlüsselten Volumes) aller Volumes in Ihrer Umgebung
- **Volume Anti-Ransomware Status:** Der Sicherheitsstatus (Anzahl der Volumes mit aktivierter oder deaktivierter Anti-Ransomware-Funktion) aller Volumes in Ihrer Umgebung
- **Clusterauthentifizierung und Zertifikate:** Die Anzahl der Cluster, die jede Art von Authentifizierungsmethode verwenden, wie SAML, Active Directory oder über Zertifikate und lokale Authentifizierung. Im Panel wird auch die Anzahl der Cluster angezeigt, deren Zertifikate entweder abgelaufen sind oder in 60 Tagen ablaufen.


Zeigen Sie auf der Seite Cluster die Sicherheitsdetails aller Cluster an

Auf der Seite **Cluster / Security** Details können Sie den Sicherheits-Compliance-Status auf Clusterebene anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage > Cluster**.
2. Wählen Sie **Ansicht > Sicherheit > Alle Cluster**.

Standardsicherheitsparameter wie Global FIPS, Telnet, unsichere SSH-Einstellungen, Anmeldebanner, Netzwerkzeitprotokoll, AutoSupport HTTPS-Transport und der Status des Cluster-Zertifikats werden angezeigt.

Sie können auf klicken  Weitere Optionen und wählen Sie, um die Sicherheitsinformationen auf der Seite **Sicherheit** von Unified Manager oder auf System Manager anzuzeigen. Sie sollten gültige Anmeldeinformationen zum Anzeigen der Details in System Manager haben.



Wenn ein Cluster ein abgelaufenes Zertifikat besitzt, können Sie auf klicken *expired* Unter **Cluster Certificate Validität**, und erneuern Sie es von System Manager (9.10.1 und höher). Sie können nicht auf klicken *expired* Wenn die System Manager Instanz eine Version vor 9.10.1 enthält.

Details zur Sicherheit aller Cluster finden Sie auf der Seite Storage-VMs

Auf der Seite **Storage VMs / Security** Details können Sie den Sicherheits-Compliance-Status auf Storage VM-Ebene anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage > Storage VMs**.
2. Wählen Sie **Ansicht > Sicherheit > Alle Storage VMs**. Es wird eine Liste der Cluster mit den Sicherheitsparametern angezeigt.

Sie können die Sicherheitskonformität der Speicher-VMs standardmäßig anzeigen, indem Sie die Sicherheitsparameter wie Storage-VMs, Cluster, Anmeldebanner, Revisionsprotokoll und unsichere SSH-Einstellungen überprüfen.

Sie können auf klicken **⋮** Weitere Optionen und wählen Sie, um die Sicherheitsinformationen auf der Seite **Sicherheit** von Unified Manager oder auf System Manager anzuzeigen. Sie sollten gültige Anmeldeinformationen zum Anzeigen der Details in System Manager haben.

Einzelheiten zur Sicherheit gegen Ransomware-Angriffe für Volumes und Storage-VMs finden Sie unter ["Anzeigen des Anti-Ransomware-Status aller Volumes und Storage-VMs"](#).

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.

Was Sie brauchen

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

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.

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.

Was Sie brauchen

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

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 **Verschlüsselungstyp**, oder verwenden Sie den Filter, um Volumes mit einem bestimmten Verschlüsselungstyp anzuzeigen oder die nicht verschlüsselt sind (Verschlüsselungstyp von „Keine“).

Anzeigen des Anti-Ransomware-Status aller Volumes und Storage-VMs

Eine Liste aller Volumes und Storage VMs (SVMs) und ihres aktuellen Status gegen Ransomware können Sie feststellen, ob die Daten auf Ihren Volumes und SVMs ausreichend vor Ransomware-Angriffen geschützt sind.

Was Sie brauchen

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

Weitere Informationen zu den verschiedenen Status gegen Ransomware finden Sie unter "[ONTAP: Anti-Ransomware](#)".

Anzeigen der Sicherheitsinformationen aller Volumes mit Ransomware-Erkennung

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage > Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Gesundheit > Sicherheit > Anti-Ransomware**
3. In der **Sicherheit: Anti-Ransomware** Ansicht können Sie nach den verschiedenen Feldern sortieren oder den Filter verwenden.



Anti-Ransomware wird nicht für Offline Volumes, eingeschränkte Volumes, SnapLock Volumes, FlexGroup Volumes, FlexCache Volumes und SAN-only Volumes, Volumes von angestoppten Storage-VMs, Root-Volumes von Storage-VMs oder Datensicherungs-Volumes

Anzeigen der Sicherheitsinformationen aller Storage-VMs mit Ransomware-Erkennung

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage > Storage VMs**.
2. Wählen Sie **Ansicht > Sicherheit > Anti-Ransomware**. Eine Liste der SVMs mit dem Ransomware-Status wird angezeigt.



Das Ransomware-Monitoring wird auf Storage-VMs, die kein NAS-Protokoll besitzen, nicht unterstützt.

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.

Was Sie brauchen

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.

Was Sie brauchen

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

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.

Was Sie brauchen

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

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* die Ereignisse, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das...
Deaktivieren von Ereignissen	<ol style="list-style-type: none">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	<ol style="list-style-type: none">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 Active IQ Unified Manager erstellen und das Backup mit der Wiederherstellungsfunktion auf dasselbe (lokale) System oder ein neues (Remote-)System im Falle eines Systemausfalls oder Datenverlust wiederherstellen.

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	Klein	Unified Manager MySQL Datenbank-Dump
	Groß	NetApp Snapshot einer Unified Manager Datenbank mit iSCSI-Protokoll

Diese verschiedenen Methoden werden in den folgenden Abschnitten beschrieben.

Backup und Restore für Unified Manager auf der virtuellen 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 Active IQ Unified Manager-Datenbank und Konfigurationsdateien, die Sie im Falle eines Systemausfalls oder

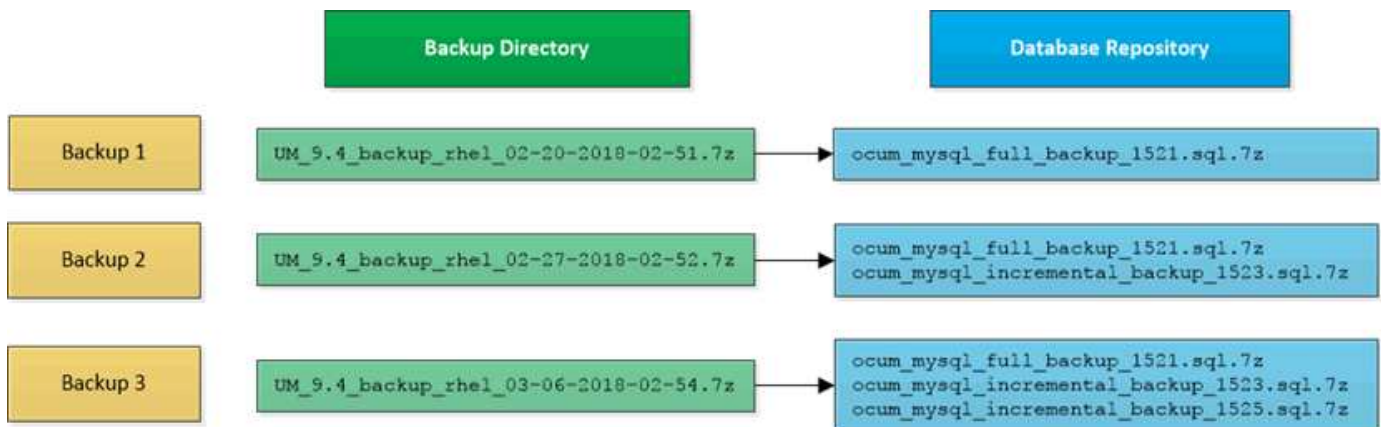
Datenverlust verwenden können. Sie können ein Backup so planen, dass es auf ein lokales Ziel oder auf ein Remote-Ziel geschrieben wird. Es wird dringend empfohlen, einen Remote-Standort außerhalb des Active IQ Unified Manager Host-Systems zu definieren.



