Allgemeine Unified Manager-Integritätsworkflows und -Aufgaben

Active IQ Unified Manager

NetApp
October 15, 2025

Inhalt

Allgemeine Unified Manager-Integritätsworkflows und -Aufgaben

Zu den allgemeinen administrativen Arbeitsabläufen und Aufgaben im Zusammenhang mit Unified Manager gehören die Auswahl der zu überwachenden Speichercluster, die Diagnose von Bedingungen, die sich negativ auf die Datenverfügbarkeit, -kapazität und -sicherheit auswirken, die Wiederherstellung verlorener Daten, die Konfiguration und Verwaltung von Volumes sowie das Bündeln und Senden von Diagnosedaten an den technischen Support (falls erforderlich).

Mit Unified Manager können Speicheradministratoren ein Dashboard anzeigen, die Gesamtkapazität, Verfügbarkeit und den Schutzzustand der verwalteten Speichercluster beurteilen und dann eventuell auftretende spezifische Probleme schnell identifizieren, lokalisieren, diagnostizieren und zur Lösung zuweisen.

Die wichtigsten Probleme im Zusammenhang mit einem Cluster, einer Storage Virtual Machine (SVM), einem Volume oder einem FlexGroup Volume, die sich auf die Speicherkapazität oder Datenverfügbarkeit Ihrer verwalteten Speicherobjekte auswirken, werden in den Systemzustandsdiagrammen und Ereignissen auf der Dashboard-Seite angezeigt. Wenn kritische Probleme erkannt werden, bietet diese Seite Links zur Unterstützung entsprechender Workflows zur Fehlerbehebung.

Unified Manager kann auch in Workflows integriert werden, die zugehörige Verwaltungstools enthalten – wie etwa OnCommand Workflow Automation (WFA) –, um die direkte Konfiguration von Speicherressourcen zu unterstützen.

In diesem Dokument werden allgemeine Arbeitsabläufe im Zusammenhang mit den folgenden Verwaltungsaufgaben beschrieben:

- Diagnose und Verwaltung von Verfügbarkeitsproblemen

  Wenn Hardwarefehler oder Konfigurationsprobleme bei Speicherressourcen dazu führen, dass Datenverfügbarkeitsereignisse auf der Dashboard-Seite angezeigt werden, können Speicheradministratoren den eingebetteten Links folgen, um Konnektivitätsinformationen zur betroffenen Speicherressource anzuzeigen, Hinweise zur Fehlerbehebung zu erhalten und die Problemlösung anderen Administratoren zuzuweisen.

- Konfigurieren und Überwachen von Leistungsvorfällen

  Der Administrator kann die Leistung der überwachten Speichersystemressourcen überwachen und verwalten. Siehe die"Einführung in die Leistungsüberwachung von Active IQ Unified Manager" für weitere Informationen.

- Diagnostizieren und Verwalten von Volume-Kapazitätsproblemen

  Wenn auf der Dashboard-Seite Probleme mit der Speicherkapazität des Volumes angezeigt werden, können Speicheradministratoren den eingebetteten Links folgen, um die aktuellen und historischen Trends in Bezug auf die Speicherkapazität des betroffenen Volumes anzuzeigen, Hinweise zur Fehlerbehebung zu erhalten und die Problemlösung anderen Administratoren zuzuweisen.

- Konfigurieren, Überwachen und Diagnostizieren von Problemen mit Schutzbeziehungen

  Nach dem Erstellen und Konfigurieren von Schutzbeziehungen können Speicheradministratoren die potenziellen Probleme im Zusammenhang mit Schutzbeziehungen, den aktuellen Status der

Schutzbeziehungen, die aktuellen und historischen Informationen zum Erfolg von Schutzaufträgen zu den betroffenen Beziehungen sowie Hinweise zur Fehlerbehebung anzeigen. Siehe die"Erstellen, Überwachen und Beheben von Problemen mit Schutzbeziehungen" für weitere Informationen.

- Erstellen von Sicherungsdateien und Wiederherstellen von Daten aus Sicherungsdateien.
- Zuordnen von Speicherobjekten zu Anmerkungen

  Durch die Verknüpfung von Speicherobjekten mit Anmerkungen können Speicheradministratoren die mit den Speicherobjekten verbundenen Ereignisse filtern und anzeigen. Dadurch können sie die mit den Ereignissen verbundenen Probleme priorisieren und lösen.

- Verwenden Sie REST-APIs, um Ihre Cluster zu verwalten, indem Sie die von Unified Manager erfassten Informationen zu Integrität, Kapazität und Leistung anzeigen. Sehen"Erste Schritte mit Active IQ Unified Manager REST-APIs" für weitere Informationen.
- Senden eines Support-Pakets an den technischen Support

  Speicheradministratoren können über die Wartungskonsole ein Supportpaket abrufen und an den technischen Support senden. Supportpakete müssen an den technischen Support gesendet werden, wenn das Problem eine detailliertere Diagnose und Fehlerbehebung erfordert, als eine AutoSupport -Nachricht bietet.

Überwachen und Beheben von Problemen mit der Datenverfügbarkeit

Unified Manager überwacht die Zuverlässigkeit, mit der autorisierte Benutzer auf Ihre gespeicherten Daten zugreifen können, weist Sie auf Bedingungen hin, die diesen Zugriff blockieren oder behindern, und ermöglicht Ihnen, diese Bedingungen zu diagnostizieren und ihre Lösung zuzuweisen und zu verfolgen.

Die Themen zum Verfügbarkeits-Workflow in diesem Abschnitt beschreiben Beispiele dafür, wie ein Speicheradministrator die Unified Manager-Web-Benutzeroberfläche verwenden kann, um Hardware- und Softwarezustände zu erkennen, zu diagnostizieren und zur Behebung zuzuweisen, die sich negativ auf die Datenverfügbarkeit auswirken.

Suchen und beheben Sie Verbindungsausfälle bei Speicher-Failovern

Dieser Workflow bietet ein Beispiel dafür, wie Sie nach ausgefallenen Speicher-Failover-Verbindungsverbindungen suchen, diese auswerten und beheben können. In diesem Szenario sind Sie ein Administrator, der Unified Manager verwendet, um nach Speicher-Failover-Risiken zu suchen, bevor Sie ein ONTAP -Versionsupgrade auf Ihren Knoten starten.

Bevor Sie beginnen

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

Wenn die Speicher-Failover-Verbindungen zwischen HA-Paarknoten während eines unterbrechungsfreien Upgradeversuchs fehlschlagen, schlägt das Upgrade fehl. Daher ist es üblich, dass der Administrator vor Beginn eines Upgrades die Zuverlässigkeit des Speicher-Failovers auf den für das Upgrade vorgesehenen Clusterknoten überwacht und bestätigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.
2. Wählen Sie auf der Inventarseite **Event Management** die Option **Active Availability-Ereignisse** aus.
3. Klicken Sie oben in der Spalte **Name** der Inventarseite **Event Management** auf und geben Sie ein `*failover` in das Textfeld, um die Anzeige des Ereignisses auf Speicherfailover-bezogene Ereignisse zu beschränken.

   Alle vergangenen Ereignisse im Zusammenhang mit Speicher-Failover-Bedingungen werden angezeigt.

   In diesem Szenario zeigt der Unified Manager im Abschnitt „Verfügbarkeitsvorfälle“ das Ereignis „Storage Failover Interconnect One or More Links Down“ an.

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

   a. Klicken Sie auf den Link zum Ereignistitel, 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 mit den 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 Veranstaltungsdetails"

"Unified Manager-Benutzerrollen und -Funktionen"

Führen Sie Korrekturmaßnahmen für ausgefallene Speicher-Failover-Verbindungsverbindungen durch

Wenn Sie die Seite mit den Ereignisdetails eines Speicherfailover-bezogenen Ereignisses anzeigen, können Sie die zusammenfassenden Informationen der Seite überprüfen, um die Dringlichkeit des Ereignisses, die mögliche Ursache des Problems und eine mögliche Lösung des Problems zu ermitteln.

Bevor Sie beginnen

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

In diesem Beispielszenario enthält die Ereigniszusammenfassung auf der Seite „Ereignisdetails“ die folgenden Informationen zum Zustand der unterbrochenen Speicher-Failover-Verbindung:

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

Summary

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

Die Beispielereignisinformationen zeigen, dass eine Speicher-Failover-Verbindung (Link1) zwischen den HA-Paarknoten „Aardvark“ und „Bonobo“ ausgefallen ist, Link0 zwischen „Apple“ und „Boy“ jedoch aktiv ist. Da eine Verbindung aktiv ist, funktioniert der Remote Dynamic Memory Access (RDMA) weiterhin und ein Speicherfailover-Job kann weiterhin erfolgreich sein.

Um jedoch sicherzustellen, dass weder beide Links ausfallen noch der Speicher-Failover-Schutz vollständig deaktiviert wird, beschließen Sie, den Grund für den Ausfall von Link1 genauer zu untersuchen.

Schritte

1. Auf der Detailseite **Ereignis** können Sie auf den Link zum im Feld „Quelle“ angegebenen Ereignis klicken, um weitere Details zu anderen Ereignissen zu erhalten, die möglicherweise mit dem Zustand „Verbindungsunterbrechung der Speicher-Failover-Verbindung“ in Zusammenhang stehen.

   In diesem Beispiel ist die Quelle des Ereignisses der Knoten mit dem Namen „Erdferkel“. Wenn Sie auf diesen Knotennamen klicken, werden die HA-Details für das betroffene HA-Paar (Aardvark und Bonobo) auf der Registerkarte „Knoten“ der Seite „Cluster-/Integritätsdetails“ angezeigt und andere Ereignisse angezeigt, die kürzlich auf dem betroffenen HA-Paar aufgetreten sind.

2. Weitere Informationen zur Veranstaltung finden Sie in den **HA-Details**.

   In diesem Beispiel befinden sich die relevanten Informationen in der Ereignistabelle. Die Tabelle zeigt das Ereignis „Storage Failover Connection One or More Link Down“, den Zeitpunkt der Ereignisgenerierung und erneut den Knoten, von dem dieses Ereignis stammt.

Fordern Sie mithilfe der Knotenstandortinformationen in den HA-Details eine physische Inspektion und Reparatur des Speicher-Failover-Problems auf den betroffenen HA-Paarknoten an oder führen Sie diese selbst durch.

Verwandte Informationen

"Seite mit Veranstaltungsdetails"

"Unified Manager-Benutzerrollen und -Funktionen"

Beheben von Volume-Offline-Problemen

Dieser Workflow bietet ein Beispiel dafür, wie Sie ein Volume-Offline-Ereignis auswerten und lösen können, das Unified Manager möglicherweise auf der Inventarseite der Ereignisverwaltung anzeigt. In diesem Szenario sind Sie ein Administrator, der Unified Manager verwendet, um ein oder mehrere Volume-Offline-Ereignisse zu beheben.

Bevor Sie beginnen

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

Volumes können aus mehreren Gründen als offline gemeldet werden:

- Der SVM-Administrator hat das Volume absichtlich offline genommen.
- Der Host-Clusterknoten des Volumes ist ausgefallen und auch das Speicher-Failover zu seinem HA-Paar-Partner ist fehlgeschlagen.
- Die Storage Virtual Machine (SVM) des Volumes wird gestoppt, da der Knoten, auf dem sich das Stammvolume dieser SVM befindet, ausgefallen ist.
- Das Hosting-Aggregat des Volumes ist aufgrund des gleichzeitigen Ausfalls zweier RAID-Festplatten ausgefallen.

Sie können die Inventarseite der Ereignisverwaltung und die Detailseiten „Cluster/Integrität“, „Speicher-VM/Integrität“ und „Volume/Integrität“ verwenden, um eine oder mehrere dieser Möglichkeiten zu bestätigen oder auszuschließen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.
2. Wählen Sie auf der Inventarseite **Event Management** die Option **Active Availability-Ereignisse** aus.
3. Klicken Sie auf den Hypertext-Link, der für das Ereignis „Volume offline“ angezeigt wird.

   Die Seite mit den Ereignisdetails für den Verfügbarkeitsvorfall wird angezeigt.

4. Überprüfen Sie auf dieser Seite die Hinweise auf Hinweise, dass der SVM-Administrator das betreffende Volume offline genommen hat.
5. Auf der Detailseite des **Ereignisses** können Sie die Informationen für eine oder mehrere der folgenden Aufgaben überprüfen:
   - Überprüfen Sie die im Feld „Ursache“ angezeigten Informationen auf mögliche Diagnosehinweise.

     In diesem Beispiel informieren Sie die Informationen im Feld „Ursache“ nur darüber, dass das Volume offline ist.

   - Überprüfen Sie den Bereich „Hinweise und Updates“ auf Hinweise, dass der SVM-Administrator das betreffende Volume absichtlich offline genommen hat.
   - Klicken Sie auf die Quelle des Ereignisses, in diesem Fall das als 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 gelöst.

Führen Sie Diagnoseaktionen für Volume-Offline-Bedingungen durch

Nachdem Sie zur Seite mit den Volume-/Integritätsdetails eines Volumes navigiert sind, das als offline gemeldet wurde, können Sie nach zusätzlichen Informationen suchen, die für die Diagnose des Offlinezustands des Volumes hilfreich sind.

Bevor Sie beginnen

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

Wenn das als offline gemeldete Volume nicht absichtlich offline genommen wurde, kann dies mehrere Gründe haben.

Von der Seite „Volume/Integritätsdetails“ des Offline-Volumes aus können Sie zu anderen Seiten und Bereichen navigieren, um mögliche Ursachen zu bestätigen oder auszuschließen:

- Klicken Sie auf die Links auf der Detailseite **Volume/Integrität**, um festzustellen, ob das Volume offline ist, weil sein Hostknoten ausgefallen ist und auch das Speicher-Failover zu seinem HA-Paarpartner fehlgeschlagen ist.

  Sehen"Feststellen, ob ein Volume-Offline-Zustand durch einen ausgefallenen Knoten verursacht wird" .

- Klicken Sie auf die Links zur Detailseite **Volume/Integrität**, um festzustellen, ob das Volume offline ist und die darauf gehostete Storage Virtual Machine (SVM) angehalten wurde, weil der Knoten, auf dem sich das Stammvolume dieser SVM befindet, ausgefallen ist.

  Sehen"Feststellen, ob ein Volume offline ist und SVM gestoppt wurde, weil ein Knoten ausgefallen ist" .

- Klicken Sie auf die Links zur Detailseite **Volume/Integrität**, um festzustellen, ob das Volume aufgrund defekter Festplatten in seinem Hostaggregat offline ist.

  Sehen"Feststellen, ob ein Volume aufgrund defekter Datenträger in einem Aggregat offline ist" .

Verwandte Informationen

"Unified Manager-Benutzerrollen und -Funktionen"

Ermitteln, ob ein Volume offline ist, weil sein Hostknoten ausgefallen ist

Sie können die Web-Benutzeroberfläche von Unified Manager verwenden, um die Möglichkeit zu bestätigen oder auszuschließen, dass ein Volume offline ist, weil sein Hostknoten ausgefallen ist und das Speicher-Failover zu seinem HA-Paarpartner nicht erfolgreich ist.

Bevor Sie beginnen

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

Um festzustellen, ob der Offlinezustand des Volumes durch einen Ausfall des Hostknotens und ein anschließendes fehlgeschlagenes Speicher-Failover verursacht wurde, führen Sie die folgenden Aktionen aus:

Schritte

1. Suchen Sie den Hypertext-Link, der unter SVM im Bereich **Verwandte Geräte** der Detailseite **Volume/Integrität** des Offline-Volumes angezeigt wird, und klicken Sie darauf.

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

2. Suchen Sie im Bereich **Verwandte Geräte** der Detailseite **Storage VM / Health** den unter „Volumes“ angezeigten Hypertext-Link und klicken Sie darauf.

   Die Ansicht „Integrität: Alle Volumes“ zeigt eine Tabelle mit Informationen zu allen vom SVM gehosteten Volumes an.

3. Klicken Sie in der Spaltenüberschrift „Health: All Volumes“ der Ansicht „State“ auf das Filtersymbol , und wählen Sie dann die Option **Offline**.

   Es werden nur die SVM-Volumes aufgelistet, die sich im Offline-Status befinden.

4. Klicken Sie in der Ansicht „Health: All Volumes“ auf das Rastersymbol und wählen Sie dann die Option **Clusterknoten** aus.

   Möglicherweise müssen Sie im Rasterauswahlfeld scrollen, um die Option **Clusterknoten** zu finden.

   Die Spalte „Clusterknoten“ wird zum Volume-Inventar hinzugefügt und zeigt den Namen des Knotens an, der jedes Offline-Volume hostet.

5. Suchen Sie in der Ansicht „Integrität: Alle Volumes“ den Eintrag für das Offline-Volume und klicken Sie in der Spalte „Clusterknoten“ auf den Namen des zugehörigen Hosting-Knotens.

   Auf der Registerkarte „Knoten“ auf der Seite „Cluster-/Integritätsdetails“ wird der Status des HA-Knotenpaars angezeigt, zu dem der Hosting-Knoten gehört. Der Status des Hostknotens und der Erfolg aller Cluster-Failover-Vorgänge werden in der Anzeige angegeben.

Nachdem Sie bestätigt haben, dass das Volume offline ist, weil sein Hostknoten ausgefallen ist und das Speicher-Failover zum HA-Paar-Partner fehlgeschlagen ist, wenden Sie sich an den entsprechenden Administrator oder Operator, um den ausgefallenen Knoten manuell neu zu starten und das Speicher-Failover-Problem zu beheben.

Ermitteln Sie, ob ein Volume offline ist und sein SVM gestoppt wurde, weil ein Knoten ausgefallen ist

Sie können die Web-Benutzeroberfläche von Unified Manager verwenden, um die Möglichkeit zu bestätigen oder auszuschließen, dass ein Volume offline ist, weil die zugehörige Host-Storage-Virtual-Machine (SVM) angehalten wurde, weil der Knoten, auf dem sich das Stammvolume dieser SVM befindet, ausgefallen ist.

Bevor Sie beginnen

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

Um festzustellen, ob der Offlinezustand des Volumes darauf zurückzuführen ist, dass das Host-SVM angehalten wurde, weil der Knoten, auf dem sich das Stammvolume dieses SVM befindet, ausgefallen ist, führen Sie die folgenden Aktionen aus:

Schritte

1. Suchen Sie den Hypertext-Link, der unter dem SVM im Bereich **Verwandte Geräte** der Detailseite **Volume/Integrität** des Offline-Volumes angezeigt wird, und klicken Sie darauf.

   Auf der Seite „Storage VM / Health Details“ wird der Status „Läuft“ oder „Gestoppt“ der Host-SVM angezeigt. Wenn der SVM-Status „Läuft“ lautet, wird der Offline-Zustand des Volumes nicht dadurch

verursacht, dass der Knoten, auf dem sich das Stammvolume dieses SVM befindet, ausgefallen ist.

2. Wenn der SVM-Status „Beendet“ lautet, klicken Sie auf „SVMs anzeigen“, um die Ursache für das Beenden des Hosting-SVMs genauer zu ermitteln.
3. Klicken Sie in der Spaltenüberschrift der Ansicht „SVM“ **Health: All Storage VMs** auf das Filtersymbol und geben Sie dann den Namen der gestoppten SVM ein.

   Die Informationen zu diesem SVM werden in einer Tabelle angezeigt.

4. Klicken Sie in der Ansicht **Health: All Storage VMs** auf und wählen Sie dann die Option **Root Volume**.

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

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

   Wenn der Status des SVM-Stammvolumes (Online) lautet, liegt der Offline-Zustand des ursprünglichen Volumes nicht daran, dass der Knoten, auf dem sich das Stammvolume dieses SVM befindet, ausgefallen ist.

6. Wenn der Status des SVM-Stammvolumes (Offline) lautet, suchen Sie den Hypertext-Link, der unter „Aggregat“ im Bereich „Verwandte Geräte“ der Seite „Volume-/Integritätsdetails“ des SVM-Stammvolumes angezeigt wird, und klicken Sie darauf.
7. Suchen Sie den Hypertext-Link, der unter „Knoten“ im Bereich „Verwandte Geräte“ der Detailseite „Aggregat/Integrität“ des Aggregats angezeigt wird, und klicken Sie darauf.

   Auf der Registerkarte „Knoten“ auf der Seite „Cluster-/Integritätsdetails“ wird der Status des HA-Knotenpaars angezeigt, zu dem der Hosting-Knoten des SVM-Stammvolumes gehört. Der Zustand des Knotens wird im Display angezeigt.

Nachdem Sie bestätigt haben, dass der Offlinezustand des Volumes durch den Offlinezustand des Host-SVM dieses Volumes verursacht wird, der wiederum durch den Ausfall des Knotens verursacht wird, der das Stammvolume dieses SVM hostet, wenden Sie sich an den entsprechenden Administrator oder Operator, um den ausgefallenen Knoten manuell neu zu starten.

Ermitteln, ob ein Volume aufgrund defekter Datenträger in einem Aggregat offline ist

Sie können die Web-Benutzeroberfläche von Unified Manager verwenden, um die Möglichkeit zu bestätigen oder auszuschließen, dass ein Volume offline ist, weil das Host-Aggregat aufgrund von RAID-Festplattenproblemen offline gegangen ist.

Bevor Sie beginnen

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

Um festzustellen, ob der Offlinezustand des Volumes durch RAID-Festplattenprobleme verursacht wird, die das Hosting-Aggregat offline schalten, führen Sie die folgenden Aktionen aus:

Schritte

1. Suchen Sie den Hypertext-Link, der unter „Aggregat“ im Bereich „Verwandte Geräte“ der Detailseite „Volume/Integrität“ angezeigt wird, und klicken Sie darauf.

   Auf der Seite „Aggregat-/Integritätsdetails“ wird der Online- oder Offline-Status des Hosting-Aggregats

angezeigt. Wenn der Aggregatstatus „Online“ lautet, sind RAID-Festplattenprobleme nicht die Ursache dafür, dass das Volume offline ist.

2. Wenn der Aggregatstatus „Offline“ lautet, klicken Sie auf „Datenträgerinformationen“ und suchen Sie in der Liste „Ereignisse“ auf der Registerkarte „Datenträgerinformationen“ nach Ereignissen bezüglich defekter Datenträger.
3. Um die defekten Festplatten genauer zu identifizieren, klicken Sie auf den Hypertext-Link, der unter „Knoten“ im Bereich „Verwandte Geräte“ angezeigt wird.

   Die Seite mit den Cluster-/Integritätsdetails wird angezeigt.

4. Klicken Sie auf **Datenträger** und wählen Sie dann im Bereich **Filter** die Option **Beschädigt** aus, um alle Datenträger im Zustand „Beschädigt“ aufzulisten.

   Wenn die Festplatten im defekten Zustand den Offline-Zustand des Hostaggregats verursacht haben, wird der Name des Aggregats in der Spalte „Betroffenes Aggregat“ angezeigt.

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

Beheben Sie Kapazitätsprobleme

Dieser Workflow bietet ein Beispiel dafür, wie Sie ein Kapazitätsproblem lösen können. In diesem Szenario sind Sie ein Administrator oder Operator und greifen auf die Dashboard-Seite des Unified Managers zu, um zu sehen, ob bei einem der überwachten Speicherobjekte Kapazitätsprobleme vorliegen. Sie möchten die mögliche Ursache des Problems ermitteln und eine Lösung dafür finden.

Bevor Sie beginnen

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

Suchen Sie auf der Dashboard-Seite im Kapazitätsbereich unter der Dropdown-Liste „Ereignisse“ nach einem Fehlerereignis „Volume Space Full“.

Schritte

1. Klicken Sie im Bereich **Kapazität** der Seite **Dashboard** auf den Namen des Fehlerereignisses „Volume-Speicherplatz voll“.

   Die Seite mit den Ereignisdetails für den Fehler wird angezeigt.

2. Auf der Detailseite **Ereignis** können Sie eine oder mehrere der folgenden Aufgaben ausführen:
   - Überprüfen Sie die Fehlermeldung im Feld „Ursache“ und klicken Sie auf die Vorschläge unter „Vorgeschlagene Abhilfemaßnahmen“, um Beschreibungen möglicher Abhilfemaßnahmen zu überprüfen.
   - Klicken Sie im Feld „Quelle“ auf den Objektnamen (in diesem Fall ein Volume), um Details zum Objekt zu erhalten.
   - Suchen Sie nach Notizen, die möglicherweise zu diesem Ereignis hinzugefügt wurden.
   - Fügen Sie dem Ereignis eine Notiz hinzu.

- Weisen Sie das Ereignis einem anderen Benutzer zu.
- Bestätigen Sie das Ereignis.
- Markieren Sie das Ereignis als gelöst.

Verwandte Informationen

"Seite mit Veranstaltungsdetails"

Führen Sie die vorgeschlagenen Abhilfemaßnahmen für ein vollständiges Volumen durch

Nachdem Sie das Fehlerereignis „Volume Space Full“ erhalten haben, überprüfen Sie die vorgeschlagenen Abhilfemaßnahmen auf der Seite mit den Ereignisdetails und entscheiden, eine der vorgeschlagenen Maßnahmen durchzuführen.

Bevor Sie beginnen

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

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

In diesem Beispiel haben Sie auf der Inventarseite von Unified ManagerEvent Management ein Fehlerereignis „Volume Space Full“ gesehen und auf den Namen des Ereignisses geklickt.

Zu den möglichen Abhilfemaßnahmen, die Sie für ein vollständiges Volume durchführen können, gehören die folgenden:

- 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 vom ONTAP System Manager oder der ONTAP CLI aus ausgeführt werden müssen, können Sie mit Unified Manager Informationen finden, die Sie möglicherweise benötigen, um zu bestimmen, welche Aktionen ausgeführt werden müssen.

Schritte

1. Klicken Sie auf der Detailseite **Ereignis** auf den Volumenamen im Feld „Quelle“, um Details zum betroffenen Volume anzuzeigen.
2. Auf der Detailseite **Volume/Integrität** klicken Sie auf **Konfiguration** und sehen, dass Deduplizierung und Komprimierung auf dem Volume bereits aktiviert sind.

   Sie entscheiden sich, die Größe des Volumes zu ändern.

3. Klicken Sie im Bereich **Verwandte Geräte** auf den Namen des Hosting-Aggregats, um zu sehen, ob das Aggregat ein größeres Volumen aufnehmen kann.
4. Auf der Detailseite **Aggregat/Integrität** sehen Sie, dass das Aggregat, auf dem sich das gesamte Volume befindet, über genügend nicht zugewiesene Kapazität verfügt. Sie verwenden also ONTAP System Manager, um die Größe des Volumes anzupassen und ihm mehr Kapazität zu geben.

Verwandte Informationen

"Seite mit Veranstaltungsdetails"

Verwalten von Integritätsschwellenwerten

Sie können globale Integritätsschwellenwerte für alle Aggregate, Volumes und Qtrees konfigurieren, um alle Verletzungen der Integritätsschwellenwerte zu verfolgen.

Welche Schwellenwerte für die Speicherkapazität gelten

Ein Integritätsschwellenwert für die Speicherkapazität ist der Punkt, an dem der Unified Manager-Server Ereignisse generiert, um etwaige Kapazitätsprobleme mit Speicherobjekten zu melden. Sie können Warnmeldungen konfigurieren, um bei Auftreten solcher Ereignisse eine Benachrichtigung zu senden.

Die Integritätsschwellenwerte der Speicherkapazität für alle Aggregate, Volumes und Qtrees sind auf Standardwerte eingestellt. Sie können die Einstellungen nach Bedarf für ein Objekt oder eine Gruppe von Objekten ändern.

Konfigurieren der globalen Integritätsschwellenwerteinstellungen

Sie können globale Integritätsschwellenwerte für Kapazität, Wachstum, Snapshot-Reserve, Kontingente und Inodes konfigurieren, um Ihre Gesamt-, Volumen- und Qtree-Größe effektiv zu überwachen. Sie können auch die Einstellungen zum Generieren von Ereignissen beim Überschreiten von Verzögerungsschwellenwerten bearbeiten.

Globale Integritätsschwellenwerteinstellungen gelten für alle Objekte, mit denen sie verknüpft sind, z. B. Aggregate, Volumes usw. Beim Überschreiten von Schwellenwerten wird ein Ereignis generiert und, sofern Warnmeldungen konfiguriert sind, eine Warnmeldung gesendet. Die Schwellenwerte sind standardmäßig auf empfohlene Werte eingestellt, Sie können sie jedoch ändern, um Ereignisse in Intervallen zu generieren, die Ihren spezifischen Anforderungen entsprechen. Wenn Schwellenwerte geändert werden, werden Ereignisse im nächsten Überwachungszyklus generiert oder verworfen.

Auf die globalen Integritätsschwellenwerteinstellungen kann über den Abschnitt „Ereignisschwellenwerte“ im linken Navigationsmenü zugegriffen werden. Sie können die Schwellenwerteinstellungen für einzelne Objekte auch auf der Inventarseite oder der Detailseite für das jeweilige Objekt ändern.

- Weitere Informationen finden Sie unter"Konfigurieren globaler aggregierter Integritätsschwellenwerte" .

  Sie können die Integritätsschwellenwerteinstellungen für Kapazität, Wachstum und Snapshot-Kopien für alle Aggregate konfigurieren, um alle Schwellenwertüberschreitungen zu verfolgen.

- Weitere Informationen finden Sie unter"Konfigurieren globaler Schwellenwerte für die Volumeintegrität" .

  Sie können die Integritätsschwellenwerteinstellungen für Kapazität, Snapshot-Kopien, Qtree-Kontingente, Volume-Wachstum, Reservespeicherplatz zum Überschreiben und Inodes für alle Volumes bearbeiten, um etwaige Schwellenwertüberschreitungen zu verfolgen.

- Weitere Informationen finden Sie unter"Konfigurieren globaler Qtree-Integritätsschwellenwerte" .

  Sie können die Integritätsschwellenwerteinstellungen für die Kapazität aller Qtrees bearbeiten, um alle Schwellenwertüberschreitungen zu verfolgen.

- Weitere Informationen finden Sie unter"Bearbeiten der Lag-Health-Schwellenwerteinstellungen für nicht verwaltete Schutzbeziehungen" .

  Sie können den Prozentsatz der Verzögerungszeit für Warnungen oder Fehler erhöhen oder verringern, sodass Ereignisse in Intervallen generiert werden, die Ihren Anforderungen besser entsprechen.

Konfigurieren globaler Schwellenwerte für die Gesamtintegrität

Sie können globale Integritätsschwellenwerte für alle Aggregate konfigurieren, um alle Schwellenwertüberschreitungen zu verfolgen. Bei Grenzwertüberschreitungen werden entsprechende Ereignisse generiert und Sie können auf Basis dieser Ereignisse vorbeugende Maßnahmen ergreifen. Sie können die globalen Werte basierend auf den Best Practice-Einstellungen für Schwellenwerte konfigurieren, die für alle überwachten Aggregate gelten.

Bevor Sie beginnen

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

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

Die Schwellenwertoptionen verfügen über Standardwerte zur besseren Überwachung. Sie können die Werte jedoch ändern, um sie an die Anforderungen Ihrer Umgebung anzupassen.

Wenn Autogrow auf Volumes aktiviert ist, die sich auf dem Aggregat befinden, gelten die Schwellenwerte für die Aggregatkapazität als überschritten, und zwar basierend auf der durch Autogrow festgelegten maximalen Volumegröße, nicht basierend auf der ursprünglichen Volumegröße.

Integritätsschwellenwerte sind auf das Stammaggregat des Knotens nicht anwendbar.

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 globaler Schwellenwerte für die Volumeintegrität

Sie können die globalen Integritätsschwellenwerte für alle Volumes konfigurieren, um alle Schwellenwertüberschreitungen zu verfolgen. Bei Verletzungen von Integritätsschwellenwerten werden entsprechende Ereignisse generiert und Sie können auf Grundlage dieser Ereignisse vorbeugende Maßnahmen ergreifen. Sie können die globalen Werte basierend auf den Best Practice-Einstellungen für Schwellenwerte konfigurieren, die für alle überwachten Volumes gelten.

Bevor Sie beginnen

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

Die meisten Schwellenwertoptionen verfügen über Standardwerte zur besseren Überwachung. Sie können die Werte jedoch ändern, um sie an die Anforderungen Ihrer Umgebung anzupassen.

Beachten Sie, dass bei aktivierter Autogrow-Funktion auf einem Volume die Kapazitätsschwellenwerte auf Grundlage der durch Autogrow festgelegten maximalen Volumegröße und nicht auf Grundlage der ursprünglichen Volumegröße als überschritten gelten.

> Der Standardwert von 1000 Snapshot-Kopien gilt nur für FlexVol -Volumes, wenn die ONTAP Version 9.4 oder höher ist, und für FlexGroup -Volumes, wenn die ONTAP Version 9.8 oder 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 Zahl 1000 (und jede 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 festlegen möchten, müssen Sie den Schwellenwert hier in der Ansicht „Integrität: Alle Volumes“ oder auf der Seite „Volume-/Integritätsdetails“ auf 250 oder weniger festlegen.

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 Sie globale Qtree-Integritätsschwellenwerte

Sie können die globalen Integritätsschwellenwerte für alle Qtrees konfigurieren, um alle Schwellenwertüberschreitungen zu verfolgen. Bei Verletzungen von Integritätsschwellenwerten werden entsprechende Ereignisse generiert und Sie können auf Grundlage dieser Ereignisse vorbeugende Maßnahmen ergreifen. Sie können die globalen Werte basierend auf den Best-Practice-Einstellungen für Schwellenwerte konfigurieren, die für alle überwachten Qtrees gelten.

Bevor Sie beginnen

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

Die Schwellenwertoptionen verfügen über Standardwerte zur besseren Überwachung. Sie können die Werte jedoch ändern, um sie an die Anforderungen Ihrer Umgebung anzupassen.

Ereignisse werden für einen Qtree nur generiert, wenn für den Qtree ein Qtree-Kontingent oder ein Standardkontingent festgelegt wurde. Es werden keine Ereignisse generiert, wenn der in einem Benutzer- 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 globalen Standardeinstellungen für Verzögerungswarnungen und Fehlerzustandsschwellenwerte für nicht verwaltete Schutzbeziehungen bearbeiten, sodass Ereignisse in Intervallen generiert werden, die Ihren Anforderungen entsprechen.

Bevor Sie beginnen

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

Die Verzögerungszeit darf nicht länger sein als das definierte Übertragungsintervall. Wenn beispielsweise stündlich verkehrt, darf die Verzögerungszeit nicht mehr als eine Stunde betragen. Der Verzögerungsschwellenwert gibt einen Prozentsatz an, den die Verzögerungszeit nicht überschreiten darf. Wenn im Beispiel einer Stunde der Verzögerungsschwellenwert auf 150 % festgelegt 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 ausschließlich für eine nicht verwaltete Schutzbeziehung festgelegt und angewendet werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisschwellenwerte** > **Beziehung**.
2. Erhöhen oder verringern Sie den Prozentsatz der globalen Standardwarnungs- oder Fehlerverzögerungszeit nach Bedarf.
3. Um zu verhindern, dass bei einem beliebigen Verzögerungsschwellenwert ein Warn- oder Fehlerereignis ausgelöst wird, deaktivieren Sie das Kontrollkästchen neben **Aktiviert**.
4. Klicken Sie auf **Speichern**.

Verwandte Informationen

"Benutzer hinzufügen"

Bearbeiten Sie die einzelnen Schwellenwerteinstellungen für die Gesamtintegrität

Sie können die Integritätsschwellenwerteinstellungen für die Aggregatkapazität, das Wachstum und die Snapshot-Kopien eines oder mehrerer Aggregate bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnungen generiert und Sie erhalten Benachrichtigungen. Diese Benachrichtigungen helfen Ihnen, basierend auf dem generierten Ereignis vorbeugende Maßnahmen zu ergreifen.

Bevor Sie beginnen

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

Basierend auf Änderungen der Schwellenwerte werden im nächsten Überwachungszyklus Ereignisse generiert oder verworfen.