MySQL Datenbank Dump ist der Standard-Backup-Mechanismus, wenn Unified Manager auf einem Linux- und Windows-Server installiert ist. Wenn Unified Manager jedoch eine große Anzahl von Clustern und Nodes managt oder die MySQL Backups viele Stunden in Anspruch nehmen, können Sie mithilfe von Snapshot Kopien ein Backup durchführen. Diese Funktion ist verfügbar für Red hat Enterprise Linux, CentOS Linux und Windows.

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 Active IQ 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.

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.

Was Sie brauchen

- 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 und MySQL-Backup verwendet, stellen Sie sicher, dass die folgenden Berechtigungen und Eigentümerschaften auf dem Backup-Verzeichnis festgelegt sind.

Berechtigungen: 0750, Eigentum: jboss:Maintenance

- Wenn Unified Manager auf einem Windows-System installiert ist und MySQL Backup verwendet wird, stellen Sie sicher, dass nur der Administrator Zugriff auf das Backup-Verzeichnis hat.

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 zu groß für den Platz ist, den Sie für Backups zugewiesen haben, können Sie regelmäßig eine vollständige Sicherung durchführen, um die alte Sicherung und die inkrementellen Dateien zu ersetzen. Als weitere Option können Sie ein Backup mit Snapshot Kopien erstellen.
- Das Backup, das während der ersten 15 Tage einer neuen Cluster-Ergänzung erstellt wurde, ist möglicherweise nicht genau genug, um die historischen Performance-Daten zu erhalten.

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**.

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

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.

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.

Verwandte Informationen

["Erstellen eines HTTPS-Sicherheitszertifikats"](#)

["Aktivieren der SAML-Authentifizierung"](#)

["Authentifizierung mit Active Directory oder OpenLDAP"](#)

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.

Was Sie brauchen

- 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.

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 Domännennamen 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.

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 Datenbankennwort 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.

Was Sie brauchen

- 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.

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 Ordernamen 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 oder die Eingabeaufforderung 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.

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

Eine NetApp Snapshot Kopie 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, eine Snapshot-Kopie regelmäßig auf ein Volume auf einem Ihrer ONTAP Cluster zu schreiben, sodass Sie immer eine aktuelle Kopie haben.



Diese Funktion ist für Active IQ Unified Manager, die auf einer virtuellen Appliance installiert sind, nicht verfügbar.

Backup wird unter Linux konfiguriert

Wenn das Active IQ Unified Manager auf einem Linux Computer installiert ist, können Sie entscheiden, Backup und Restore mit NetApp Snapshots zu konfigurieren.

Snapshot-Kopien nehmen in der Regel nur ein paar Minuten Zeit in Anspruch und die Unified Manager-Datenbank ist innerhalb eines sehr kurzen Zeitrahmens gesperrt, sodass Ihre Installation nur geringfügig 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.

- Sie können eine Snapshot-Kopie nur auf derselben Version von Active IQ Unified Manager wiederherstellen.



Wenn Sie beispielsweise ein Backup mit Unified Manager 9.13 erstellt haben, kann das Backup nur auf Unified Manager 9.13-Systemen wiederhergestellt werden.

- Wenn sich die Snapshot-Konfiguration ändert, kann dies zu einem ungültigen Snapshot führen.

Speicherort für Snapshot-Kopien wird konfiguriert

Sie können das Volume mithilfe von ONTAP System Manager oder über die ONTAP CLI so konfigurieren, dass Snapshot Kopien auf einem Ihrer ONTAP Cluster gespeichert werden.

Was Sie brauchen

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:
 - Der Namensschalter und die Namenszuweisung müssen auf „files“ gesetzt werden.
 - 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
 - NFS für NetApp Snapshot für Linux
 - NFSv4 muss auf dem NFS-Server und der NFSv4-ID-Domäne aktiviert sein, die auf dem Client und der Storage-VM angegeben ist
 - Das Volume sollte mindestens die doppelte Größe von Unified Manager/opt/netapp/Data Directory haben

Überprüfen Sie mit dem Befehl `du -sh /opt/netapp/Data/` die aktuelle Größe.

- Volume-Anforderungen:
 - Das Volume sollte mindestens die doppelte Größe des Unified Manager/opt/netapp/Datenverzeichnis haben
 - 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.

Detaillierte Schritte zur Erstellung des NFS-Volume finden Sie unter ["So konfigurieren Sie NFSv4 in ONTAP 9"](#) Und das ["ONTAP 9 NFS Configuration Express-Handbuch"](#).

Angeben des Zielorts für Snapshot Kopien

Sie sollten den Zielspeicherort für Active IQ Unified Manager Snapshot Kopien auf einem Volume konfigurieren, das Sie bereits in einem der ONTAP Cluster konfiguriert haben. Sie sollten die Wartungskonsole verwenden, um die Position zu definieren.

- Sie müssen über die Stammbenutzeranmeldeinformationen für den Linux-Host verfügen, auf dem Active IQ 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 Active IQ Unified Manager-Host angehängt haben, und Sie müssen den Mount-Pfad verwenden.

Schritte

1. Verwenden Sie Secure Shell, um eine Verbindung mit der IP-Adresse oder dem FQDN des Active IQ Unified Manager-Systems herzustellen.
2. Melden Sie sich beim System mit dem Wartungs-Benutzer (umadmin) und dem Passwort an.
3. Geben Sie den Befehl `in 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 ein, die NFS konfiguriert werden soll.
7. Überprüfen Sie die Informationen, die Sie angeben müssen, und geben Sie dann die Nummer für **Backup Configuration Details** ein.
8. Um das Volume zum Schreiben des Snapshot zu identifizieren, geben Sie die IP-Adresse der Cluster Management Schnittstelle, den Namen der Storage VM, den Namen des Volumes, LUN-Namen, den Benutzernamen und das Passwort des Storage-Systems sowie 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 Active IQ Unified Manager Datenbank
 - Löscht die Dateien aus Active IQ Unified Manager und erstellt ein Symlink zum neuen Datenbankverzeichnis
 - Startet alle Dienste neu
10. Beenden Sie die Wartungskonsole und starten Sie die Schnittstelle Active IQ Unified Manager, um einen Zeitplan für die Snapshot Kopie zu erstellen, falls Sie dies noch nicht getan haben.

Backup wird unter Windows konfiguriert

Active IQ Unified Manager unterstützt Backup und Restore mithilfe von NetApp Snapshots auf dem Windows Betriebssystem mithilfe von LUN über das iSCSI-Protokoll.

Snapshot-basiertes Backup kann erstellt werden, während alle Unified Manager Services ausgeführt werden. Im Rahmen des Snapshots wird ein konsistenter Zustand der Datenbank erfasst, während das Backup eine globale Lesesperre auf die gesamte Datenbank setzt, die einen gleichzeitigen Schreibvorgang verhindert. Um Ihr Unified Manager System unter Windows durchzuführen und Backups und Restores mithilfe von NetApp Snapshots durchzuführen, sollten Sie zuerst Unified Manager Backup auf Snapshot basierend auf der Wartungskonsole konfigurieren.

Bevor Sie Unified Manager zum Erstellen von Snapshot Kopien konfigurieren, sollten Sie die folgenden Konfigurationsaufgaben ausführen.

- Konfigurieren Sie den ONTAP Cluster
- Konfigurieren Sie den Windows-Hostcomputer

Konfigurieren des Backup-Standorts für Windows

Sie sollten das Volume zum Speichern von Snapshot Kopien konfigurieren, nachdem Sie Unified Manager auf Windows gesichert haben.

Was Sie brauchen

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 Überwachung erfolgt durch Unified Manager
- Storage-VM-Anforderungen:
 - iSCSI-Konnektivität auf ONTAP-Cluster
 - Das iSCSI-Protokoll muss für den konfigurierten Computer aktiviert sein
 - Sie sollten ein dediziertes Volume und eine LUN für die Backup-Konfiguration verwenden. Das ausgewählte Volume sollte nur eine LUN und nichts anderes enthalten.
 - Die LUN-Größe sollte mindestens die doppelte Datenmenge sein, die voraussichtlich in den 9.9 Active IQ Unified Manager verarbeitet werden soll.

Dadurch wird auch auf dem Volume die gleiche Größenanforderung festgelegt.

 - Stellen Sie sicher, dass alle Lese-/Schreibzugriff ausgewählt ist
 - Stellen Sie sicher, dass Superuser Access in der Exportrichtlinie auf „any“ eingestellt ist
- Volume- und LUN-Anforderungen:
 - Das Volume sollte mindestens die doppelte Größe im Unified Manager MySQL-Datenverzeichnis haben.
 - Der Sicherheitsstil muss auf Windows 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.

ONTAP-Cluster wird konfiguriert

Sie müssen einige Konfigurationsschritte auf ONTAP Clustern durchführen, bevor Sie Active IQ Unified Manager mithilfe von Snapshot Kopien auf Windows Systemen sichern und wiederherstellen können.

Sie können das ONTAP Cluster entweder mit der Eingabeaufforderung oder der Benutzeroberfläche von System Manager konfigurieren. Die Konfiguration des ONTAP Clusters umfasst die Konfiguration von Daten-LIFs, die der Storage-VM als iSCSI LIFs zugewiesen werden können. Im nächsten Schritt werden Sie eine iSCSI-fähige Storage-VM mithilfe der Benutzeroberfläche von System Manager konfigurieren. Sie müssen eine statische Netzwerkroute für diese Storage-VM konfigurieren, um zu steuern, wie LIFs das Netzwerk für Outbound-Datenverkehr verwenden.



Sie sollten über ein dediziertes Volume und eine LUN für die Sicherungskonfiguration verfügen. Das ausgewählte Volume sollte nur eine LUN enthalten. Die LUN-Größe sollte mindestens die doppelte Datenmenge sein, die voraussichtlich von Active IQ Unified Manager verarbeitet werden soll.

Sie müssen folgende Konfiguration durchführen:

Schritte

1. Konfigurieren Sie eine iSCSI-fähige Storage-VM oder verwenden Sie eine vorhandene Storage-VM mit derselben Konfiguration.
2. Konfigurieren Sie eine Netzwerkroute für die konfigurierte Storage-VM.
3. Konfigurieren Sie ein Volume mit entsprechender Kapazität und eine einzelne LUN darin, damit das Volume nur für diese LUN reserviert ist.



In einem Szenario, in dem die LUN auf System Manager erstellt wird, kann das Aufheben der LUN die Initiatorgruppe löschen, und die Wiederherstellung kann fehlschlagen. Um dieses Szenario zu vermeiden, stellen Sie sicher, dass während des Erstellens einer LUN explizit erstellt und nicht gelöscht wird, wenn die LUN nicht zugeordnet wird.

4. Konfigurieren Sie eine Initiatorgruppe in der Storage-VM.
5. Konfigurieren Sie einen Portsatz.
6. Integrieren der Initiatorgruppe in das Portset
7. Ordnen Sie die LUN der Initiatorgruppe zu.

Windows-Hostcomputer wird konfiguriert

Sie müssen Ihren Windows Host Machine konfigurieren, bevor Sie Active IQ Unified Manager mit NetApp Snapshot sichern und wiederherstellen können. Um den Microsoft iSCSI-Initiator auf einem Windows-Hostcomputer zu starten, geben Sie in der Suchleiste „iscsi“ ein und klicken Sie auf **iSCSI-Initiator**.

Was Sie brauchen

Sie sollten alle früheren Konfigurationen auf dem Host-Rechner bereinigen.

Wenn Sie versuchen, den iSCSI-Initiator bei einer Neuinstallation von Windows zu starten, werden Sie zur Bestätigung aufgefordert. Anschließend wird das Dialogfeld iSCSI-Eigenschaften angezeigt. Wenn es sich um eine vorhandene Windows-Installation handelt, wird das Dialogfeld iSCSI-Eigenschaften mit einem Ziel angezeigt, das entweder inaktiv ist oder versucht, eine Verbindung herzustellen. Sie müssen also sicherstellen, dass alle vorherigen Konfigurationen auf dem Windows-Host entfernt werden.

Schritte

1. Entfernen Sie alle früheren Konfigurationen auf dem Host-Rechner.
2. Entdecken Sie das Zielportal.
3. Stellen Sie eine Verbindung zum Zielportal her.
4. Multipath wird mit dem Zielportal verbunden.
5. Ermitteln Sie die beiden LIFs.
6. Ermitteln Sie die LUN, die auf dem Windows-Rechner als Gerät konfiguriert ist.
7. Konfigurieren Sie die erkannte LUN als neues Volume-Laufwerk in Windows.

Festlegen des Zielorts für Snapshot Kopien unter Windows

Sie sollten den Zielspeicherort für Active IQ Unified Manager Snapshot Kopien auf einem Volume konfigurieren, das Sie bereits in einem der ONTAP Cluster konfiguriert haben. Sie sollten die Wartungskonsole verwenden, um die Position zu definieren.

- Sie müssen über die Administratorberechtigung für Windows Host verfügen, auf dem Active IQ 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 Volumes, den LUN-Namen und den Benutzernamen und das Kennwort des Speichersystems verfügen.
- Sie müssen das Volume als Netzwerklaufwerk auf den Active IQ Unified Manager-Host gemountet haben, und Sie müssen das Mount-Laufwerk haben.

Schritte

1. Stellen Sie mithilfe von Power Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domännennamen des Active IQ 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 ein, die iSCSI konfiguriert werden soll.
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, den LUN-Namen, den Benutzernamen und das Kennwort des Storage-Systems und das Mount-Laufwerk ein.
9. Überprüfen Sie diese Informationen, und geben Sie ein `y`.

Das System führt die folgenden Aufgaben aus:

- Storage VM ist validiert
 - Volume wird validiert
 - Mount-Laufwerk und Status werden validiert
 - Die LUN ist vorhanden und ihr Status ist
 - Netzwerklaufwerk vorhanden
 - Die Existenz des empfohlenen Speicherplatzes (mehr als doppelt so viele mysql-Datenverzeichnisses) auf gemounttem Volume wird validiert
 - LUN-Pfad, der der dedizierten LUN in dem Volume entspricht
 - der initiatorgruppenname
 - GUID des Volumes, auf dem das Netzwerklaufwerk angehängt ist
 - ISCSI Initiator zur Kommunikation mit ONTAP
10. Beenden Sie die Wartungskonsole und starten Sie die Schnittstelle Active IQ Unified Manager, um einen Zeitplan für Snapshot Kopien zu erstellen.

Konfigurieren eines Backups mit Snapshot-Kopie von der Wartungskonsole

Um Active IQ Unified Manager-Backup mit Snapshot-Kopie zu erstellen, sollten Sie ein paar Konfigurationsschritte von der Wartungskonsole aus durchführen.