Wenn Autogrow auf Volumes aktiviert ist, die sich auf dem Aggregat befinden, gelten die Schwellenwerte für die Aggregatkapazität als überschritten, und zwar basierend auf der durch Autogrow festgelegten maximalen Volumegröße, nicht basierend auf der ursprünglichen Volumegröße.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate**.
2. Wählen Sie in der Ansicht **Health: Alle Aggregate** ein oder mehrere Aggregate aus und klicken Sie dann auf **Schwellenwerte bearbeiten**.
3. Bearbeiten Sie im Dialogfeld **Aggregatschwellenwerte bearbeiten** die Schwellenwerteinstellungen für eine 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 der Schwellenwerteinstellungen für die Integrität einzelner Volumes

Sie können die Integritätsschwellenwerteinstellungen für Volumekapazität, Wachstum, Kontingent und Speicherplatzreserve eines oder mehrerer Volumes bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnungen generiert und Sie erhalten Benachrichtigungen. Diese Benachrichtigungen helfen Ihnen, basierend auf dem generierten Ereignis vorbeugende Maßnahmen zu ergreifen.

Bevor Sie beginnen

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

Basierend auf Änderungen der Schwellenwerte werden im nächsten Überwachungszyklus Ereignisse generiert oder verworfen.

Beachten Sie, dass bei aktivierter Autogrow-Funktion auf einem Volume die Kapazitätsschwellenwerte auf Grundlage der durch Autogrow festgelegten maximalen Volumegröße und nicht auf Grundlage der ursprünglichen Volumegröße als überschritten gelten.

> Der Standardwert von 1000 Snapshot-Kopien gilt nur für FlexVol -Volumes, wenn die ONTAP Version 9.4 oder höher ist, und für FlexGroup -Volumes, wenn die ONTAP Version 9.8 oder 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 Zahl 1000 (und jede 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 festlegen möchten, müssen Sie den Schwellenwert hier in der Ansicht „Integrität: Alle Volumes“ oder auf der Seite „Volume-/Integritätsdetails“ auf 250 oder weniger festlegen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie in der Ansicht **Health: All Volumes** ein oder mehrere Volumes aus und klicken Sie dann auf **Edit Thresholds**.
3. Bearbeiten Sie im Dialogfeld **Volume-Schwellenwerte bearbeiten** die Schwellenwerteinstellungen für einen der folgenden Punkte: 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 Sie die individuellen Qtree-Integritätsschwellenwerteinstellungen

Sie können die Integritätsschwellenwerteinstellungen für die Qtree-Kapazität für einen oder mehrere Qtrees bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnungen generiert und Sie erhalten Benachrichtigungen. Diese Benachrichtigungen helfen Ihnen, basierend auf dem generierten Ereignis vorbeugende Maßnahmen zu ergreifen.

Bevor Sie beginnen

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

Basierend auf Änderungen der Schwellenwerte werden im nächsten Überwachungszyklus Ereignisse generiert oder verworfen.

Schritte

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

Sie können auch einzelne Qtree-Schwellenwerte auf der Registerkarte „Qtrees“ auf der Seite „Storage VM / Health Details“ festlegen.

Verwalten von Cluster-Sicherheitszielen

Unified Manager bietet ein Dashboard, das anhand der im „NetApp Security Hardening Guide for ONTAP 9“ definierten Empfehlungen ermittelt, wie sicher Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes sind.

Das Ziel des Sicherheits-Dashboards besteht darin, alle Bereiche anzuzeigen, in denen Ihre ONTAP Cluster nicht den von NetApp empfohlenen Richtlinien entsprechen, damit Sie diese potenziellen Probleme beheben können. In den meisten Fällen können Sie die Probleme mit dem ONTAP System Manager oder der ONTAP CLI beheben. Ihre Organisation befolgt möglicherweise nicht alle Empfehlungen, sodass Sie in einigen Fällen keine Änderungen vornehmen müssen.

Siehe die "NetApp Security Hardening Guide für ONTAP 9" (TR-4569) für detaillierte Empfehlungen und Lösungen.

Zusätzlich zur Meldung des Sicherheitsstatus generiert Unified Manager auch Sicherheitsereignisse für alle Cluster oder SVMs mit Sicherheitsverletzungen. Sie können diese Probleme auf der Inventarseite der Ereignisverwaltung verfolgen und Warnmeldungen für diese Ereignisse konfigurieren, sodass 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 anhand der im *NetApp Security Hardening Guide für ONTAP 9* definierten Empfehlungen bewertet.

Zu den Sicherheitskontrollen gehören unter anderem:

- ob ein Cluster eine sichere Authentifizierungsmethode wie SAML verwendet
- ob die Kommunikation zwischen Peering-Clustern verschlüsselt ist
- ob für eine Speicher-VM das Überwachungsprotokoll aktiviert ist
- ob auf Ihren Volumes Software- oder Hardwareverschlüsselung aktiviert ist

Siehe die Themen zu Compliance-Kategorien und den "NetApp Security Hardening Guide für ONTAP 9" für detaillierte Informationen.

> Von der Active IQ Plattform gemeldete Upgrade-Ereignisse gelten ebenfalls als Sicherheitsereignisse. Diese Ereignisse identifizieren Probleme, bei denen zur Lösung ein Upgrade der ONTAP -Software, der Knoten-Firmware oder der Betriebssystemsoftware (für Sicherheitshinweise) erforderlich ist. Diese Ereignisse werden nicht im Sicherheitsbereich angezeigt, sind aber auf der Inventarseite der Ereignisverwaltung verfügbar.

Weitere Informationen finden Sie unter "Verwalten von Cluster-Sicherheitszielen".

Cluster-Compliance-Kategorien

Diese Tabelle beschreibt die von Unified Manager ausgewerteten Parameter zur Cluster-Sicherheitskonformität, die NetApp -Empfehlung und ob der Parameter die Gesamtfeststellung beeinflusst, ob der Cluster den Anforderungen entspricht oder nicht.

Wenn sich in einem Cluster nicht konforme SVMs befinden, wirkt sich dies auf den Konformitätswert des Clusters aus. Daher müssen Sie in einigen Fällen möglicherweise ein Sicherheitsproblem mit einem SVM beheben, bevor die Sicherheit Ihres Clusters als konform angesehen wird.

Beachten Sie, dass nicht jeder der unten aufgeführten Parameter bei allen Installationen angezeigt wird. Wenn Sie beispielsweise keine Peering-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	Beeinflusst die Cluster-Compliance
Globales FIPS	Gibt an, ob der Konformitätsmodus 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 sind zulässig.	Ermöglicht	Ja
Telnet	Gibt an, ob der Telnet-Zugriff auf das System aktiviert oder deaktiviert ist. NetApp empfiehlt Secure Shell (SSH) für sicheren Fernzugriff.	Deaktiviert	Ja
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, beispielsweise Chiffren, die mit *cbc beginnen.	Nein	Ja
Login-Banner	Gibt an, ob das Anmeldebanner für Benutzer, die auf das System zugreifen, aktiviert oder deaktiviert ist.	Ermöglicht	Ja
Cluster-Peering	Gibt an, ob die Kommunikation zwischen Peering-Clustern verschlüsselt oder unverschlüsselt ist. Damit dieser Parameter als konform gilt, muss die Verschlüsselung sowohl auf dem Quell- als auch auf dem Zielcluster konfiguriert sein.	Verschlüsselt	Ja

Parameter	Beschreibung	Empfehlung	Beeinflusst die Cluster-Compliance
Netzwerkzeitprotokoll	Gibt an, ob der Cluster über einen oder mehrere konfigurierte NTP-Server verfügt. Aus Redundanzgründen und für einen optimalen Service empfiehlt NetApp , dem Cluster mindestens drei NTP-Server zuzuordnen.	Konfiguriert	Ja
OCSP	Ab Version 9.14.1 bietet Active IQ Unified Manager Statusinformationen zum Online Certificate Status Protocol (OCSP) auf der Ebene der Storage Virtual Machine (SVM, früher als Vserver bezeichnet). Dies bedeutet, dass die OCSP-Validierung auf alle SSL/TLS-Verbindungen zum SVM angewendet wird und die Integrität und Gültigkeit der in diesen Verbindungen verwendeten Zertifikate gewährleistet.	Ermöglicht	Nein
Remote-Audit-Protokollierung	Gibt an, ob die Protokollweiterleitung (Syslog) verschlüsselt oder unverschlüsselt ist.	Verschlüsselt	Ja
AutoSupport HTTPS-Transport	Gibt an, ob HTTPS als Standardtransportprotokoll zum Senden von AutoSupport -Nachrichten an den NetApp Support verwendet wird.	Ermöglicht	Ja
Standard-Administratorbenutzer	Gibt an, ob der Standardadministratorbenutzer (integriert) aktiviert oder deaktiviert ist. NetApp empfiehlt, alle nicht benötigten integrierten Konten zu sperren (deaktivieren).	Deaktiviert	Ja

Parameter	Beschreibung	Empfehlung	Beeinflusst die Cluster-Compliance
SAML-Benutzer	Gibt an, ob SAML konfiguriert ist. SAML ermöglicht Ihnen die Konfiguration der Multi-Faktor-Authentifizierung (MFA) als Anmeldemethode für Single Sign-On.	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 gegenüber lokalen Benutzern verwalten.	Nein	Nein
Zertifikatsbenutzer	Gibt an, ob ein Zertifikatsbenutzer für die Anmeldung beim Cluster konfiguriert ist.	Nein	Nein
Lokale Benutzer	Gibt an, ob lokale Benutzer für die Anmeldung beim Cluster konfiguriert sind.	Nein	Nein
Remote-Shell	Gibt an, ob RSH aktiviert ist. Aus Sicherheitsgründen sollte RSH deaktiviert werden. Für den sicheren Fernzugriff wird die Secure Shell (SSH) bevorzugt.	Deaktiviert	Ja

Parameter	Beschreibung	Empfehlung	Beeinflusst die Cluster-Compliance
MD5 im Einsatz	Gibt an, ob ONTAP Benutzerkonten die weniger sichere MD5-Hash-Funktion verwenden. Die Migration von MD5-gehashten Benutzerkonten zur sichereren kryptografischen Hashfunktion wie SHA-512 wird bevorzugt.	Nein	Ja
Zertifikatsausstellertyp	Gibt den Typ des verwendeten digitalen Zertifikats an.	CA-signiert	Nein

Storage-VM-Compliance-Kategorien

Diese Tabelle beschreibt die Sicherheitskonformitätskriterien für virtuelle Speichermaschinen (SVMs), die Unified Manager auswertet, die NetApp -Empfehlung und ob der Parameter die Gesamtfeststellung beeinflusst, ob die SVM den Anforderungen entspricht oder nicht.

Parameter	Beschreibung	Empfehlung	Beeinflusst die SVM-Konformität
Prüfprotokoll	Gibt an, ob die Überwachungsprotokollierung aktiviert oder deaktiviert ist.	Ermöglicht	Ja
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, beispielsweise Chiffren, die mit `cbc*` .	Nein	Ja
Login-Banner	Gibt an, ob das Anmeldebanner für Benutzer aktiviert oder deaktiviert ist, die auf SVMs im System zugreifen.	Ermöglicht	Ja
LDAP-Verschlüsselung	Gibt an, ob die LDAP-Verschlüsselung aktiviert oder deaktiviert ist.	Ermöglicht	Nein

Parameter	Beschreibung	Empfehlung	Beeinflusst die SVM-Konformität
NTLM-Authentifizierung	Gibt an, ob die NTLM-Authentifizierung aktiviert oder deaktiviert ist.	Ermöglicht	Nein
LDAP-Nutzlastsignatur	Gibt an, ob die LDAP-Nutzlastsignatur aktiviert oder deaktiviert ist.	Ermöglicht	Nein
CHAP-Einstellungen	Gibt an, ob CHAP aktiviert oder deaktiviert ist.	Ermöglicht	Nein
Kerberos V5	Gibt an, ob die Kerberos V5-Authentifizierung aktiviert oder deaktiviert ist.	Ermöglicht	Nein
NIS-Authentifizierung	Gibt an, ob die Verwendung der NIS-Authentifizierung konfiguriert ist.	Deaktiviert	Nein
FPolicy-Status „Aktiv“	Gibt an, ob FPolicy erstellt wurde oder nicht.	Ja	Nein
SMB-Verschlüsselung aktiviert	Gibt an, ob SMB-Signieren und Versiegeln nicht aktiviert ist.	Ja	Nein
SMB-Signierung aktiviert	Gibt an, ob die SMB-Signatur nicht aktiviert ist.	Ja	Nein

Volumen-Compliance-Kategorien

Diese Tabelle beschreibt die Volume-Verschlüsselungsparameter, die Unified Manager auswertet, um zu bestimmen, ob die Daten auf Ihren Volumes ausreichend vor dem Zugriff durch nicht autorisierte Benutzer geschützt sind.

Beachten Sie, dass die Volume-Verschlüsselungsparameter keinen Einfluss darauf haben, ob der Cluster oder die Speicher-VM als konform gilt.

Parameter	Beschreibung
Softwareverschlüsselt	Zeigt die Anzahl der Volumes an, die mit den Softwareverschlüsselungslösungen NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) geschützt sind.

Parameter	Beschreibung
Hardwareverschlüsselt	Zeigt die Anzahl der Volumes an, die mit der Hardwareverschlüsselung NetApp Storage Encryption (NSE) geschützt sind.
Software- und Hardwareverschlüsselung	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 konform

Cluster und virtuelle Speichermaschinen (SVMs) gelten als nicht konform, wenn eines der Sicherheitskriterien, die anhand der im „NetApp Security Hardening Guide für ONTAP 9“ definierten Empfehlungen bewertet werden, nicht erfüllt ist. Darüber hinaus gilt ein Cluster als nicht konform, wenn ein SVM als nicht konform gekennzeichnet ist.

Die Statussymbole in den Sicherheitskarten haben im Hinblick auf ihre Konformität folgende Bedeutung:

- - Der Parameter ist wie empfohlen konfiguriert.
- - Der Parameter ist nicht wie empfohlen konfiguriert.
- – Entweder ist die Funktionalität auf dem Cluster nicht aktiviert oder der Parameter ist nicht wie empfohlen konfiguriert, trägt aber nicht zur Konformität des Objekts bei.

Beachten Sie, dass der Volume-Verschlüsselungsstatus keinen Einfluss darauf hat, ob der Cluster oder die SVM als konform gelten.

Sicherheitsstatus für Cluster und Storage-VMs anzeigen

Mit Active IQ Unified Manager können Sie den Sicherheitsstatus der Speicherobjekte in Ihrer Umgebung von verschiedenen Punkten der Benutzeroberfläche aus anzeigen. Sie können Informationen und Berichte basierend auf definierten Parametern sammeln und analysieren und verdächtiges Verhalten oder nicht autorisierte Systemänderungen auf den überwachten Clustern und Speicher-VMs erkennen.

Die Sicherheitsempfehlungen finden Sie im "NetApp Security Hardening Guide für ONTAP 9"

Zeigen Sie den Sicherheitsstatus auf Objektebene auf der Seite „Sicherheit“ an

Als Systemadministrator können Sie die Seite **Sicherheit** verwenden, um Einblick in die Sicherheitsstärke Ihrer ONTAP -Cluster und Speicher-VMs auf Rechenzentrums- und Standortebene zu erhalten. Die unterstützten Objekte sind Cluster, Speicher-VMs und Volumes. Gehen Sie folgendermaßen vor:

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 einen einzelnen Cluster aus dem Dropdown-Menü aus.
3. Klicken Sie im Bereich **Sicherheit** auf den Rechtspfeil. Die Seite „Sicherheit“ wird angezeigt.

Klicken Sie auf die Balkendiagramme, Zählungen und `View Reports` Über diese Links gelangen Sie zur Seite „Volumes“, „Cluster“ oder „Storage-VMs“, wo Sie die entsprechenden Details anzeigen oder bei Bedarf Berichte erstellen können.

Auf der Seite „Sicherheit“ werden die folgenden Bereiche angezeigt:

- **Cluster-Compliance**: der Sicherheitsstatus (Anzahl der Cluster, die konform oder nicht konform sind) aller Cluster in einem Rechenzentrum
- **Storage VM Compliance**: der Sicherheitsstatus (Anzahl der Storage VMs, die konform oder nicht konform sind) für alle Storage VMs in Ihrem Rechenzentrum
- **Volume-Verschlüsselung**: 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 aktiviertem oder deaktiviertem Anti-Ransomware-Schutz) aller Volumes in Ihrer Umgebung
- **Clusterauthentifizierung und -zertifikate**: Die Anzahl der Cluster, die die einzelnen Authentifizierungsmethoden verwenden, z. B. SAML, Active Directory oder Zertifikate und lokale Authentifizierung. Das Panel zeigt auch die Anzahl der Cluster an, deren Zertifikate entweder abgelaufen sind oder in 60 Tagen ablaufen.

Sicherheitsdetails aller Cluster auf der Seite „Cluster“ anzeigen

Auf der Detailseite **Cluster/Sicherheit** können Sie den Sicherheitskonformitätsstatus auf Clusterebene anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher > 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 Ablaufs des Clusterzertifikats werden angezeigt.

Sie können auf das Symbol ⋮ Klicken Sie auf die Schaltfläche „Weitere Optionen“ und wählen Sie, ob Sie die Sicherheitsdetails auf der Seite „Sicherheit“ von Unified Manager oder im System Manager anzeigen möchten. Sie sollten über gültige Anmeldeinformationen verfügen, um die Details im System Manager anzuzeigen.

> ⓘ Wenn ein Cluster ein abgelaufenes Zertifikat hat, können Sie auf `expired` unter **Gültigkeit des Cluster-Zertifikats** und erneuern Sie es über System Manager (9.10.1 und höher). Sie können nicht auf `expired` wenn die System Manager-Instanz eine Version vor 9.10.1 hat.

Sicherheitsdetails aller Cluster auf der Seite „Speicher-VMs“ anzeigen

Auf der Detailseite **Speicher-VMs/Sicherheit** können Sie den Sicherheitskonformitätsstatus auf Speicher-VM-Ebene anzeigen.

Schritte

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

Sie können eine Standardansicht der Sicherheitskonformität der Speicher-VMs erhalten, indem Sie die Sicherheitsparameter wie Speicher-VMs, Cluster, Anmeldebanner, Prüfprotokoll und unsichere SSH-Einstellungen überprüfen.

Sie können auf das Symbol Klicken Sie auf die Schaltfläche „Weitere Optionen“ und wählen Sie, ob Sie die Sicherheitsdetails auf der Seite „Sicherheit“ von Unified Manager oder im System Manager anzeigen möchten. Sie sollten über gültige Anmeldeinformationen verfügen, um die Details im System Manager anzuzeigen.

Weitere Informationen zur Anti-Ransomware-Sicherheit für Volumes und Speicher-VMs finden Sie unter"Anzeigen des Anti-Ransomware-Status aller Volumes und Storage-VMs" .

Zeigen Sie Sicherheitsereignisse an, die möglicherweise Software- oder Firmware-Updates erfordern

Es gibt bestimmte Sicherheitsereignisse, die den Auswirkungsbereich „Upgrade“ haben. Diese Ereignisse werden von der Active IQ Plattform gemeldet und identifizieren Probleme, für deren Lösung Sie ein Upgrade der ONTAP -Software, der Knoten-Firmware oder der Betriebssystemsoftware (für Sicherheitshinweise) durchführen müssen.

Bevor Sie beginnen

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

Bei einigen dieser Probleme möchten Sie möglicherweise sofort Abhilfemaßnahmen ergreifen, während andere Probleme möglicherweise bis zu Ihrer nächsten planmäßigen Wartung warten können. Sie können alle diese Ereignisse anzeigen und sie Benutzern zuweisen, die die Probleme lösen können. Wenn es außerdem bestimmte Sicherheitsupgrade-Ereignisse gibt, über die Sie nicht benachrichtigt werden möchten, kann Ihnen diese Liste dabei helfen, diese Ereignisse zu identifizieren, sodass Sie sie deaktivieren können.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.

   Standardmäßig werden alle aktiven (neuen und bestätigten) Ereignisse auf der Inventarseite der Ereignisverwaltung angezeigt.

2. Wählen Sie im Menü „Ansicht“ die Option „Upgrade-Ereignisse“ aus.

   Auf der Seite werden alle aktiven Upgrade-Sicherheitsereignisse angezeigt.

Anzeigen, wie die Benutzerauthentifizierung auf allen Clustern verwaltet wird

Auf der Seite „Sicherheit“ werden die Authentifizierungstypen angezeigt, die zur Authentifizierung der Benutzer in den einzelnen Clustern verwendet werden, sowie die Anzahl der Benutzer, die mit den einzelnen Typen auf den Cluster zugreifen. Auf diese Weise können Sie überprüfen, ob die Benutzerauthentifizierung gemäß den Vorgaben Ihrer Organisation 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 Bereich **Sicherheit** auf den Rechtspfeil, und die Seite **Sicherheit** wird angezeigt.
4. Zeigen Sie die Karte **Cluster-Authentifizierung** an, um die Anzahl der Benutzer anzuzeigen, die mit jedem Authentifizierungstyp auf das System zugreifen.
5. Zeigen Sie die Karte **Clustersicherheit** an, um die Authentifizierungsmechanismen anzuzeigen, die zur Authentifizierung von Benutzern in jedem Cluster verwendet werden.

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

Den Verschlüsselungsstatus aller Volumes anzeigen

Sie können eine Liste aller Volumes und ihres aktuellen Verschlüsselungsstatus anzeigen, um festzustellen, ob die Daten auf Ihren Volumes ausreichend vor dem Zugriff durch unbefugte Benutzer geschützt sind.

Bevor Sie beginnen

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

Die folgenden Verschlüsselungstypen können auf ein Volume angewendet werden:

- Software – Volumes, die mit den Softwareverschlüsselungslösungen NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) geschützt sind.
- Hardware – Volumes, die mit der Hardwareverschlüsselung NetApp Storage Encryption (NSE) geschützt sind.
- Software und Hardware – Volumes, die sowohl durch Software- als auch durch Hardwareverschlüsselung geschützt sind.
- Keine – Volumes, die nicht verschlüsselt sind.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Integrität“ > „Volumes-Verschlüsselung“ aus.
3. Sortieren Sie in der Ansicht **Integrität: Volume-Verschlüsselung** nach dem Feld **Verschlüsselungstyp** oder verwenden Sie den Filter, um Volumes anzuzeigen, die einen bestimmten Verschlüsselungstyp haben oder die nicht verschlüsselt sind (Verschlüsselungstyp „Keine“).

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

Sie können eine Liste aller Volumes und Storage-VMs (SVMs) und deren aktuellen Anti-Ransomware-Status anzeigen, sodass Sie feststellen können, ob die Daten auf Ihren Volumes und SVMs ausreichend vor Ransomware-Angriffen geschützt sind.

Bevor Sie beginnen

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

Weitere Informationen zu den verschiedenen Anti-Ransomware-Status finden Sie unter"ONTAP: Anti-

Ransomware aktivieren" .

Zeigen Sie Sicherheitsdetails aller Volumes mit Anti-Ransomware-Erkennung an

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Integrität“ > „Sicherheit“ > „Anti-Ransomware“
3. In der Ansicht **Sicherheit: Anti-Ransomware** 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, reine SAN-Volumes, Volumes gestoppter Speicher-VMs, Root-Volumes von Speicher-VMs oder Datensicherungs-Volumes unterstützt.

Sicherheitsdetails aller Storage-VMs mit Anti-Ransomware-Erkennung anzeigen

Schritte

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

> Die Anti-Ransomware-Überwachung wird auf Speicher-VMs, bei denen das NAS-Protokoll nicht aktiviert ist, nicht unterstützt.

Alle aktiven Sicherheitsereignisse anzeigen

Sie können alle aktiven Sicherheitsereignisse anzeigen und jedes davon einem Benutzer zuweisen, der das Problem lösen kann. Wenn es außerdem bestimmte Sicherheitsereignisse gibt, die Sie nicht erhalten möchten, kann Ihnen diese Liste dabei helfen, die Ereignisse zu identifizieren, die Sie deaktivieren möchten.

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.

   Standardmäßig werden neue und bestätigte Ereignisse auf der Inventarseite der Ereignisverwaltung 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 Warnungen für Sicherheitsereignisse

Sie können Warnungen für einzelne Sicherheitsereignisse konfigurieren, genau wie für alle anderen Ereignisse, die von Unified Manager empfangen werden. Wenn Sie

außerdem alle Sicherheitsereignisse gleich behandeln und E-Mails an dieselbe Person senden möchten, können Sie eine einzelne Warnung erstellen, die Sie benachrichtigt, wenn Sicherheitsereignisse ausgelöst werden.

Bevor Sie beginnen

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

Das folgende Beispiel zeigt, wie Sie eine Warnung für das Sicherheitsereignis „Telnet-Protokoll aktiviert“ erstellen. Dadurch wird eine Warnung gesendet, wenn der Telnet-Zugriff für den Remote-Verwaltungszugriff auf den Cluster konfiguriert ist. Mit derselben Methode können Sie Warnungen für alle Sicherheitsereignisse erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
2. Klicken Sie auf der Seite **Alarm-Setup** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Warnung hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für die Warnung ein.
4. Klicken Sie auf **Ressourcen** und wählen Sie den Cluster oder die Cluster aus, für die Sie diese Warnung aktivieren möchten.
5. Klicken Sie auf **Ereignisse** und führen Sie die folgenden Aktionen aus:
   a. Wählen Sie in der Liste „Ereignisschweregrad“ **Warnung** aus.
   b. Wählen Sie in der Liste „Übereinstimmende Ereignisse“ **Telnet-Protokoll aktiviert** aus.
6. Klicken Sie auf **Aktionen** und wählen Sie dann im Feld **Diese Benutzer benachrichtigen** den Namen des Benutzers aus, der die Warn-E-Mail erhalten soll.
7. Konfigurieren Sie auf dieser Seite alle anderen Optionen für die Benachrichtigungshäufigkeit, das Ausgeben von SNMP-Taps und das Ausführen eines Skripts.
8. Klicken Sie auf **Speichern**.

Deaktivieren bestimmter Sicherheitsereignisse

Alle Ereignisse sind standardmäßig aktiviert. Sie können bestimmte Ereignisse deaktivieren, um die Generierung von Benachrichtigungen für Ereignisse zu verhindern, die in Ihrer Umgebung nicht wichtig sind. Sie können deaktivierte Ereignisse aktivieren, wenn Sie weiterhin Benachrichtigungen dafür erhalten möchten.

Bevor Sie beginnen

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 Warnungen werden nicht ausgelöst. Wenn Sie deaktivierte Ereignisse aktivieren, werden die Benachrichtigungen für diese Ereignisse ab dem nächsten Überwachungszyklus generiert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Ereigniseinrichtung**.
2. Deaktivieren oder aktivieren Sie Ereignisse auf der Seite „Ereignis-Setup“, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Ereignisse deaktivieren	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 „Übereinstimmende Ereignisse“ die Sicherheitsereignisse aus, die Sie deaktivieren möchten, und klicken Sie dann auf den Rechtspfeil, um diese Ereignisse in die Spalte „Ereignisse deaktivieren“ zu verschieben. d. Klicken Sie auf **Speichern und schließen**. e. Überprüfen Sie, ob die von Ihnen deaktivierten Ereignisse in der Listenansicht der Seite „Ereigniseinrichtung“ angezeigt werden.
Ereignisse aktivieren	a. Aktivieren Sie in der Liste der deaktivierten Ereignisse das Kontrollkästchen für das bzw. die Ereignisse, die Sie wieder aktivieren möchten. b. Klicken Sie auf **Aktivieren**.

Sicherheitsereignisse

Sicherheitsereignisse liefern Ihnen Informationen zum Sicherheitsstatus von ONTAP -Clustern, Storage Virtual Machines (SVMs) und Volumes basierend auf den im *NetApp Security Hardening Guide für ONTAP 9* definierten Parametern. Diese Ereignisse benachrichtigen Sie über potenzielle Probleme, sodass Sie deren Schweregrad einschätzen und das Problem gegebenenfalls beheben können.

Sicherheitsereignisse werden nach Quelltyp gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe und den Schweregrad. Diese Ereignisse werden in den Cluster- und Speicher-VM-Ereigniskategorien angezeigt.

Verwalten von Sicherungs- und Wiederherstellungsvorgängen

Sie können Backups von Active IQ Unified Manager erstellen und die Wiederherstellungsfunktion verwenden, um das Backup im Falle eines Systemausfalls oder Datenverlusts auf demselben (lokalen) System oder einem neuen (Remote-)System wiederherzustellen.

Abhängig vom Betriebssystem, auf dem Sie Unified Manager installiert haben, und von der Anzahl der verwalteten Cluster und Knoten gibt es drei Sicherungs- und Wiederherstellungsmethoden:

Betriebssystem	Größe der Bereitstellung	Empfohlene Sicherungsmethode
VMware vSphere	Beliebig	VMware-Snapshot der virtuellen Unified Manager-Appliance
Red Hat Enterprise 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 der Unified Manager-Datenbank mit iSCSI-Protokoll

Diese verschiedenen Methoden werden in den folgenden Abschnitten beschrieben.

Sicherung und Wiederherstellung für Unified Manager auf virtueller Appliance

Das Sicherungs- und Wiederherstellungsmodell für Unified Manager bei Installation auf einer virtuellen Appliance besteht darin, ein Image der vollständigen virtuellen Anwendung zu erfassen und wiederherzustellen.

Mit den folgenden Aufgaben können Sie eine Sicherung 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 Datenspeicher nicht auf einem System gehostet wird, auf dem ONTAP -Software ausgeführt wird, befolgen Sie die Richtlinien des Speicheranbieters, um eine Sicherung des VMware-Snapshots zu erstellen.

3. Replizieren Sie die NetApp Snapshot-Kopie oder ein Snapshot-Äquivalent auf einen alternativen Speicher.
4. Löschen Sie den VMware-Snapshot.

Sie sollten mithilfe dieser Aufgaben einen Sicherungszeitplan implementieren, um sicherzustellen, dass die virtuelle Unified Manager-Appliance geschützt ist, falls Probleme auftreten.

Um die VM wiederherzustellen, können Sie den von Ihnen erstellten VMware-Snapshot verwenden, um die VM in den Zustand zum Zeitpunkt der Sicherung zurückzusetzen.

Sichern und Wiederherstellen mithilfe eines MySQL-Datenbank-Dumps

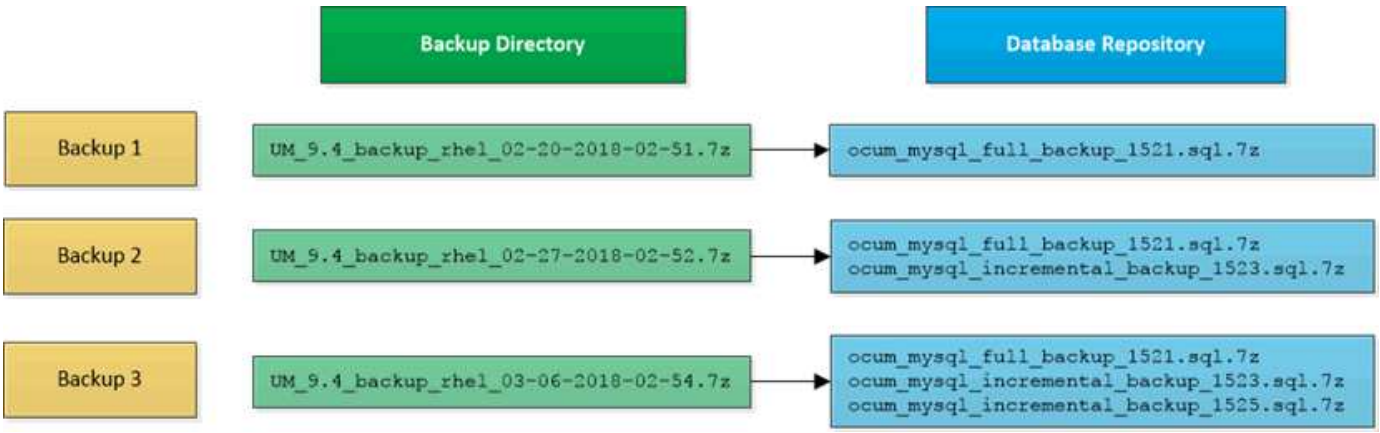
Ein MySQL-Datenbank-Dump-Backup ist eine Kopie der Active IQ Unified Manager -Datenbank und der Konfigurationsdateien, die Sie im Falle eines Systemausfalls oder

Datenverlusts verwenden können. Sie können eine Sicherung so planen, dass sie an ein lokales oder ein Remoteziel geschrieben wird. Es wird dringend empfohlen, einen Remote-Standort außerhalb des Active IQ Unified Manager Hostsystems zu definieren.

Der MySQL-Datenbank-Dump ist der Standard-Sicherungsmechanismus, wenn Unified Manager auf einem Linux- und Windows-Server installiert ist. Wenn Unified Manager jedoch eine große Anzahl von Clustern und Knoten verwaltet oder die Fertigstellung Ihrer MySQL-Sicherungen viele Stunden dauert, können Sie mithilfe von Snapshot-Kopien eine Sicherung durchführen. Diese Funktionalität ist unter Red Hat Enterprise Linux und Windows verfügbar.

Eine Datenbank-Dump-Sicherung besteht aus einer einzelnen Datei im Sicherungsverzeichnis und einer oder mehreren Dateien im Datenbank-Repository-Verzeichnis. Die Datei im Sicherungsverzeichnis ist sehr klein, da sie nur einen Zeiger auf die Dateien im Datenbank-Repository-Verzeichnis enthält, die zum erneuten Erstellen der Sicherung erforderlich sind.

Wenn Sie zum ersten Mal eine Datenbanksicherung erstellen, wird eine einzelne Datei im Sicherungsverzeichnis und eine vollständige Sicherungsdatei im Datenbank-Repository-Verzeichnis erstellt. Wenn Sie das nächste Mal eine Sicherung erstellen, wird eine einzelne Datei im Sicherungsverzeichnis und eine inkrementelle Sicherungsdatei im Datenbank-Repository-Verzeichnis erstellt, die die Unterschiede zur vollständigen Sicherungsdatei enthält. Dieser Vorgang wird fortgesetzt, während Sie weitere Sicherungen erstellen, bis die maximale Aufbewahrungseinstellung erreicht ist, wie in der folgenden Abbildung dargestellt.



Benennen Sie keine der Sicherungsdateien in diesen beiden Verzeichnissen um und entfernen Sie sie auch nicht, da sonst alle nachfolgenden Wiederherstellungsvorgänge fehlschlagen.

Wenn Sie Ihre Sicherungsdateien auf das lokale System schreiben, sollten Sie einen Prozess zum Kopieren der Sicherungsdateien an einen Remote-Speicherort einleiten, damit sie verfügbar sind, falls ein Systemproblem auftritt, das eine vollständige Wiederherstellung erfordert.

Vor Beginn eines Sicherungsvorgangs führt Active IQ Unified Manager eine Integritätsprüfung durch, um sicherzustellen, dass alle erforderlichen Sicherungsdateien und Sicherungsverzeichnisse vorhanden und beschreibbar sind. Außerdem wird überprüft, ob auf dem System genügend Speicherplatz zum Erstellen der Sicherungsdatei vorhanden ist.

Konfigurieren Sie das Ziel und den Zeitplan für Datenbank-Dump-Backups

Sie können die Einstellungen für die Datenbank-Dump-Sicherung von Unified Manager konfigurieren, um den Datenbank-Sicherungspfad, die Aufbewahrungsanzahl und den Sicherungszeitplan festzulegen. Sie können täglich oder wöchentlich geplante

Sicherungen aktivieren. Standardmäßig sind geplante Sicherungen deaktiviert, Sie sollten jedoch einen Sicherungszeitplan festlegen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- An dem Speicherort, den Sie als Sicherungspfad definieren, müssen mindestens 150 GB Speicherplatz verfügbar sein.

  Es wird empfohlen, einen Remote-Standort außerhalb des Unified Manager-Hostsystems zu verwenden.