Was Sie brauchen

Sie sollten für Ihr System die folgenden Informationen haben:

- Cluster-IP-Adresse
- Name der Storage-VM
- Volume-Name
- Der LUN-Name
- Mount-Pfad
- Zugangsdaten für das Storage-System

Schritte

1. Zugriff auf die Wartungskonsole von Unified Manager.
2. Geben Sie 4 ein, um **Wiederherstellung der Sicherung** auszuwählen.
3. Geben Sie 2 ein, um **Backup und Restore mit NetApp Snapshot** auszuwählen.



Wenn Sie die Backup-Konfiguration ändern möchten, geben Sie 3 ein, um **NetApp Snapshot Backup Konfiguration aktualisieren** auszuwählen. Sie können nur das Passwort aktualisieren.

4. Geben Sie im Menü 1 ein, um **NetApp Snapshot Backup konfigurieren** auszuwählen.
5. Geben Sie 1 ein, um die erforderlichen Informationen einzugeben.
6. Geben Sie den Benutzernamen und das Passwort für die Wartungskonsole ein, und bestätigen Sie, dass die LUN auf dem Host installiert ist.

Anschließend wird überprüft, ob das Datenverzeichnis, der LUN-Pfad, die Storage-VM, die Volumes, die Speicherplatzverfügbarkeit, und so weiter von Ihnen bereitgestellt sind richtig. Die Vorgänge, die im Hintergrund ausgeführt werden, sind:

- Dienste werden angehalten
- Datenbankverzeichnis wird in gemounteten Speicher verschoben
- Das Datenbankverzeichnis wird gelöscht und Symlinks werden erstellt
- Dienste werden neu gestartet Nachdem die Konfiguration in der Active IQ Unified Manager-Schnittstelle abgeschlossen ist, wird der Backup-Typ in NetApp-Snapshot geändert und wird in der Benutzeroberfläche als Datenbank-Backup (Snapshot-basiert) wiedergegeben.

Vor Beginn eines Backup-Vorgangs müssen Sie prüfen, ob eine Änderung der Snapshot-Konfiguration vorhanden ist, da dieser dazu führen kann, dass der Snapshot ungültig wird. Angenommen, Sie haben Backup in G-Laufwerk konfiguriert und der Snapshot erstellt. Sie haben später das Backup auf das E-Laufwerk konfiguriert und die Daten werden gemäß der neuen Konfiguration auf dem Laufwerk E gespeichert. Wenn Sie versuchen, Snapshot, der während des Laufwerk G erstellt wurde, wiederherzustellen, schlägt es mit dem Fehler fehl, dass G-Laufwerk nicht vorhanden ist.

Definieren eines Backup-Zeitplans für Linux und Windows

Sie können den Zeitplan, auf dem Unified Manager Snapshot Kopien unter Verwendung der Benutzeroberfläche von Unified Manager erstellt werden, konfigurieren.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen die Einstellungen für das Erstellen von Snapshot Kopien von der Wartungskonsole konfiguriert haben, um das Ziel zu bestimmen, an dem die Snapshots erstellt werden.

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



Das Backup, das während der ersten 15 Tage einer neuen Cluster-Ergänzung erstellt wurde, ist möglicherweise nicht genau genug, um die historischen Performance-Daten zu erhalten.

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 Software ONTAP auf dem Cluster bestimmt. 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**.

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

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 Snapshots mit ONTAP System Manager oder der ONTAP CLI löschen, sodass immer Platz für neue Snapshot Kopien ist.

Auf der Seite „Alarmkonfiguration“ konfigurieren Sie Warnmeldungen.

Wiederherstellung von Unified Manager mithilfe von Snapshot Kopien

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 Snapshot-Datenbank von Unified Manager mithilfe der Wartungskonsole auf einem lokalen oder Remote-Betriebssystem wiederherstellen.

Was Sie brauchen

- Sie müssen über die Stammbenutzeranmeldeinformationen für den Linux-Host und die Administratorrechte für Windows-Hostcomputer 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.

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

Schritte

1. Stellen Sie eine Verbindung mit der IP-Adresse oder dem vollqualifizierten Domännennamen des Unified Manager Systems her.
 - Linux: Sichere Shell
 - Windows: Power Shell
2. Melden Sie sich mit den Anmeldedaten des Root-Benutzers beim System an.
3. Geben Sie den Befehl ein `maintenance_console` Und drücken Sie die Eingabetaste.
4. Geben Sie in der Wartungskonsole **Hauptmenü 4** für die Option **Sicherungswiederherstellung** ein.
5. Geben Sie 2 ein, um **Backup und Restore mit NetApp Snapshot** auszuwählen.

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 1 ein, um **NetApp Snapshot Backup konfigurieren** auszuwählen und die Einstellungen für Snapshot Kopien so zu konfigurieren, wie sie sich auf dem Originalsystem befinden.

6. Geben Sie 3 ein, um **Restore mit NetApp Snapshot** auszuwählen.
7. Wählen Sie die Snapshot Kopie aus, aus der Sie Unified Manager wiederherstellen möchten. Drücken Sie **Enter**.
8. Melden Sie sich nach Abschluss des Wiederherstellungsprozesses in der Benutzeroberfläche von Unified Manager an.

Wenn der 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.

Ändern des Backup-Typs

Wenn Sie den Backup-Typ für Ihr Active IQ Unified Manager System ändern möchten, können Sie die Wartungskonsolen-Optionen verwenden. Die **Unconfigure NetApp Snapshot Backup** Option ermöglicht es Ihnen, auf das MySQL basierte Backup zurückzufallen.

Was Sie brauchen

Sie müssen über eine Benutzer-ID und ein Passwort verfügen, um sich bei der Wartungskonsole des Unified Manager-Servers anzumelden.

Schritte

1. Öffnen Sie die Wartungskonsole.
2. Wählen Sie 4 aus dem **Hauptmenü** für die Sicherung und Wiederherstellung.
3. Wählen Sie im Menü * Sicherung und Wiederherstellung * 2.
4. Wählen Sie 4 für * NetApp Snapshot Backup aufheben*.

Die ausgeführten Aktionen werden angezeigt, d. h., die Dienste anzuhalten, das Symlink zu unterbrechen, die Daten von Speicher in Verzeichnis zu verschieben und dann die Dienste erneut zu starten.

Nach der Änderung der Backup-Methode wird der Backup-Mechanismus von der Snapshot Kopie in das standardmäßige MySQL Backup geändert. Diese Änderung wird im Abschnitt Datenbank-Backup der allgemeinen Einstellungen angezeigt.

On-Demand Backup für Unified Manager

Über die Benutzeroberfläche von Active IQ Unified Manager können bei Bedarf Backups erstellt werden. Mit dem On-Demand Backup können Sie mit der bestehenden Backup-Methode umgehend ein Backup erstellen. Das On-Demand Backup unterscheidet nicht zwischen MySQL oder NetApp Snapshot basierten Backups.

Sie können On-Demand-Backups mithilfe der Schaltfläche **Jetzt sichern** auf der Seite Datenbank-Backup durchführen. Das On-Demand-Backup hängt nicht von den für Active IQ Unified Manager konfigurierten Zeitplänen ab.

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.

Was Sie brauchen

- Auf der virtuellen Appliance:
 - Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
 - Sie müssen den Namen des Unified Manager-Wartungsbenedutzers für den Wiederherstellungsvorgang kennen.

- Auf dem Linux-System:
 - Sie müssen Unified Manager auf einem Linux-Server gemäß den Anweisungen in installiert haben "[Installation von Unified Manager auf Linux Systemen](#)".
 - 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.