- Wenn Unified Manager auf einem Linux-System installiert ist und MySQL-Backup verwendet, stellen Sie sicher, dass die folgenden Berechtigungen und Eigentümer für das Backup-Verzeichnis festgelegt sind.

  Berechtigungen: 0750, Eigentum: jboss:maintenance

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

Für die Durchführung einer ersten Sicherung ist mehr Zeit erforderlich als für nachfolgende Sicherungen, da es sich bei der ersten Sicherung um eine vollständige Sicherung handelt. Eine vollständige Sicherung kann über 1 GB groß sein und drei bis vier Stunden dauern. Nachfolgende Sicherungen erfolgen inkrementell und benötigen weniger Zeit.

- Wenn Sie feststellen, dass die Anzahl der inkrementellen Sicherungsdateien für den für Sicherungen zugewiesenen Speicherplatz zu groß ist, können Sie regelmäßig eine vollständige Sicherung durchführen, um die alte Sicherung und ihre inkrementellen Dateien zu ersetzen. Alternativ können Sie mithilfe von Snapshot-Kopien eine Sicherung erstellen.
- Die Sicherung, die während der ersten 15 Tage nach der Hinzufügung eines neuen Clusters erstellt wurde, ist möglicherweise nicht genau genug, um die historischen Leistungsdaten zu erhalten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Datenbanksicherung**.
2. Klicken Sie auf der Seite **Datenbanksicherung** auf **Sicherungseinstellungen**.
3. Konfigurieren Sie die entsprechenden Werte für einen Sicherungspfad, eine Aufbewahrungsanzahl und einen Zeitplan.

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

4. Wählen Sie die Schaltfläche **Täglich geplant** oder **Wöchentlich geplant** und geben Sie dann die Zeitplandetails an.
5. Klicken Sie auf **Übernehmen**.

Datenbank-Dump-Sicherungsdateien werden basierend auf dem Zeitplan erstellt. Sie können die verfügbaren Sicherungsdateien auf der Seite „Datenbanksicherung“ sehen.

Was eine Datenbankwiederherstellung ist

Bei der Wiederherstellung einer MySQL-Datenbank handelt es sich um den Vorgang, bei dem eine vorhandene Unified Manager-Sicherungsdatei auf demselben oder einem

anderen Unified Manager-Server wiederhergestellt wird. Sie führen den Wiederherstellungsvorgang über die Wartungskonsole von Unified Manager aus.

Wenn Sie einen Wiederherstellungsvorgang auf demselben (lokalen) System durchführen und alle Sicherungsdateien lokal gespeichert sind, können Sie die Wiederherstellungsoption unter Verwendung des Standardspeicherorts ausführen. Wenn Sie einen Wiederherstellungsvorgang auf einem anderen Unified Manager-System (einem Remote-System) durchführen, müssen Sie die Sicherungsdatei(en) vom sekundären Speicher auf die lokale Festplatte kopieren, bevor Sie die Wiederherstellungsoption ausführen.

Während des Wiederherstellungsvorgangs werden Sie von Unified Manager abgemeldet. Sie können sich beim System anmelden, nachdem der Wiederherstellungsvorgang abgeschlossen ist.

Wenn Sie das Sicherungsimage auf einem neuen Server wiederherstellen, müssen Sie nach Abschluss des Wiederherstellungsvorgangs ein neues HTTPS-Sicherheitszertifikat generieren und den Unified Manager-Server neu starten. Sie müssen außerdem die SAML-Authentifizierungseinstellungen neu konfigurieren, falls diese erforderlich sind, wenn Sie das Sicherungsimage auf einem neuen Server wiederherstellen.

> Alte Sicherungsdateien können nicht zum Wiederherstellen eines Images verwendet werden, nachdem Unified Manager auf eine neuere Softwareversion aktualisiert wurde. Um Speicherplatz zu sparen, werden alle alten Sicherungsdateien, mit Ausnahme der neuesten Datei, automatisch entfernt, wenn Sie Unified Manager aktualisieren.

Verwandte Informationen

"Generieren eines HTTPS-Sicherheitszertifikats"

"Aktivieren der SAML-Authentifizierung"

"Authentifizierung mit Active Directory oder OpenLDAP"

Wiederherstellen einer MySQL-Datenbanksicherung unter Windows

Im Falle eines Datenverlusts oder einer Datenbeschädigung können Sie die Wiederherstellungsfunktion verwenden, um Unified Manager mit minimalem Verlust in den vorherigen stabilen Zustand zurückzusetzen. Sie können die Unified Manager MySQL-Datenbank mithilfe der Unified Manager-Wartungskonsole auf einem lokalen Windows-System oder einem Remote-Windows-System wiederherstellen.

Bevor Sie beginnen

- Sie müssen über Windows-Administratorrechte verfügen.
- Sie müssen die Unified Manager-Sicherungsdatei und den Inhalt des Datenbank-Repository-Verzeichnisses auf das System kopiert haben, auf dem Sie den Wiederherstellungsvorgang durchführen.

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

- Die Sicherungsdateien müssen `.7z` Typ.