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 Backupdateien 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 die Sicherungsdatei .7z und alle Dateien des .7z-Repository im Unterverzeichnis /Database-Dumps-repo kopiert haben.

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.

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 auf einen neuen Pfad Ihrer Wahl, da auf dem Linux-System kein /jail/Support-Pfad vorhanden ist.
- 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.



Wenn Sie ein benutzerdefiniertes Skript erstellt und mit einer Warnung für einen bestimmten Ereignistyp verknüpft haben, werden Aktionen basierend auf Ihrem benutzerdefinierten Skript für diesen Ereignistyp ausgeführt, und die Aktionen **Fix it** sind auf der Seite „Management Actions“ oder im Unified Manager Dashboard standardmäßig nicht verfügbar.

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.

Was Sie brauchen

- 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, Python und `.bat` Dateien:

Plattform, auf der Unified Manager installiert ist	Unterstützte Sprachen
VMware	Perl- und Shell-Skripte
Linux	Perl-, Python- und Shell-Skripte
Windows	PowerShell, Perl, Python und <code>.bat</code> 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.

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.

Was Sie brauchen

- 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.

- 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	<ul style="list-style-type: none">• Objektname• Der Name des Clusters• Name der SVM• Anmerkungen
SVM	<ul style="list-style-type: none">• Objektname• Der Name des Clusters• Anmerkungen
Cluster	<ul style="list-style-type: none">• 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: „data_svm“ Bedingungsgruppe 1 wählt alle Volumes aus, die in ihren Namen „vol“ enthalten und auf SVMs mit dem Namen „data_svm“ gehostet werden.
- Bedingungsgruppe 2
 - Name enthält „vol“
 - Der Anmerkungswert der Datenpriorität ist „Critical“ Bedingungsgruppe 2 wählt alle Volumes aus, die „vol“ in ihren Namen enthalten und mit dem Anmerkungswert für die Datenpriorität als „critical“ versehen 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.

Was Sie brauchen

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

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.

Was Sie brauchen

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

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.

Was Sie brauchen

- 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.

Was Sie brauchen

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

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	<ol style="list-style-type: none">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	<ol style="list-style-type: none">a. Klicken Sie Auf Bedingungsgruppe Hinzufügenb. 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:

Schritte

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.

Was Sie brauchen

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.

Was Sie brauchen

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

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.

Was Sie brauchen

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.

Was Sie brauchen

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.

Was Sie brauchen

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

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.

Was Sie brauchen

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

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.

Was Sie brauchen

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

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 Anmerksungsregeln 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 Anmerksungsregeln 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 Anmerksungsregeln in Unified Manager

Eine Anmerksungsregel 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 Anmerksungsregel einer Anmerkung zuordnen.
- Sie müssen einen Objekttyp für eine Anmerksungsregel zuordnen. Für eine Anmerksungsregel kann nur ein Objekttyp zugeordnet werden.
- Unified Manager fügt nach jedem Überwachungszyklus oder bei dem Erstellen, Bearbeiten, Löschen oder Neuordnen einer Regel Anmerkungen zu Storage-Objekten hinzu oder entfernt diese.
- Eine Anmerksungsregel kann eine oder mehrere Bedingungsgruppen haben, und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben.
- Speicherobjekte können mehrere Anmerkungen enthalten. Eine Anmerksungsregel 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 Anmerksungsregel 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 Anmerksungsregel 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	<ul style="list-style-type: none"> • Objektname • Der Name des Clusters • Name der SVM • Anmerkungen

Storage-Objekttyp	Anwendbare Operanden
SVM	<ul style="list-style-type: none"> • Objektname • Der Name des Clusters • Anmerkungen
Cluster	<ul style="list-style-type: none"> • 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 Anmerksungsregel mit Bedingungen

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

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

Diese Anmerksungsregel bezeichnet alle Volumes, die „vol“ in ihren Namen enthalten und auf SVMs mit dem Namen „data_svm“ mit der ausgewählten Annotation und dem Anmerkungsstyp 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 Anmerksungsregel mit Bedingungsgruppen

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

- Bedingungsgruppe 1
 - Name enthält „vol“
 - SVM-Name: „data_svm“ Diese Bedingungsgruppe notiert alle Volumes, die in ihren Namen „vol“ enthalten und auf SVMs mit dem Namen „data_svm“ gehostet werden.
- Bedingungsgruppe 2
 - Name enthält „vol“

- Der Anmerkungswert der Datenpriorität ist „Critical“ Diese Bedingungsgruppe beschriftet alle Volumes, die „vol“ in ihren Namen enthalten und die mit dem Anmerkungswert für die Datenpriorität als „critical“ 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.

Was Sie brauchen

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.

Was Sie brauchen

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

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.

Was Sie brauchen

- 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.

Was Sie brauchen

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

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.

Anmerksungsregeln werden erstellt

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

Was Sie brauchen

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

Aktuell überwachte Storage-Objekte werden kommentiert, sobald die Anmerksungsregel 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 **Anmerksungsregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerksungsregel hinzufügen** einen Namen für die Anmerksungsregel 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 Anmerksungsregel

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

Schritte

1. Geben Sie einen Namen für die Anmerksungsregel 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.

Was Sie brauchen

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	<ol style="list-style-type: none"> a. Klicken Sie Auf Storage > Cluster. b. Wählen Sie ein oder mehrere Cluster aus.
Volumes	<ol style="list-style-type: none"> a. Klicken Sie Auf Storage > Volumes. b. Wählen Sie ein oder mehrere Volumes aus.
SVMs	<ol style="list-style-type: none"> 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**.

Anmerungsregeln werden bearbeitet

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

Was Sie brauchen

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management > Anmerkungen**.

2. Wählen Sie auf der Registerkarte **Anmerksungsregeln** die Anmerksungsregel aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Aktionen > Bearbeiten**.
3. Ändern Sie im Dialogfeld **Anmerksungsregel bearbeiten** den Regelnamen, den Anmerksungsnamen und den Wert, die Bedingungsgruppen und die Bedingungen nach Bedarf.

Sie können den Zielobjekttyp für eine Anmerksungsregel nicht ändern.

4. Klicken Sie Auf **Speichern**.

Konfigurieren von Bedingungen für Anmerksungsregeln

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

Was Sie brauchen

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 **Anmerksungsregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerksungsregel hinzufügen** einen Namen für die Regel ein.
4. Wählen Sie einen Objekttyp aus der Liste Zielobjekttyp aus, und wählen Sie dann einen Anmerksungsnamen 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 Anmerksungsregel

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

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

Schritte

1. Geben Sie einen Namen für die Anmerksungsregel 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.

Was Sie brauchen

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

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 angewendet. 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.

Was Sie brauchen

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

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.

Senden eines Support-Bundles über eine Web-UI und eine Wartungskonsole

Sie sollten ein Support-Bundle senden, wenn das Problem, das Sie haben, detailliertere Diagnose und Fehlerbehebung erfordert als eine AutoSupport-Meldung. Sie können ein

Support-Paket über die Unified Manager Web-UI und die Wartungskonsole an den technischen Support senden.

Unified Manager speichert maximal zwei komplette Support Bundles und drei schlanke Support-Bundles gleichzeitig.

Verwandte Informationen

["Unified Manager Benutzer-Rollen und -Funktionen"](#)

Senden von AutoSupport Meldungen und Support Bundles an den technischen Support

Auf der Seite AutoSupport können Sie vordefinierte und On-Demand AutoSupport Meldungen an Ihr technisches Support-Team senden, um einen ordnungsgemäßen Betrieb Ihrer Umgebung zu gewährleisten und die Integrität Ihrer Umgebung zu wahren. AutoSupport ist standardmäßig aktiviert und sollte nicht deaktiviert werden, damit Sie die Vorteile von NetAppActive IQ nutzen können.