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

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

Schritte

1. Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager nicht die Benutzeroberfläche und konfigurieren Sie keine Cluster, Benutzer oder Authentifizierungseinstellungen, wenn die Installation abgeschlossen ist. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsvorgangs.
2. Melden Sie sich mit 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 im **Hauptmenü** der Wartungskonsole die Nummer für die Option **Backup-Wiederherstellung** ein.
6. Geben Sie die Nummer für die **Wiederherstellung des MySQL-Backups** ein.
7. Geben Sie bei der entsprechenden 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
   ```

   Nachdem der Wiederherstellungsvorgang abgeschlossen ist, können Sie sich bei Unified Manager anmelden.

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

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

Sichern und Wiederherstellen mit NetApp Snapshots

Eine NetApp Snapshot-Kopie erstellt ein zeitpunktbezogenes Image der Unified Manager-Datenbank und der Konfigurationsdateien, das Sie im Falle eines Systemausfalls oder Datenverlusts zur Wiederherstellung verwenden können. Sie planen, dass regelmäßig eine Snapshot-Kopie auf ein Volume auf einem Ihrer ONTAP Cluster geschrieben wird, sodass Sie immer über eine aktuelle Kopie verfügen.

Diese Funktionalität ist für Active IQ Unified Manager, der auf einer virtuellen Appliance installiert ist, nicht verfügbar.

Konfigurieren der Sicherung unter Linux

Wenn Ihr Active IQ Unified Manager auf einem Linux-Computer installiert ist, können Sie

Ihre Sicherung und Wiederherstellung mithilfe von NetApp Snapshots konfigurieren.

Snapshot-Kopien dauern nur sehr wenig Zeit, normalerweise nur wenige Minuten, und die Unified Manager-Datenbank wird für einen sehr kurzen Zeitraum gesperrt, sodass Ihre Installation kaum unterbrochen wird. Das Image benötigt nur minimalen Speicherplatz und verursacht nur einen vernachlässigbaren Leistungsaufwand, da es nur die Änderungen an Dateien seit der letzten Snapshot-Kopie aufzeichnet. Da der Snapshot auf einem ONTAP Cluster erstellt wird, können Sie bei Bedarf andere NetApp -Funktionen wie SnapMirror nutzen, um einen sekundären Schutz zu erstellen.

Vor Beginn eines Sicherungsvorgangs führt Unified Manager eine Integritätsprüfung durch, um sicherzustellen, dass das Zielsystem verfügbar ist.

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

  Wenn Sie beispielsweise ein Backup auf Unified Manager 9.16 erstellt haben, kann das Backup nur auf Unified Manager 9.16-Systemen wiederhergestellt werden.

- Wenn sich die Snapshot-Konfiguration ändert, kann dies dazu führen, dass der Snapshot ungültig wird.

Konfigurieren des Speicherorts für die Snapshot-Kopie

Sie können das Volume, auf dem Snapshot-Kopien gespeichert werden, auf einem Ihrer ONTAP Cluster mithilfe des ONTAP System Manager oder der ONTAP CLI konfigurieren.

Bevor Sie beginnen

Cluster, Speicher-VM und Volume müssen die folgenden Anforderungen erfüllen:

- Clusteranforderungen:
  - ONTAP 9.3 oder höher muss installiert sein
  - Es sollte sich geografisch in der Nähe des Unified Manager-Servers befinden
  - Es kann von Unified Manager überwacht werden, ist aber nicht erforderlich
- Anforderungen an die Speicher-VM:
  - Der Namensschalter und die Namenszuordnung müssen auf die Verwendung von „`files`“ eingestellt sein.
  - Lokale Benutzer, die zur Korrespondenz mit clientseitigen Benutzern erstellt wurden
  - Stellen Sie sicher, dass „Alle Lese-/Schreibzugriffe“ ausgewählt ist.
  - Stellen Sie sicher, dass der Superuser-Zugriff in der Exportrichtlinie auf „any“ eingestellt ist.
  - NFS für NetApp Snapshot für Linux
  - NFSv4 muss auf dem NFS-Server aktiviert sein und die NFSv4-ID-Domäne muss auf dem Client und der Speicher-VM angegeben sein
  - Das Volume sollte mindestens doppelt so groß sein wie das Verzeichnis Unified Manager/opt/netapp/data

    Verwenden Sie den Befehl du -sh /opt/netapp/data/, um die aktuelle Größe zu überprüfen.
- Volumenanforderungen:

- Das Volume sollte mindestens doppelt so groß sein wie das Unified Manager-Verzeichnis /opt/netapp/data
- Der Sicherheitsstil muss auf UNIX eingestellt sein
- Die lokale Snapshot-Richtlinie muss deaktiviert sein
- Die automatische Volume-Größe sollte aktiviert sein
- Das Leistungs-Servicelevel sollte auf eine Richtlinie mit hohen IOPS und geringer Latenz eingestellt werden, z. B. „Extrem“.

Ausführliche Schritte zum Erstellen des NFS-Volumes finden Sie unter "So konfigurieren Sie NFSv4 in ONTAP 9" und die "ONTAP 9 NFS-Konfigurations-Expresshandbuch" .

Geben Sie den Zielspeicherort für Snapshot-Kopien an

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

- Sie müssen über die Root-Benutzeranmeldeinformationen für den Linux-Host verfügen, auf dem Active IQ Unified Manager installiert ist.
- Sie müssen über eine Benutzer-ID und ein Kennwort verfügen, die Sie zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigen.
- Sie müssen über die Cluster-Management-IP-Adresse, den Namen der Speicher-VM, den Namen des Volumes sowie den Benutzernamen und das Kennwort des Speichersystems verfügen.
- Sie müssen das Volume auf dem Active IQ Unified Manager Host gemountet haben und Sie müssen über den Mount-Pfad verfügen.

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 mit dem Namen und Kennwort des Wartungsbenutzers (umadmin) beim System an.
3. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
4. Geben Sie im **Hauptmenü** der Wartungskonsole die Nummer für die Option **Backup-Wiederherstellung** ein.
5. Geben Sie die Nummer für * NetApp Snapshot Backup konfigurieren* ein.
6. Geben Sie die Nummer ein, um NFS zu konfigurieren.
7. Überprüfen Sie die Informationen, die Sie angeben müssen, und geben Sie dann die Nummer für **Backup-Konfigurationsdetails eingeben** ein.
8. Um das Volume zu identifizieren, auf das der Snapshot geschrieben wird, geben Sie die IP-Adresse der Cluster-Management-Schnittstelle, den Namen der Speicher-VM, den Namen des Volumes, den LUN-Namen, den Benutzernamen und das Kennwort des Speichersystems sowie den Mount-Pfad ein.
9. Überprüfen Sie diese Informationen und geben Sie `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 einen Symlink zum neuen Datenbankverzeichnis
- Startet alle Dienste neu

10. Beenden Sie die Wartungskonsole und starten Sie die Active IQ Unified Manager Schnittstelle, um einen Zeitplan für die Snapshot-Kopie zu erstellen, falls Sie dies noch nicht getan haben.

Konfigurieren der Sicherung unter Windows

Active IQ Unified Manager unterstützt die Sicherung und Wiederherstellung mithilfe von NetApp Snapshots auf dem Windows-Betriebssystem mithilfe von LUN unter Verwendung des iSCSI-Protokolls.

Snapshot-basierte Sicherungen können durchgeführt werden, während alle Unified Manager-Dienste ausgeführt werden. Ein konsistenter Status der Datenbank wird als Teil des Snapshots erfasst, da das Backup eine globale Lesesperre auf die gesamte Datenbank setzt, die alle gleichzeitigen Schreibvorgänge verhindert. Damit Ihr unter Windows installiertes Unified Manager-System mithilfe von NetApp Snapshots Sicherungen und Wiederherstellungen durchführen kann, sollten Sie zunächst mithilfe der Wartungskonsole die Unified Manager-Sicherung auf Snapshot-Basis konfigurieren.

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

- ONTAP Cluster konfigurieren
- Konfigurieren des Windows-Hostcomputers

Konfigurieren des Sicherungsspeicherorts für Windows

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

Bevor Sie beginnen

Cluster, Speicher-VM und Volume müssen die folgenden Anforderungen erfüllen:

- Clusteranforderungen:
  - ONTAP 9.3 oder höher muss installiert sein
  - Es sollte sich geografisch in der Nähe des Unified Manager-Servers befinden
  - Es wird von Unified Manager überwacht
- Anforderungen an die Speicher-VM:
  - iSCSI-Konnektivität auf ONTAP Cluster
  - Das iSCSI-Protokoll muss für die konfigurierte Maschine aktiviert sein
  - Sie sollten über ein dediziertes Volume und LUN für die Sicherungskonfiguration verfügen. Das ausgewählte Volume sollte nur eine LUN und sonst nichts enthalten.
  - Die Größe der LUN sollte mindestens doppelt so groß sein wie die Datengröße, die voraussichtlich im 9.9 Active IQ Unified Manager verarbeitet werden kann.

    Dadurch werden auch für das Volumen dieselben Größenanforderungen festgelegt.

- Stellen Sie sicher, dass „Alle Lese-/Schreibzugriffe“ ausgewählt ist.
- Stellen Sie sicher, dass der Superuser-Zugriff in der Exportrichtlinie auf „any“ eingestellt ist.

- Volume- und LUN-Anforderungen:
  - Das Volume sollte mindestens doppelt so groß sein wie das MySQL-Datenverzeichnis von Unified Manager.
  - Der Sicherheitsstil muss auf Windows eingestellt sein
  - Die lokale Snapshot-Richtlinie muss deaktiviert sein
  - Die automatische Volume-Größe sollte aktiviert sein
  - Das Leistungs-Servicelevel sollte auf eine Richtlinie mit hohen IOPS und geringer Latenz eingestellt werden, z. B. „Extrem“.

ONTAP Cluster konfigurieren

Sie müssen einige Vorkonfigurationsschritte auf ONTAP -Clustern durchführen, bevor Sie Active IQ Unified Manager mithilfe einer Snapshot-Kopie auf Windows-Systemen sichern und wiederherstellen können.

Sie können den ONTAP Cluster entweder über die Eingabeaufforderung oder die Benutzeroberfläche des System Managers konfigurieren. Die Konfiguration des ONTAP Clusters umfasst die Konfiguration von Daten-LIFs, die als iSCSI-LIFs der Speicher-VM zugewiesen werden können. Der nächste Schritt besteht darin, eine iSCSI-fähige Speicher-VM über die Benutzeroberfläche des System Managers zu konfigurieren. Sie müssen eine statische Netzwerkroute für diese Speicher-VM konfigurieren, um zu steuern, wie LIFs das Netzwerk für ausgehenden Datenverkehr verwenden.

> Sie sollten über ein dediziertes Volume und eine LUN für die Sicherungskonfiguration verfügen. Das ausgewählte Volume sollte nur eine LUN enthalten. Die Größe der LUN sollte mindestens doppelt so groß sein wie die Datengröße, die voraussichtlich von Active IQ Unified Manager verarbeitet wird.

Sie müssen die folgende Konfiguration durchführen:

Schritte

1. Konfigurieren Sie eine iSCSI-fähige Speicher-VM oder verwenden Sie eine vorhandene Speicher-VM mit derselben Konfiguration.
2. Konfigurieren Sie eine Netzwerkroute für die konfigurierte Speicher-VM.
3. Konfigurieren Sie ein Volume mit entsprechender Kapazität und einer einzelnen LUN darin und stellen Sie sicher, dass das Volume nur für diese LUN reserviert ist.

   > In einem Szenario, in dem die LUN im System Manager erstellt wird, kann das Aufheben der Zuordnung der LUN dazu führen, dass die igroup gelöscht wird und die Wiederherstellung fehlschlägt. Um dieses Szenario zu vermeiden, stellen Sie sicher, dass beim Erstellen einer LUN diese explizit erstellt und nicht gelöscht wird, wenn die Zuordnung der LUN aufgehoben wird.

4. Konfigurieren Sie eine Initiatorgruppe in der Speicher-VM.
5. Konfigurieren Sie einen Portsatz.
6. Integrieren Sie die Igroup mit dem Portset.

7. Ordnen Sie die LUN der igroup zu.

Konfigurieren des Windows-Hostcomputers

Sie müssen Ihren Windows-Hostcomputer konfigurieren, bevor Sie NetApp Snapshot zum Sichern und Wiederherstellen von Active IQ Unified Manager verwenden können. Um den Microsoft iSCSI-Initiator auf einem Windows-Hostcomputer zu starten, geben Sie „`iscsi`“ in die Suchleiste ein und klicken Sie auf **iSCSI-Initiator**.

Bevor Sie beginnen

Sie sollten alle vorherigen Konfigurationen auf dem Hostcomputer bereinigen.

Wenn Sie versuchen, den iSCSI-Initiator bei einer Neuinstallation von Windows zu starten, werden Sie zur Bestätigung aufgefordert. Nach Ihrer Bestätigung 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. Bereinigen Sie alle vorherigen Konfigurationen auf dem Hostcomputer.
2. Entdecken Sie das Zielportal.
3. Stellen Sie eine Verbindung zum Zielportal her.
4. Stellen Sie über Multipath eine Verbindung zum Zielportal her.
5. Entdecken Sie beide LIFs.
6. Ermitteln Sie die im Windows-Computer als Gerät konfigurierte LUN.
7. Konfigurieren Sie die erkannte LUN als neues Volume-Laufwerk in Windows.

Geben Sie den Zielspeicherort für Snapshot-Kopien unter Windows an

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

- Sie müssen über Administratorrechte für den Windows-Host verfügen, auf dem Active IQ Unified Manager installiert ist.
- Sie müssen über eine Benutzer-ID und ein Kennwort verfügen, die Sie zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigen.
- Sie müssen über die Cluster-Management-IP-Adresse, den Namen der Speicher-VM, den Namen des Volumes, den LUN-Namen sowie den Benutzernamen und das Kennwort des Speichersystems verfügen.
- Sie müssen das Volume als Netzwerklaufwerk auf dem Active IQ Unified Manager Host bereitgestellt haben und über das Bereitstellungslaufwerk verfügen.

Schritte

1. Stellen Sie mithilfe von Power Shell eine Verbindung zur IP-Adresse oder zum vollqualifizierten Domänennamen des Active IQ Unified Manager Systems her.
2. Melden Sie sich mit dem Namen und Kennwort des Wartungsbenutzers (umadmin) beim System an.
3. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.

4. Geben Sie im **Hauptmenü** der Wartungskonsole die Nummer für die Option **Backup-Wiederherstellung** ein.
5. Geben Sie die Nummer für * NetApp Snapshot Backup konfigurieren* ein.
6. Geben Sie die Nummer ein, um iSCSI zu konfigurieren.
7. Überprüfen Sie die Informationen, die Sie angeben müssen, und geben Sie dann die Nummer für **Backup-Konfigurationsdetails eingeben** ein.
8. Um das Volume zu identifizieren, auf das der Snapshot geschrieben wird, geben Sie die IP-Adresse der Cluster-Management-Schnittstelle, den Namen der Speicher-VM, den Namen des Volumes, den LUN-Namen, den Benutzernamen und das Kennwort des Speichersystems sowie das Mount-Laufwerk ein.
9. Überprüfen Sie diese Informationen und geben Sie `y` .

   Das System führt die folgenden Aufgaben aus:

   - Speicher-VM ist validiert
   - Volumen ist validiert
   - Laufwerk einbinden und Status wird validiert
   - Existenz und Status der LUN
   - Existenz eines Netzlaufwerks
   - Das Vorhandensein des empfohlenen Speicherplatzes (mehr als das Doppelte des MySQL-Datenverzeichnisses) auf dem bereitgestellten Volume wird überprüft
   - LUN-Pfad, der der dedizierten LUN im Volume entspricht
   - igroup-Name
   - GUID des Volumes, auf dem das Netzlaufwerk eingebunden ist
   - iSCSI-Initiator zur Kommunikation mit ONTAP
10. Beenden Sie die Wartungskonsole und starten Sie die Active IQ Unified Manager Schnittstelle, um einen Zeitplan für Snapshot-Kopien zu erstellen.

Konfigurieren Sie die Sicherung per Snapshot-Kopie von der Wartungskonsole aus

Um mithilfe einer Snapshot-Kopie ein Active IQ Unified Manager -Backup durchzuführen, sollten Sie einige Konfigurationsschritte über die Wartungskonsole ausführen.

Bevor Sie beginnen

Sie sollten über die folgenden Details zu Ihrem System verfügen:

- Cluster-IP-Adresse
- Speicher-VM-Name
- Datenträgername
- LUN-Name
- Mount-Pfad
- Anmeldeinformationen für das Speichersystem

Schritte

1. Greifen Sie auf die Wartungskonsole von Unified Manager zu.

2. Geben Sie 4 ein, um **Backup-Wiederherstellung** auszuwählen.
3. Geben Sie 2 ein, um **Sichern und Wiederherstellen mit NetApp Snapshot** auszuwählen.

> Wenn Sie die Sicherungskonfiguration ändern möchten, geben Sie 3 ein, um * NetApp Snapshot-Sicherungskonfiguration 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 bereitzustellen.
6. Geben Sie den Benutzernamen und das Kennwort für die Wartungskonsole ein und bestätigen Sie anschließend, dass die LUN auf dem Host gemountet ist.

   Der Prozess überprüft dann, ob das von Ihnen angegebene Datenverzeichnis, der LUN-Pfad, die Speicher-VM, die Volumes, die Speicherplatzverfügbarkeit, das Laufwerk usw. korrekt sind. Die im Hintergrund ablaufende Vorgänge sind:

   - Dienste werden gestoppt
   - Das Datenbankverzeichnis wird in den bereitgestellten Speicher verschoben
   - Datenbankverzeichnis wird gelöscht und Symlinks werden erstellt
   - Die Dienste werden neu gestartet. Nachdem die Konfiguration in der Active IQ Unified Manager Schnittstelle abgeschlossen ist, wird der Sicherungstyp in NetApp Snapshot geändert und in der Benutzeroberfläche als Datenbanksicherung (Snapshot-basiert) angezeigt.

Bevor Sie mit einem Sicherungsvorgang beginnen, müssen Sie prüfen, ob es Änderungen an der Snapshot-Konfiguration gibt, da dies dazu führen könnte, dass der Snapshot ungültig wird. Angenommen, Sie haben die Sicherung auf dem Laufwerk G konfiguriert und einen Snapshot erstellt. Sie haben die Sicherung später auf Laufwerk E neu konfiguriert und die Daten werden gemäß der neuen Konfiguration auf Laufwerk E gespeichert. Wenn Sie versuchen, einen Snapshot wiederherzustellen, der erstellt wurde, als er sich auf dem Laufwerk G befand, schlägt dies mit der Fehlermeldung fehl, dass das Laufwerk G nicht existiert.

Definieren Sie einen Sicherungszeitplan für Linux und Windows

Sie können den Zeitplan, nach dem Unified Manager-Snapshot-Kopien erstellt werden, mithilfe der Unified Manager-Benutzeroberfläche konfigurieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Einstellungen zum Erstellen von Snapshot-Kopien über die Wartungskonsole konfiguriert haben, um das Ziel zu identifizieren, an dem die Snapshots erstellt werden.

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

> Die Sicherung, die während der ersten 15 Tage nach der Hinzufügung eines neuen Clusters erstellt wurde, ist möglicherweise nicht genau genug, um die historischen Leistungsdaten zu erhalten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Datenbanksicherung**.

2. Klicken Sie auf der Seite **Datenbanksicherung** auf **Sicherungseinstellungen**.
3. Geben Sie im Feld **Aufbewahrungsanzahl** die maximale Anzahl der Snapshot-Kopien ein, die Sie aufbewahren möchten.

   Der Standardwert für die Aufbewahrungsanzahl ist 10. Die maximale Anzahl von Snapshot-Kopien wird durch die Version der ONTAP -Software 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 **Täglich geplant** oder **Wöchentlich geplant** und geben Sie dann die Zeitplandetails an.
5. Klicken Sie auf **Übernehmen**.

Snapshot-Kopien werden basierend auf dem Zeitplan erstellt. Sie können die verfügbaren Sicherungsdateien auf der Seite „Datenbanksicherung“ sehen.

Aufgrund der Wichtigkeit dieses Volumes und der Snapshots möchten Sie möglicherweise ein oder zwei Warnmeldungen für dieses Volume erstellen, damit Sie benachrichtigt werden, wenn Folgendes eintritt:

- Der Speicherplatz des Volumes ist zu 90 % belegt. Verwenden Sie das Ereignis **Volume Space Full**, um die Warnung einzurichten.

  Sie können dem Volume mithilfe des ONTAP System Manager oder der ONTAP CLI Kapazität hinzufügen, damit der Speicherplatz in der Unified Manager-Datenbank nicht ausgeht.

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

  Sie können ältere Snapshots mit dem ONTAP System Manager oder der ONTAP CLI löschen, sodass immer Platz für neue Snapshot-Kopien vorhanden ist.

Sie konfigurieren Warnungen auf der Seite „Warnungseinrichtung“.

Wiederherstellen von Unified Manager mithilfe von Snapshot-Kopien

Bei Datenverlust oder Datenbeschädigung können Sie Unified Manager mit minimalem Datenverlust in den vorherigen stabilen Zustand zurückversetzen. Sie können die Unified Manager Snapshot-Datenbank mithilfe der Unified Manager-Wartungskonsole auf einem lokalen oder Remote-Betriebssystem wiederherstellen.

Bevor Sie beginnen

- Sie müssen über die Root-Benutzeranmeldeinformationen für den Linux-Host und über Administratorrechte für den Windows-Hostcomputer verfügen, auf dem Unified Manager installiert ist.
- Sie müssen über eine Benutzer-ID und ein Kennwort verfügen, die Sie zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigen.

Die Wiederherstellungsfunktion ist plattform- und versionsspezifisch. Sie können eine Unified Manager-Sicherung nur auf derselben Version von Unified Manager wiederherstellen.

Schritte

1. Stellen Sie eine Verbindung zur IP-Adresse oder zum vollqualifizierten Domänennamen des Unified Manager-Systems her.

- Linux: Secure Shell
- Windows: Power Shell

2. Melden Sie sich mit den Root-Benutzeranmeldeinformationen beim System an.
3. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
4. Geben Sie im **Hauptmenü** der Wartungskonsole 4 für die Option **Backup-Wiederherstellung** ein.
5. Geben Sie 2 ein, um **Sichern und Wiederherstellen mit NetApp Snapshot** auszuwählen.

   Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager nicht die Benutzeroberfläche und konfigurieren Sie keine Cluster, Benutzer oder Authentifizierungseinstellungen, wenn die Installation abgeschlossen ist. Geben Sie 1 ein, um * NetApp Snapshot Backup konfigurieren* auszuwählen, und konfigurieren Sie die Einstellungen für Snapshot-Kopien so, wie sie auf dem Originalsystem sind.

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

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

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

Ändern des Sicherungstyps

Wenn Sie den Sicherungstyp für Ihr Active IQ Unified Manager System ändern möchten, können Sie die Optionen der Wartungskonsole verwenden. Mit der Option * NetApp Snapshot Backup dekonfigurieren* können Sie auf das MySQL-basierte Backup zurückgreifen.

Bevor Sie beginnen

Sie müssen über eine Benutzer-ID und ein Kennwort verfügen, die Sie zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigen.

Schritte

1. Greifen Sie auf die Wartungskonsole zu.
2. Wählen Sie 4 aus dem **Hauptmenü** zum Sichern und Wiederherstellen.
3. Wählen Sie 2 aus dem **Sichern und Wiederherstellen-Menü**.
4. Wählen Sie 4 für * NetApp Snapshot Backup dekonfigurieren*.

   Die ausgeführten Aktionen werden angezeigt: Beenden Sie die Dienste, trennen Sie den symbolischen Link, verschieben Sie die Daten vom Speicher in das Verzeichnis und starten Sie die Dienste anschließend erneut.

Nachdem die Sicherungsmethode geändert wurde, wird der Sicherungsmechanismus von der Snapshot-Kopie auf die standardmäßige MySQL-Sicherung geändert. Diese Änderung wird im Abschnitt „Datenbanksicherung“ der allgemeinen Einstellungen angezeigt.

On-Demand-Backup für Unified Manager

Sie können die Benutzeroberfläche von Active IQ Unified Manager verwenden, um bei Bedarf bei Bedarf ein Backup zu erstellen. Mit der On-Demand-Sicherung können Sie mithilfe der vorhandenen Sicherungsmethode sofort eine Sicherung erstellen. Bei der On-Demand-Sicherung wird nicht zwischen MySQL- oder NetApp Snapshot-basierter Sicherung unterschieden.

Sie können eine On-Demand-Sicherung mit der Schaltfläche **Jetzt sichern** auf der Seite „Datenbanksicherung“ durchführen. Die On-Demand-Sicherung ist nicht von den Zeitplänen abhängig, die Sie für Active IQ Unified Manager konfiguriert haben.

Migrieren einer virtuellen Unified Manager-Appliance auf ein Linux-System

Sie können ein Dump-Backup der MySQL-Datenbank von Unified Manager von einer virtuellen Appliance auf einem Red Hat Enterprise Linux-System wiederherstellen, wenn Sie das Host-Betriebssystem ändern möchten, auf dem Unified Manager ausgeführt wird.

Bevor Sie beginnen

- Auf der virtuellen Appliance:
  - Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
  - Für den Wiederherstellungsvorgang müssen Sie den Namen des Unified Manager-Wartungsbenutzers kennen.
- Auf dem Linux-System:
  - Sie müssen Unified Manager auf einem Linux-Server installiert haben, indem Sie die Anweisungen in"Installieren von Unified Manager auf Linux-Systemen" .
  - Die Version von Unified Manager auf diesem Server muss mit der Version auf der virtuellen Appliance übereinstimmen, von der Sie die Sicherungsdatei verwenden.
  - Starten Sie nach der Installation nicht die Benutzeroberfläche und konfigurieren Sie keine Cluster, Benutzer oder Authentifizierungseinstellungen auf dem Linux-System. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsvorgangs.
  - Sie müssen über die Root-Benutzeranmeldeinformationen für den Linux-Host verfügen.

Diese Schritte beschreiben, wie Sie eine Sicherungsdatei auf der virtuellen Appliance erstellen, die Sicherungsdateien auf Red Hat Enterprise Linux kopieren und dann die Datenbanksicherung auf dem neuen System wiederherstellen.

Schritte

1. Klicken Sie auf der virtuellen Appliance auf **Verwaltung** > **Datenbanksicherung**.
2. Klicken Sie auf der Seite **Datenbanksicherung** auf **Sicherungseinstellungen**.
3. Ändern Sie den Sicherungspfad in /jail/support.
4. Wählen Sie im Abschnitt „Zeitplan“ die Option „Täglich geplant“ aus und geben Sie eine Zeit ein, die einige

Minuten nach der aktuellen Zeit liegt, damit die Sicherung in Kürze erstellt wird.

5. Klicken Sie auf **Übernehmen**.
6. Warten Sie einige Stunden, bis die Sicherung erstellt wurde.

   Eine vollständige Sicherung kann über 1 GB groß sein und drei bis vier Stunden dauern.

7. Melden Sie sich als Root-Benutzer beim Linux-Host an, auf dem Unified Manager installiert ist, und kopieren Sie die Sicherungsdateien mithilfe von SCP von /support auf die virtuelle Appliance.`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 .7z-Sicherungsdatei und alle .7z-Repository-Dateien in das Unterverzeichnis /database-dumps-repo kopiert haben.

8. Stellen Sie die Sicherung in der Eingabeaufforderung 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 des Wiederherstellungsvorgangs bei der Unified Manager-Web-Benutzeroberfläche an.

Sie sollten die folgenden Aufgaben ausführen:

- Generieren Sie ein neues HTTPS-Sicherheitszertifikat und starten Sie den Unified Manager-Server neu.
- Ändern Sie den Sicherungspfad auf die Standardeinstellung für Ihr Linux-System (/data/ocum-backup) oder auf einen neuen Pfad Ihrer Wahl, da auf dem Linux-System kein Pfad /jail/support vorhanden ist.
- Konfigurieren Sie beide Seiten Ihrer Workflow Automation-Verbindung neu, wenn WFA verwendet wird.
- Konfigurieren Sie die SAML-Authentifizierungseinstellungen neu, wenn Sie SAML verwenden.

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

Skripte verwalten

Sie können Skripte verwenden, um mehrere Speicherobjekte in Unified Manager automatisch zu ändern oder zu aktualisieren. Das Skript ist mit einer Warnung verknüpft. Wenn ein Ereignis eine Warnung auslöst, wird das Skript ausgeführt. Sie können benutzerdefinierte Skripte hochladen und deren Ausführung testen, wenn eine Warnung generiert wird.

Die Möglichkeit, Skripte in Unified Manager hochzuladen und auszuführen, ist standardmäßig aktiviert. Wenn Ihre Organisation diese Funktion aus Sicherheitsgründen nicht zulassen möchte, können Sie sie unter **Speicherverwaltung** > **Funktionseinstellungen** deaktivieren.

So funktionieren Skripte mit Warnungen

Sie können Ihrem Skript eine Warnung zuordnen, sodass das Skript ausgeführt wird,

wenn für ein Ereignis in Unified Manager eine Warnung ausgelöst wird. Sie können die Skripts verwenden, um Probleme mit Speicherobjekten zu beheben oder zu ermitteln, welche Speicherobjekte die Ereignisse generieren.

Wenn für ein Ereignis in Unified Manager eine Warnung generiert wird, wird eine Warn-E-Mail an die angegebenen Empfänger gesendet. Wenn Sie eine Warnung mit einem Skript verknüpft haben, wird das Skript ausgeführt. Die Einzelheiten zu den an das Skript übergebenen Argumenten können Sie der Warn-E-Mail entnehmen.

Wenn Sie ein benutzerdefiniertes Skript erstellt und es 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 standardmäßig auf der Seite „Verwaltungsaktionen“ oder im Unified Manager-Dashboard 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 und zugehörige Ereignisinformationen sammeln oder Speicherobjekte ändern.

Beispiel zum Abrufen von Argumenten aus Skripten

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

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

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

Skripts hinzufügen

Sie können in Unified Manager Skripte hinzufügen und die Skripte mit Warnungen verknüpfen. Diese Skripte werden automatisch ausgeführt, wenn eine Warnung generiert wird, und ermöglichen es Ihnen, Informationen zu Speicherobjekten zu erhalten, für die das Ereignis generiert wird.

Bevor Sie beginnen

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

  - Für Perl-Skripte muss Perl auf dem Unified Manager-Server installiert sein. Bei VMware-Installationen wird Perl 5 standardmäßig installiert und Skripte unterstützen nur das, was Perl 5 unterstützt. Wenn Perl nach Unified Manager installiert wurde, müssen Sie den Unified Manager-Server neu starten.
  - Für PowerShell-Skripte 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 Warnskripts zu verfolgen, müssen Sie sicherstellen, dass die Protokolldateien nicht irgendwo im Installationsordner von Unified Manager erstellt werden.

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

Sie können benutzerdefinierte Skripte hochladen und Ereignisdetails zur Warnung sammeln.

> Wenn diese Funktion in der Benutzeroberfläche nicht verfügbar ist, liegt das daran, dass Ihr Administrator sie deaktiviert hat. Bei Bedarf können Sie diese Funktion unter **Speicherverwaltung** > **Funktionseinstellungen** aktivieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Skripte**.
2. Klicken Sie auf der Seite **Skripte** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Skript hinzufügen** auf **Durchsuchen**, um Ihre Skriptdatei auszuwählen.
4. Geben Sie eine Beschreibung für das ausgewählte Skript ein.
5. Klicken Sie auf **Hinzufügen**.

Skripte löschen

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

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Das Skript darf nicht mit einer Warnung verknüpft sein.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Skripte**.
2. Wählen Sie auf der Seite **Skripte** das Skript aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang mit einem Klick auf **Ja**.

Testskriptausführung

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 in Unified Manager hochgeladen haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Skripte**.
2. Fügen Sie auf der Seite „Skripte“ Ihr Testskript hinzu.
3. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
4. Führen Sie auf der Seite **Alarm-Setup** eine der folgenden Aktionen aus:

Zu…	Machen Sie Folgendes…
Hinzufügen einer Benachrichtigung	a. Klicken Sie auf **Hinzufügen**. b. Ordnen Sie im Abschnitt „Aktionen“ die Warnung Ihrem Testskript zu.
Bearbeiten einer Benachrichtigung	a. Wählen Sie eine Warnung aus und klicken Sie dann auf **Bearbeiten**. b. Ordnen Sie im Abschnitt „Aktionen“ die Warnung Ihrem Testskript zu.

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

   Das Skript wird mit dem Argument „-test“ ausgeführt und eine Benachrichtigungswarnung wird an die E-Mail-Adressen gesendet, die beim Erstellen der Warnung angegeben wurden.

Verwalten und Überwachen von Gruppen

Sie können in Unified Manager Gruppen erstellen, um Speicherobjekte zu verwalten.

Gruppen verstehen

Sie können in Unified Manager Gruppen erstellen, um Speicherobjekte zu verwalten. Wenn Sie sich mit den Konzepten von Gruppen auskennen und wissen, wie Sie durch Gruppenregeln Speicherobjekte zu einer Gruppe hinzufügen können, können Sie die

Speicherobjekte in Ihrer Umgebung besser verwalten.

Was eine Gruppe ist

Eine Gruppe ist eine dynamische Sammlung heterogener Speicherobjekte (Cluster, SVMs oder Volumes). Sie können in Unified Manager Gruppen erstellen, um eine Reihe von Speicherobjekten einfach zu verwalten. Die Mitglieder einer Gruppe können sich ändern, abhängig von den Speicherobjekten, 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 mehr als eine Gruppenregel zuordnen.
- Jede Gruppe kann mehrere Arten von Speicherobjekten wie Cluster, SVMs oder Volumes enthalten.
- Speicherobjekte werden einer Gruppe dynamisch hinzugefügt, je nachdem, wann eine Gruppenregel erstellt wird oder wann Unified Manager einen Überwachungszyklus abschließt.
- Sie können Aktionen gleichzeitig auf alle Speicherobjekte in einer Gruppe anwenden, beispielsweise Schwellenwerte für Volumes festlegen.

So funktionieren Gruppenregeln für Gruppen

Eine Gruppenregel ist ein Kriterium, das Sie definieren, um die Aufnahme von Speicherobjekten (Volumes, Cluster oder SVMs) in eine bestimmte Gruppe zu ermöglichen. Sie können Bedingungsgruppen oder Bedingungen verwenden, um Gruppenregeln für eine Gruppe zu definieren.

- Sie müssen einer Gruppe eine Gruppenregel zuordnen.
- Sie müssen einer Gruppenregel einen Objekttyp zuordnen. Einer Gruppenregel ist nur ein Objekttyp zugeordnet.
- Speicherobjekte werden nach jedem Überwachungszyklus oder beim Erstellen, Bearbeiten oder Löschen einer Regel zur Gruppe hinzugefügt oder daraus 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.

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 festzulegen, welche Speicherobjekte in die Gruppe aufgenommen werden.

Bedingungen innerhalb einer Bedingungsgruppe werden mit einem logischen UND ausgeführt. Alle Bedingungen einer Bedingungsgruppe müssen erfüllt sein. Wenn Sie eine Gruppenregel erstellen oder ändern, wird eine Bedingung erstellt, die nur diejenigen 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 in eine Gruppe aufzunehmenden Speicherobjekte einschränken möchten.

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

Speicherobjekttyp	Anwendbare Operanden
Volumen	• Objektname • Name des besitzenden Clusters • Name des besitzenden SVM • Anmerkungen
SVM	• Objektname • Name des besitzenden Clusters • Anmerkungen
Cluster	• Objektname • Anmerkungen

Wenn Sie eine Annotation als Operand für ein beliebiges Speicherobjekt auswählen, ist der Operator „Ist“ verfügbar. Für alle anderen Operanden können Sie als Operator entweder „Ist“ oder „Enthält“ auswählen.

- Operand

  Die Liste der Operanden im Unified Manager ändert sich je nach ausgewähltem Objekttyp. Die Liste enthält den Objektnamen, den Namen des besitzenden Clusters, den Namen des besitzenden SVM und Anmerkungen, die Sie in Unified Manager definieren.

- Operator

  Die Liste der Operatoren ändert sich basierend auf dem ausgewählten Operanden für eine Bedingung. Die in Unified Manager unterstützten Operatoren sind „Ist“ und „Enthält“.

  Wenn Sie den Operator „Ist“ auswählen, wird die Bedingung auf eine genaue Übereinstimmung des Operandenwerts mit dem für den ausgewählten Operanden bereitgestellten Wert geprüft.

  Wenn Sie den Operator „Enthält“ auswählen, wird die Bedingung ausgewertet, um eines der folgenden Kriterien zu erfüllen:

  ◦ Der Operandenwert entspricht genau dem für den ausgewählten Operanden angegebenen Wert.
  ◦ Der Operandenwert enthält den für den ausgewählten Operanden bereitgestellten Wert

- Wert

  Das Wertefeld ändert sich je nach ausgewähltem Operanden.

Beispiel einer Gruppenregel mit Bedingungen

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

- Name enthält „`vol`“

- Der SVM-Name lautet „data_svm“

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

Bedingungsgruppen

Bedingungsgruppen werden mithilfe eines logischen ODER ausgeführt und dann auf Speicherobjekte angewendet. Um in eine Gruppe aufgenommen zu werden, müssen die Speicherobjekte eine der Bedingungsgruppen erfüllen. Die Lagerobjekte aller Konditionsgruppen werden zusammengefasst. Mithilfe von Bedingungsgruppen können Sie den Umfang der in eine Gruppe aufzunehmenden Speicherobjekte erweitern.

Beispiel einer Gruppenregel mit Bedingungsgruppen

Betrachten Sie zwei Bedingungsgruppen für ein Volume, wobei jede Gruppe die folgenden zwei Bedingungen enthält:

- Bedingungsgruppe 1
  - Name enthält „vol“
  - Der SVM-Name lautet „data_svm“. Bedingungsgruppe 1 wählt alle Volumes aus, deren Namen „vol“ enthalten und die auf SVMs mit dem Namen „data_svm“ gehostet werden.
- Bedingungsgruppe 2
  - Name enthält „vol“
  - Der Annotationswert von data-priority ist „critical“. Bedingungsgruppe 2 wählt alle Volumes aus, deren Namen „vol“ enthalten und die mit dem Annotationswert data-priority als „critical“ annotiert sind.

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

- Alle Volumes, deren Namen „vol“ enthalten und die auf der SVM mit dem Namen „data_svm“ gehostet werden.
- Alle Datenträger, deren Namen „vol“ enthalten und die mit dem Datenprioritätsannotationswert „critical“ annotiert sind.

So funktionieren Gruppenaktionen bei Speicherobjekten

Eine Gruppenaktion ist ein Vorgang, der für alle Speicherobjekte in einer Gruppe ausgeführt wird. Sie können beispielsweise die Aktion „Volume-Schwellenwertgruppe“ so konfigurieren, dass die Volume-Schwellenwerte aller Volumes in einer Gruppe gleichzeitig geändert werden.

Gruppen unterstützen eindeutige Gruppenaktionstypen. Sie können eine Gruppe mit nur einem Gruppenaktionstyp für den Volume-Integritätsschwellenwert haben. Sie können jedoch für dieselbe Gruppe einen anderen Gruppenaktionstyp konfigurieren, sofern verfügbar. Der Rang einer Gruppenaktion bestimmt die Reihenfolge, in der die Aktion auf Speicherobjekte angewendet wird. Die Detailseite eines Speicherobjekts bietet Informationen darüber, welche Gruppenaktion auf das Speicherobjekt angewendet wird.

Beispiel für einzigartige Gruppenaktionen

Stellen Sie sich ein Volume A vor, das zu den Gruppen G1 und G2 gehört. Für diese Gruppen sind die folgenden Volume-Integritätsschwellenwert-Gruppenaktionen konfiguriert:

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

Der `Change_capacity_threshold` Gruppenaktionen haben immer Vorrang vor der `Change_snapshot_copies` Gruppenaktion und wird auf Volume A angewendet. Wenn Unified Manager einen Überwachungszyklus abschließt, werden die mit dem Integritätsschwellenwert verbundenen Ereignisse von Volume A gemäß der `Change_capacity_threshold` Gruppenaktion. Sie können für die Gruppenaktionen G1 und G2 keinen anderen Volumenschwellenwerttyp konfigurieren.

Gruppen hinzufügen

Sie können Gruppen erstellen, um Cluster, Volumes und virtuelle Speichermaschinen (SVMs) zur einfacheren Verwaltung zu kombinieren.

Bevor Sie beginnen

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

Sie können Gruppenregeln definieren, um Mitglieder zur Gruppe hinzuzufügen oder daraus zu entfernen und um 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 bearbeiten

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

Bevor Sie beginnen

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

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 löschen

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

Bevor Sie beginnen

- Keines der Speicherobjekte (Cluster, SVMs oder Volumes) darf einer Gruppenregel zugeordnet sein, die der Gruppe zugeordnet ist, die Sie löschen möchten.
- 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 mit einem Klick auf **Ja**.

   Durch das Löschen einer Gruppe werden die mit der Gruppe verknüpften Gruppenaktionen nicht gelöscht. Die Zuordnung dieser Gruppenaktionen wird jedoch aufgehoben, nachdem die Gruppe gelöscht wurde.

Gruppenregeln hinzufügen

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

Bevor Sie beginnen

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

Aktuell überwachte Speicherobjekte 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 beides zu erstellen:

Erstellen….	Machen Sie Folgendes…
Eine Bedingung	a. Wählen Sie einen Operanden aus der Operandenliste aus. b. Wählen Sie als Operator entweder **Enthält** oder **Ist** aus. c. Geben Sie einen Wert ein oder wählen Sie einen Wert aus der verfügbaren Liste aus.
Eine Bedingungsgruppe	a. Klicken Sie auf **Bedingungsgruppe hinzufügen** b. Wählen Sie einen Operanden aus der Operandenliste aus. c. Wählen Sie als Operator entweder **Enthält** oder **Ist** aus. d. Geben Sie einen Wert ein oder wählen Sie einen Wert aus der verfügbaren Liste 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 zum Erstellen einer Gruppenregel

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

Schritte

1. Geben Sie einen Namen für die Gruppenregel an.
2. Wählen Sie als Objekttyp „Storage Virtual Machine“ (SVM) aus.
3. Wählen Sie eine Gruppe aus der Gruppenliste aus.
4. Wählen Sie im Abschnitt „Bedingungen“ als Operanden „**Objektname**“ aus.
5. Wählen Sie als Operator **Enthält** aus.
6. Geben Sie den Wert als `svm_data` .
7. Klicken Sie auf **Bedingungsgruppe hinzufügen**.
8. Wählen Sie als Operand **Objektname**.
9. Wählen Sie als Operator **Enthält** aus.
10. Geben Sie den Wert als `vol` .
11. Klicken Sie auf **Bedingung hinzufügen**.
12. Wiederholen Sie die Schritte 8 bis 10, indem Sie in Schritt 8 **data-priority** als Operanden, in Schritt 9 **Is** als Operator und in Schritt 10 **critical** als Wert auswählen.
13. Klicken Sie auf **Hinzufügen**, um die Bedingung für die Gruppenregel zu erstellen.

Gruppenregeln bearbeiten

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

Bevor Sie beginnen

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

Schritte

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

   Sie können den Zielobjekttyp für eine Gruppenregel nicht ändern.

4. Klicken Sie auf **Speichern**.

Gruppenregeln löschen

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

Bevor Sie beginnen

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

Wenn eine Gruppenregel gelöscht wird, werden die zugehörigen 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 mit einem Klick auf **Ja**.

Gruppenaktionen hinzufügen

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

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenaktionen** auf **Hinzufügen**.

3. Geben Sie im Dialogfeld **Gruppenaktion hinzufügen** 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 und ermöglicht Ihnen, den ausgewählten Aktionstyp mit den erforderlichen Parametern zu konfigurieren.

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

Gruppenaktionen bearbeiten

Sie können die Gruppenaktionsparameter bearbeiten, die Sie in Unified Manager konfiguriert haben, z. B. den Gruppenaktionsnamen, die Beschreibung, den zugehörigen Gruppennamen und die Parameter des Aktionstyps.

Bevor Sie beginnen

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

Schritte

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

Konfigurieren von Volume-Integritätsschwellenwerten für Gruppen

Sie können Volume-Integritätsschwellenwerte auf Gruppenebene für Kapazität, Snapshot-Kopien, Qtree-Kontingente, Wachstum und Inodes konfigurieren.

Bevor Sie beginnen

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

Der Gruppenaktionstyp „Volume-Integritätsschwelle“ 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 der Dropdown-Liste **Gruppe** eine Gruppe aus, für die Sie eine Gruppenaktion konfigurieren möchten.
5. Wählen Sie **Aktionstyp** als Schwellenwert für die Volumeintegrität aus.
6. Wählen Sie die Kategorie aus, für die Sie den Schwellenwert festlegen möchten.

7. Geben Sie die erforderlichen Werte für den Integritätsschwellenwert ein.
8. Klicken Sie auf **Hinzufügen**.

Gruppenaktionen löschen

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

Bevor Sie beginnen

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

Wenn Sie die Gruppenaktion für den Volume-Integritätsschwellenwert löschen, werden globale Schwellenwerte auf die Speicherobjekte in dieser Gruppe angewendet. Auf Objektebene festgelegte Integritätsschwellenwerte für das Speicherobjekt sind hiervon nicht betroffen.

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 mit einem Klick auf **Ja**.

Gruppenaktionen neu anordnen

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

Bevor Sie beginnen

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

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

Schritte

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

Priorisieren Sie Speicherobjektereignisse mithilfe von Anmerkungen

Sie können Anmerkungsregeln erstellen und auf Speicherobjekte anwenden, sodass Sie

diese Objekte basierend auf der Art der angewendeten Anmerkung und ihrer Priorität identifizieren und filtern können.

Erfahren Sie mehr über Anmerkungen

Wenn Sie die Konzepte zu Anmerkungen verstehen, können Sie die Ereignisse im Zusammenhang mit den Speicherobjekten in Ihrer Umgebung besser verwalten.

Was sind Anmerkungen

Eine Anmerkung ist eine Textzeichenfolge (der Name), die einer anderen Textzeichenfolge (dem Wert) zugewiesen wird. Jedes Annotation-Name-Wert-Paar kann mithilfe von Annotationsregeln dynamisch mit Speicherobjekten verknüpft werden. Wenn Sie Speicherobjekte mit vordefinierten Anmerkungen verknüpfen, können Sie die damit verbundenen Ereignisse filtern und anzeigen. Sie können Anmerkungen auf Cluster, Volumes und virtuelle Speichermaschinen (SVMs) anwenden.

Jeder Annotationsname kann mehrere Werte haben; jedes Name-Wert-Paar kann über Regeln mit einem Speicherobjekt verknüpft werden.

Sie können beispielsweise eine Annotation mit dem Namen „data-center“ mit den Werten „Boston“ und „Canada“ erstellen. Anschließend können Sie die Annotation „`data-center`“ mit dem Wert „`Boston`“ auf Volume v1 anwenden. Wenn für ein beliebiges Ereignis auf einem Volume v1, das mit „data-center“ gekennzeichnet ist, eine Warnung generiert wird, gibt die generierte E-Mail den Speicherort des Volumes, „Boston“, an, sodass Sie das Problem priorisieren und beheben können.

So funktionieren Anmerkungsregeln in Unified Manager

Eine Annotationsregel ist ein von Ihnen definiertes Kriterium zum Annotieren von Speicherobjekten (Volumes, Clustern oder Storage Virtual Machines (SVMs)). Sie können zum Definieren von Anmerkungsregeln entweder Bedingungsgruppen oder Bedingungen verwenden.

- Sie müssen einer Anmerkung eine Anmerkungsregel zuordnen.
- Sie müssen einer Anmerkungsregel einen Objekttyp zuordnen. Einer Anmerkungsregel kann nur ein Objekttyp zugeordnet werden.
- Unified Manager fügt nach jedem Überwachungszyklus oder beim Erstellen, Bearbeiten, Löschen oder Neuordnen einer Regel Anmerkungen zu Speicherobjekten hinzu oder entfernt sie.
- Eine Anmerkungsregel kann eine oder mehrere Bedingungsgruppen haben und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben.
- Speicherobjekte können mehrere Anmerkungen haben. Eine Annotationsregel für eine bestimmte Annotation kann in den Regelbedingungen auch unterschiedliche Annotationen verwenden, um bereits annotierten Objekten eine weitere Annotation hinzuzufügen.

Bedingungen

Sie können mehrere Bedingungsgruppen erstellen und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben. Sie können alle definierten Bedingungsgruppen in einer Annotationsregel einer Annotation anwenden, um Speicherobjekte zu annotieren.

Bedingungen innerhalb einer Bedingungsgruppe werden mit einem logischen UND ausgeführt. Alle Bedingungen einer Bedingungsgruppe müssen erfüllt sein. Wenn Sie eine Anmerkungsregel erstellen oder ändern, wird eine Bedingung erstellt, die nur diejenigen Speicherobjekte anwendet, auswählt und mit Anmerkungen versieht, die alle Bedingungen in der Bedingungsgruppe erfüllen. Sie können mehrere Bedingungen innerhalb einer Bedingungsgruppe verwenden, wenn Sie den Umfang der zu kommentierenden Speicherobjekte eingrenzen möchten.

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

Speicherobjekttyp	Anwendbare Operanden
Volumen	• Objektname • Name des besitzenden Clusters • Name des besitzenden SVM • Anmerkungen
SVM	• Objektname • Name des besitzenden Clusters • Anmerkungen
Cluster	• Objektname • Anmerkungen

Wenn Sie eine Annotation als Operand für ein beliebiges Speicherobjekt auswählen, ist der Operator „Ist“ verfügbar. Für alle anderen Operanden können Sie als Operator entweder „Ist“ oder „Enthält“ auswählen. Wenn Sie den Operator „Ist“ auswählen, wird die Bedingung auf eine genaue Übereinstimmung des Operandenwerts mit dem für den ausgewählten Operanden bereitgestellten Wert ausgewertet. Wenn Sie den Operator „Enthält“ auswählen, wird die Bedingung ausgewertet, um eines der folgenden Kriterien zu erfüllen:

- Der Operandenwert entspricht genau dem Wert des ausgewählten Operanden.
- Der Operandenwert enthält den für den ausgewählten Operanden bereitgestellten Wert.

Beispiel einer Annotationsregel mit Bedingungen

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

- Name enthält „`vol`“
- Der SVM-Name lautet „`data_svm`“

Diese Annotationsregel versieht alle Volumes, deren Namen „`vol`“ enthalten und die auf SVMs mit dem Namen „`data_svm`“ gehostet werden, mit der ausgewählten Annotation und dem Annotationstyp.

Bedingungsgruppen

Bedingungsgruppen werden mithilfe eines logischen ODER ausgeführt und dann auf Speicherobjekte angewendet. Um annotiert zu werden, müssen die Speicherobjekte die Anforderungen einer der Bedingungsgruppen erfüllen. Die Speicherobjekte, die die Bedingungen aller Bedingungsgruppen erfüllen,

werden annotiert. Mithilfe von Bedingungsgruppen können Sie den Umfang der zu annotierenden Speicherobjekte erweitern.

Beispiel einer Annotationsregel mit Bedingungsgruppen

Betrachten Sie eine Anmerkungsregel mit zwei Bedingungsgruppen für ein Volume. Jede Gruppe enthält die folgenden zwei Bedingungen:

- Bedingungsgruppe 1
  - Name enthält „`vol`“
  - Der SVM-Name lautet „`data_svm`“. Diese Bedingungsgruppe kommentiert alle Volumes, deren Namen „`vol`“ enthalten und die auf SVMs mit dem Namen „`data_svm`“ gehostet werden.
- Bedingungsgruppe 2
  - Name enthält „`vol`“
  - Der Annotationswert von data-priority ist „`critical`“. Diese Bedingungsgruppe annotiert alle Volumes, deren Namen „`vol`“ enthalten und die mit dem Annotationswert data-priority als „`critical`“ annotiert sind.

Wenn eine Annotationsregel, die diese beiden Bedingungsgruppen enthält, auf Speicherobjekte angewendet wird, werden die folgenden Speicherobjekte annotiert:

- Alle Volumes, deren Namen „`vol`“ enthalten und die auf SVM mit dem Namen „`data_svm`“ gehostet werden.
- Alle Datenträger, deren Name „`vol`“ enthält und die mit dem Datenprioritätsannotationswert „`critical`“ annotiert sind.

Beschreibung vordefinierter Annotationswerte

Datenpriorität ist eine vordefinierte Anmerkung mit den Werten „Missionskritisch“, „Hoch“ und „Niedrig“. Mit diesen Werten können Sie Speicherobjekte basierend auf der Priorität der darin enthaltenen Daten mit Anmerkungen versehen. Sie können die vordefinierten Anmerkungswerte weder bearbeiten noch löschen.

- **Datenpriorität:Missionskritisch**

  Diese Annotation wird auf Speicherobjekte angewendet, die unternehmenskritische Daten enthalten. Beispielsweise können Objekte, die Produktionsanwendungen enthalten, als unternehmenskritisch betrachtet werden.

- **Datenpriorität: Hoch**

  Diese Annotation wird auf Speicherobjekte angewendet, die Daten mit hoher Priorität enthalten. Beispielsweise können Objekte, die Geschäftsanwendungen hosten, als Objekte mit hoher Priorität betrachtet werden.

- **Datenpriorität: Niedrig**

  Diese Annotation wird auf Speicherobjekte angewendet, die Daten mit niedriger Priorität enthalten. Beispielsweise können Objekte, die sich auf sekundären Speicherorten wie Sicherungs- und Spiegelzielen befinden, eine niedrige Priorität haben.

Anmerkungen dynamisch hinzufügen

Wenn Sie benutzerdefinierte Anmerkungen erstellen, verknüpft Unified Manager mithilfe von Regeln dynamisch Cluster, virtuelle Speichermaschinen (SVMs) und Volumes mit den Anmerkungen. Diese Regeln ordnen die Anmerkungen automatisch Speicherobjekten zu.

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **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 **Annotationswerte** auf **Hinzufügen**, um der Annotation Werte hinzuzufügen.
5. Klicken Sie auf **Speichern**.

Hinzufügen von Werten zu Anmerkungen

Sie können Anmerkungen Werte hinzufügen und dann Speicherobjekte mit einem bestimmten Name-Wert-Paar aus Anmerkungen verknüpfen. Durch das Hinzufügen von Werten zu Anmerkungen können Sie Speicherobjekte effektiver verwalten.

Bevor Sie beginnen

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

Sie können vordefinierten Anmerkungen keine Werte hinzufügen.

Schritte

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

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

4. Klicken Sie auf **Hinzufügen**.

Anmerkungen löschen

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

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungen** die Anmerkung aus, die Sie löschen möchten.

   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 Warndialogfeld auf **Ja**, um den Löschvorgang zu bestätigen.

Anzeigen der Anmerkungsliste und Details

Sie können die Liste der Anmerkungen anzeigen, die dynamisch mit Clustern, Volumes und virtuellen Speichermaschinen (SVMs) verknüpft sind. Sie können auch Details wie die Beschreibung, den Ersteller, das Erstellungsdatum, Werte, Regeln und die mit der Anmerkung verknüpften Objekte anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungen** auf den Namen der Anmerkung, um die zugehörigen Details anzuzeigen.

Werte aus Anmerkungen löschen

Sie können mit benutzerdefinierten Anmerkungen verknüpfte Werte löschen, wenn dieser Wert nicht mehr auf die Anmerkung zutrifft.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Der Annotationswert darf keinen Annotationsregeln oder Gruppenregeln zugeordnet sein.

Sie können keine Werte aus vordefinierten Anmerkungen löschen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **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 Werteliste der ausgewählten Annotation angezeigt.

Erstellen von Anmerkungsregeln

Sie können Anmerkungsregeln erstellen, die Unified Manager verwendet, um Speicherobjekte wie Volumes, Cluster oder Storage Virtual Machines (SVMs) dynamisch zu annotieren.

Bevor Sie beginnen

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

Speicherobjekte, die derzeit überwacht werden, werden mit Anmerkungen versehen, sobald die Anmerkungsregel erstellt wird. Neue Objekte werden erst nach Abschluss des Überwachungszyklus annotiert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Annotationsregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkungsregel hinzufügen** einen Namen für die Anmerkungsregel an.
4. Wählen Sie im Feld **Zielobjekttyp** den Typ des Speicherobjekts aus, das Sie mit Anmerkungen versehen möchten.
5. Wählen Sie in den Feldern **Anmerkung anwenden** die Anmerkung und den Anmerkungswert aus, die Sie verwenden möchten.
6. Führen Sie im Abschnitt „Bedingungen“ die entsprechende Aktion aus, um eine Bedingung, eine Bedingungsgruppe oder beides zu erstellen:

Erstellen…	Machen Sie Folgendes…
Eine Bedingung	a. Wählen Sie einen Operanden aus der Operandenliste aus. b. Wählen Sie als Operator entweder **Enthält** oder **Ist** aus. c. Geben Sie einen Wert ein oder wählen Sie einen Wert aus der verfügbaren Liste aus.
Eine Bedingungsgruppe	a. Klicken Sie auf **Bedingungsgruppe hinzufügen**. b. Wählen Sie einen Operanden aus der Operandenliste aus. c. Wählen Sie als Operator entweder **Enthält** oder **Ist** aus. d. Geben Sie einen Wert ein oder wählen Sie einen Wert aus der verfügbaren Liste aus. e. Klicken Sie auf **Bedingung hinzufügen**, um bei Bedarf weitere Bedingungen zu erstellen, und wiederholen Sie die Schritte a bis d für jede Bedingung.

7. Klicken Sie auf **Hinzufügen**.

Beispiel für das Erstellen einer Anmerkungsregel

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

Schritte

1. Geben Sie einen Namen für die Anmerkungsregel an.
2. Wählen Sie als Zielobjekttyp „Storage Virtual Machine“ (SVM) aus.
3. Wählen Sie eine Anmerkung aus der Anmerkungsliste aus und geben Sie einen Wert an.
4. Wählen Sie im Abschnitt „Bedingungen“ als Operanden „**Objektname**“ aus.
5. Wählen Sie als Operator **Enthält** aus.
6. Geben Sie den Wert als `svm_data` .
7. Klicken Sie auf **Bedingungsgruppe hinzufügen**.
8. Wählen Sie als Operand **Objektname**.
9. Wählen Sie als Operator **Enthält** aus.
10. Geben Sie den Wert als `vol` .
11. Klicken Sie auf **Bedingung hinzufügen**.
12. Wiederholen Sie die Schritte 8 bis 10, indem Sie in Schritt 8 **data-priority** als Operanden, in Schritt 9 **Is** als Operator und in Schritt 10 **mission-critical** als Wert auswählen.
13. Klicken Sie auf **Hinzufügen**.

Fügen Sie einzelnen Speicherobjekten manuell Anmerkungen hinzu

Sie können ausgewählte Volumes, Cluster und SVMs manuell mit Anmerkungen versehen, ohne Anmerkungsregeln zu verwenden. Sie können ein einzelnes Speicherobjekt oder mehrere Speicherobjekte mit Anmerkungen versehen und die erforderliche Name-Wert-Paarkombination für die Anmerkung angeben.

Bevor Sie beginnen

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

Schritte

1. Navigieren Sie zu den Speicherobjekten, die Sie mit Anmerkungen versehen möchten:

So fügen Sie eine Anmerkung hinzu zu…	Machen Sie Folgendes…
Cluster	a. Klicken Sie auf **Speicher** > **Cluster**. b. Wählen Sie einen oder mehrere Cluster aus.
Bände	a. Klicken Sie auf **Speicher** > **Volumes**. b. Wählen Sie ein oder mehrere Volumes aus.
SVMs	a. Klicken Sie auf **Speicher** > **SVMs**. b. Wählen Sie eine oder mehrere SVMs aus.

2. Klicken Sie auf **Kommentieren** und wählen Sie ein Name-Wert-Paar aus.
3. Klicken Sie auf **Übernehmen**.

Bearbeiten von Anmerkungsregeln

Sie können Anmerkungsregeln bearbeiten, um die Bedingungsgruppen und Bedingungen innerhalb der Bedingungsgruppe zu ändern und so Anmerkungen zu Speicherobjekten hinzuzufügen oder daraus zu entfernen.

Bevor Sie beginnen

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

Anmerkungen werden von Speicherobjekten getrennt, wenn Sie die zugehörigen Anmerkungsregeln bearbeiten.

Schritte

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

   Sie können den Zielobjekttyp für eine Anmerkungsregel nicht ändern.

4. Klicken Sie auf **Speichern**.

Konfigurieren von Bedingungen für Anmerkungsregeln

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

Bevor Sie beginnen

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

Schritte

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

Beispiel für die Konfiguration einer Bedingung für eine Anmerkungsregel

Betrachten Sie eine Bedingung für den Objekttyp SVM, bei der der Objektname „`svm_data`“ enthält.

Führen Sie im Dialogfeld „Anmerkungsregel hinzufügen“ die folgenden Schritte aus, um die Bedingung zu

konfigurieren:

Schritte

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

Annotationsregeln löschen

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

Bevor Sie beginnen

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **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 das Löschen zu bestätigen.

Neuordnen von Anmerkungsregeln

Sie können die Reihenfolge ändern, in der Unified Manager Anmerkungsregeln auf Speicherobjekte anwendet. Annotationsregeln werden auf Speicherobjekte sequenziell basierend auf ihrem Rang angewendet. Wenn Sie eine Anmerkungsregel konfigurieren, ist der Rang am niedrigsten. Sie können den Rang der Anmerkungsregel jedoch je nach Ihren Anforderungen ändern.

Bevor Sie beginnen

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungsregeln** auf **Neu anordnen**.
3. Im Dialogfeld **Anmerkungsregel neu anordnen** können Sie per Drag & Drop einzelne oder mehrere

Zeilen verschieben, um die Reihenfolge der Anmerkungsregeln neu anzuordnen.

4. Klicken Sie auf **Speichern**.

   Damit die Nachbestellung angezeigt wird, müssen Sie die Änderungen speichern.

Senden Sie ein Support-Paket über die Web-Benutzeroberfläche und die Wartungskonsole

Sie sollten ein Supportpaket senden, wenn Ihr Problem eine detailliertere Diagnose und Fehlerbehebung erfordert, als eine AutoSupport -Nachricht bietet. Sie können über die Web-Benutzeroberfläche und Wartungskonsole von Unified Manager ein Support-Paket an den technischen Support senden.

Unified Manager speichert maximal zwei vollständige Support-Pakete und drei leichte Support-Pakete gleichzeitig.

Verwandte Informationen

"Unified Manager-Benutzerrollen und -Funktionen"

Senden Sie AutoSupport -Nachrichten und Support-Pakete an den technischen Support

Auf der AutoSupport -Seite können Sie vordefinierte und On-Demand AutoSupport Nachrichten an Ihr technisches Supportteam senden, um einen ordnungsgemäßen Betrieb Ihrer Umgebung sicherzustellen und Sie bei der Aufrechterhaltung der Integrität Ihrer Umgebung zu unterstützen. AutoSupport ist standardmäßig aktiviert und sollte nicht deaktiviert werden, damit Sie die Vorteile von NetAppActive IQ nutzen können.

Sie können bei Bedarf diagnostische Systeminformationen und detaillierte Daten zum Unified Manager-Server in einer Nachricht senden, den regelmäßigen Versand einer Nachricht planen oder sogar Supportpakete erstellen und an das technische Supportteam senden.

> Ein Benutzer mit der Rolle eines Speicheradministrators kann bei Bedarf AutoSupport Nachrichten und Supportpakete generieren und an den technischen Support senden. Allerdings kann nur ein Administrator oder Wartungsbenutzer den regelmäßigen AutoSupport aktivieren oder deaktivieren und die HTTP-Einstellungen wie im Abschnitt „Einrichten des HTTP-Proxyservers“ beschrieben konfigurieren. In einer Umgebung, in der ein HTTP-Proxyserver verwendet werden muss, sollte die Konfiguration abgeschlossen sein, bevor ein Speicheradministrator On-Demand- AutoSupport Nachrichten und Support-Pakete an den technischen Support senden kann.

Senden Sie AutoSupport -Nachrichten auf Abruf

Sie können eine On-Demand-Nachricht generieren und an den technischen Support oder an einen angegebenen 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 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 senden** und geben Sie die E-Mail-Adresse des Empfängers ein.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie auf * AutoSupport generieren und senden*.

Aktivieren Sie den regelmäßigen AutoSupport

Sie können dem technischen Support regelmäßig bestimmte, vordefinierte Nachrichten zur Problemdiagnose und -lösung senden. Diese Funktion ist standardmäßig aktiviert. Wenn deaktiviert, kann ein Administrator oder Wartungsbenutzer die Einstellungen aktivieren.

Schritte

1. Navigieren Sie zu **Allgemein** > * AutoSupport*.
2. Aktivieren Sie im Abschnitt „Periodischer AutoSupport“ das Kontrollkästchen **Regelmäßiges Senden von AutoSupport -Daten an Active IQ aktivieren**.
3. Definieren Sie bei Bedarf den Namen, den Port und die Authentifizierungsinformationen für den HTTP-Proxyserver, wie im Abschnitt „Einrichten des HTTP-Proxyservers“ beschrieben.
4. Klicken Sie auf **Speichern**.

Laden Sie ein On-Demand-Supportpaket hoch

Sie können je nach Bedarf zur Fehlerbehebung ein Supportpaket erstellen und an den technischen Support senden. Unified Manager speichert nur die beiden zuletzt erstellten Support-Pakete. Ältere Support-Pakete werden aus dem System gelöscht.

Da einige Supportdatentypen große Mengen an Clusterressourcen beanspruchen oder ihre Fertigstellung viel Zeit in Anspruch nehmen kann, können Sie bei Auswahl des vollständigen Supportpakets bestimmte Datentypen ein- oder ausschließen, um die Größe des Supportpakets zu reduzieren. Sie haben auch die Möglichkeit, ein einfaches Supportpaket zu erstellen, das nur 30 Tage Protokolle und Konfigurationsdatenbankeinträge enthält – Leistungsdaten, Erfassungsaufzeichnungsdateien und Server-Heap-Dumps sind davon ausgenommen.

Schritte

1. Navigieren Sie zu **Allgemein** > * AutoSupport*.
2. Klicken Sie im Abschnitt „On-Demand-Support-Paket“ auf **Support-Paket generieren und senden**.
3. Um ein Light-Support-Paket an den technischen Support zu senden, aktivieren Sie im Popup „Support-Paket generieren und senden“ das Kontrollkästchen **Light-Support-Paket generieren**.
4. Alternativ können Sie zum Senden eines vollständigen Support-Pakets das Kontrollkästchen **Vollständiges Support-Paket generieren** aktivieren. Wählen Sie die spezifischen Datentypen aus, die in das Support-Paket aufgenommen oder davon ausgeschlossen werden sollen.

   Auch wenn Sie keinen Datentyp auswählen, wird das Support-Paket dennoch mit anderen Unified Manager-Daten generiert.

5. Aktivieren Sie das Kontrollkästchen **Paket an den technischen Support senden**, um das Paket zu erstellen und an den technischen Support zu senden. Wenn Sie dieses Kontrollkästchen nicht aktivieren,

wird das Paket generiert und lokal auf dem Unified Manager-Server gespeichert. Das generierte Support-Paket steht zur späteren Verwendung im Verzeichnis /support auf VMware-Systemen zur Verfügung, in `/opt/netapp/data/support/` auf Linux-Systemen und in `ProgramData\NetApp\OnCommandAppData\ocum\support` auf Windows-Systemen.

6. Klicken Sie auf **Senden**.

Einrichten eines HTTP-Proxyservers

Sie können einen Proxy für den Internetzugang festlegen, um AutoSupport Inhalte an den Support zu senden, wenn 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 als HTTP-Proxy verwendeten Server zu identifizieren.

  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 angeben müssen, um auf den als HTTP-Proxy verwendeten Server zuzugreifen.

  Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung beim HTTP-Proxy erforderlich sind.

HTTP-Proxys, die nur eine Basisauthentifizierung bereitstellen, werden nicht unterstützt.

Zugriff auf die Wartungskonsole

Wenn die Benutzeroberfläche des Unified Managers nicht in Betrieb ist oder Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Wartungskonsole zugreifen, um Ihr Unified Manager-System zu verwalten.

Bevor Sie beginnen

Sie müssen Unified Manager installiert und konfiguriert haben.

Nach 15 Minuten Inaktivität werden Sie von der Wartungskonsole abgemeldet.

Wenn Sie bei der Installation auf VMware bereits über die VMware-Konsole als Wartungsbenutzer angemeldet sind, können Sie sich nicht gleichzeitig über Secure Shell anmelden.

Schritt

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

Auf diesem Betriebssystem …	Befolgen Sie diese Schritte…
VMware	a. Stellen Sie mithilfe von Secure Shell eine Verbindung zur IP-Adresse oder zum vollqualifizierten Domänennamen der virtuellen Unified Manager-Appliance her. b. Melden Sie sich mit Ihrem Wartungsbenutzernamen und Kennwort bei der Wartungskonsole an.
Linux	a. Stellen Sie mithilfe von Secure Shell eine Verbindung zur IP-Adresse oder zum vollqualifizierten Domänennamen des Unified Manager-Systems her. b. Melden Sie sich mit dem Namen und Kennwort des Wartungsbenutzers (umadmin) beim System an. c. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
Windows	a. Melden Sie sich mit Administratoranmeldeinformationen beim Unified Manager-System an. b. Starten Sie PowerShell als Windows-Administrator. c. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.

Das Menü der Wartungskonsole von Unified Manager wird angezeigt.

Erstellen und Hochladen eines Support-Pakets

Sie können ein Support-Paket mit Diagnoseinformationen erstellen, sodass Sie es zur Hilfe bei der Fehlerbehebung an den technischen Support senden können.

Ab Unified Manager 9.8 können Sie das Support-Paket auch von der Wartungskonsole auf NetApp hochladen, wenn Ihr Unified Manager-Server mit dem Internet verbunden ist.

Bevor Sie beginnen

Sie müssen als Wartungsbenutzer Zugriff auf die Wartungskonsole haben.

Da manche Supportdatentypen große Mengen an Clusterressourcen beanspruchen oder ihre Verarbeitung viel Zeit in Anspruch nehmen kann, können Sie bei Auswahl des vollständigen Supportpakets die einzuschließenden oder auszuschließenden Datentypen angeben, um die Größe des Supportpakets zu reduzieren. Sie haben auch die Möglichkeit, ein einfaches Supportpaket zu erstellen, das nur 30 Tage Protokolle und Konfigurationsdatenbankeinträge enthält – Leistungsdaten, Erfassungsaufzeichnungsdateien und Server-Heap-Dumps sind davon ausgenommen.

Unified Manager speichert nur die beiden zuletzt erstellten Support-Pakete. Ältere Support-Pakete werden aus dem System gelöscht.

Schritte

1. Wählen Sie im **Hauptmenü** der Wartungskonsole **Support/Diagnose**.
2. Wählen Sie **Light-Support-Paket generieren** oder **Support-Paket generieren**, je nachdem, wie detailliert das Support-Paket sein soll.
3. Wenn Sie das vollständige Support-Paket auswählen, wählen Sie die folgenden Datentypen aus oder heben Sie die Auswahl auf, um sie in das Support-Paket aufzunehmen oder davon auszuschließen:

   - **Datenbank-Dump**

     Ein Dump der MySQL-Serverdatenbank.

   - **Heap-Dump**

     Eine Momentaufnahme des Status der wichtigsten Unified Manager-Serverprozesse. Diese Option ist standardmäßig deaktiviert und sollte nur auf Anfrage des Kundensupports ausgewählt werden.

   - **Akquisitionsaufzeichnungen**

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

   Wenn Sie alle Datentypen abwählen, wird das Support-Paket dennoch mit anderen Unified Manager-Daten generiert.

4. Typ `g` und drücken Sie dann die Eingabetaste, um das Support-Paket zu generieren.

   Da die Generierung eines Support-Pakets ein speicherintensiver Vorgang ist, werden Sie aufgefordert zu bestätigen, dass Sie das Support-Paket zu diesem Zeitpunkt wirklich generieren möchten.

5. Typ `y` und drücken Sie dann die Eingabetaste, um das Support-Paket zu generieren.

   Wenn Sie das Support-Paket jetzt nicht generieren möchten, geben Sie `n` und drücken Sie dann die Eingabetaste.

6. Wenn Sie Datenbank-Dump-Dateien in das vollständige Support-Paket aufgenommen haben, werden Sie aufgefordert, den Zeitraum anzugeben, für den Leistungsstatistiken einbezogen werden sollen. Das Einbeziehen von Leistungsstatistiken kann viel Zeit und Speicherplatz beanspruchen. Sie können die Datenbank daher auch ohne Einbeziehen von Leistungsstatistiken sichern:

   a. Geben Sie das Startdatum im Format JJJJMMTT ein.

      Geben Sie beispielsweise `20210101` für den 1. Januar 2021. Eingeben `n` wenn Sie nicht möchten, dass Leistungsstatistiken einbezogen werden.

   b. Geben Sie die Anzahl der Tage ein, für die Statistiken ab 0:00 Uhr des angegebenen Startdatums einbezogen werden sollen.

      Sie können eine Zahl zwischen 1 und 10 eingeben.

   Wenn Sie Leistungsstatistiken einbeziehen, zeigt das System den Zeitraum an, für den Leistungsstatistiken

erfasst werden.

7. Nachdem das Support-Paket erstellt wurde, werden Sie gefragt, ob Sie es zu NetApp hochladen möchten. Typ `y` und drücken Sie dann die Eingabetaste.

   Sie werden aufgefordert, Ihre Support-Fallnummer einzugeben.

8. Wenn Sie bereits eine Fallnummer haben, geben Sie die Nummer ein und drücken Sie die Eingabetaste. Andernfalls drücken Sie einfach die Eingabetaste.

   Das Support-Paket 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 es mit einem SFTP-Client oder mithilfe von UNIX- oder Linux-CLI-Befehlen abrufen. Bei Windows-Installationen können Sie Remote Desktop (RDP) verwenden, um das Support-Paket abzurufen.

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

Verwandte Informationen

"Unified Manager-Benutzerrollen und -Funktionen"

Abrufen des Support-Pakets mit einem Windows-Client

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

Bevor Sie beginnen

Sie müssen der Wartungsbenutzer sein, um diese Aufgabe auszuführen.

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

Schritte

1. Laden Sie ein Tool herunter und installieren Sie es, um das Support-Paket abzurufen.
2. Öffnen Sie das Tool.
3. Stellen Sie über SFTP eine Verbindung zu Ihrem Unified Manager-Verwaltungsserver her.

   Das Tool zeigt den Inhalt des Verzeichnisses /support an und Sie können alle vorhandenen Support-Pakete anzeigen.

4. Wählen Sie das Zielverzeichnis für das Support-Paket aus, das Sie kopieren möchten.
5. Wählen Sie das Support-Paket aus, das Sie kopieren möchten, und verwenden Sie das Tool, um die Datei vom Unified Manager-Server auf Ihr lokales System zu kopieren.

Rufen Sie das Support-Paket mit einem UNIX- oder Linux-Client ab

Wenn Sie ein UNIX- oder Linux-Benutzer sind, können Sie das Support-Paket von Ihrer vApp abrufen, indem Sie die Befehlszeilenschnittstelle (CLI) auf Ihrem Linux-Clientserver verwenden. Sie können entweder SCP oder SFTP verwenden, um das Support-Paket abzurufen.

Bevor Sie beginnen

Sie müssen der Wartungsbenutzer sein, um diese Aufgabe auszuführen.

Sie müssen mithilfe der Wartungskonsole ein Support-Paket erstellt haben und über den Namen des Support-Pakets verfügen.

Schritte

1. Greifen Sie über Telnet oder die Konsole auf die CLI zu, indem Sie Ihren Linux-Clientserver verwenden.
2. Zugriff auf die/`support` Verzeichnis.
3. Rufen Sie das Support-Paket ab und kopieren Sie es mit dem folgenden Befehl in das lokale Verzeichnis:

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

   Der Name des Support-Pakets wird Ihnen mitgeteilt, wenn Sie es mithilfe der Wartungskonsole generieren.

4. Geben Sie das Kennwort des Wartungsbenutzers ein.

Beispiele

Im folgenden Beispiel wird SCP zum Abrufen des Support-Pakets verwendet:

```
        `$ 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 Support-Pakets 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 Sie ein Support-Paket an den technischen Support

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

Bevor Sie beginnen

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

Sie müssen über eine Fallnummer verfügen, die über die Website des technischen Supports generiert wurde.

Schritte

1. Melden Sie sich bei der NetApp Support-Site an.
2. Laden Sie die Datei hoch.

   "So laden Sie eine Datei zu NetApp hoch"

Aufgaben und Informationen zu verschiedenen Arbeitsabläufen

Einige Aufgaben und Referenztexte, die Ihnen beim Verstehen und Abschließen eines Workflows helfen können, sind vielen Workflows in Unified Manager gemeinsam, darunter das Hinzufügen und Überprüfen von Notizen zu einem Ereignis, das Zuweisen eines Ereignisses, das Bestätigen und Auflösen von Ereignissen sowie Details zu Volumes, virtuellen Speichermaschinen (SVMs), Aggregaten usw.

Clusterkomponenten und warum sie kontrovers diskutiert werden können

Sie können Leistungsprobleme im Cluster erkennen, wenn eine Clusterkomponente in einen Konflikt gerät. Die Leistung von Workloads, die die Komponente verwenden, verlangsamt sich und ihre Antwortzeit (Latenz) für Clientanforderungen erhöht sich, was ein Ereignis in Unified Manager auslöst.

Eine Komponente, die im Streit liegt, kann nicht die optimale Leistung erbringen. Seine Leistung hat nachgelassen und die Leistung anderer Clusterkomponenten und Workloads, sogenannter *Opfer*, hat möglicherweise die Latenz erhöht. Um eine Komponente aus dem Wettbewerb zu nehmen, müssen Sie ihre Arbeitslast reduzieren oder ihre Fähigkeit erhöhen, mehr Arbeit zu bewältigen, damit die Leistung wieder auf ein normales Niveau zurückkehren kann. Da Unified Manager die Workload-Leistung in Fünf-Minuten-

Intervallen erfasst und analysiert, erkennt er nur, wenn eine Clusterkomponente dauerhaft überbeansprucht wird. Vorübergehende Überlastungsspitzen, die innerhalb des Fünf-Minuten-Intervalls nur von kurzer Dauer sind, werden nicht erkannt.

Beispielsweise kann es zu einem Konflikt um ein Speicheraggregat kommen, weil eine oder mehrere Workloads darauf um die Erfüllung ihrer E/A-Anforderungen konkurrieren. Andere Arbeitslasten im Aggregat können beeinträchtigt werden, was zu einer Leistungsminderung führt. Um die Aktivität auf dem Aggregat zu reduzieren, können Sie verschiedene Schritte unternehmen, z. B. eine oder mehrere Arbeitslasten auf ein weniger ausgelastetes Aggregat oder einen weniger ausgelasteten Knoten verschieben, um die Gesamtarbeitslastanforderung an das aktuelle Aggregat zu verringern. Für eine QoS-Richtliniengruppe können Sie die Durchsatzgrenze anpassen oder Workloads in eine andere Richtliniengruppe verschieben, sodass die Workloads nicht mehr gedrosselt werden.

Unified Manager überwacht die folgenden Clusterkomponenten, um Sie zu warnen, wenn es zu Konflikten kommt:

- **Netzwerk**

  Stellt die Wartezeit von E/A-Anfragen durch die externen Netzwerkprotokolle im Cluster dar. Die Wartezeit ist die Zeit, die darauf gewartet wird, dass die „Transfer Ready“-Transaktionen abgeschlossen werden, bevor der Cluster auf eine E/A-Anforderung antworten kann. Wenn es zu Konflikten mit der Netzwerkkomponente kommt, bedeutet dies, dass eine hohe Wartezeit auf der Protokollebene die Latenz einer oder mehrerer Workloads beeinträchtigt.

- **Netzwerkverarbeitung**

  Stellt die Softwarekomponente im Cluster dar, die an der E/A-Verarbeitung zwischen der Protokollschicht und dem Cluster beteiligt ist. Der Knoten, der die Netzwerkverarbeitung durchführt, hat sich möglicherweise seit der Erkennung des Ereignisses geändert. Wenn es bei der Netzwerkverarbeitungskomponente zu Konflikten kommt, bedeutet dies, dass eine hohe Auslastung des Netzwerkverarbeitungsknotens die Latenz einer oder mehrerer Arbeitslasten beeinträchtigt.

  Wenn Sie einen All-SAN-Array-Cluster in einer Aktiv-Aktiv-Konfiguration verwenden, wird der Latenzwert der Netzwerkverarbeitung für beide Knoten angezeigt, sodass Sie überprüfen können, ob die Knoten die Last gleichmäßig teilen.

- **QoS-Limit Max**

  Stellt die maximale Durchsatzeinstellung (Spitzenwert) der der Arbeitslast zugewiesenen Speicher-QoS-Richtliniengruppe (Quality of Service) dar. Wenn die Richtliniengruppenkomponente im Konflikt steht, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch die festgelegte Durchsatzgrenze gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- **Mindest-QoS-Limit**

  Stellt die Latenz einer Arbeitslast dar, die durch die anderen Arbeitslasten zugewiesene Einstellung für den minimalen (erwarteten) QoS-Durchsatz verursacht wird. Wenn das für bestimmte Workloads festgelegte QoS-Minimum den Großteil der Bandbreite nutzt, um den versprochenen Durchsatz zu garantieren, werden andere Workloads gedrosselt und weisen eine höhere Latenz auf.

- **Cluster-Verbindung**

  Stellt die Kabel und Adapter dar, mit denen Clusterknoten physisch verbunden sind. Wenn es bei der Cluster-Interconnect-Komponente zu Konflikten kommt, bedeutet dies, dass die lange Wartezeit für E/A-Anfragen bei der Cluster-Interconnect-Komponente die Latenz einer oder mehrerer Workloads

beeinträchtigt.

- * Data Processing*

  Stellt die Softwarekomponente im Cluster dar, die an der E/A-Verarbeitung zwischen dem Cluster und dem Speicheraggregat beteiligt ist, das die Arbeitslast enthält. Der Knoten, der die Datenverarbeitung durchführt, hat sich möglicherweise seit der Erkennung des Ereignisses geändert. Wenn es bei der Datenverarbeitungskomponente zu Konflikten kommt, bedeutet dies, dass eine hohe Auslastung des Datenverarbeitungsknotens die Latenz einer oder mehrerer Arbeitslasten beeinträchtigt.

- **Lautstärkeaktivierung**

  Stellt den Prozess dar, der die Nutzung aller aktiven Volumes verfolgt. In großen Umgebungen mit mehr als 1.000 aktiven Volumes verfolgt dieser Prozess, wie viele kritische Volumes gleichzeitig über den Knoten auf Ressourcen zugreifen müssen. Wenn die Anzahl gleichzeitig aktiver Volumes den empfohlenen Höchstschwellenwert überschreitet, kommt es bei einigen der nicht kritischen Volumes zu Latenzen, wie hier angegeben.

- * MetroCluster -Ressourcen*

  Stellt die MetroCluster Ressourcen dar, einschließlich NVRAM und Interswitch-Links (ISLs), die zum Spiegeln von Daten zwischen Clustern in einer MetroCluster -Konfiguration verwendet werden. Wenn die MetroCluster Komponente im Konflikt steht, bedeutet dies, dass ein hoher Schreibdurchsatz von Workloads auf dem lokalen Cluster oder ein Link-Health-Problem die Latenz einer oder mehrerer Workloads auf dem lokalen Cluster beeinträchtigt. Wenn sich der Cluster nicht in einer MetroCluster -Konfiguration befindet, wird dieses Symbol nicht angezeigt.

- **Aggregate- oder SSD-Aggregate-Operationen**

  Stellt das Speicheraggregat dar, auf dem die Workloads ausgeführt werden. Wenn es zu Konflikten bei der Aggregatkomponente kommt, bedeutet dies, dass eine hohe Auslastung des Aggregats die Latenz einer oder mehrerer Workloads beeinträchtigt. Ein Aggregat besteht aus allen HDDs oder einer Mischung aus HDDs und SSDs (ein Flash Pool-Aggregat) oder einer Mischung aus HDDs und einer Cloud-Ebene (ein FabricPool -Aggregat). Ein „SSD-Aggregat“ besteht aus allen SSDs (einem All-Flash-Aggregat) oder einer Mischung aus SSDs und einer Cloud-Ebene (einem FabricPool -Aggregat).

- **Cloud-Latenz**

  Stellt die Softwarekomponente im Cluster dar, die an der E/A-Verarbeitung zwischen dem Cluster und der Cloud-Ebene beteiligt ist, auf der Benutzerdaten gespeichert sind. Wenn die Cloud-Latenzkomponente in Konflikt steht, bedeutet dies, dass eine große Anzahl von Lesevorgängen von Volumes, die auf der Cloud-Ebene gehostet werden, die Latenz einer oder mehrerer Workloads beeinträchtigt.

- * SnapMirror synchronisieren*

  Stellt die Softwarekomponente im Cluster dar, die in einer synchronen SnapMirror -Beziehung an der Replikation von Benutzerdaten vom primären Volume auf das sekundäre Volume beteiligt ist. Wenn es bei der Synchronisierungskomponente von SnapMirror zu Konflikten kommt, bedeutet dies, dass die Aktivität der synchronen SnapMirror -Vorgänge die Latenz einer oder mehrerer Arbeitslasten beeinträchtigt.

Seite mit den Volumen-/Gesundheitsdetails

Auf der Seite „Volume-/Integritätsdetails“ können Sie ausführliche Informationen zu einem ausgewählten Volume anzeigen, beispielsweise Kapazität, Speichereffizienz,

Konfiguration, Schutz, Anmerkungen und generierte Ereignisse. Sie können auch Informationen zu den zugehörigen Objekten und zugehörigen Warnungen 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:

- **Zur Leistungsansicht wechseln**

  Ermöglicht Ihnen die Navigation zur Seite mit den Lautstärke-/Leistungsdetails.

- **Aktionen**
  - Benachrichtigung hinzufügen

    Ermöglicht Ihnen, dem ausgewählten Volume eine Warnung hinzuzufügen.

  - Schwellenwerte bearbeiten

    Ermöglicht Ihnen, die Schwellenwerteinstellungen für das ausgewählte Volume zu ändern.

  - Kommentieren

    Ermöglicht Ihnen, das ausgewählte Volumen mit Anmerkungen zu versehen.

  - Schützen

    Ermöglicht Ihnen, entweder SnapMirror oder SnapVault -Beziehungen für das ausgewählte Volume zu erstellen.

  - Beziehung

    Ermöglicht Ihnen die Ausführung der folgenden Schutzbeziehungsvorgänge:

    - Bearbeiten

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

    - Abbrechen

      Bricht laufende Übertragungen für eine ausgewählte Beziehung ab. Optional können Sie den Neustart-Checkpoint für andere Übertragungen als die Basisübertragung entfernen. Sie können den Prüfpunkt für eine Baseline-Übertragung nicht entfernen.

    - Ruhen

      Deaktiviert vorübergehend geplante Updates für eine ausgewählte Beziehung. Bereits laufende Übertragungen müssen abgeschlossen sein, bevor die Beziehung beendet wird.

    - Brechen

Bricht die Beziehung zwischen Quell- und Zielvolume auf und ändert das Ziel in ein Lese-/Schreibvolume.

- Entfernen

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

- Wieder aufnehmen

  Ermöglicht geplante Übertragungen für eine ruhende Beziehung. Beim nächsten geplanten Übertragungsintervall wird ein Neustart-Checkpoint verwendet, sofern einer vorhanden ist.

- Neu synchronisieren

  Ermöglicht Ihnen, eine zuvor unterbrochene Beziehung erneut zu synchronisieren.

- Initialisieren/Aktualisieren

  Ermöglicht Ihnen die Durchführung einer erstmaligen Baseline-Übertragung für eine neue Schutzbeziehung oder die Durchführung einer manuellen Aktualisierung, wenn die Beziehung bereits initialisiert ist.

- Umgekehrte Neusynchronisierung

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

◦ Wiederherstellen

Ermöglicht Ihnen, Daten von einem Volume auf einem anderen Volume wiederherzustellen. Weitere Informationen finden Sie unter"Wiederherstellen von Daten mithilfe der Seite „Volume-/Integritätsdetails“" .

Die Schaltflächen „Wiederherstellen“ und „Beziehungsvorgang“ sind für Volumes in synchronen Schutzbeziehungen nicht verfügbar.

- **Volumen anzeigen**

  Ermöglicht Ihnen die Navigation zur Ansicht „Health: All Volumes“.

Registerkarte „Kapazität“

Auf der Registerkarte „Kapazität“ werden Details zum ausgewählten Volume angezeigt, z. B. seine physische Kapazität, logische Kapazität, Schwellenwerteinstellungen, Kontingentkapazität und Informationen zu allen Volume-Verschiebungsvorgängen:

- **Physische Kapazität**

  Details zur physischen Kapazität des Datenträgers:

- Snapshot-Überlauf

  Zeigt den Datenspeicherplatz an, der von den Snapshot-Kopien belegt wird.

- Gebraucht

  Zeigt den von Daten im Volume belegten Speicherplatz an.

- Warnung

  Zeigt an, dass der Speicherplatz im Datenträger fast voll ist. Wenn dieser Schwellenwert überschritten wird, wird das Ereignis „Speicherplatz fast voll“ generiert.

- Fehler

  Zeigt an, dass der Speicherplatz im Datenträger voll ist. Wenn dieser Schwellenwert überschritten wird, wird das Ereignis „Speicherplatz voll“ generiert.

- Unbrauchbar

  Zeigt an, dass das Ereignis „Speicherplatz im Thin-Provisioned-Volume gefährdet“ generiert wird und dass der Speicherplatz im Thin-Provisioned-Volume aufgrund von Problemen mit der Gesamtkapazität gefährdet ist. Die nicht nutzbare Kapazität wird nur für Thin Provisioning-Volumes angezeigt.

- Datendiagramm

  Zeigt die gesamte Datenkapazität und die verwendete Datenkapazität des Volumes an.

  Wenn die automatische Vergrößerung aktiviert ist, zeigt das Datendiagramm auch den im Aggregat verfügbaren Speicherplatz an. Das Datendiagramm zeigt den effektiven Speicherplatz an, der von Daten im Volume verwendet werden kann. Dabei kann es sich um einen der folgenden Werte handeln:

  - Tatsächliche Datenkapazität des Datenträgers unter den folgenden Bedingungen:
    - Autogrow ist deaktiviert.
    - Das Volume mit aktivierter Autogrow-Funktion hat die maximale Größe erreicht.
    - Das Autogrow-fähige Thick-Provisioning-Volume kann nicht weiter wachsen.
  - Datenkapazität des Volumes unter Berücksichtigung der maximalen Volumegröße (für Thin Provisioning-Volumes und für Thick Provisioning-Volumes, wenn das Aggregat Platz für das Erreichen der maximalen Volumegröße bietet)
  - Datenkapazität des Volumes nach Berücksichtigung der nächstmöglichen Autogrow-Größe (für Thick Provisioning-Volumes mit einem Autogrow-Prozentschwellenwert)

- 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 übersteigt, wenn die verwendete Snapshot-Kapazität die Snapshot-Reserve übersteigt.

- **Kapazität logisch**

Zeigt die logischen Speicherplatzeigenschaften des Datenträgers an. Der logische Speicherplatz gibt die tatsächliche Größe der auf der Festplatte gespeicherten Daten an, ohne die Einsparungen durch die

Verwendung von ONTAP Speichereffizienztechnologien zu berücksichtigen.

- Logische Speicherplatzberichte

  Zeigt an, ob für das Volume die logische Speicherplatzberichterstattung konfiguriert ist. Der Wert kann „Aktiviert“, „Deaktiviert“ oder „Nicht zutreffend“ sein. Für Volumes auf älteren Versionen von ONTAP oder auf Volumes, die die logische Speicherplatzberichterstattung nicht unterstützen, wird „Nicht zutreffend“ angezeigt.

- Gebraucht

  Zeigt die Menge des logischen Speicherplatzes an, der von Daten im Volume verwendet wird, sowie den Prozentsatz des verwendeten logischen Speicherplatzes basierend auf der gesamten Datenkapazität.

- Durchsetzung des logischen Speicherplatzes

  Zeigt an, ob die Durchsetzung des logischen Speicherplatzes für Thin Provisioning-Volumes konfiguriert ist. Wenn die Option auf „Aktiviert“ eingestellt ist, kann die logisch verwendete Größe des Datenträgers nicht größer sein als die aktuell eingestellte physische Datenträgergröße.

- **Automatisches Wachstum**

  Zeigt an, ob das Volume automatisch vergrößert wird, wenn der Speicherplatz erschöpft ist.

- **Platzgarantie**

  Zeigt die FlexVol volume -Einstellungssteuerung an, wenn ein Volume freie Blöcke aus einem Aggregat entfernt. Diese Blöcke stehen dann garantiert für Schreibvorgänge in Dateien im Volume zur Verfügung. Die Speicherplatzgarantie kann auf einen der folgenden Werte eingestellt werden:

  - Keine

    Für das Volume ist keine Speicherplatzgarantie konfiguriert.

  - Datei

    Die volle Größe spärlich geschriebener Dateien (z. B. LUNs) ist garantiert.

  - Volumen

    Die volle Größe des Volumens ist garantiert.

  - Teilweise

    Das FlexCache -Volume reserviert Speicherplatz basierend auf seiner Größe. Wenn die Größe des FlexCache Volumes 100 MB oder mehr beträgt, wird die Mindestspeicherplatzgarantie standardmäßig auf 100 MB festgelegt. Wenn die Größe des FlexCache Volumes weniger als 100 MB beträgt, wird die Mindestspeicherplatzgarantie auf die Größe des FlexCache Volumes festgelegt. Wenn die Größe des FlexCache Volumes später vergrößert wird, wird die Mindestspeicherplatzgarantie nicht erhöht.

  Die Speicherplatzgarantie ist teilweise, wenn das Volume vom Typ „Datencache“ ist.

- **Details (physisch)**

Zeigt die physikalischen Eigenschaften des Datenträgers an.

- **Gesamtkapazität**

  Zeigt die gesamte physische Kapazität des Datenträgers an.

- **Datenkapazität**

  Zeigt die Menge des vom Volume verwendeten physischen Speicherplatzes (genutzte Kapazität) und die Menge des physischen Speicherplatzes an, der im Volume noch verfügbar ist (freie Kapazität). Diese Werte werden auch als Prozentsatz der gesamten körperlichen Leistungsfähigkeit angezeigt.

  Wenn das Ereignis „Gefährdeter Speicherplatz für Thin-Provisioned-Volume“ für Thin-Provisioned-Volumes generiert wird, wird die vom Volume verwendete Speicherplatzmenge (verwendete Kapazität) und die Speicherplatzmenge angezeigt, die im Volume verfügbar ist, aber aufgrund von Problemen mit der Gesamtkapazität nicht verwendet werden kann (unverwendbare Kapazität).

- **Schnappschuss-Reserve**

  Zeigt die von den Snapshot-Kopien verwendete Speicherplatzmenge (genutzte Kapazität) und die für Snapshot-Kopien verfügbare Speicherplatzmenge (freie Kapazität) im Volume an. Diese Werte werden auch als Prozentsatz der gesamten Snapshot-Reserve angezeigt.

  Wenn das Ereignis „Speicherplatz im Thin-Provisioning-Volume gefährdet“ für Thin-Provisioning-Volumes generiert wird, wird die von den Snapshot-Kopien verwendete Speicherplatzmenge (verwendete Kapazität) und die Speicherplatzmenge angezeigt, die im Volume verfügbar ist, aber aufgrund von Problemen mit der Gesamtkapazität nicht zum Erstellen von Snapshot-Kopien verwendet werden kann (unbrauchbare Kapazität).

- **Lautstärkeschwellenwerte**

  Zeigt die folgenden Schwellenwerte für die Volume-Kapazität an:

  - Fast volle Schwelle

    Gibt den Prozentsatz an, bei dem ein Volume fast voll ist.

  - Voller Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Volume voll ist.

- **Weitere Details**

  - Maximale Größe automatisch vergrößern

    Zeigt die maximale Größe an, bis zu der das Volume automatisch wachsen kann. Der Standardwert beträgt 120 % der Volumegröße bei der Erstellung. Dieses Feld wird nur angezeigt, wenn die automatische Vergrößerung für das Volume aktiviert ist.

  - Qtree-Kontingent – Zugesicherte Kapazität

    Zeigt den in den Kontingenten reservierten Speicherplatz an.

  - Überbelegte Kapazität des Qtree-Kontingents

    Zeigt die Menge an Speicherplatz an, die verwendet werden kann, bevor das System das Ereignis

„Volume Qtree Quota Overcommitted“ generiert.

- Teilreserve

  Steuert die Größe der Überschreibreserve. Standardmäßig ist die Teilreserve auf 100 eingestellt. Dies bedeutet, dass 100 Prozent des erforderlichen reservierten Speicherplatzes reserviert sind, sodass die Objekte vollständig vor Überschreibungen geschützt sind. Wenn die Teilreserve weniger als 100 Prozent beträgt, wird der reservierte Speicherplatz für alle reservierten Dateien in diesem Volume auf den Prozentsatz der Teilreserve reduziert.

- Momentaufnahme der täglichen Wachstumsrate

  Zeigt die Änderung (in Prozent oder in KB, MB, GB usw.) an, die alle 24 Stunden in den Snapshot-Kopien im ausgewählten Volume auftritt.

- Snapshot Tage bis Voll

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor der für die Snapshot-Kopien im Volume reservierte Speicherplatz den angegebenen Schwellenwert erreicht.

  Im Feld „Snapshot-Tage bis zur Vollendung“ wird der Wert „Nicht zutreffend“ angezeigt, wenn die Wachstumsrate der Snapshot-Kopien im Volume null oder negativ ist oder wenn nicht genügend Daten zum Berechnen der Wachstumsrate vorhanden sind.

- Automatisches Löschen von Schnappschüssen

  Gibt an, ob Snapshot-Kopien automatisch gelöscht werden, um Speicherplatz freizugeben, wenn ein Schreibvorgang auf ein Volume aufgrund von Speicherplatzmangel im Aggregat fehlschlägt.

- Snapshot-Kopien

  Zeigt Informationen zu den Snapshot-Kopien im Volume an.

  Die Anzahl der Snapshot-Kopien im Volume wird als Link angezeigt. Durch Klicken auf den Link wird das Dialogfeld „Snapshot-Kopien auf einem Volume“ geöffnet, in dem Details zu den Snapshot-Kopien angezeigt werden.

Die Anzahl der Snapshot-Kopien wird etwa stündlich aktualisiert. Die Liste der Snapshot-Kopien wird jedoch aktualisiert, wenn Sie auf das Symbol klicken. Dies kann zu einer Abweichung zwischen der in der Topologie angezeigten Anzahl der Snapshot-Kopien und der Anzahl der Snapshot-Kopien führen, die beim Klicken auf das Symbol aufgelistet werden.

- **Lautstärke verschieben**

  Zeigt den Status des aktuellen oder des letzten Volume-Verschiebevorgangs an, der auf dem Volume ausgeführt wurde, sowie weitere Details, z. B. die aktuelle Phase des laufenden Volume-Verschiebevorgangs, Quellaggregat, Zielaggregat, Startzeit, Endzeit und geschätzte Endzeit.

  Zeigt außerdem die Anzahl der Volume-Verschiebungsvorgänge an, die für das ausgewählte Volume ausgeführt wurden. Weitere Informationen zu den Volume-Verschiebungsvorgängen können Sie anzeigen, indem Sie auf den Link **Volume-Verschiebungsverlauf** klicken.

Registerkarte „Konfiguration“

Auf der Registerkarte „Konfiguration“ werden Details zum ausgewählten Volume angezeigt, z. B. die

Exportrichtlinie, der RAID-Typ, die Kapazität und die mit der Speichereffizienz verbundenen Funktionen des Volumes:

- **Überblick**
  - Vollständiger Name

    Zeigt den vollständigen Namen des Datenträgers an.

  - Aggregate

    Zeigt den Namen des Aggregats an, auf dem sich das Volume befindet, oder die Anzahl der Aggregate, auf denen sich das FlexGroup -Volume befindet.

  - Tiering-Richtlinie

    Zeigt die für das Volume festgelegte Tiering-Richtlinie an, wenn das Volume auf einem FabricPool-fähigen Aggregat bereitgestellt wird. Die Richtlinie kann „Keine“, „Nur Snapshot“, „Backup“, „Auto“ oder „Alle“ sein.

  - Speicher-VM

    Zeigt den Namen der SVM an, die das Volume enthält.

  - Kreuzungspfad

    Zeigt den Status des Pfads an, der aktiv oder inaktiv sein kann. Außerdem wird der Pfad in der SVM angezeigt, in dem das Volume eingebunden ist. Sie können auf den Link **Verlauf** klicken, um die letzten fünf Änderungen am Kreuzungspfad anzuzeigen.

  - Exportrichtlinie

    Zeigt den Namen der Exportrichtlinie an, die für das Volume erstellt wird. Sie können auf den Link klicken, um Details zu den Exportrichtlinien, Authentifizierungsprotokollen und dem aktivierten Zugriff auf die Volumes anzuzeigen, die zur SVM gehören.

  - Stil

    Zeigt den Lautstärkestil an. Der Volume-Stil kann FlexVol oder FlexGroup sein.

  - Typ

    Zeigt den Typ des ausgewählten Volumes an. Der Datenträgertyp kann „Lesen/Schreiben“, „Lastverteilung“, „Datenschutz“, „Datencache“ oder „Temporär“ sein.

  - RAID-Typ

    Zeigt den RAID-Typ des ausgewählten Volumes an. Der RAID-Typ kann RAID0, RAID4, RAID-DP oder RAID-TEC sein.

    > Für FlexGroup -Volumes werden möglicherweise mehrere RAID-Typen angezeigt, da sich die einzelnen Volumes für FlexGroups auf Aggregaten unterschiedlicher Typen befinden können.

  - SnapLock -Typ

Zeigt den SnapLock -Typ des Aggregats an, das das Volume enthält.

- SnapLock -Ablauf

  Zeigt das Ablaufdatum des SnapLock -Volumes an.

- **Kapazität**
  - Thin Provisioning

    Zeigt an, ob Thin Provisioning für das Volume konfiguriert ist.

  - Automatisches Wachstum

    Zeigt an, ob das flexible Volumen innerhalb eines Aggregats automatisch wächst.