Sie können Diagnosesystem-Informationen und detaillierte Daten zum Unified Manager Server in einer Meldung senden, die bei Bedarf gesendet werden soll, eine Meldung in regelmäßigen Abständen planen oder sogar Support-Bundles an das technische Support-Team generieren und versenden.



Ein Benutzer mit einer Storage-Administratorrolle kann AutoSupport Meldungen und Support Bundles nach Bedarf an den technischen Support generieren und senden. Jedoch kann nur ein Administrator oder ein Wartungsb Benutzer periodische AutoSupport aktivieren oder deaktivieren und die HTTP-Einstellungen wie im Abschnitt Einrichten des HTTP-Proxyservers beschrieben konfigurieren. In einer Umgebung, in der ein HTTP Proxy-Server verwendet werden muss, sollte die Konfiguration abgeschlossen sein, bevor ein Storage-Administrator AutoSupport Meldungen und Support Bundles nach Bedarf an den technischen Support senden kann.

Senden von On-Demand AutoSupport Nachrichten

Sie können eine On-Demand-Nachricht an den technischen Support, an einen bestimmten E-Mail-Empfänger oder an beide senden.

Schritte

1. Navigieren Sie zu **Allgemein > AutoSupport**, und führen Sie eine oder beide der folgenden Aktionen aus:
2. Wenn Sie die AutoSupport-Nachricht an den technischen Support senden möchten, aktivieren Sie das Kontrollkästchen **an den technischen Support senden**.
3. Wenn Sie die AutoSupport-Nachricht an einen bestimmten E-Mail-Empfänger senden möchten, aktivieren Sie das Kontrollkästchen **an E-Mail-Empfänger** und geben Sie die E-Mail-Adresse des Empfängers ein.
4. Klicken Sie Auf **Speichern**.
5. Klicken Sie auf **AutoSupport generieren und senden**.

Aktivieren von regelmäßigen AutoSupport

Sie können dem technischen Support spezifische, vordefinierte Meldungen zur Fehlerbehebung in regelmäßigen Abständen senden. Diese Funktion ist standardmäßig aktiviert. Wenn diese Option deaktiviert ist, kann ein Administrator oder Wartungsb Benutzer die Einstellungen aktivieren.

Schritte

1. Navigieren Sie zu **Allgemein > AutoSupport**.
2. Aktivieren Sie im Abschnitt Periodensystem AutoSupport das Kontrollkästchen **AutoSupport-Daten regelmäßig an Active IQ** senden aktivieren.
3. Legen Sie bei Bedarf den Namen, den Port und die Authentifizierungsinformationen für den HTTP-Proxy-Server fest, wie im Abschnitt Einrichten des HTTP-Proxyservers beschrieben.
4. Klicken Sie Auf **Speichern**.

Supportpaket nach Bedarf hochladen

Je nach Anforderung zur Fehlerbehebung können Sie ein Support Bundle an den technischen Support generieren und senden. Unified Manager speichert nur die zwei zuletzt erstellten Support Bundles. Ältere Supportpakete werden aus dem System gelöscht.

Da einige Arten von Support-Daten große Mengen von Cluster-Ressourcen nutzen oder sehr lange in Anspruch nehmen können, wenn Sie das vollständige Support Bundle auswählen, können Sie bestimmte Datentypen ein- oder ausschließen, um die Größe des Support-Paketes 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.

Schritte

1. Navigieren Sie zu **Allgemein > AutoSupport**.
2. Klicken Sie im Bereich „On-Demand Support Bundle“ auf **Support Bundle generieren und senden**.
3. Um ein leichtes Supportpaket an den technischen Support zu senden, aktivieren Sie im Pop-up-Pop-up-Paket Erzeugen und Senden das Kontrollkästchen **Lichtstützpaket erzeugen**.
4. Wenn Sie ein komplettes Supportpaket senden möchten, aktivieren Sie alternativ das Kontrollkästchen **komplettes Supportpaket erzeugen**. Wählen Sie die spezifischen Datentypen aus, die im Supportpaket enthalten oder ausgeschlossen werden sollen.



Auch wenn Sie keine Datentypen auswählen, wird das Support-Paket immer noch mit anderen Unified Manager-Daten generiert.

5. Aktivieren Sie das Kontrollkästchen **Paket an technischen Support senden**, um das Paket zu generieren und an den technischen Support zu senden. Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird das Bundle lokal auf dem Unified Manager-Server generiert und gespeichert. Das generierte Supportpaket steht zur späteren Verwendung im Verzeichnis /Support auf VMware Systemen in zur Verfügung /opt/netapp/data/support/ Auf Linux-Systemen und in ProgramData\NetApp\OnCommandAppData\ocum\support Auf Windows-Systemen.
6. Klicken Sie Auf **Senden**.

Einrichten des HTTP-Proxyservers

Sie können einen Proxy für den Internetzugriff festlegen, um AutoSupport-Inhalte zu unterstützen, falls Ihre Umgebung keinen direkten Zugriff vom Unified Manager-Server bietet. Dieser Abschnitt ist nur für Administrator- und Wartungsbenutzer verfügbar.

• HTTP Proxy verwenden

Aktivieren Sie dieses Kontrollkästchen, um den Server zu identifizieren, der als HTTP-Proxy verwendet

wird.

Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers und die Portnummer ein, die für die Verbindung mit dem Server verwendet wird.

• Authentifizierung verwenden

Aktivieren Sie dieses Kontrollkästchen, wenn Sie Authentifizierungsinformationen für den Zugriff auf den Server angeben müssen, der als HTTP-Proxy verwendet wird.

Geben Sie den Benutzernamen und das Kennwort ein, das für die Authentifizierung mit dem HTTP-Proxy erforderlich ist.



HTTP-Proxys, die nur grundlegende Authentifizierung bereitstellen, werden nicht unterstützt.

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.

Was Sie brauchen

Sie müssen Unified Manager installiert und konfiguriert haben.

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.

Schritt

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

Auf diesem Betriebssystem...	Führen Sie die folgenden Schritte aus...
VMware	<ol style="list-style-type: none">Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domännennamen der virtuellen Unified Manager-Appliance her.Melden Sie sich mit Ihrem Wartungs-Benutzernamen und -Passwort an der Wartungskonsole an.

Auf diesem Betriebssystem...	Führen Sie die folgenden Schritte aus...
Linux	<ul style="list-style-type: none"> a. Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domännennamen 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 <code>maintenance_console</code> Und drücken Sie die Eingabetaste.
Windows	<ul style="list-style-type: none"> 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 <code>maintenance_console</code> 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.

Was Sie brauchen

Sie müssen als Wartungbenutzer Zugriff auf die Wartungskonsole haben.

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.

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 Verzeichnis /Support auf VMware Systemen, in /opt/netapp/Data/Support/ auf Linux Systemen und in ProgramData\NetApp\OnCommandAppData\ocum\Unterstützung auf Windows Systemen.

Verwandte Informationen

["Unified Manager Benutzer-Rollen und -Funktionen"](#)

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.

Was Sie brauchen

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 Tool zeigt den Inhalt des /Support-Verzeichnisses an 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.

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.

Was Sie brauchen

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	<code>scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>
SFTP	<code>sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>

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.

Was Sie brauchen

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.

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 Clusters 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 Datenverarbeitungskomponente 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.

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. Weitere Informationen finden Sie unter "[Wiederherstellen von Daten mithilfe der Seite Volume / Health Details](#)".