  - Automatisches Löschen von Schnappschüssen

    Gibt an, ob Snapshot-Kopien automatisch gelöscht werden, um Speicherplatz freizugeben, wenn ein Schreibvorgang auf ein Volume aufgrund von Speicherplatzmangel im Aggregat fehlschlägt.

  - Kontingente

    Gibt an, ob die Kontingente 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 Betriebszeitplan angezeigt, und wenn der Modus auf „Richtlinie“ eingestellt ist, wird der Richtlinienname angezeigt.

  - Deduplizierungstyp

    Gibt den Typ des Deduplizierungsvorgangs an, der auf dem Volume ausgeführt wird. Wenn sich das Volume in einer SnapVault -Beziehung befindet, wird der Typ SnapVault angezeigt. Für alle anderen Volumes wird der Typ als „Regulär“ angezeigt.

  - Richtlinie zur Speichereffizienz

    Gibt den Namen der Speichereffizienzrichtlinie an, die diesem Volume über Unified Manager zugewiesen wurde. Diese Richtlinie kann die Komprimierungs- und Deduplizierungseinstellungen steuern.

- **Schutz**
  - Snapshot-Kopien

    Gibt an, ob automatische Snapshot-Kopien aktiviert oder deaktiviert sind.

Registerkarte „Schutz“

Auf der Registerkarte „Schutz“ werden Schutzdetails zum ausgewählten Volume angezeigt, z. B. Verzögerungsinformationen, Beziehungstyp und Topologie der Beziehung.

- **Zusammenfassung**

  Zeigt Eigenschaften der Schutzbeziehungen (SnapMirror, SnapVault oder Storage VM DR) für ein ausgewähltes Volume an. Für alle anderen Beziehungstypen wird nur die Eigenschaft „Beziehungstyp“ angezeigt. Wenn ein primäres Volume ausgewählt ist, werden nur die verwalteten und lokalen Snapshot-Kopierrichtlinien angezeigt. Zu den für SnapMirror und SnapVault -Beziehungen angezeigten Eigenschaften gehören die folgenden:

  - Quellvolumen

    Zeigt den Namen der Quelle des ausgewählten Volumes an, wenn das ausgewählte Volume ein Ziel ist.

  - Verzögerungsstatus

    Zeigt den Update- oder Übertragungsverzögerungsstatus für eine Schutzbeziehung an. Der Status kann „Fehler“, „Warnung“ oder „Kritisch“ sein.

    Der Verzögerungsstatus ist für synchrone Beziehungen nicht anwendbar.

  - Verzögerungsdauer

    Zeigt die Zeit an, um die die Daten auf dem Spiegel hinter der Quelle zurückliegen.

  - Letztes erfolgreiches Update

    Zeigt Datum und Uhrzeit des letzten erfolgreichen Schutzupdates an.

    Das letzte erfolgreiche Update ist für synchrone Beziehungen nicht anwendbar.

  - Speicherdienstmitarbeiter

    Zeigt entweder „Ja“ oder „Nein“ an, um anzugeben, ob das Volume zu einem Speicherdienst gehört und von diesem verwaltet wird.

  - Versionsflexible Replikation

    Zeigt entweder „Ja“, „Ja mit Sicherungsoption“ oder „Keine“ an. „Ja“ bedeutet, dass die SnapMirror Replikation auch dann möglich ist, wenn auf Quell- und Zielvolumes unterschiedliche Versionen der ONTAP -Software ausgeführt werden. „Ja mit Sicherungsoption“ bedeutet die Implementierung des SnapMirror Schutzes mit der Möglichkeit, mehrere Versionen von Sicherungskopien auf dem Ziel aufzubewahren. „Keine“ bedeutet, dass die Version Flexible Replication nicht aktiviert ist.

  - Beziehungsfähigkeit

    Gibt die für die Schutzbeziehung verfügbaren ONTAP Funktionen an.

  - Schutzdienst

    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 Sync.

- Beziehungsstatus

  Zeigt den Status der SnapMirror oder SnapVault -Beziehung an. Der Status kann „Nicht initialisiert“, „SnapMirrored“ oder „Abgebrochen“ sein. Wenn ein Quellvolume ausgewählt ist, ist der Beziehungsstatus nicht anwendbar und wird nicht angezeigt.

- Übertragungsstatus

  Zeigt den Übertragungsstatus für die Schutzbeziehung an. Der Übertragungsstatus kann einer der folgenden sein:

  - Abbruch

    SnapMirror -Übertragungen sind aktiviert. Es wird jedoch ein Übertragungsabbruchvorgang ausgeführt, der möglicherweise die Entfernung des Prüfpunkts umfasst.

  - Überprüfung

    Das Zielvolume wird einer Diagnoseprüfung unterzogen und es findet keine Übertragung statt.

  - Finalisieren

    SnapMirror Übertragungen sind aktiviert. Das Volume befindet sich derzeit in der Nachübertragungsphase für inkrementelle SnapVault Übertragungen.

  - Leerlauf

    Übertragungen sind aktiviert und es findet keine Übertragung statt.

  - Synchron

    Die Daten in den beiden Volumes in der synchronen Beziehung werden synchronisiert.

  - Nicht synchron

    Die Daten im Zielvolume werden nicht mit dem Quellvolume synchronisiert.

  - Vorbereitung

    SnapMirror Übertragungen sind aktiviert. Das Volume befindet sich derzeit in der Vorübertragungsphase für inkrementelle SnapVault Übertragungen.

  - In der Warteschlange

    SnapMirror Übertragungen sind aktiviert. Es sind keine Überweisungen im Gange.

  - Ruhezustand

    SnapMirror -Übertragungen sind deaktiviert. Es ist keine Übertragung im Gange.

  - Stilllegung

Eine SnapMirror -Übertragung ist im Gange. Weitere Übertragungen sind deaktiviert.

- Übertragen

  SnapMirror Übertragungen sind aktiviert und eine Übertragung ist im Gange.

- Übergang

  Die asynchrone Datenübertragung vom Quell- zum Zieldatenträger ist abgeschlossen und der Übergang zum synchronen Betrieb hat begonnen.

- Warten

  Eine SnapMirror Übertragung wurde eingeleitet, aber einige zugehörige Aufgaben warten darauf, in die Warteschlange gestellt zu werden.

◦ Max. Übertragungsrate

Zeigt die maximale Übertragungsrate für die Beziehung an. Die maximale Übertragungsrate kann ein numerischer Wert in Kilobyte pro Sekunde (Kbps), Megabyte pro Sekunde (Mbps), Gigabyte pro Sekunde (Gbps) oder Terabyte pro Sekunde (Tbps) sein. Wenn „Keine Begrenzung“ angezeigt wird, ist die Basisübertragung zwischen Beziehungen unbegrenzt.

◦ SnapMirror -Richtlinie

Zeigt die Schutzrichtlinie für das Volume an. DPDefault gibt die standardmäßige asynchrone Spiegelschutzrichtlinie an, XDPDefault gibt die standardmäßige asynchrone Vault-Richtlinie an und DPSyncDefault gibt die standardmäßige asynchrone MirrorVault-Richtlinie an. StrictSync gibt die standardmäßige synchrone strikte Schutzrichtlinie 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
- Zugriffszeiteinstellung ignorieren
- Versuchslimit
- Kommentare
- SnapMirror -Etiketten
- Aufbewahrungseinstellungen
- Tatsächliche Snapshot-Kopien
- Snapshot-Kopien aufbewahren
- Schwellenwert für die Aufbewahrungswarnung
- Snapshot-Kopien ohne Aufbewahrungseinstellungen. In einer kaskadierenden SnapVault -Beziehung, bei der die Quelle ein Datenschutz-Volume (DP) ist, gilt nur die Regel „sm_created“.

◦ Aktualisierungszeitplan

Zeigt den der Beziehung zugewiesenen SnapMirror Zeitplan an. Wenn Sie den Cursor über das Informationssymbol bewegen, werden die Zeitplandetails angezeigt.

◦ Lokale Snapshot-Richtlinie

Zeigt die Snapshot-Kopierrichtlinie für das Volume an. Die Richtlinie ist „Standard“, „Keine“ oder ein

beliebiger Name, der einer benutzerdefinierten Richtlinie zugewiesen wird.

- Geschützt durch

  Zeigt den für das ausgewählte Volume verwendeten Schutztyp an. Wenn ein Volume beispielsweise durch Consistency Group- und SnapMirror Volume-Beziehungen geschützt ist, werden in diesem Feld sowohl SnapMirror als auch Consistency Group angezeigt. Dieses Feld enthält auch einen Link, der Sie zur Seite „Beziehungen“ weiterleitet, um den einheitlichen Beziehungsstatus anzuzeigen. Die Verknüpfung ist nur auf Bestandteilsbeziehungen anwendbar.

- Konsistenzgruppe

  Für Volumes, die durch SnapMirror Active Sync-Beziehungen geschützt sind, zeigt diese Spalte die Konsistenzgruppe des Volumes an.

- **Ansichten**

  Zeigt die Schutztopologie des ausgewählten Volumes an. Die Topologie umfasst grafische Darstellungen aller Volumes, die mit dem ausgewählten Volume in Zusammenhang stehen. Das ausgewählte Volume wird durch einen dunkelgrauen Rahmen angezeigt und Linien zwischen Volumes in der Topologie zeigen den Schutzbeziehungstyp an. Die Richtung der Beziehungen in der Topologie wird von links nach rechts angezeigt, wobei sich die Quelle jeder Beziehung links und das Ziel rechts befindet.

  Doppelte fettgedruckte Linien geben eine asynchrone Spiegelbeziehung an, eine einfache fettgedruckte Linie gibt eine asynchrone Vault-Beziehung an, doppelte einfache Linien geben eine asynchrone MirrorVault-Beziehung an und eine fettgedruckte und eine nicht fettgedruckte Linie geben eine synchrone Beziehung an. Die folgende Tabelle gibt an, ob es sich bei der synchronen Beziehung um StrictSync oder Sync handelt.

  Wenn Sie mit der rechten Maustaste auf ein Volume klicken, wird ein Menü angezeigt, in dem Sie entweder das Volume schützen oder Daten darauf wiederherstellen können. Wenn Sie mit der rechten Maustaste auf eine Beziehung klicken, wird ein Menü angezeigt, in dem Sie eine Beziehung bearbeiten, abbrechen, stilllegen, unterbrechen, entfernen oder fortsetzen können.

  In den folgenden Fällen werden die Menüs nicht angezeigt:

  - Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operator-Berechtigungen verfügen
  - Wenn sich das Volume in einer synchronen Schutzbeziehung befindet
  - Wenn die Volume-ID unbekannt ist, beispielsweise wenn Sie eine Intercluster-Beziehung haben und der Zielcluster noch nicht erkannt wurde, können Sie durch Klicken auf ein anderes Volume in der Topologie Informationen zu diesem Volume auswählen und anzeigen. Ein Fragezeichen ( ) in der oberen linken Ecke eines Volumes zeigt an, dass das Volume entweder fehlt oder noch nicht erkannt wurde. Es kann auch darauf hinweisen, dass die Kapazitätsinformationen fehlen. Wenn Sie den Cursor über das Fragezeichen bewegen, werden zusätzliche Informationen angezeigt, darunter auch Vorschläge für Abhilfemaßnahmen.

  Die Topologie zeigt Informationen zu Volumekapazität, Verzögerung, Snapshot-Kopien und der letzten erfolgreichen Datenübertragung an, wenn sie einer der mehreren gängigen Topologievorlagen entspricht. Wenn eine Topologie nicht einer dieser Vorlagen entspricht, werden Informationen zur Volumeverzögerung und zur letzten erfolgreichen Datenübertragung in einer Beziehungstabelle unter der Topologie angezeigt. In diesem Fall zeigt die hervorgehobene Zeile in der Tabelle das ausgewählte Volume an und in der Topologieansicht zeigen fette Linien mit einem blauen Punkt die Beziehung zwischen dem ausgewählten Volume und seinem Quellvolume an.

Topologieansichten enthalten die folgenden Informationen:

- Kapazität

  Zeigt die Gesamtkapazität an, die vom Volume verwendet wird. Wenn Sie den Cursor über einem Volume in der Topologie positionieren, werden im Dialogfeld „Aktuelle Schwellenwerteinstellungen“ die aktuellen Warn- und kritischen Schwellenwerteinstellungen für dieses Volume angezeigt. Sie können die Schwellenwerteinstellungen auch bearbeiten, indem Sie im Dialogfeld „Aktuelle Schwellenwerteinstellungen“ auf den Link **Schwellenwerte bearbeiten** klicken. Wenn Sie das Kontrollkästchen **Kapazität** deaktivieren, werden alle Kapazitätsinformationen für alle Volumes in der Topologie ausgeblendet.

- Verzögerung

  Zeigt die Verzögerungsdauer und den Verzögerungsstatus der eingehenden Schutzbeziehungen an. Durch Deaktivieren des Kontrollkästchens **Lag** werden alle Verzögerungsinformationen für alle Volumes in der Topologie ausgeblendet. Wenn das Kontrollkästchen **Lag** abgeblendet ist, werden die Lag-Informationen für das ausgewählte Volume in der Beziehungstabelle unter der Topologie angezeigt, sowie die Lag-Informationen für alle zugehörigen Volumes.

- Schnappschuss

  Zeigt die Anzahl der für ein Volume verfügbaren Snapshot-Kopien an. Durch Deaktivieren des Kontrollkästchens **Snapshot** werden alle Snapshot-Kopierinformationen für alle Volumes in der Topologie ausgeblendet. Klicken Sie auf das Symbol zum Kopieren eines Snapshots () zeigt die Snapshot-Kopienliste für ein Volume an. Die neben dem Symbol angezeigte Anzahl der Snapshot-Kopien wird etwa stündlich aktualisiert. Die Liste der Snapshot-Kopien wird jedoch aktualisiert, wenn Sie auf das Symbol klicken. Dies kann zu einer Abweichung zwischen der in der Topologie angezeigten Anzahl der Snapshot-Kopien und der Anzahl der Snapshot-Kopien führen, die beim Klicken auf das Symbol aufgelistet werden.

- Letzte erfolgreiche Übertragung

  Zeigt Betrag, Dauer, Uhrzeit und Datum der letzten erfolgreichen Datenübertragung an. Wenn das Kontrollkästchen **Letzte erfolgreiche Übertragung** abgeblendet ist, werden die Informationen zur letzten erfolgreichen Übertragung für das ausgewählte Volume in der Beziehungstabelle unter der Topologie sowie die Informationen zur letzten erfolgreichen Übertragung für alle zugehörigen Volumes angezeigt.

    - **Geschichte**

      Zeigt in einem Diagramm den Verlauf der eingehenden SnapMirror und SnapVault -Schutzbeziehungen für das ausgewählte Volume an. Es stehen drei Verlaufsdiagramme zur Verfügung: Verzögerungsdauer eingehender Beziehungen, Dauer eingehender Beziehungsübertragungen und Größe eingehender Beziehungsübertragungen. Verlaufsinformationen 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 synchrone Consistency Group- und SnapMirror -Beziehungen geschützt sind, werden keine Informationen zur Übertragungsdauer und Übertragungsgröße der Beziehung angezeigt.

  Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Verlaufsbereich auswählen. Sie können auch Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Mithilfe von Verlaufsdiagrammen können Sie Trends erkennen: Wenn beispielsweise große Datenmengen zur gleichen Tages- oder Wochenzeit übertragen werden oder wenn der Schwellenwert für Verzögerungswarnungen oder Verzögerungsfehler ständig überschritten wird, können Sie entsprechende Maßnahmen ergreifen. Darüber hinaus können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie gerade anzeigen.

In den Schutzverlaufsdiagrammen werden die folgenden Informationen angezeigt:

- **Dauer der Beziehungsverzögerung**

  Zeigt je nach ausgewähltem Zeitraum Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Tage, Monate oder Jahre auf der horizontalen Achse (x) an. Der obere Wert auf der y-Achse gibt die maximale Verzögerungsdauer an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. Die horizontale orange Linie im Diagramm stellt den Schwellenwert für den Verzögerungsfehler dar und die horizontale gelbe Linie stellt den Schwellenwert für die Verzögerungswarnung dar. Wenn Sie den Cursor über diese Linien bewegen, wird die Schwellenwerteinstellung angezeigt. Die horizontale blaue Linie stellt die Verzögerungsdauer dar. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen gewünschten Bereich bewegen.

- **Dauer der Beziehungsübertragung**

  Zeigt je nach ausgewähltem Zeitraum Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Tage, Monate oder Jahre auf der horizontalen Achse (x) an. Der obere Wert auf der y-Achse gibt die maximale Übertragungsdauer an, die in dem auf der x-Achse dargestellten Zeitraum erreicht wurde. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den gewünschten Bereich bewegen.

  Dieses Diagramm ist für Datenträger in synchronen Schutzbeziehungen nicht verfügbar.

- **Beziehung übertragene Größe**

  Zeigt je nach Übertragungsgröße Bytes, Kilobytes, Megabytes usw. auf der vertikalen Achse (y) an und zeigt je nach ausgewähltem Zeitraum Tage, Monate oder Jahre auf der horizontalen Achse (x) an. Der obere Wert auf der y-Achse gibt die maximale Übertragungsgröße an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen gewünschten Bereich bewegen.

  Dieses Diagramm ist für Datenträger in synchronen Schutzbeziehungen nicht verfügbar.

Geschichtsbereich

Im Bereich „Verlauf“ werden Diagramme angezeigt, die Informationen zur Kapazität und den Speicherplatzreservierungen des ausgewählten Volumes liefern. Darüber hinaus können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie gerade anzeigen.

Wenn die Daten oder der Zustand des Datenträgers über einen bestimmten Zeitraum unverändert bleiben, sind die Diagramme möglicherweise leer und die Meldung „Keine Daten gefunden“ wird angezeigt.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Verlaufsbereich auswählen. Sie können auch Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Mithilfe von Verlaufsdiagrammen können Sie Trends erkennen. Wenn beispielsweise die Datenträgernutzung ständig den Schwellenwert „Fast voll“ überschreitet, können Sie entsprechende Maßnahmen ergreifen.

Verlaufsdiagramme zeigen die folgenden Informationen an:

- **Verwendete Volumenkapazität**

  Zeigt die verwendete Kapazität des Datenträgers und den Trend der Datenträgerkapazitätsnutzung

basierend auf dem Nutzungsverlauf als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der vertikalen Achse (y) an. Der Zeitraum wird auf der horizontalen (x) Achse angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen bestimmten Bereich bewegen. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Volume Used Capacity“ klicken, wird die Diagrammlinie „Volume Used Capacity“ ausgeblendet.

- **Verwendete Volumenkapazität im Vergleich zum Gesamtvolumen**

  Zeigt den Trend der Nutzung der Volume-Kapazität basierend auf dem Nutzungsverlauf sowie die genutzte Kapazität, die Gesamtkapazität und Details zu den Speicherplatzeinsparungen durch Deduplizierung und Komprimierung als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der vertikalen (y-)Achse an. Der Zeitraum wird auf der horizontalen (x) Achse angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen bestimmten Bereich bewegen. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Trend der genutzten Kapazität“ klicken, wird die Diagrammlinie „Trend der genutzten Kapazität“ ausgeblendet.

- **Genutzte Volumenkapazität (%)**

  Zeigt die genutzte Kapazität des Datenträgers und den Trend der Nutzung der Datenträgerkapazität basierend auf dem Nutzungsverlauf als Liniendiagramm in Prozent auf der vertikalen Achse (y) an. Der Zeitraum wird auf der horizontalen (x) Achse angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen bestimmten Bereich bewegen. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Volume Used Capacity“ klicken, wird die Diagrammlinie „Volume Used Capacity“ ausgeblendet.

- **Genutzte Snapshot-Kapazität (%)**

  Zeigt die Snapshot-Reserve und den Snapshot-Warnschwellenwert als Liniendiagramme und die von den Snapshot-Kopien verwendete Kapazität als Flächendiagramm in Prozent auf der vertikalen (y) Achse an. Der Snapshot-Überlauf wird mit unterschiedlichen Farben dargestellt. Der Zeitraum wird auf der horizontalen (x) Achse angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen bestimmten Bereich bewegen. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Snapshot Reserve“ klicken, wird die Diagrammlinie „Snapshot Reserve“ ausgeblendet.

Ereignisliste

In der Ereignisliste werden Details zu neuen und bestätigten Ereignissen angezeigt:

- **Schwere**

  Zeigt den Schweregrad des Ereignisses an.

- **Ereignis**

  Zeigt den Ereignisnamen an.

- **Ausgelöste Zeit**

Zeigt die Zeit an, die seit der Generierung des Ereignisses vergangen ist. Wenn die verstrichene Zeit mehr als eine Woche beträgt, wird der Zeitstempel angezeigt, wann das Ereignis generiert wurde.

Bereich „Zugehörige Anmerkungen“

Im Bereich „Zugehörige Anmerkungen“ können Sie Anmerkungsdetails anzeigen, die mit dem ausgewählten Datenträger verknüpft sind. Zu den Details gehören der Anmerkungsname und die Anmerkungswerte, die auf das Volume angewendet werden. Sie können manuelle Anmerkungen auch aus dem Bereich „Verwandte Anmerkungen“ entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie die SVMs, Aggregate, Qtrees, LUNs und Snapshot-Kopien anzeigen und zu ihnen navigieren, die mit dem Volume in Zusammenhang stehen:

- **Virtuelle Speichermaschine**

  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. Bei FlexGroup -Volumes wird die Anzahl der Aggregate aufgelistet, aus denen die FlexGroup besteht.

- **Volumina im Aggregat**

  Zeigt die Anzahl und Kapazität aller Volumes an, die zum übergeordneten Aggregat des ausgewählten Volumes gehören. Außerdem wird der Integritätsstatus der Volumes basierend auf dem höchsten Schweregrad angezeigt. Wenn ein Aggregat beispielsweise zehn Volumes enthält, von denen fünf den Status „Warnung“ und die restlichen fünf den Status „Kritisch“ anzeigen, wird der Status „Kritisch“ angezeigt. Diese Komponente wird für FlexGroup -Volumes nicht angezeigt.

- **Qtrees**

  Zeigt die Anzahl der Qtrees an, die das ausgewählte Volume enthält, und die Kapazität der Qtrees mit Kontingent, die das ausgewählte Volume enthält. Die Kapazität der Qtrees mit Quota wird im Verhältnis zur Datenkapazität des Volumes angezeigt. Der Gesundheitszustand der Qtrees wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Wenn ein Volume beispielsweise zehn Qtrees hat, fünf mit dem Status „Warnung“ und die restlichen fünf mit dem Status „Kritisch“, dann wird der Status „Kritisch“ angezeigt.

- **NFS-Freigaben**

  Zeigt die Anzahl und den Status der mit dem Volume verknüpften NFS-Freigaben an.

- **SMB-Freigaben**

  Zeigt die Anzahl und den Status der SMB/CIFS-Freigaben an.

- **LUNs**

  Zeigt die Anzahl und Gesamtgröße aller LUNs im ausgewählten Volume an. Der Integritätsstatus der LUNs wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad.

- **Benutzer- und Gruppenkontingente**

Zeigt die Anzahl und den Status der Benutzer- und Benutzergruppenkontingente an, die dem Volume und seinen Qtrees zugeordnet sind.

- * FlexClone -Volumes*

  Zeigt die Anzahl und Kapazität aller geklonten Volumes des ausgewählten Volumes an. Die Anzahl und Kapazität werden nur angezeigt, wenn das ausgewählte Volume geklonte Volumes enthält.

- **Übergeordnetes Volume**

  Zeigt den Namen und die Kapazität des übergeordneten Volumes eines ausgewählten FlexClone -Volumes 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 mit dem ausgewählten Volume verknüpften Gruppen anzeigen.

Bereich „Zugehörige Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnungen 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 Warnungsnamen klicken.

Seite mit Speicher-VM-/Integritätsdetails

Auf der Seite „Storage VM / Health Details“ können Sie ausführliche Informationen zur ausgewählten Storage VM anzeigen, beispielsweise deren Integrität, Kapazität, Konfiguration, Datenrichtlinien, logische Schnittstellen (LIFs), LUNs, Qtrees, Benutzer, Benutzergruppenkontingente und Schutzdetails. Sie können auch Informationen zu den zugehörigen Objekten und zugehörigen Warnungen für die Speicher-VM anzeigen.

Sie können nur die Datenspeicher-VM überwachen.

Befehlsschaltflächen

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

- **Zur Leistungsansicht wechseln**

  Ermöglicht Ihnen die Navigation zur Seite mit den Storage-VM-/Leistungsdetails.

- **Aktionen**
  - Benachrichtigung hinzufügen

    Ermöglicht Ihnen, der ausgewählten Speicher-VM eine Warnung hinzuzufügen.

  - Kommentieren

    Ermöglicht Ihnen, die ausgewählte Speicher-VM mit Anmerkungen zu versehen.

- **Speicher-VMs anzeigen**

  Ermöglicht Ihnen die Navigation zur Ansicht „Integrität: Alle Speicher-VMs“.

Registerkarte „Integrität“

Auf der Registerkarte „Integrität“ werden detaillierte Informationen zur Datenverfügbarkeit, Datenkapazität und zu Schutzproblemen verschiedener Objekte wie Volumes, Aggregaten, NAS-LIFs, SAN-LIFs, LUNs, Protokollen, Diensten, NFS-Freigaben und CIFS-Freigaben angezeigt.

Sie können auf das Diagramm eines Objekts klicken, um die gefilterte Objektliste anzuzeigen. Sie können beispielsweise auf das Volume-Kapazitätsdiagramm klicken, das Warnungen anzeigt, um die Liste der Volumes anzuzeigen, bei denen Kapazitätsprobleme mit dem Schweregrad „Warnung“ vorliegen.

- **Verfügbarkeitsprobleme**

  Zeigt die Gesamtzahl der Objekte als Diagramm an, einschließlich der Objekte mit Verfügbarkeitsproblemen und der Objekte ohne Verfügbarkeitsprobleme. Die Farben im Diagramm stellen die unterschiedlichen Schweregrade der Probleme dar. Die Informationen unter dem Diagramm enthalten Details zu Verfügbarkeitsproblemen, die die Verfügbarkeit von Daten in der Speicher-VM beeinträchtigen können oder bereits beeinträchtigt haben. Beispielsweise werden Informationen zu den ausgefallenen NAS-LIFs und SAN-LIFs sowie zu den offline geschalteten Volumes angezeigt.

  Sie können auch Informationen zu den zugehörigen Protokollen und Diensten anzeigen, die derzeit ausgeführt werden, sowie die Anzahl und den Status der NFS- und CIFS-Freigaben.

- **Kapazitätsprobleme**

  Zeigt die Gesamtzahl der Objekte als Diagramm an, einschließlich der Objekte mit Kapazitätsproblemen und der Objekte ohne kapazitätsbezogene Probleme. Die Farben im Diagramm stellen die unterschiedlichen Schweregrade der Probleme dar. Die Informationen unter dem Diagramm enthalten Einzelheiten zu Kapazitätsproblemen, die sich auf die Datenkapazität in der Speicher-VM auswirken können oder bereits ausgewirkt haben. Beispielsweise werden Informationen zu Aggregaten angezeigt, bei denen die Wahrscheinlichkeit einer Überschreitung der festgelegten Schwellenwerte besteht.

- **Schutzprobleme**

  Bietet einen schnellen Überblick über den schutzbezogenen Zustand der Speicher-VM, indem in einem Felddialogfeld die Gesamtzahl der Beziehungen angezeigt wird, einschließlich der Beziehungen mit Schutzproblemen und der Beziehungen ohne schutzbezogene Probleme. Sie können auch den Status der Speicher-VM-DR-Beziehung für die ausgewählte Speicher-VM anzeigen. Die Ereignisse der Speicher-VM-DR-Beziehungen werden hier angezeigt. Durch Klicken auf die Ereignisse gelangen Sie zur Seite mit den Ereignisdetails. Wenn ungeschützte Volumes vorhanden sind, gelangen Sie durch Klicken auf den Link zur Ansicht „Integrität: Alle Volumes“, wo Sie eine gefilterte Liste der ungeschützten Volumes auf der Speicher-VM anzeigen können. Die Farben im Diagramm stellen die unterschiedlichen Schweregrade der Probleme dar. Durch Klicken auf ein Diagramm gelangen Sie zur Ansicht „Beziehung: Alle Beziehungen“, in der Sie eine gefilterte Liste mit Details zu Schutzbeziehungen anzeigen können. Die Informationen unter dem Diagramm enthalten Einzelheiten zu Schutzproblemen, die den Schutz der Daten in der Speicher-VM beeinträchtigen können oder bereits beeinträchtigt haben. Beispielsweise werden Informationen zu Volumes angezeigt, deren Snapshot-Kopierreserve fast voll ist, oder zu Verzögerungsproblemen bei der SnapMirror Beziehung.

Registerkarte „Kapazität“

Auf der Registerkarte „Kapazität“ werden detaillierte Informationen zur Datenkapazität der ausgewählten SVM angezeigt.

Für eine Storage-VM mit FlexVol volume oder FlexGroup -Volume werden folgende Informationen angezeigt:

- **Kapazität**

  Im Bereich „Kapazität“ werden Details zur verwendeten und verfügbaren Kapazität angezeigt, die allen Volumes zugewiesen wurde:

  - Gesamtkapazität

    Zeigt die Gesamtkapazität der Storage-VM an.

  - Gebraucht

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

  - Garantiert verfügbar

    Zeigt den garantiert verfügbaren Speicherplatz für Daten an, der für Volumes in der Storage-VM verfügbar ist.

  - Nicht garantiert

    Zeigt den verbleibenden verfügbaren Speicherplatz für Daten an, der Thin Provisioning-Volumes in der Storage-VM zugewiesen ist.

- **Volumes mit Kapazitätsproblemen**

  Die Liste „Volumes mit Kapazitätsproblemen“ zeigt in tabellarischer Form Details zu den Volumes mit Kapazitätsproblemen an:

  - Status

    Zeigt an, dass das Volume ein kapazitätsbezogenes Problem mit einem angegebenen Schweregrad aufweist.

    Sie können den Zeiger über den Status bewegen, um weitere Informationen zu dem bzw. den für das Volume generierten kapazitätsbezogenen Ereignissen anzuzeigen.

    Wenn der Status des Volumes durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum der Ereignisauslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Über die Schaltfläche **Details anzeigen** können Sie weitere Informationen zur Veranstaltung anzeigen.

    Wenn der Status des Volumes durch mehrere Ereignisse mit demselben Schweregrad bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu jedem dieser Ereignisse 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 mit demselben oder unterschiedlichen Schweregrad aufweisen. Es wird jedoch nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Volume zwei Ereignisse mit den Schweregraden „Fehler“ und „Warnung“ aufweist, wird nur der Schweregrad „Fehler“ angezeigt.

- Volumen

  Zeigt den Namen des Volumes an.

- Verwendete Datenkapazität

  Zeigt als Diagramm Informationen zur Volume-Kapazitätsnutzung (in Prozent) an.

- Tage bis zur vollständigen

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor das Volume seine volle Kapazität erreicht.

- Thin Provisioning

  Zeigt an, ob für das ausgewählte Volume eine Speicherplatzgarantie festgelegt ist. Gültige Werte sind Ja und Nein.

- Aggregate

  Zeigt bei FlexVol -Volumes den Namen des Aggregats an, das das Volume enthält. Zeigt für FlexGroup -Volumes die Anzahl der Aggregate an, die in der FlexGroup verwendet werden.

Registerkarte „Konfiguration“

Auf der Registerkarte „Konfiguration“ werden Konfigurationsdetails zur ausgewählten Speicher-VM angezeigt, z. B. ihr Cluster, ihr Stammvolume, der Typ der darin enthaltenen Volumes (FlexVol Volumes), Richtlinien und der auf der Speicher-VM erstellte Schutz:

- **Überblick**
  - Cluster

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

  - Zulässiger Datenträgertyp

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

  - Stammvolumen

    Zeigt den Namen des Stammvolumes der Speicher-VM an.

  - Erlaubte Protokolle

    Zeigt die Art der Protokolle an, die auf der Speicher-VM konfiguriert werden können. Zeigt außerdem an, ob ein Protokoll aktiv ist ( ), runter ( ) oder ist nicht konfiguriert ( ).

- **Datennetzwerkschnittstellen**

- NAS

  Zeigt die Anzahl der NAS-Schnittstellen an, die mit der Speicher-VM verknüpft sind. Zeigt außerdem an, ob die Schnittstellen aktiv sind ( ) oder nach unten ( ).

- SAN

  Zeigt die Anzahl der SAN-Schnittstellen an, die mit der Speicher-VM verknüpft sind. Zeigt außerdem an, ob die Schnittstellen aktiv sind ( ) oder nach unten ( ).

- FC-NVMe

  Zeigt die Anzahl der FC-NVMe-Schnittstellen an, die mit der Storage-VM verknüpft sind. Zeigt außerdem an, ob die Schnittstellen aktiv sind ( ) oder nach unten ( ).

- **Verwaltungsnetzwerkschnittstellen**
  - Verfügbarkeit

    Zeigt die Anzahl der Verwaltungsschnittstellen an, die mit der Storage-VM verknüpft sind. Zeigt außerdem an, ob die Verwaltungsschnittstellen aktiv sind ( ) oder nach unten ( ).

- **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 die Anzahl der Exportrichtlinien, wenn mehrere Richtlinien erstellt werden.

- **Schutz**
  - Speicher-VM-DR

    Zeigt an, ob die ausgewählte Speicher-VM geschützt, Ziel- oder ungeschützt ist, und den Namen des Ziels, auf dem die Speicher-VM geschützt ist. Wenn die ausgewählte Speicher-VM das Ziel ist, werden die Details der Quell-Speicher-VM angezeigt. Im Falle einer Fan-Out-Aufteilung zeigt dieses Feld die Gesamtzahl der Ziel-Speicher-VMs an, auf denen die Speicher-VM geschützt ist. Über den Zähllink gelangen Sie zum Beziehungsraster der Speicher-VM, gefiltert nach der Quell-Speicher-VM.

  - Geschützte Volumes

    Zeigt die Anzahl der geschützten Volumes auf der ausgewählten Speicher-VM im Verhältnis zur Gesamtzahl der Volumes an. Wenn Sie eine Ziel-Speicher-VM anzeigen, gilt der Nummernlink für die Zielvolumes der ausgewählten Speicher-VM.

  - Ungeschützte Volumes

    Zeigt die Anzahl der ungeschützten Volumes auf der ausgewählten Speicher-VM an.

- **Dienstleistungen**
  - Typ

    Zeigt den Diensttyp an, der auf der Speicher-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 ( ), Runter ( ) oder Nicht konfiguriert ( ).

- Domänenname

  Zeigt die vollqualifizierten Domänennamen (FQDNs) des DNS-Servers für die DNS-Dienste oder des NIS-Servers 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 Speicher-VM erstellt werden:

- **Netzwerkschnittstelle**

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

- **Betriebsstatus**

  Zeigt den Betriebsstatus der Schnittstelle an, der Aktiv sein kann ( ), Runter ( ) oder Unbekannt ( ). Der Betriebsstatus einer Schnittstelle wird durch den Status ihrer physischen Ports bestimmt.

- **Verwaltungsstatus**

  Zeigt den Verwaltungsstatus der Schnittstelle an, der Aktiv sein kann ( ), Runter ( ) oder Unbekannt ( ). Der Verwaltungsstatus einer Schnittstelle wird vom Speicheradministrator gesteuert, um Änderungen an der Konfiguration vorzunehmen oder zu Wartungszwecken. Der Verwaltungsstatus kann vom Betriebsstatus abweichen. Wenn der Verwaltungsstatus einer Schnittstelle jedoch „Down“ lautet, ist der Betriebsstatus standardmäßig „Down“.

- **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.

- **Heimathafen**

Zeigt den physischen Port an, mit dem die Schnittstelle ursprünglich verknüpft war.

- **Aktueller Hafen**

  Zeigt den physischen Port an, mit dem die Schnittstelle derzeit verknüpft ist. Wenn die Schnittstelle migriert wird, kann der aktuelle Port vom Home-Port abweichen.

- **Port-Set**

  Zeigt den Portsatz 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 Standard-Failover-Richtlinie „Next Available“ (Nächste verfügbare Option). Die Failover-Richtlinie gilt nicht für FC- und iSCSI-Schnittstellen.

- **Routing-Gruppen**

  Zeigt den Namen der Routinggruppe an. Weitere Informationen zu den Routen und dem Ziel-Gateway können Sie anzeigen, indem Sie auf den Namen der Routinggruppe klicken.

  Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt und 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 Integritätsschwellenwerteinstellungen für die Qtree-Kapazität für einen oder mehrere Qtrees bearbeiten möchten.

Verwenden Sie die Schaltfläche **Exportieren**, um eine Datei mit durch Kommas getrennten Werten (.csv) zu erstellen, die die Details aller überwachten Qtrees enthält. Beim Exportieren in eine CSV-Datei können Sie wählen, ob Sie einen Qtrees-Bericht für die aktuelle Speicher-VM, für alle Speicher-VMs im aktuellen Cluster oder für alle Speicher-VMs für alle Cluster in Ihrem Rechenzentrum erstellen möchten. In der exportierten CSV-Datei werden einige zusätzliche Qtrees-Felder angezeigt.

- **Status**

  Zeigt den aktuellen Status des Qtree an. Der Status kann „Kritisch“ ( ), Fehler ( ), Warnung ( ) oder Normal ( ).

  Sie können den Zeiger über das Statussymbol bewegen, um weitere Informationen zu dem oder den für den Qtree generierten Ereignissen anzuzeigen.

  Wenn der Status des Qtree durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum der Ereignisauslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Mit **Details anzeigen** können Sie weitere Informationen zur Veranstaltung anzeigen.

  Wenn der Status des Qtree durch mehrere Ereignisse mit demselben Schweregrad bestimmt wird, werden

die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu jedem dieser Ereignisse 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 mit derselben oder unterschiedlichen Schweregraden aufweisen. Es wird jedoch nur der höchste Schweregrad angezeigt. Wenn ein Qtree beispielsweise zwei Ereignisse mit den Schweregraden „Fehler“ und „Warnung“ aufweist, wird nur der Schweregrad „Fehler“ angezeigt.

- **Qtree**

  Zeigt den Namen des Qtree an.

- **Cluster**

  Zeigt den Namen des Clusters an, der den Qtree enthält. Erscheint nur in der exportierten CSV-Datei.

- **Virtuelle Speichermaschine**

  Zeigt den Namen der Storage Virtual Machine (SVM) an, die den Qtree enthält. Erscheint nur in der exportierten CSV-Datei.

- **Volumen**

  Zeigt den Namen des Datenträgers an, der den Qtree enthält.

  Sie können den Zeiger über den Datenträgernamen bewegen, um weitere Informationen zum Datenträger anzuzeigen.

- **Kontingent festgelegt**

  Gibt an, ob im Qtree ein Kontingent aktiviert oder deaktiviert ist.

- **Kontingenttyp**

  Gibt an, ob das Kontingent für einen Benutzer, eine Benutzergruppe oder einen Qtree gilt. Erscheint nur in der exportierten CSV-Datei.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Für jeden Benutzer und jede Benutzergruppe gibt es mehrere Zeilen. Wenn der Kontingenttyp „qtree“ ist oder das Kontingent nicht festgelegt ist, ist die Spalte leer. Erscheint nur in der exportierten CSV-Datei.

- **Datenträgernutzung %**

  Zeigt den Prozentsatz des belegten Speicherplatzes an. Wenn ein Festplattenlimit festgelegt ist, basiert dieser Wert auf dem Festplattenlimit. Wenn das Kontingent ohne festes Festplattenlimit festgelegt wird, basiert der Wert auf dem Datenspeicherplatz des Volumes. Wenn das Kontingent nicht festgelegt ist oder die Kontingente auf dem Volume, zu dem der Qtree gehört, deaktiviert sind, wird auf der Rasterseite „Nicht zutreffend“ angezeigt und das Feld in den CSV-Exportdaten ist leer.

- **Festplattenlimit**

Zeigt die maximale Menge an Speicherplatz an, die dem Qtree zugewiesen ist. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht ist und keine weiteren Schreibvorgänge auf die Festplatte mehr zulässig sind. Der Wert wird unter den folgenden Bedingungen als „Unbegrenzt“ angezeigt: wenn das Kontingent ohne Festplattenlimit festgelegt ist, wenn das Kontingent nicht festgelegt ist oder wenn die Kontingente auf dem Volume, zu dem der Qtree gehört, deaktiviert sind.

- **Festplatten-Softlimit**

  Zeigt die Menge an Speicherplatz an, die dem Qtree zugewiesen wird, bevor ein Warnereignis generiert wird. Der Wert wird unter den folgenden Bedingungen als „Unbegrenzt“ angezeigt: wenn das Kontingent ohne weiche Festplattenbegrenzung festgelegt ist, wenn das Kontingent nicht festgelegt ist oder wenn die Kontingente auf dem Volume, zu dem der Qtree gehört, deaktiviert sind. Standardmäßig ist diese Spalte ausgeblendet.

- **Festplattenschwelle**

  Zeigt den für den Speicherplatz festgelegten Schwellenwert an. Der Wert wird unter den folgenden Bedingungen als „Unbegrenzt“ angezeigt: wenn das Kontingent ohne Festplattenschwellenwert festgelegt ist, wenn das Kontingent nicht festgelegt ist oder wenn die Kontingente auf dem Volume, zu dem der Qtree gehört, deaktiviert sind. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im Qtree verwendeten Dateien an. Wenn das harte Dateilimit festgelegt ist, basiert dieser Wert auf dem harten Dateilimit. Wenn das Kontingent ohne feste Dateibeschränkung festgelegt ist, wird kein Wert angezeigt. Wenn das Kontingent nicht festgelegt ist oder die Kontingente auf dem Volume, zu dem der Qtree gehört, deaktiviert sind, wird auf der Rasterseite „Nicht zutreffend“ angezeigt und das Feld in den CSV-Exportdaten ist leer.

- **Datei-Hartlimit**

  Zeigt die feste Grenze für die Anzahl der in den Qtrees zulässigen Dateien an. Der Wert wird unter den folgenden Bedingungen als „Unbegrenzt“ angezeigt: wenn das Kontingent ohne harte Dateibeschränkung festgelegt ist, wenn das Kontingent nicht festgelegt ist oder wenn die Kontingente auf dem Volume, zu dem der Qtree gehört, deaktiviert sind.

- **Datei-Softlimit**

  Zeigt das Soft-Limit für die Anzahl der in den Qtrees zulässigen Dateien an. Der Wert wird unter den folgenden Bedingungen als „Unbegrenzt“ angezeigt: wenn das Kontingent ohne weiche Dateibegrenzung festgelegt ist, wenn das Kontingent nicht festgelegt ist oder wenn die Kontingente auf dem Datenträger, zu dem der Qtree gehört, deaktiviert sind. Standardmäßig ist diese Spalte ausgeblendet.

Registerkarte „Benutzer- und Gruppenkontingente“

Zeigt Details zu den Benutzer- und Benutzergruppenkontingenten für die ausgewählte Speicher-VM an. Sie können Informationen wie den Status des Kontingents, den Namen des Benutzers oder der Benutzergruppe, die für die Datenträger und Dateien festgelegten weichen und harten Grenzwerte, die Menge des verwendeten Speicherplatzes und die Anzahl der Dateien sowie den Datenträgerschwellenwert anzeigen. Sie können auch die einem Benutzer oder einer Benutzergruppe zugeordnete E-Mail-Adresse ändern.

- **Befehlsschaltfläche „E-Mail-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 über dasselbe Kontingent verfügen, werden die Namen der Benutzer als durch Kommas getrennte Werte angezeigt. Außerdem wird die Standardregel nicht zum Generieren der E-Mail-Adresse verwendet. Daher müssen Sie die erforderliche E-Mail-Adresse angeben, damit Benachrichtigungen gesendet werden können.

- **Befehlsschaltfläche „E-Mail-Regeln konfigurieren“**

  Ermöglicht Ihnen das Erstellen oder Ändern von Regeln zum Generieren einer E-Mail-Adresse für die Benutzer- oder Benutzergruppenkontingente, die auf der Speicher-VM konfiguriert sind. Bei einer Quotenüberschreitung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

- **Status**

  Zeigt den aktuellen Status des Kontingents an. Der Status kann „Kritisch“ ( ), Warnung ( ) oder Normal ( ).

  Sie können den Zeiger über das Statussymbol bewegen, um weitere Informationen zu dem oder den für das Kontingent generierten Ereignissen anzuzeigen.

  Wenn der Status des Kontingents durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum der Ereignisauslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Mit **Details anzeigen** können Sie weitere Informationen zur Veranstaltung anzeigen.

  Wenn der Status des Kontingents durch mehrere Ereignisse mit demselben Schweregrad bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu jedem dieser Ereignisse anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch **Alle Ereignisse anzeigen** verwenden, um die Liste der generierten Ereignisse anzuzeigen.

  > Ein Kontingent kann mehrere Ereignisse mit demselben oder unterschiedlichen Schweregrad enthalten. Es wird jedoch nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Kontingent zwei Ereignisse mit den Schweregraden „Fehler“ und „Warnung“ aufweist, wird nur der Schweregrad „Fehler“ angezeigt.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Wenn mehrere Benutzer über dasselbe Kontingent verfügen, werden die Namen der Benutzer als durch Kommas getrennte Werte angezeigt.

  Der Wert wird als „Unbekannt“ angezeigt, wenn ONTAP aufgrund von SecD-Fehlern keinen gültigen Benutzernamen bereitstellt.

- **Typ**

  Gibt an, ob das Kontingent für einen Benutzer oder eine Benutzergruppe gilt.

- **Volume oder Qtree**

  Zeigt den Namen des Volumes oder Qtree an, auf dem das Benutzer- oder Benutzergruppenkontingent angegeben ist.

Sie können den Zeiger über den Namen des Volumes oder Qtree bewegen, um weitere Informationen zum Volume oder Qtree anzuzeigen.

- **Datenträgernutzung %**

  Zeigt den Prozentsatz des belegten Speicherplatzes an. Der Wert wird als „Nicht zutreffend“ angezeigt, wenn das Kontingent ohne feste Festplattenbegrenzung festgelegt ist.

- **Festplattenlimit**

  Zeigt die maximale Menge an Speicherplatz an, die für das Kontingent zugewiesen ist. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht ist und keine weiteren Schreibvorgänge auf die Festplatte mehr zulässig sind. Der Wert wird als „Unbegrenzt“ angezeigt, wenn das Kontingent ohne feste Festplattenbegrenzung festgelegt ist.

- **Festplatten-Softlimit**

  Zeigt die Menge an Speicherplatz an, die dem Kontingent zugewiesen ist, bevor ein Warnereignis generiert wird. Der Wert wird als „Unbegrenzt“ angezeigt, wenn das Kontingent ohne weiche Festplattenbegrenzung festgelegt ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Festplattenschwelle**

  Zeigt den für den Speicherplatz festgelegten Schwellenwert an. Der Wert wird als „Unbegrenzt“ angezeigt, wenn das Kontingent ohne Festplattenschwellenwert festgelegt ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im Qtree verwendeten Dateien an. Der Wert wird als „Nicht zutreffend“ angezeigt, wenn das Kontingent ohne harte Dateibeschränkung festgelegt ist.

- **Datei-Hartlimit**

  Zeigt die feste Grenze für die Anzahl der im Kontingent zulässigen Dateien an. Der Wert wird als „Unbegrenzt“ angezeigt, wenn das Kontingent ohne feste Dateibeschränkung festgelegt ist.

- **Datei-Softlimit**

  Zeigt das Soft-Limit für die Anzahl der im Kontingent zulässigen Dateien an. Der Wert wird als „Unbegrenzt“ angezeigt, wenn das Kontingent ohne weiche Dateibeschränkung festgelegt ist. 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 es zu einer Quotenüberschreitung kommt.

Registerkarte „NFS-Freigaben“

Auf der Registerkarte „NFS-Freigaben“ werden Informationen zu NFS-Freigaben angezeigt, z. B. deren Status, der mit dem Volume verknüpfte Pfad (FlexGroup Volumes oder FlexVol -Volumes), Zugriffsebenen von Clients auf die NFS-Freigaben und die für die exportierten Volumes definierte Exportrichtlinie. NFS-Freigaben werden unter folgenden Bedingungen nicht angezeigt: wenn das Volume nicht gemountet ist 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 ( ) oder Normal ( ).

- **Kreuzungspfad**

  Zeigt den Pfad an, in dem das Volume eingebunden ist. Wenn eine explizite NFS-Exportrichtlinie auf einen Qtree angewendet wird, zeigt die Spalte den Pfad des Volumes an, über das auf den Qtree zugegriffen werden kann.

- **Kreuzungspfad aktiv**

  Zeigt an, ob der Pfad zum Zugriff auf das bereitgestellte Volume aktiv oder inaktiv ist.

- **Volume 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, zeigt die Spalte sowohl den Namen des Volumes als auch den des Qtree an.

  Über den Link können Sie sich Details zum Objekt auf der jeweiligen Detailseite anzeigen lassen. Wenn es sich bei dem Objekt um einen Qtree handelt, werden Links sowohl für den Qtree als auch für das Volume angezeigt.

- **Volumenstatus**

  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 erlaubt.

  - Eingeschränkt

    Eingeschränkte Vorgänge, wie etwa die Rekonstruktion der Parität, sind zulässig, der Datenzugriff ist jedoch nicht gestattet.

  - Gemischt

    Die Bestandteile eines FlexGroup -Volumes befinden sich nicht alle im gleichen Zustand.

- **Sicherheitsstil**

  Zeigt die Zugriffsberechtigung für die zu exportierenden Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder Mixed sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume verfügen über UNIX-Berechtigungen.

  - Einheitlich

Dateien und Verzeichnisse im Volume haben einen einheitlichen Sicherheitsstil.

- NTFS (CIFS-Clients)

  Dateien und Verzeichnisse im Volume verfügen über Windows NTFS-Berechtigungen.

- Gemischt

  Dateien und Verzeichnisse im Volume können entweder UNIX-Berechtigungen oder Windows NTFS-Berechtigungen haben.

- **UNIX-Berechtigung**

  Zeigt die UNIX-Berechtigungsbits in einem oktalen Zeichenfolgenformat an, das für die exportierten Datenträger 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 mit der Exportrichtlinie verknüpften Regeln anzuzeigen, z. B. zu den Authentifizierungsprotokollen und der Zugriffsberechtigung.

Registerkarte „SMB-Freigaben“

Zeigt Informationen zu den SMB-Freigaben auf der ausgewählten Speicher-VM an. Sie können Informationen wie den Status der SMB-Freigabe, den Freigabenamen, den mit der Speicher-VM verknüpften Pfad, den Status des Verbindungspfads der Freigabe, das enthaltene Objekt, den Status des enthaltenden Volumes, die Sicherheitsdaten der Freigabe und die für die Freigabe definierten Exportrichtlinien anzeigen. Sie können auch feststellen, 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 Speicher-VM anzeigen.

- **ACL-Befehlsschaltfläche 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 ( ).

- **Freigabename**

  Zeigt den Namen der SMB-Freigabe an.

- **Weg**

  Zeigt den Verbindungspfad an, auf dem die Freigabe erstellt wird.

- **Kreuzungspfad aktiv**

  Zeigt an, ob der Pfad zum Zugriff auf die Freigabe aktiv oder inaktiv ist.

- **Enthaltendes Objekt**

  Zeigt den Namen des enthaltenen Objekts an, zu dem die Freigabe gehört. Das enthaltene Objekt kann ein Volume oder ein Qtree sein.

  Durch Klicken auf den Link können Sie Details zum enthaltenen Objekt auf der jeweiligen Detailseite anzeigen. Wenn das enthaltene Objekt ein Qtree ist, werden Links sowohl für den Qtree als auch für das Volume angezeigt.

- **Volumenstatus**

  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 erlaubt.

  - Eingeschränkt

    Eingeschränkte Vorgänge, wie etwa die Rekonstruktion der Parität, sind zulässig, der Datenzugriff ist jedoch nicht gestattet.

  - Gemischt

    Die Bestandteile eines FlexGroup -Volumes befinden sich nicht alle im gleichen Zustand.

- **Sicherheit**

  Zeigt die Zugriffsberechtigung für die zu exportierenden Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder Mixed sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume verfügen über UNIX-Berechtigungen.

  - Einheitlich

    Dateien und Verzeichnisse im Volume haben einen einheitlichen Sicherheitsstil.

  - NTFS (CIFS-Clients)

    Dateien und Verzeichnisse im Volume verfügen über Windows NTFS-Berechtigungen.

  - Gemischt

    Dateien und Verzeichnisse im Volume können entweder UNIX-Berechtigungen oder Windows NTFS-Berechtigungen haben.

- **Exportrichtlinie**

  Zeigt den Namen der für die Freigabe geltenden Exportrichtlinie an. Wenn für die Speicher-VM keine Exportrichtlinie angegeben ist, wird der Wert als „Nicht aktiviert“ angezeigt.

  Sie können auf den Link klicken, um Details zu den mit der Exportrichtlinie verknüpften Regeln anzuzeigen, z. B. Zugriffsprotokolle und Berechtigungen. Der Link ist deaktiviert, wenn die Exportrichtlinie für die ausgewählte Speicher-VM deaktiviert ist.

- **NFS-Äquivalent**

  Gibt an, ob es für die Freigabe ein NFS-Äquivalent gibt.

Registerkarte „SAN“

Zeigt Details zu LUNs, Initiatorgruppen und Initiatoren für die ausgewählte Speicher-VM an. Standardmäßig wird die LUN-Ansicht angezeigt. Sie können Details zu den Initiatorgruppen auf der Registerkarte „Initiatorgruppen“ und Details zu Initiatoren auf der Registerkarte „Initiatoren“ anzeigen.

- **Registerkarte „LUNs“**

  Zeigt Details zu den LUNs an, die zur ausgewählten Speicher-VM gehören. Sie können Informationen wie den LUN-Namen, den LUN-Status (online oder offline), den Namen des Dateisystems (Volume oder Qtree), das die LUN enthält, den Typ des Host-Betriebssystems, die Gesamtdatenkapazität und die Seriennummer der LUN anzeigen. Die Spalte „LUN-Leistung“ enthält einen Link zur Seite mit den LUN-/Leistungsdetails.

  Sie können auch Informationen darüber anzeigen, ob Thin Provisioning auf der LUN aktiviert ist und ob die LUN einer Initiatorgruppe zugeordnet ist. Wenn es 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 wie den Namen der Initiatorgruppe, den Zugriffsstatus, den Typ des Hostbetriebssystems, das von allen Initiatoren in der Gruppe verwendet wird, und das unterstützte Protokoll anzeigen. Wenn Sie auf den Link in der Spalte „Zugriffsstatus“ klicken, können Sie den aktuellen Zugriffsstatus der Initiatorgruppe anzeigen.

  - **Normal**

    Die Initiatorgruppe ist mit mehreren Zugriffspfaden verbunden.

  - **Einzelpfad**

    Die Initiatorgruppe ist mit einem einzigen Zugriffspfad verbunden.

  - **Keine Pfade**

    Es ist kein Zugriffspfad mit der Initiatorgruppe verbunden.

    Sie können anzeigen, ob Initiatorgruppen allen Schnittstellen oder bestimmten Schnittstellen über einen Portsatz zugeordnet sind. Wenn Sie in der Spalte „Zugeordnete Schnittstellen“ auf den Zähllink klicken, werden entweder alle Schnittstellen oder bestimmte Schnittstellen für einen Portsatz angezeigt. Schnittstellen, die über das Zielportal abgebildet werden, 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 diesem Initiator zugeordneten Initiatorgruppen für die ausgewählte Speicher-VM an.

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

Bereich „Zugehörige Anmerkungen“

Im Bereich „Verwandte Anmerkungen“ können Sie die Anmerkungsdetails anzeigen, die mit der ausgewählten Speicher-VM verknüpft sind. Zu den Details gehören der Annotation-Name und die Annotation-Werte, die auf die Speicher-VM angewendet werden. Sie können manuelle Anmerkungen auch aus dem Bereich „Verwandte Anmerkungen“ entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie die Cluster, Aggregate und Volumes anzeigen, die mit der Speicher-VM in Zusammenhang stehen:

- **Cluster**

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

- **Aggregate**

  Zeigt die Anzahl der Aggregate an, die zur ausgewählten Speicher-VM gehören. Der Integritätsstatus der Aggregate wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Wenn eine Speicher-VM beispielsweise zehn Aggregate enthält, von denen fünf den Status „Warnung“ und die restlichen fünf den Status „Kritisch“ anzeigen, wird der Status „Kritisch“ angezeigt.

- **Zugewiesene Aggregate**

  Zeigt die Anzahl der Aggregate an, die einer Speicher-VM zugewiesen sind. Der Integritätsstatus der Aggregate wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad.

- **Bände**

  Zeigt die Anzahl und Kapazität der Volumes an, die zur ausgewählten Speicher-VM gehören. Der Integritätsstatus der Volumes wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Wenn in der Speicher-VM FlexGroup -Volumes vorhanden sind, umfasst die Zählung auch FlexGroups, nicht jedoch FlexGroup Bestandteile.

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ können Sie die Liste der Gruppen anzeigen, die mit der ausgewählten Speicher-VM verknüpft sind.

Bereich „Zugehörige Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnungen anzeigen, die für die ausgewählte

Speicher-VM 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 Warnungsnamen klicken.

Cluster-/Integritätsdetailseite

Die Seite „Cluster-/Integritätsdetails“ bietet ausführliche Informationen zu einem ausgewählten Cluster, z. B. Integrität, Kapazität und Konfigurationsdetails. Sie können auch Informationen zu den Netzwerkschnittstellen (LIFs), Knoten, Datenträgern, zugehörigen Geräten und zugehörigen Warnungen für den Cluster anzeigen.

Der Status neben dem Clusternamen, z. B. (Gut), stellt den Kommunikationsstatus dar, d. h., ob Unified Manager mit dem Cluster kommunizieren kann. Es stellt nicht den Failover-Status oder den Gesamtstatus des Clusters dar.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für den ausgewählten Cluster ausführen:

- **Zur Leistungsansicht wechseln**

  Ermöglicht Ihnen die Navigation zur Seite mit den Cluster-/Leistungsdetails.

- **Aktionen**

  - Alarm hinzufügen: Öffnet das Dialogfeld „Alarm hinzufügen“, in dem Sie dem ausgewählten Cluster einen Alarm hinzufügen können.
  - Neu erkennen: Leitet eine manuelle Aktualisierung des Clusters ein, wodurch Unified Manager aktuelle Änderungen am Cluster erkennen kann.

    Wenn Unified Manager mit OnCommand Workflow Automation gekoppelt ist, werden beim Wiedererkennungsvorgang auch zwischengespeicherte Daten von WFA erneut abgerufen, sofern vorhanden.

  Nachdem der Neuerkennungsvorgang gestartet wurde, wird ein Link zu den zugehörigen Auftragsdetails angezeigt, um die Verfolgung des Auftragsstatus zu ermöglichen.

  - Kommentieren: Ermöglicht Ihnen, den ausgewählten Cluster mit Anmerkungen zu versehen.

- **Cluster anzeigen**

  Ermöglicht Ihnen die Navigation zur Ansicht „Integrität: Alle Cluster“.

Registerkarte „Integrität“

Zeigt detaillierte Informationen zu Problemen mit der Datenverfügbarkeit und Datenkapazität verschiedener Clusterobjekte wie Knoten, SVMs und Aggregaten an. Verfügbarkeitsprobleme hängen mit der Datenbereitstellungskapazität der Clusterobjekte zusammen. Kapazitätsprobleme hängen mit der Datenspeicherkapazität der Clusterobjekte zusammen.

Sie können auf das Diagramm eines Objekts klicken, um eine gefilterte Liste der Objekte anzuzeigen. Sie können beispielsweise auf das SVM-Kapazitätsdiagramm klicken, das Warnungen anzeigt, um eine gefilterte Liste von SVMs anzuzeigen. Diese Liste enthält SVMs mit Volumes oder Qtrees, die Kapazitätsprobleme mit dem Schweregrad „Warnung“ aufweisen. Sie können auch auf das SVM-Verfügbarkeitsdiagramm klicken, das Warnungen anzeigt, um die Liste der SVMs anzuzeigen, bei denen Verfügbarkeitsprobleme mit dem

Schweregrad „Warnung“ vorliegen.

Verfügbarkeitsprobleme

Zeigt grafisch die Gesamtzahl der Objekte an, einschließlich der Objekte mit Verfügbarkeitsproblemen und der Objekte ohne Verfügbarkeitsprobleme. Die Farben im Diagramm stellen die unterschiedlichen Schweregrade der Probleme dar. Die Informationen unter dem Diagramm enthalten Einzelheiten zu Verfügbarkeitsproblemen, die die Verfügbarkeit von Daten im Cluster beeinträchtigen können oder bereits beeinträchtigt haben. Beispielsweise werden Informationen zu ausgefallenen Festplatten-Shelves und offline geschalteten Aggregaten angezeigt.

Die für das SFO-Balkendiagramm angezeigten Daten basieren auf dem HA-Status der Knoten. Die für alle anderen Balkendiagramme angezeigten Daten werden basierend auf den generierten Ereignissen berechnet.

Kapazitätsprobleme

Zeigt grafisch die Gesamtzahl der Objekte an, einschließlich der Objekte mit Kapazitätsproblemen und der Objekte ohne kapazitätsbezogene Probleme. Die Farben im Diagramm stellen die unterschiedlichen Schweregrade der Probleme dar. Die Informationen unter dem Diagramm liefern Details zu Kapazitätsproblemen, die sich auf die Datenkapazität im Cluster auswirken können oder bereits ausgewirkt haben. Beispielsweise werden Informationen zu Aggregaten angezeigt, bei denen die Wahrscheinlichkeit einer Überschreitung der festgelegten Schwellenwerte besteht.

Registerkarte „Kapazität“

Zeigt detaillierte Informationen zur Kapazität des ausgewählten Clusters an.

Kapazität

Zeigt das Datenkapazitätsdiagramm zur genutzten und verfügbaren Kapazität aller zugewiesenen Aggregate an:

- Verwendeter logischer Speicherplatz

  Die tatsächliche Größe der Daten, die auf allen Aggregaten dieses Clusters gespeichert werden, ohne Berücksichtigung der Einsparungen durch die Verwendung von ONTAP Speichereffizienztechnologien. Snapshot-Kopien sind hiervon nicht umfasst.

- Datenreduktion

  Zeigt das Verhältnis ohne Snapshot-Kopien und mit zwei signifikanten Ziffern an, beispielsweise 1,8 zu 1. Dieses Verhältnis basiert auf den konfigurierten ONTAP Speichereffizienzeinstellungen.

- Gebraucht

  Die physische Kapazität, die von Daten auf allen Aggregaten verwendet wird. Darin ist die Kapazität nicht enthalten, die für Parität, Größenanpassung und Reservierung verwendet wird.

- Verfügbar

  Zeigt die für Daten verfügbare Kapazität an.

- Ersatzteile

Zeigt die verfügbare Speicherkapazität aller Ersatzfestplatten an.

- Bereitgestellt

  Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

Details

Zeigt detaillierte Informationen zur genutzten und verfügbaren Kapazität an. Die Berechnung schließt die Stammaggregatdaten aus.

- Gesamtkapazität

  Zeigt die Gesamtkapazität des Clusters an. Darin ist die für die Parität zugewiesene Kapazität nicht enthalten.

- Gebraucht

  Zeigt die von Daten verwendete Kapazität an. Darin ist die Kapazität nicht enthalten, die für Parität, Größenanpassung und Reservierung verwendet wird.

- Verfügbar

  Zeigt die für Daten verfügbare Kapazität an.

- Bereitgestellt

  Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

- Ersatzteile

  Zeigt die verfügbare Speicherkapazität aller Ersatzfestplatten an.

Cloud-Ebene

Zeigt die insgesamt verwendete Cloud-Tier-Kapazität und die für jede verbundene Cloud-Tier verwendete Kapazität für FabricPool-fähige Aggregate im Cluster an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

Aufschlüsselung der physischen Kapazität nach Festplattentyp

Im Bereich „Aufschlüsselung der physischen Kapazität nach Datenträgertyp“ werden ausführliche Informationen zur Datenträgerkapazität der verschiedenen Datenträgertypen im Cluster angezeigt. Durch Klicken auf den Datenträgertyp können Sie auf der Registerkarte „Datenträger“ weitere Informationen zum Datenträgertyp anzeigen.

- Gesamtnutzkapazität

  Zeigt die verfügbare Kapazität und die freie Kapazität der Datenträger an.

- Festplatte

  Zeigt die genutzte und die verfügbare Kapazität aller HDD-Datenträger im Cluster grafisch an. Die gepunktete Linie stellt die freie Kapazität der Datenträger in der Festplatte dar.

- Blitz
  - SSD-Daten

    Zeigt die genutzte und die verfügbare Kapazität der SSD-Datenträger im Cluster grafisch an.

  - SSD-Cache

    Zeigt grafisch die speicherbare Kapazität der SSD-Cache-Festplatten im Cluster an.

  - SSD-Ersatz

    Zeigt die freie Kapazität der SSD-, Daten- und Cache-Festplatten im Cluster grafisch an.

- Nicht zugewiesene Datenträger

  Zeigt die Anzahl nicht zugewiesener Festplatten im Cluster an.

Liste der Aggregate mit Kapazitätsproblemen

Zeigt in tabellarischer Form Details zur genutzten und verfügbaren Kapazität der Aggregate an, bei denen Kapazitätsrisikoprobleme vorliegen.

- Status

  Zeigt an, dass das Aggregat ein kapazitätsbezogenes Problem einer bestimmten Schwere aufweist.

  Sie können den Zeiger über den Status bewegen, um weitere Informationen zu dem Ereignis oder den für das Aggregat generierten Ereignissen anzuzeigen.

  Wenn der Status des Aggregats durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum der Ereignisauslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Sie können auf die Schaltfläche **Details anzeigen** klicken, um weitere Informationen zum Ereignis anzuzeigen.

  Wenn der Status des Aggregats durch mehrere Ereignisse mit demselben Schweregrad bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu jedem dieser Ereignisse 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 mit demselben oder unterschiedlichen Schweregrad aufweisen. Es wird jedoch nur der höchste Schweregrad angezeigt. Wenn ein Aggregat beispielsweise zwei Ereignisse mit den Schweregraden „Fehler“ und „Kritisch“ aufweist, wird nur der Schweregrad „Kritisch“ angezeigt.

- Aggregat

  Zeigt den Namen des Aggregats an.

- Verwendete Datenkapazität

  Zeigt grafisch Informationen zur Gesamtkapazitätsnutzung (in Prozent) an.

- Tage bis zur vollständigen

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor das Aggregat seine volle Kapazität erreicht.

Registerkarte „Konfiguration“

Zeigt Details zum ausgewählten Cluster an, z. B. IP-Adresse, Kontakt und Standort:

Clusterübersicht

- Verwaltungsschnittstelle

  Zeigt das Cluster-Management-LIF an, das Unified Manager zum Herstellen einer Verbindung mit dem Cluster verwendet. Außerdem wird der Betriebszustand der Schnittstelle angezeigt.

- Hostname oder IP-Adresse

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Cluster-Management-LIF an, das Unified Manager für die Verbindung mit dem Cluster verwendet.

- FQDN

  Zeigt den vollqualifizierten Domänennamen (FQDN) des Clusters an.

- Betriebssystemversion

  Zeigt die ONTAP -Version an, die im Cluster ausgeführt wird. Wenn auf den Knoten im Cluster unterschiedliche Versionen von ONTAP ausgeführt werden, wird die früheste ONTAP Version angezeigt.

- Kontakt

  Zeigt Details zum Administrator an, den Sie bei Problemen mit dem Cluster kontaktieren sollten.

- Standort

  Zeigt den Standort des Clusters an.

- Persönlichkeit

  Gibt an, ob es sich um einen als All-SAN-Array konfigurierten Cluster handelt.

Übersicht über Remote-Cluster

Bietet 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 Clusternamen klicken, um zur Detailseite des Clusters zu navigieren.

- Hostname oder IP-Adresse

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Remote-Clusters an.

- Standort

  Zeigt den Standort des Remote-Clusters an.

MetroCluster -Übersicht

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

- Typ

  Zeigt an, ob der MetroCluster -Typ zwei oder vier Knoten hat. Für MetroCluster über IP werden nur vier Knoten unterstützt.

- Konfiguration

  Zeigt die MetroCluster -Konfiguration über FC und IP an, die die folgenden Werte haben kann:

Für FC

- Stretch-Konfiguration mit SAS-Kabeln
- Stretch-Konfiguration mit FC-SAS-Brücke
- Fabric-Konfiguration mit FC-Switches

> Für einen MetroCluster mit vier Knoten wird nur die Fabric-Konfiguration mit FC-Switches unterstützt.

Für IP

- IP-Konfiguration mit Ethernet-Switches (L2 oder L3, je nach Konfiguration des Clusters)
  - Automatische ungeplante Umschaltung (AUSO)

    Zeigt an, ob für den lokalen Cluster ein automatisierter ungeplanter Switchover 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` .

Nodes

- Verfügbarkeit

  Zeigt die Anzahl der aktiven Knoten an ( ) oder nach unten ( ) im Cluster.

- Betriebssystemversionen

  Zeigt die ONTAP -Versionen an, die auf den Knoten ausgeführt werden, sowie die Anzahl der Knoten, auf denen eine bestimmte Version von ONTAP ausgeführt wird. Beispielsweise gibt 9.6 (2), 9.3 (1) an, dass

auf zwei Knoten ONTAP 9.6 und auf einem Knoten ONTAP 9.3 ausgeführt wird.

Virtuelle Speichermaschinen

- Verfügbarkeit

  Zeigt die Anzahl der aktiven SVMs an ( ) oder nach unten ( ) im Cluster.

Netzwerkschnittstellen

- Verfügbarkeit

  Zeigt die Anzahl der aktiven Nicht-Daten-LIFs an ( ) oder nach unten ( ) im Cluster.

- Cluster-Management-Schnittstellen

  Zeigt die Anzahl der Cluster-Management-LIFs an.

- Knotenverwaltungsschnittstellen

  Zeigt die Anzahl der Knotenverwaltungs-LIFs 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. Zu den Datenprotokollen gehören iSCSI, CIFS, NFS, NVMe und FC/FCoE.

Schutz

- Mediatoren

  Zeigt an, ob der Cluster Mediatoren unterstützt und den Konnektivitätsstatus des Mediators. Es zeigt an, ob der Mediator konfiguriert ist, und wenn ja, wird der Status der Mediatoren angezeigt.

  - Nicht zutreffend

    Wird angezeigt, wenn der Cluster keine Mediatoren unterstützt.

  - Nicht konfiguriert

    Wird angezeigt, wenn der Cluster Mediatoren unterstützt, der Mediator jedoch nicht konfiguriert ist.

  - IP-Adresse

Wird angezeigt, wenn der Cluster Mediatoren unterstützt und der Mediator konfiguriert ist. Der Mediatorstatus wird durch die Farbe angezeigt. Die Farbe Grün zeigt an, dass der Mediatorstatus erreichbar ist. Die Farbe Rot zeigt an, dass der Mediatorstatus nicht erreichbar ist.

Cloud-Ebenen

Listet die Namen der Cloud-Ebenen auf, mit denen dieser Cluster verbunden ist. Außerdem werden der Typ (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage oder StorageGRID) und der Status der Cloud-Ebenen (Verfügbar oder Nicht verfügbar) aufgelistet.

Registerkarte „MetroCluster -Konnektivität“

Zeigt die Probleme und den Verbindungsstatus der Clusterkomponenten in der MetroCluster -over-FC -Konfiguration an. Ein Cluster wird in einem roten Kästchen 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-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 Knotens im Cluster klicken, wird die Knotenregisterkarte auf der Detailseite des Clusters angezeigt. Wenn Sie auf den Link „Zählen“ der Datenträger im Remote-Cluster klicken, wird die Registerkarte „Datenträger“ auf der Detailseite des Remote-Clusters angezeigt.