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-Volumens 100 MB oder mehr ist, ist die Mindestplatzgarantie standardmäßig auf 100 MB gesetzt. Wenn die Größe des FlexCache-Volumens weniger als 100 MB ist, wird die Mindestplatzgarantie auf die Größe des FlexCache-Volumens gesetzt. Wenn die Größe des FlexCache-Volumens 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 Volumens 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 Volumens 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 der Sicherungsbeziehungen (SnapMirror, SnapVault oder Storage VM DR) 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 Volumens 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, bei der die Quelle ein Datensicherungs-Volume 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.

- Geschützt Durch

Zeigt den Schutztyp an, der für das ausgewählte Volume verwendet wird. Wenn ein Volume z. B. durch Konsistenzgruppe und SnapMirror Volume-Beziehungen geschützt ist, wird in diesem Feld sowohl SnapMirror als auch die Konsistenzgruppe angezeigt. Dieses Feld enthält auch einen Link, über den Sie zur Seite „Beziehungen“ weitergeleitet werden, um den Status einer einheitlichen Beziehung anzuzeigen. Der Link gilt nur für zusammengebende Beziehungen.

- Konsistenzgruppe

Für Volumes, die durch SnapMirror Business Continuity (SM-BC)-Beziehungen geschützt sind, wird in dieser Spalte die Konsistenzgruppe des Volumes angezeigt.

- **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.

Zweifelt 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 Sie über eine Cluster-übergreifende Beziehung verfügen und der Ziel-Cluster noch nicht erkannt wurde Wenn Sie auf ein anderes Volume in der Topologie klicken, werden Informationen für dieses 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 Volumens an. Wenn Sie den Cursor auf ein Volumen in der Topologie positionieren, werden im Dialogfeld Aktuelle Schwellenwerteinstellungen die aktuellen Warn- und kritischen Schwellenwerte 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 Volumens 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 Volumens 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 Volumens 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 Volumens 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** ausgeblendet 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 Beziehungsübertragung und die Größe der eingehenden Beziehungsübertragung. Die Verlaufsdaten werden nur angezeigt, wenn Sie ein Zielvolume auswählen. Wenn Sie ein primäres Volume auswählen, sind die Diagramme leer und die Meldung Keine Daten gefunden wird angezeigt. Wenn die Volumes durch eine Konsistenzgruppe und synchrone SnapMirror Beziehungen geschützt sind, werden die Informationen für die Dauer der Beziehungsübertragung und die Größe der Beziehungsübertragung nicht 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 Keine Daten gefunden, die angezeigt werden, wenn die Daten oder der Status des Volumes für einen bestimmten Zeitraum 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-Shares**

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 über die ausgewählte Storage-VM anzeigen, z. B. Systemzustand, Kapazität, Konfiguration, Datenrichtlinien, logische Schnittstellen (LIFs), LUNs, qtrees, Benutzer, User Group Quotas und Sicherungsdetails . Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für die Storage-VM anzeigen.



Sie können nur Storage VM überwachen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für die ausgewählte Storage-VM ausführen:

- **Wechseln Sie zur Leistungsansicht**

Ermöglicht Ihnen die Navigation zur Seite Storage VM / Performance Details.

- **Aktionen**

- Alarm Hinzufügen

Ermöglicht Ihnen das Hinzufügen einer Warnung zur ausgewählten Speicher-VM.

- Anmerkungen Hinzufügen

Ermöglicht Ihnen, die ausgewählte Storage-VM Anmerkungen zu machen.

- **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 Storage-VM 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 Informationen unten im Diagramm enthalten Details zu Kapazitätsproblemen, die sich auf die Kapazität von Daten in der Storage-VM auswirken oder bereits beeinträchtigen können. Beispielsweise werden Informationen zu Aggregaten angezeigt, die mit hoher Wahrscheinlichkeit die festgelegten Schwellenwerte überschreiten.

- **Schutzprobleme**

Bietet eine schnelle Übersicht über den Schutz von Storage-VMs, indem die Gesamtzahl der Beziehungen, einschließlich Beziehungen mit Schutzproblemen und Beziehungen, die keine Probleme mit der Sicherung haben, als Feld angezeigt wird. Sie können auch den Status der Storage-VM-DR-Beziehung für die ausgewählte Storage-VM anzeigen. Die Ereignisse für Storage-VM-DR-Beziehungen werden hier angezeigt und durch Klicken auf die Ereignisse gelangen Sie zur Seite mit den Ereignisdetails. 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 Storage-VM 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 Informationen unten im Diagramm enthalten Details zu Sicherungsproblemen, die sich auf den Schutz von Daten in der Storage-VM auswirken oder bereits davon betroffen sein 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.

Registerkarte „Kapazität“

Auf der Registerkarte Kapazität werden ausführliche Informationen zur Datenkapazität der ausgewählten SVM angezeigt.

Die folgenden Informationen werden für eine Storage-VM 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 Storage-VM an.

- Verwendet

Zeigt den Speicherplatz an, der von Daten in den Volumes verwendet wird, die zur Storage-VM gehören.

- Garantiert Verfügbar

Zeigt den garantierten verfügbaren Speicherplatz für Daten an, die für Volumes in der Storage-VM verfügbar sind.

- Nicht Garantiert

Zeigt den verfügbaren Speicherplatz für Daten an, die in der Storage-VM 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 Konfiguration werden Konfigurationsdetails zur ausgewählten Storage-VM angezeigt, z. B. Cluster, Root-Volume, der zugehörige Volume-Typ (FlexVol-Volumes), Richtlinien und Sicherung, die auf der Storage-VM erstellt wurden:

• Übersicht

- Cluster

Zeigt den Namen des Clusters an, zu dem die Storage-VM gehört.

- Zulässiger Volume-Typ

Zeigt den Typ der Volumes an, die in der Storage-VM erstellt werden können. Der Typ kann FlexVol oder FlexVol/FlexGroup sein.

- Root-Volume

Zeigt den Namen des Root-Volumes der Speicher-VM an.

- Zulässige Protokolle

Zeigt den Typ der Protokolle an, die auf der Storage-VM 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 Storage-VM zugeordnet sind. Außerdem gibt an, ob die Schnittstellen aktiv sind (●) Oder runter (●).

- San

Zeigt die Anzahl der SAN-Schnittstellen an, die der Speicher-VM zugeordnet sind. Außerdem gibt an, ob die Schnittstellen aktiv sind (●) Oder runter (●).

- FC-NVMe

Zeigt die Anzahl der FC-NVMe-Schnittstellen an, die der Storage-VM zugeordnet sind. Außerdem gibt an, ob die Schnittstellen aktiv sind (●) Oder runter (●).

• Management-Netzwerk-Schnittstellen

- Gesteigerte

Zeigt die Anzahl der Managementschnittstellen an, die der Storage-VM 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 Storage-VM erstellt wird.

- 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.

• Schutz

- DR von Storage-VMs

Zeigt an, ob die ausgewählte Storage-VM geschützt, Ziel oder ungeschützt ist, und den Namen des Ziels, auf dem die Storage-VM geschützt ist. Wenn die ausgewählte Speicher-VM Ziel ist, werden die Details der Quell-Speicher-VM angezeigt. Im Falle eines Fan-out zeigt dieses Feld die Anzahl der gesamten Ziel-Storage-VMs an, auf denen die Speicher-VM geschützt ist. Der Link „count“ führt Sie zum Storage-VM-Beziehungsraster, das auf der Quell-Storage-VM gefiltert ist.