Wenn Sie bei der Verwaltung einer MetroCluster Konfiguration mit acht Knoten auf den Link „Zählen“ der Komponente „Disk Shelves“ klicken, werden nur die lokalen Shelves des Standard-HA-Paares angezeigt. Außerdem gibt es keine Möglichkeit, die lokalen Regale auf dem anderen HA-Paar anzuzeigen.

Sie können den Zeiger über die Komponenten bewegen, um im Falle eines Problems die Details und den Konnektivitätsstatus der Cluster anzuzeigen und weitere Informationen zu dem oder den für das Problem generierten Ereignissen anzuzeigen.

Wenn der Status des Konnektivitätsproblems zwischen Komponenten durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum der Ereignisauslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Über die Schaltfläche „Details anzeigen“ erhalten Sie weitere Informationen zum Ereignis.

Wenn der Status des Konnektivitätsproblems zwischen Komponenten durch mehrere Ereignisse mit demselben Schweregrad bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu jedem dieser Ereignisse 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 den Datenschutz sicherzustellen, indem Sie die Daten synchron mit den bereits per Peering verbundenen Clustern spiegeln. Ein Cluster wird in einem roten Kästchen 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-FC-Konfiguration befinden.

In einer MetroCluster Umgebung können Sie diese Registerkarte verwenden, um die logischen Verbindungen und das Peering des lokalen Clusters mit dem Remote-Cluster zu überprüfen. Sie können die objektive Darstellung der Clusterkomponenten mit ihren logischen Verbindungen einsehen. Dies hilft dabei, die Probleme zu identifizieren, die beim Spiegeln von Metadaten und Daten auftreten können.

Auf der Registerkarte „MetroCluster -Replikation“ bietet der lokale Cluster die detaillierte grafische Darstellung des ausgewählten Clusters und der MetroCluster Partner bezieht sich auf den Remote-Cluster.

Registerkarte „Netzwerkschnittstellen“

Zeigt Details zu allen Nicht-Daten-LIFs an, die auf dem ausgewählten Cluster erstellt werden.

Netzwerkschnittstelle

Zeigt den Namen des LIF an, das auf dem ausgewählten Cluster erstellt wird.

Betriebsstatus

Zeigt den Betriebsstatus der Schnittstelle an, der Aktiv sein kann ( ), Runter ( ) oder Unbekannt ( ). Der Betriebsstatus einer Netzwerkschnittstelle wird durch den Status ihrer physischen Ports bestimmt.

Verwaltungsstatus

Zeigt den Verwaltungsstatus der Schnittstelle an, der Aktiv sein kann ( ), Runter ( ) oder Unbekannt ( ). Sie können den Verwaltungsstatus einer Schnittstelle steuern, wenn Sie Änderungen an der Konfiguration vornehmen oder während der Wartung. Der Verwaltungsstatus kann vom Betriebsstatus abweichen. Wenn der Verwaltungsstatus eines LIF jedoch „Down“ lautet, ist der Betriebsstatus standardmäßig „Down“.

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.

Heimathafen

Zeigt den physischen Port an, mit dem die Schnittstelle ursprünglich verknüpft war.

Aktueller Port

Zeigt den physischen Port an, mit dem die Schnittstelle derzeit verknüpft ist. Nach der LIF-Migration kann der aktuelle Port vom Home-Port abweichen.

Failover-Richtlinie

Zeigt die Failover-Richtlinie an, die für die Schnittstelle konfiguriert ist.

Routinggruppen

Zeigt den Namen der Routinggruppe an. Weitere Informationen zu den Routen und dem Ziel-Gateway können Sie anzeigen, indem Sie auf den Namen der Routinggruppe klicken.

Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt und daher wird für diese Cluster eine leere Spalte angezeigt.

Failover-Gruppe

Zeigt den Namen der Failover-Gruppe an.

Registerkarte „Knoten“

Zeigt Informationen zu Knoten im ausgewählten Cluster an. Sie können detaillierte Informationen zu den HA-Paaren, Festplatten-Shelves und Ports anzeigen:

HA-Details

Bietet eine bildliche Darstellung des HA-Status und des Integritätsstatus der Knoten im HA-Paar. Der Integritätsstatus des Knotens wird durch die folgenden Farben angezeigt:

- **Grün**

  Der Knoten ist in einem funktionsfähigen Zustand.

- **Gelb**

  Der Knoten hat den Partnerknoten übernommen oder der Knoten hat mit Umweltproblemen zu kämpfen.

- **Rot**

  Der Knoten ist ausgefallen.

Sie können Informationen zur Verfügbarkeit des HA-Paares anzeigen und die erforderlichen Maßnahmen ergreifen, um Risiken zu vermeiden. Beispielsweise wird im Falle einer möglichen Übernahmeoperation die folgende Meldung angezeigt: Speicher-Failover möglich.

Sie können eine Liste der Ereignisse im Zusammenhang mit dem HA-Paar und seiner Umgebung anzeigen, z. B. Lüfter, Netzteile, NVRAM Batterie, Flash-Karten, Serviceprozessor und Konnektivität von Festplattenregalen. Sie können auch den Zeitpunkt anzeigen, zu dem die Ereignisse ausgelöst wurden.

Sie können weitere knotenbezogene Informationen anzeigen, beispielsweise die Modellnummer.

Wenn Cluster mit einem einzigen Knoten vorhanden sind, können Sie auch Details zu den Knoten anzeigen.

Festplattenregale

Zeigt Informationen zu den Festplatten-Shelves im HA-Paar an.

Sie können auch die für die Festplatten-Shelves und die Umgebungskomponenten generierten Ereignisse sowie den Zeitpunkt der Auslösung der Ereignisse anzeigen.

- **Regal-ID**

  Zeigt die ID des Shelfs an, in dem sich die Festplatte befindet.

- **Komponentenstatus**

  Zeigt Umgebungsdetails der Festplattenregale an, z. B. Netzteile, Lüfter, Temperatursensoren, Stromsensoren, Festplattenkonnektivität und Spannungssensoren. Die Umgebungsdetails werden als Symbole in den folgenden Farben angezeigt:

  - **Grün**

    Die Umweltkomponenten funktionieren ordnungsgemäß.

  - **Grau**

    Zu den Umweltkomponenten liegen keine Daten vor.

  - **Rot**

    Einige der Umweltkomponenten sind ausgefallen.

- **Zustand**

  Zeigt den Status des Festplattenregals an. Die möglichen Zustände sind „Offline“, „Online“, „Kein Status“, „Initialisierung erforderlich“, „Fehlt“ und „Unbekannt“.

- **Modell**

  Zeigt die Modellnummer des Festplattenregals an.

- **Lokales Festplattenregal**

  Gibt an, ob sich das Festplattenregal auf dem lokalen Cluster oder dem Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster -Konfiguration angezeigt.

- **Eindeutige ID**

  Zeigt die eindeutige Kennung des Festplatten-Shelfs an.

- **Firmware-Version**

  Zeigt die Firmware-Version des Festplatten-Shelfs an.

Häfen

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 Portsymbole klicken.

Sie können auch die für die Ports generierten Ereignisse anzeigen.

Sie können die folgenden Portdetails anzeigen:

- Port-ID

  Zeigt den Namen des Ports an. Die Portnamen können beispielsweise e0M, e0a und e0b sein.

- Rolle

  Zeigt die Rolle des Ports an. Die möglichen Rollen sind Cluster, Daten, Intercluster, Knotenverwaltung und

Undefiniert.

- Typ

  Zeigt das für den Port verwendete Protokoll der physischen Schicht an. Mögliche Typen sind Ethernet, Fibre Channel und FCoE.

- WWPN

  Zeigt den World Wide Port Name (WWPN) des Ports an.

- Firmware Rev

  Zeigt die Firmware-Revision des FC/FCoE-Ports an.

- Status

  Zeigt den aktuellen Status des Ports an. Die möglichen Zustände sind „Up“, „Down“, „Link Not Connected“ oder „Unknown“ ( ).

  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, Name der mit dem LIF verknüpften SVM, aktueller Port, Failover-Richtlinie und Failover-Gruppe.

Registerkarte „Datenträger“

Zeigt Details zu den Datenträgern im ausgewählten Cluster an. Sie können datenträgerbezogene Informationen anzeigen, beispielsweise die Anzahl der verwendeten Datenträger, Ersatzdatenträger, defekten Datenträger und nicht zugewiesenen Datenträger. Sie können auch andere Details wie den Datenträgernamen, den Datenträgertyp und den Besitzerknoten des Datenträgers anzeigen.

Zusammenfassung des Datenträgerpools

Zeigt die Anzahl der Datenträger an, die nach effektiven Typen (FCAL, SAS, SATA, MSATA, SSD, NVMe SSD, SSD CAP, Array LUN und VMDISK) kategorisiert sind, sowie den Status der Datenträger. Sie können auch andere Details anzeigen, beispielsweise die Anzahl der Aggregate, gemeinsam genutzten Datenträger, Ersatzdatenträger, defekten Datenträger, nicht zugewiesenen Datenträger und nicht unterstützten Datenträger. Wenn Sie auf den Link zur Anzahl der effektiven Datenträgertypen klicken, werden Datenträger des ausgewählten Status und des effektiven Typs angezeigt. Wenn Sie beispielsweise auf den Zähllink für den Datenträgerstatus „Defekt“ und den effektiven Typ „SAS“ klicken, werden alle Datenträger mit dem Datenträgerstatus „Defekt“ und dem effektiven Typ „SAS“ angezeigt.

Scheibe

Zeigt den Namen der Festplatte an.

RAID-Gruppen

Zeigt den Namen der RAID-Gruppe an.

Besitzerknoten

Zeigt den Namen des Knotens 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: Aggregiert, Gemeinsam genutzt, Ersatz, Defekt, Nicht zugewiesen, Nicht unterstützt oder Unbekannt. Standardmäßig ist diese Spalte so sortiert, dass die Zustände in der folgenden Reihenfolge angezeigt werden: Defekt, Nicht zugewiesen, Nicht unterstützt, Ersatz, Aggregiert und Gemeinsam genutzt.

Lokale Festplatte

Zeigt entweder „Ja“ oder „Nein“ an, um anzugeben, ob sich die Festplatte im lokalen Cluster oder im Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster -Konfiguration angezeigt.

Position

Zeigt die Position der Festplatte basierend auf ihrem Containertyp an: beispielsweise Kopie, 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 Zeiger über den Zähllink bewegen, um die betroffenen Aggregate anzuzeigen, und dann auf den Aggregatnamen klicken, um Details des Aggregats anzuzeigen. Sie können auch auf die Gesamtanzahl klicken, um die Liste der betroffenen Aggregate in der Ansicht „Integrität: Alle Aggregate“ anzuzeigen.

In den folgenden Fällen wird in dieser Spalte kein Wert angezeigt:

- Für defekte Festplatten, wenn ein Cluster mit solchen Festplatten zu Unified Manager hinzugefügt wird
- Wenn keine Festplatten ausgefallen sind

Speicherpool

Zeigt den Namen des Speicherpools an, zu dem die SSD gehört. Sie können den Zeiger über den Namen des Speicherpools bewegen, um Details zum Speicherpool anzuzeigen.

Speicherkapazität

Zeigt die zur Nutzung verfügbare Festplattenkapazität an.

Rohkapazität

Zeigt die Kapazität der unformatierten Rohfestplatte vor der Größenanpassung und RAID-Konfiguration an. Standardmäßig ist diese Spalte ausgeblendet.

Typ

Zeigt die Festplattentypen an: beispielsweise ATA, SATA, FCAL oder VMDISK.

Effektiver Typ

Zeigt den von ONTAP zugewiesenen Festplattentyp an.

Bestimmte ONTAP Festplattentypen werden zum Erstellen und Hinzufügen zu Aggregaten sowie zur Ersatzteilverwaltung als gleichwertig angesehen. ONTAP weist jedem Festplattentyp einen effektiven Festplattentyp zu.

Verbrauchte Ersatzblöcke %

Zeigt die in der SSD-Festplatte verbrauchten Ersatzblöcke in Prozent an. Diese Spalte ist für andere Datenträger als SSD-Datenträger leer.

Nennlebensdauer %

Zeigt eine Schätzung der verwendeten SSD-Lebensdauer in Prozent an, basierend auf der tatsächlichen SSD-Nutzung und der Vorhersage des Herstellers zur SSD-Lebensdauer. Ein Wert größer als 99 zeigt an, dass die geschätzte Lebensdauer aufgebraucht ist, weist aber möglicherweise nicht auf einen SSD-Fehler hin. Wenn der Wert unbekannt ist, wird die Festplatte weggelassen.

Firmware

Zeigt die Firmware-Version der Festplatte an.

Drehzahl

Zeigt die Umdrehungen pro Minute (RPM) der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

Modell

Zeigt die Modellnummer der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

Verkäufer

Zeigt den Namen des Festplattenherstellers an. Standardmäßig ist diese Spalte ausgeblendet.

Regal-ID

Zeigt die ID des Shelfs an, in dem sich die Festplatte befindet.

Einschub

Zeigt die ID des Schachts an, in dem sich die Festplatte befindet.

Bereich „Zugehörige Anmerkungen“

Ermöglicht Ihnen, die mit dem ausgewählten Cluster verknüpften Anmerkungsdetails anzuzeigen. Zu den Details gehören der Annotation-Name und die Annotation-Werte, die auf den Cluster angewendet werden. Sie können manuelle Anmerkungen auch aus dem Bereich „Verwandte Anmerkungen“ entfernen.

Bereich „Verwandte Geräte“

Ermöglicht Ihnen, Gerätedetails anzuzeigen, die mit dem ausgewählten Cluster verknüpft sind.

Die Details umfassen Eigenschaften des mit dem Cluster verbundenen Geräts, wie Gerätetyp, Größe, Anzahl und Integritätsstatus. Sie können auf den Zähllink klicken, um weitere Analysen zu diesem bestimmten Gerät durchzuführen.

Sie können den Bereich „MetroCluster -Partner“ verwenden, um die Anzahl und auch Details zum Remote MetroCluster -Partner sowie den zugehörigen Clusterkomponenten wie Knoten, Aggregaten und SVMs abzurufen. Der Bereich „MetroCluster -Partner“ wird nur für Cluster in einer MetroCluster -Konfiguration angezeigt.

Im Bereich „Verwandte Geräte“ können Sie die Knoten, SVMs und Aggregate anzeigen und zu ihnen

navigieren, die mit dem Cluster in Zusammenhang stehen:

MetroCluster Partner

Zeigt den Integritätsstatus des MetroCluster Partners an. Über den Zähllink können Sie weiter navigieren und Informationen zum Zustand und zur Kapazität der Clusterkomponenten erhalten.

Nodes

Zeigt die Anzahl, Kapazität und den Integritätsstatus der Knoten an, die zum ausgewählten Cluster gehören. Die Kapazität gibt die gesamte nutzbare Kapazität im Verhältnis zur verfügbaren Kapazität an.

Virtuelle Speichermaschinen

Zeigt die Anzahl der SVMs an, die zum ausgewählten Cluster gehören.

Aggregate

Zeigt die Anzahl, Kapazität und den Integritätsstatus der Aggregate an, die zum ausgewählten Cluster gehören.

Bereich „Verwandte Gruppen“

Ermöglicht Ihnen, die Liste der Gruppen anzuzeigen, die den ausgewählten Cluster enthalten.

Bereich „Zugehörige Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnungen für den ausgewählten 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 Warnungsnamen klicken.

Verwandte Informationen

"Seite „Bände“" "Anzeigen der Clusterliste und Details"

Seite mit Aggregat-/Gesundheitsdetails

Auf der Seite „Aggregat-/Integritätsdetails“ können Sie ausführliche Informationen zum ausgewählten Aggregat anzeigen, beispielsweise Kapazität, Datenträgerinformationen, Konfigurationsdetails und generierte Ereignisse. Sie können auch Informationen zu den zugehörigen Objekten und zugehörigen Warnungen für dieses Aggregat anzeigen.

Befehlsschaltflächen

> Beim Überwachen eines FabricPool-fähigen Aggregats sind die zugesagten und überzugesagten Werte auf dieser Seite nur für die lokale Kapazität bzw. die Kapazität der Leistungsebene relevant. Die Menge des in der Cloud-Ebene verfügbaren Speicherplatzes spiegelt sich nicht in den überbelegten Werten wider. Ebenso sind die aggregierten Schwellenwerte nur für die lokale Leistungsebene relevant.

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

- **Zur Leistungsansicht wechseln**

Ermöglicht Ihnen die Navigation zur Seite mit den Gesamt-/Leistungsdetails.

- **Aktionen**
  - Benachrichtigung hinzufügen

    Ermöglicht Ihnen, dem ausgewählten Aggregat eine Warnung hinzuzufügen.

  - Schwellenwerte bearbeiten

    Ermöglicht Ihnen, die Schwellenwerteinstellungen für das ausgewählte Aggregat zu ändern.
- **Aggregate anzeigen**

  Ermöglicht Ihnen die Navigation zur Ansicht „Integrität: Alle Aggregate“.

Registerkarte „Kapazität“

Auf der Registerkarte „Kapazität“ werden ausführliche Informationen zum ausgewählten Aggregat angezeigt, beispielsweise dessen Kapazität, Schwellenwerte und tägliche Wachstumsrate.

Standardmäßig werden für Root-Aggregate keine Kapazitätsereignisse generiert. Außerdem sind die von Unified Manager verwendeten Schwellenwerte nicht auf Knotenstammaggregate anwendbar. Nur ein Mitarbeiter des technischen Supports kann die Einstellungen für die Generierung dieser Ereignisse ändern. Wenn die Einstellungen von einem Mitarbeiter des technischen Supports geändert werden, werden die Schwellenwerte auf das Knotenstammaggregat angewendet.

- **Kapazität**

  Zeigt das Datenkapazitätsdiagramm und das Snapshot-Kopiendiagramm an, die Kapazitätsdetails zum Aggregat anzeigen:

  - Verwendeter logischer Speicherplatz

    Die tatsächliche Größe der auf dem Aggregat gespeicherten Daten ohne Berücksichtigung der Einsparungen durch den Einsatz von ONTAP Speichereffizienztechnologien.

  - Gebraucht

    Die von den Daten insgesamt genutzte physische Kapazität.

  - Überlastet

    Wenn der Speicherplatz im Aggregat überbelegt ist, wird im Diagramm eine Markierung mit dem überbelegten Betrag angezeigt.

  - Warnung

    Zeigt eine gepunktete Linie an der Stelle an, an der der Warnschwellenwert festgelegt ist. Dies bedeutet, dass der Speicherplatz im Aggregat fast voll ist. Wenn dieser Schwellenwert überschritten wird, wird das Ereignis „Speicherplatz fast voll“ generiert.

  - Fehler

    Zeigt eine durchgezogene Linie an der Stelle an, an der der Fehlerschwellenwert festgelegt ist. Dies bedeutet, dass der Speicherplatz im Aggregat voll ist. Wenn dieser Schwellenwert überschritten wird,

wird das Ereignis „Speicherplatz voll“ 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, um die die Snapshot-Kapazität die Snapshot-Reserve übersteigt, wenn die verwendete Snapshot-Kapazität die Snapshot-Reserve übersteigt.

- **Cloud-Ebene**

  Zeigt den von Daten in der Cloud-Ebene für FabricPool-fähige Aggregate verwendeten Speicherplatz an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

  Wenn die Cloud-Ebene auf einen anderen Cloud-Anbieter gespiegelt wird (die „Spiegelebene“), werden hier beide Cloud-Ebenen angezeigt.

- **Details**

  Zeigt detaillierte Informationen zur Kapazität an.

  - Gesamtkapazität

    Zeigt die Gesamtkapazität im Aggregat an.

  - Datenkapazität

    Zeigt die vom Aggregat verwendete Speicherplatzmenge (genutzte Kapazität) und die Menge des im Aggregat verfügbaren Speicherplatzes (freie Kapazität) an.

  - Schnappschuss-Reserve

    Zeigt die verwendete und freie Snapshot-Kapazität des Aggregats an.

  - Überbelegte Kapazität

    Zeigt die gesamte Überbelegung an. Durch die Überbelegung von Aggregaten können Sie mehr Speicher bereitstellen, als tatsächlich von einem bestimmten Aggregat verfügbar ist, solange nicht der gesamte Speicher derzeit verwendet wird. Wenn Thin Provisioning verwendet wird, kann die Gesamtgröße der Volumes im Aggregat die Gesamtkapazität des Aggregats überschreiten.

    Wenn Sie Ihr Aggregat überlastet haben, müssen Sie den verfügbaren Speicherplatz sorgfältig überwachen und bei Bedarf Speicher hinzufügen, um Schreibfehler aufgrund von Speicherplatzmangel zu vermeiden.

  - Cloud-Ebene

    Zeigt den von Daten in der Cloud-Ebene für FabricPool-fähige Aggregate verwendeten Speicherplatz an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein. Wenn die Cloud-Ebene auf einen anderen Cloud-Anbieter (die Spiegelebene) gespiegelt wird, werden hier beide Cloud-Ebenen angezeigt.

  - Gesamter Cache-Speicherplatz

Zeigt den Gesamtspeicherplatz der Solid-State-Laufwerke (SSDs) oder Zuordnungseinheiten 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.

- Aggregierte Schwellenwerte

  Zeigt die folgenden Schwellenwerte für die Gesamtkapazität an:

  - Fast volle Schwelle

    Gibt den Prozentsatz an, bei dem ein Aggregat fast voll ist.

  - Voller Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Aggregat voll ist.

  - Fast überbelegter Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Aggregat nahezu überlastet ist.

  - Überbelegter Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Aggregat überbelegt ist.

- Weitere Details: Tägliche Wachstumsrate

  Zeigt den im Aggregat verwendeten Speicherplatz an, wenn die Änderungsrate zwischen den letzten beiden Stichproben 24 Stunden lang anhält.

  Wenn ein Aggregat beispielsweise um 14:00 Uhr 10 GB und um 18:00 Uhr 12 GB Speicherplatz verwendet, beträgt die tägliche Wachstumsrate (GB) für dieses Aggregat 2 GB.

- Volumen verschieben

  Zeigt die Anzahl der Volume-Verschiebungsvorgänge an, die derzeit ausgeführt werden:

  - Ausgehende Volumen

    Zeigt die Anzahl und Kapazität der Volumes an, die aus dem Aggregat verschoben werden.

  Sie können auf den Link klicken, um weitere Details anzuzeigen, z. B. den Volumenamen, das Aggregat, in das das Volume verschoben wird, den Status des Volumeverschiebungsvorgangs und die voraussichtliche Endzeit.

  - Volumen in

    Zeigt die Anzahl und die verbleibende Kapazität der Volumes an, die in das Aggregat verschoben werden.

Sie können auf den Link klicken, um weitere Details anzuzeigen, z. B. den Volumenamen, das Aggregat, aus dem das Volume verschoben wird, den Status des Volumeverschiebungsvorgangs und die voraussichtliche Endzeit.

- Geschätzte genutzte Kapazität nach der Volumeverschiebung

  Zeigt die geschätzte Menge des verwendeten Speicherplatzes (als Prozentsatz und in KB, MB, GB usw.) insgesamt an, nachdem die Volume-Verschiebungsvorgänge abgeschlossen sind.

- **Kapazitätsübersicht - Volumen**

  Zeigt Diagramme an, die Informationen zur Kapazität der im Aggregat enthaltenen Volumes liefern. Es wird die vom Volume verwendete Speicherplatzmenge (genutzte Kapazität) und die Menge des verfügbaren Speicherplatzes (freie Kapazität) im Volume angezeigt. Wenn das Ereignis „Gefährdeter Speicherplatz für Thin-Provisioned-Volume“ für Thin-Provisioned-Volumes generiert wird, wird die vom Volume verwendete Speicherplatzmenge (verwendete Kapazität) und die Speicherplatzmenge angezeigt, die im Volume verfügbar ist, aber aufgrund von Problemen mit der Gesamtkapazität nicht verwendet werden kann (unverwendbare Kapazität).

  Sie können das Diagramm, das Sie anzeigen möchten, aus den Dropdown-Listen auswählen. Sie können die im Diagramm angezeigten Daten sortieren, um Details wie die verwendete Größe, die bereitgestellte Größe, die verfügbare Kapazität, die schnellste tägliche Wachstumsrate und die langsamste Wachstumsrate anzuzeigen. Sie können die Daten basierend auf den Storage Virtual Machines (SVMs) filtern, die die Volumes im Aggregat enthalten. Sie können auch Details zu Thin Provisioning-Volumes anzeigen. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den gewünschten Bereich bewegen. Standardmäßig zeigt das Diagramm die 30 wichtigsten gefilterten Volumina im Aggregat an.

Registerkarte „Datenträgerinformationen“

Zeigt detaillierte Informationen zu den Festplatten im ausgewählten Aggregat an, einschließlich RAID-Typ und -Größe sowie den Typ der im Aggregat verwendeten Festplatten. Die Registerkarte zeigt auch grafisch die RAID-Gruppen und die verwendeten Festplattentypen (z. B. SAS, ATA, FCAL, SSD oder VMDISK) an. Sie können weitere Informationen anzeigen, beispielsweise den Schacht, das Regal und die Rotationsgeschwindigkeit der Festplatte, indem Sie den Cursor über die Paritätsfestplatten und Datenfestplatten bewegen.

- **Daten**

  Zeigt grafisch Details zu dedizierten Datenträgern, gemeinsam genutzten Datenträgern oder beidem an. Wenn die Datenträger gemeinsam genutzte Datenträger enthalten, werden grafische Details der gemeinsam genutzten Datenträger angezeigt. Wenn die Datenträger dedizierte und gemeinsam genutzte Datenträger enthalten, werden grafische Details sowohl der dedizierten als auch der gemeinsam genutzten 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 der in der RAID-Gruppe zulässigen Festplatten an.

    - Gruppen

Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

- **Verwendete Datenträger**
  - Effektiver Typ

    Zeigt die Typen der Datenträger (z. B. ATA, SATA, FCAL, SSD oder VMDISK) im Aggregat an.

  - Datenträger

    Zeigt die Anzahl und Kapazität der Datenträger an, die einem Aggregat zugewiesen sind. Datenträgerdetails werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Datenträger enthält.

  - Paritätsfestplatten

    Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat zugewiesen sind. Paritätsdatenträgerdetails werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Datenträger enthält.

  - Gemeinsam genutzte Datenträger

    Zeigt die Anzahl und Kapazität der gemeinsam genutzten Datenträger an, die einem Aggregat zugewiesen sind. Details zu gemeinsam genutzten Datenträgern werden nur angezeigt, wenn das Aggregat gemeinsam genutzte Datenträger enthält.

- **Ersatzdisketten**

  Zeigt den effektiven Datenträgertyp, die Anzahl und die Kapazität der Ersatzdatenträger an, die für den Knoten im ausgewählten Aggregat verfügbar sind.

  Wenn ein Aggregat per Failover auf den Partnerknoten umgeschaltet wird, zeigt Unified Manager nicht alle Ersatzfestplatten an, die mit dem Aggregat kompatibel sind.

- **SSD-Cache**

  Bietet Details zu dedizierten Cache-SSD-Festplatten und gemeinsam genutzten Cache-SSD-Festplatten.

  Die folgenden Details für die dedizierten Cache-SSD-Festplatten werden angezeigt:

  - **RAID-Details**
    - Typ

      Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

    - Gruppengröße

      Zeigt die maximale Anzahl der in der RAID-Gruppe zulässigen Festplatten an.

    - Gruppen

      Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

  - **Verwendete Datenträger**
    - Effektiver Typ

Gibt an, dass die für den Cache im Aggregat verwendeten Datenträger vom Typ SSD sind.

- Datenträger

  Zeigt die Anzahl und Kapazität der Datenträger an, die einem Aggregat für den Cache zugewiesen sind.

- Paritätsfestplatten

  Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat für den Cache zugewiesen sind.

◦ **Ersatzdisketten**

Zeigt den effektiven Datenträgertyp, die Anzahl und die Kapazität der Ersatzdatenträger an, die für den Knoten im ausgewählten Aggregat für den Cache verfügbar sind.

> Wenn ein Aggregat per Failover auf den Partnerknoten umgeschaltet wird, zeigt Unified Manager nicht alle Ersatzfestplatten an, die mit dem Aggregat kompatibel sind.

Bietet die folgenden Details zum gemeinsam genutzten Cache:

◦ **Speicherpool**

Zeigt den Namen des Speicherpools an. Sie können den Zeiger über den Namen des Speicherpools bewegen, um die folgenden Details anzuzeigen:

- Status

  Zeigt den Status des Speicherpools an, der fehlerfrei oder fehlerhaft sein kann.

- Gesamtzuweisungen

  Zeigt die gesamten Zuordnungseinheiten und die Größe im Speicherpool an.

- Größe der Zuordnungseinheit

  Zeigt die Mindestmenge an Speicherplatz im Speicherpool an, die einem Aggregat zugewiesen werden kann.

- Festplatten

  Zeigt die Anzahl der zum Erstellen des Speicherpools verwendeten Datenträger an. Wenn die Datenträgeranzahl in der Spalte „Speicherpool“ und die Anzahl der Datenträger, die auf der Registerkarte „Datenträgerinformationen“ für diesen Speicherpool angezeigt werden, nicht übereinstimmen, weist dies darauf hin, dass ein oder mehrere Datenträger defekt sind und der Speicherpool nicht fehlerfrei ist.

- Verwendete Zuordnung

  Zeigt die Anzahl und Größe der von den Aggregaten verwendeten Zuordnungseinheiten an. Sie können auf den Aggregatnamen klicken, um die Aggregatdetails anzuzeigen.

- Verfügbare Zuteilung

Zeigt die Anzahl und Größe der für die Knoten verfügbaren Zuordnungseinheiten an. Sie können auf den Knotennamen klicken, um die Gesamtdetails 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 im Speicherpool enthaltenen Datenträger an.

- **Details**
  - Speicherpool

    Zeigt die Anzahl der Speicherpools an.

  - Gesamtgröße

    Zeigt die Gesamtgröße der Speicherpools an.

- **Cloud-Ebene**

  Zeigt den Namen der Cloud-Ebene an, wenn Sie ein FabricPool-fähiges Aggregat konfiguriert haben, und zeigt den insgesamt verwendeten Speicherplatz an. Wenn die Cloud-Ebene auf einen anderen Cloud-Anbieter (die Spiegelebene) gespiegelt wird, werden hier die Details für beide Cloud-Ebenen angezeigt.

Registerkarte „Konfiguration“

Auf der Registerkarte „Konfiguration“ werden Details zum ausgewählten Aggregat angezeigt, z. B. Clusterknoten, Blocktyp, RAID-Typ, RAID-Größe und Anzahl der RAID-Gruppen:

- **Überblick**
  - Node

    Zeigt den Namen des Knotens 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 Mixed 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-Ebene**

  Wenn es sich um ein FabricPool-fähiges Aggregat handelt, werden die Details für die Cloud-Ebene angezeigt. Einige Felder sind je nach Speicheranbieter unterschiedlich. Wenn die Cloud-Ebene auf einen anderen Cloud-Anbieter gespiegelt wird (die „Spiegelebene“), werden hier beide Cloud-Ebenen angezeigt.

  - Anbieter

    Zeigt den Namen des Speicheranbieters 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 der Cloud-Ebene an, als sie von ONTAP erstellt wurde.

  - Server

    Zeigt den FQDN der Cloud-Ebene an.

  - Hafen

    Der Port, der für die Kommunikation mit dem Cloud-Anbieter verwendet wird.

  - Zugriffsschlüssel oder Konto

    Zeigt den Zugriffsschlüssel oder das Konto für die Cloud-Ebene an.

  - Containername

    Zeigt den Bucket- oder Containernamen der Cloud-Ebene an.

  - SSL

    Zeigt an, ob die SSL-Verschlüsselung für die Cloud-Ebene aktiviert ist.

Geschichtsbereich

Im Bereich „Verlauf“ werden Diagramme angezeigt, die Informationen zur Kapazität des ausgewählten Aggregats liefern. Darüber hinaus können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie gerade anzeigen.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Verlaufsbereich auswählen. Sie können auch Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Mithilfe von Verlaufsdiagrammen können Sie Trends erkennen: Wenn beispielsweise die Gesamtnutzung ständig den Schwellenwert „Fast voll“ überschreitet, können Sie entsprechende Maßnahmen ergreifen.

Verlaufsdiagramme zeigen die folgenden Informationen an:

- **Genutzte Gesamtkapazität (%)**

Zeigt die genutzte Kapazität im Aggregat und den Trend zur Nutzung der Aggregatkapazität basierend auf dem Nutzungsverlauf als Liniendiagramme in Prozent auf der vertikalen (y-)Achse an. Der Zeitraum wird auf der horizontalen (x) Achse angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen bestimmten Bereich bewegen. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Kapazitätsnutzung“ klicken, wird die Diagrammlinie „Kapazitätsnutzung“ ausgeblendet.

- **Genutzte Gesamtkapazität im Vergleich zur Gesamtkapazität**

  Zeigt den Trend der Nutzung der Gesamtkapazität basierend auf dem Nutzungsverlauf sowie die genutzte Kapazität und die Gesamtkapazität als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der vertikalen Achse (y) an. Der Zeitraum wird auf der horizontalen (x) Achse angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen bestimmten Bereich bewegen. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Trend der genutzten Kapazität“ klicken, wird die Diagrammlinie „Trend der genutzten Kapazität“ ausgeblendet.

- **Genutzte Gesamtkapazität (%) vs. zugesagte Kapazität (%)**

  Zeigt den Trend der Nutzung der Gesamtkapazität basierend auf dem Nutzungsverlauf sowie den zugesicherten Speicherplatz als Liniendiagramme in Prozent auf der vertikalen (y-)Achse an. Der Zeitraum wird auf der horizontalen (x) Achse angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen bestimmten Bereich bewegen. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Space Committed“ klicken, wird die Diagrammlinie „Space Committed“ ausgeblendet.

Ereignisliste

In der Ereignisliste werden Details zu neuen und bestätigten Ereignissen angezeigt:

- **Schwere**

  Zeigt den Schweregrad des Ereignisses an.

- **Ereignis**

  Zeigt den Ereignisnamen an.

- **Ausgelöste Zeit**

  Zeigt die Zeit an, die seit der Generierung des Ereignisses vergangen ist. Wenn die verstrichene Zeit mehr als eine Woche beträgt, wird der Zeitstempel für die Generierung des Ereignisses angezeigt.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie die Clusterknoten, Volumes und Datenträger anzeigen, die mit dem Aggregat in Zusammenhang stehen:

- **Knoten**

  Zeigt die Kapazität und den Integritätsstatus des Knotens an, der das Aggregat enthält. Die Kapazität gibt

die gesamte nutzbare Kapazität im Verhältnis zur verfügbaren Kapazität an.

- **Aggregate im Knoten**

  Zeigt die Anzahl und Kapazität aller Aggregate im Clusterknoten an, der das ausgewählte Aggregat enthält. Der Integritätsstatus der Aggregate wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Wenn ein Clusterknoten beispielsweise zehn Aggregate enthält, von denen fünf den Status „Warnung“ und die restlichen fünf den Status „Kritisch“ anzeigen, wird der Status „Kritisch“ angezeigt.

- **Bände**

  Zeigt die Anzahl und Kapazität der FlexVol -Volumes und FlexGroup -Volumes insgesamt an; die Zahl umfasst keine FlexGroup -Bestandteile. Außerdem wird der Integritätsstatus der Volumes basierend auf dem höchsten Schweregrad angezeigt.

- **Ressourcenpool**

  Zeigt die mit dem Aggregat verbundenen Ressourcenpools an.

- **Festplatten**

  Zeigt die Anzahl der Festplatten im ausgewählten Aggregat an.

Bereich „Zugehörige Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnungen 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 Warnungsnamen klicken.

Verwandte Informationen

"Anzeigen von Speicherpooldetails"