- Geschützte Volumes

Zeigt die Anzahl der geschützten Volumes auf der ausgewählten Speicher-VM aus den gesamten Volumes an. Wenn Sie eine Ziel-Storage-VM anzeigen, ist der Zahlenlink für die Ziel-Volumes der ausgewählten Speicher-VM.

- Ungesicherte Volumes

Zeigt die Anzahl der ungeschützten Volumes in der ausgewählten Storage-VM an.

• Services

- Typ

Zeigt den Servicetyp an, der auf der Storage-VM konfiguriert ist. Der Typ kann Domain Name System (DNS) oder Network Information Service (NIS) sein.

- Status

Zeigt den Status des Dienstes an, der aktiv sein kann (●), Down (●), oder nicht konfiguriert (●).

- Domain-Name

Zeigt die vollständig qualifizierten Domännennamen (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 Storage-VM erstellt wurden:

- **Netzwerkschnittstelle**

Zeigt den Namen der Schnittstelle an, die auf der ausgewählten Speicher-VM erstellt wird.

- **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 **Export**, um eine kommagetrennte Datei (.csv) zu erstellen, die die Details aller überwachten qtrees enthält. Beim Export in eine CSV-Datei können Sie wahlweise einen qtrees-Bericht für die aktuelle Storage VM, alle Storage VMs im aktuellen Cluster oder alle Storage VMs für alle Cluster im 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-Exportdaten 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-Exportdaten 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 Storage-VM 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 diesem Service können Sie Regeln erstellen oder ändern, um eine E-Mail-Adresse für die Kontingente von Benutzern oder Benutzergruppen zu erstellen, die für die Storage-VM konfiguriert sind. 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 Storage-VM an. Sie können Informationen anzeigen, wie z. B. den Status der SMB-Freigabe, den Freigabennamen, den mit der Storage-VM verknüpften Pfad, den Status des Verbindungspfads der Freigabe, das Objekt, 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 die Details der Benutzerzuordnung für die Storage-VM anzeigen.

- **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 Storage-VM 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. Der Link ist deaktiviert, wenn die Exportrichtlinie für die ausgewählte Speicher-VM 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 Storage-VM 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 Speicher-VM 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 Storage-VM zugeordnet sind.

```
initiator groups that are mapped to the selected initiator group.
```

Bereich „Verwandte Anmerkungen“

Im Fensterbereich Verwandte Anmerkungen können Sie die mit der ausgewählten Speicher-VM verknüpften Anmerkungsdetails anzeigen. Details umfassen den Anmerkungsnamen und die Anmerkungswerte, die auf die Storage-VM angewendet werden. 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 Storage-VM in Verbindung stehen:

- * Cluster*

Zeigt den Integritätsstatus des Clusters an, zu dem die Storage-VM gehört.

- **Aggregate**

Zeigt die Anzahl der Aggregate an, die zur ausgewählten Storage-VM gehören. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt. Wenn z. B. eine Speicher-VM zehn Aggregate enthält, von denen fünf den Warnstatus und die übrigen fünf den kritischen Status anzeigen, ist der angezeigte Status kritisch.

- * Zugewiesene Aggregate*

Zeigt die Anzahl der Aggregate an, die einer Storage-VM zugewiesen sind. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt.

- **Bänder**

Zeigt die Anzahl und Kapazität der Volumes an, die zur ausgewählten Speicher-VM gehören. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt. In der Storage-VM sind FlexGroup Volumes enthalten, die Anzahl auch FlexGroups. FlexGroup Komponenten sind darin nicht enthalten.

Bereich „Verwandte Gruppen“

Im Fensterbereich Verwandte Gruppen können Sie die Liste der Gruppen anzeigen, die der ausgewählten Speicher-VM zugeordnet sind.

Bereich „Verwandte Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnmeldungen anzeigen, die für die ausgewählte Storage-VM 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 Wiederauffindungsvorgang 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-Shelves 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. Dies umfasst keine Snapshot-Kopien.

- Datenreduzierung

Zeigt das Verhältnis ohne Snapshot-Kopien und mit zwei signifikanten Ziffern, z. B. 1.8 zu 1, an. Dieses Verhältnis basiert auf den konfigurierten ONTAP Storage-Effizienzeinstellungen.

- 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. Die Berechnung schließt die Daten des Root-Aggregats aus.

- 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 Festplattentyp

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 Kapazitätsproblemen

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, Kontakt und Standort:

Cluster – Überblick

- 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 Domännennamen (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.

- 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.

Überblick Über Das Remote-Cluster

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.

- Standort

Zeigt den Speicherort des Remote-Clusters an.

Übersicht über MetroCluster

Details zum lokalen Cluster in MetroCluster over FC oder MetroCluster over IP Konfigurationen Diese Informationen werden nur für MetroCluster über FC- oder IP-Konfigurationen angezeigt.

- Typ

Zeigt an, ob es sich bei dem MetroCluster-Typ um zwei oder vier Nodes handelt. Bei MetroCluster over IP werden nur vier Nodes unterstützt.

- Konfiguration

Zeigt die MetroCluster-Konfiguration über FC und IP an, die folgende Werte aufweisen kann:

- Für FC*
- 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.

Für IP

- IP-Konfiguration mit Ethernet-Switches (L2 oder L3, je nach Konfiguration des Clusters)
 - 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. Dies wird nur für MetroCluster über FC unterstützt.

- Umschaltmodus

Zeigt den Umschaltmodus für die MetroCluster-over-IP-Konfiguration an. Die verfügbaren Werte sind: `Active`, `Negotiated Switchover`, und `Automatic Unplanned Switchover`.

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.

Darstellt

- Mediatoren

Zeigt an, ob das Cluster Mediatoren unterstützt und der Verbindungsstatus des Mediators. Er gibt an, ob der Mediator konfiguriert ist, und wenn er konfiguriert ist, zeigt er den Status der Mediatoren an.

- Keine Angabe

Wird angezeigt, wenn das Cluster keine Mediatoren unterstützt.

- Nicht Konfiguriert

Zeigt an, wenn das Cluster Mediatoren unterstützt, aber der Mediator nicht konfiguriert ist.

- IP-Adresse

Zeigt an, wenn das Cluster Mediatoren unterstützt und der Mediator konfiguriert ist. Der Mediatorstatus wird durch Farbe angezeigt. Die Farbe grün zeigt an, dass der Mediatorstatus erreichbar ist. Die Farbe Rot zeigt an, dass der Mediator-Status nicht erreichbar ist.

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 Cluster-Komponenten in der MetroCluster over FC-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 über die FC-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 in einer MetroCluster over FC-Konfiguration 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 über die FC-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.

Administrationsstatus

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.

Routinggruppen

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-Shelves 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 Übernahmenvorgangs wird beispielsweise die folgende Meldung angezeigt: Storage Failover möglich.

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 Node-bezogene Informationen anzeigen, z. B. die Modellnummer.

Bei Single-Node-Clustern können Sie auch Details zu den Nodes anzeigen.

Platten-Shelfs

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.

Festplatte

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.

Status

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.

Lokale Festplatte

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

Storage-Pool

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.

Bruttokapazität

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-Blöcke Verbrauchen %

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.

Shelf-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.

Verwandte Informationen

["Volume-Seite" "Anzeigen der Cluster-Liste und der Details"](#)

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 anzuzeigende 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. Verlaufsdigramme können Ihnen bei der Identifizierung von Trends helfen: Wenn beispielsweise die Aggregatnutzung konsistent den Schwellenwert „nahezu voll“ überschreitet, können Sie die entsprechenden Maßnahmen ergreifen.

Verlaufsdigramme 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“.

- **Bänder**

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.

Verwandte Informationen

["Anzeigen von Details zum Speicherpool"](#)

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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