



Überwachen und Verwalten des Speichers

Active IQ Unified Manager

NetApp
October 15, 2025

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-916/storage-mgmt/concept_introduction_to_unified_manager_health_monitoring.html on October 15, 2025. Always check docs.netapp.com for the latest.

Inhalt

Überwachen und Verwalten des Speichers	1
Einführung in Active IQ Unified Manager	1
Einführung in die Integritätsüberwachung von Active IQ Unified Manager	1
Einführung in die Leistungsüberwachung von Active IQ Unified Manager	2
Verwenden Sie Unified Manager REST-APIs	3
Was der Unified Manager-Server macht	3
Verstehen Sie die Benutzeroberfläche	4
Typische Fensterlayouts	4
Anpassung des Fensterlayouts	5
Verwenden Sie die Unified Manager-Hilfe	6
Setzen Sie ein Lesezeichen für Ihre bevorzugten Hilfethemen	7
Suche nach Speicherobjekten	7
Speicherdaten als Berichte exportieren	8
Inhalt der Inventarseite filtern	10
Zeigen Sie aktive Ereignisse über die Benachrichtigungsglocke an	11
Überwachen und verwalten Sie Cluster über das Dashboard	11
Dashboard-Seite	12
Verwalten Sie ONTAP -Probleme oder -Funktionen direkt vom Unified Manager	15
Verwalten von Clustern	23
So funktioniert der Cluster-Erkennungsprozess	23
Liste der überwachten Cluster anzeigen	24
Cluster hinzufügen	25
Cluster bearbeiten	27
Cluster entfernen	28
Cluster neu entdecken	28
Überwachen Sie die virtuelle VMware-Infrastruktur	29
Was wird nicht unterstützt?	31
Anzeigen und Hinzufügen von vCenter Server	32
Entfernen von vCenter Server	34
Überwachen virtueller Maschinen	34
Anzeigen der virtuellen Infrastruktur in einem Disaster Recovery-Setup	36
Bereitstellen und Verwalten von Workloads	38
Übersicht über Workloads	39
Leistungsservice-Levels	46
Verwalten von Speichereffizienzrichtlinien	53
Verwalten und Überwachen von MetroCluster -Konfigurationen	55
Lautstärkeverhalten beim Umschalten und Zurückschalten	55
Cluster-Konnektivitätsstatusdefinitionen für die MetroCluster über-FC-Konfiguration	57
Datenspiegelungsstatusdefinitionen für MetroCluster über FC	58
Überwachen Sie MetroCluster -Konfigurationen	58
Überwachen der MetroCluster -Replikation	61
Verwalten von Kontingenten	62
Welche Kontingentgrenzen gibt es	62

Anzeigen von Benutzer- und Benutzergruppenkontingenten	63
Erstellen Sie Regeln zum Generieren von E-Mail-Adressen	63
Erstellen Sie ein E-Mail-Benachrichtigungsformat für Benutzer- und Benutzergruppenkontingente	64
Bearbeiten Sie die E-Mail-Adressen der Benutzer- und Gruppenkontingente	64
Erfahren Sie mehr über Quoten	65
Beschreibung der Kontingentdialogfelder	66
Fehlerbehebung	69
Fügen Sie dem Unified Manager-Datenbankverzeichnis Speicherplatz hinzu	69
Ändern des Erfassungsintervalls für Leistungsstatistiken	73
Ändern Sie die Dauer, für die Unified Manager Ereignis- und Leistungsdaten speichert	74
Unbekannter Authentifizierungsfehler	75
Benutzer nicht gefunden	75
Problem beim Hinzufügen von LDAP mithilfe anderer Authentifizierungsdienste	75
Problem mit der Protokollrotation des NetApp Manageability SDK auf Windows-Systemen	76

Überwachen und Verwalten des Speichers

Einführung in Active IQ Unified Manager

Mit Active IQ Unified Manager (früher OnCommand Unified Manager) können Sie den Zustand und die Leistung Ihrer ONTAP -Speichersysteme über eine einzige Schnittstelle überwachen und verwalten.

Unified Manager bietet die folgenden Funktionen:

- Erkennung, Überwachung und Benachrichtigungen für Systeme, auf denen ONTAP -Software installiert ist.
- Dashboard zur Anzeige der Kapazität, Sicherheit und Leistungsintegrität der Umgebung.
- Verbesserte Warn-, Ereignis- und Schwellenwertinfrastruktur.
- Zeigt detaillierte Diagramme an, die die Workload-Aktivität im Zeitverlauf darstellen, einschließlich IOPS (Operationen), MBps (Durchsatz), Latenz (Reaktionszeit), Auslastung, Leistungskapazität und Cache-Verhältnis.
- Identifiziert Workloads, die Clusterkomponenten übermäßig beanspruchen, und die Workloads, deren Leistung durch die erhöhte Aktivität beeinträchtigt wird.
- Bietet Vorschläge für Korrekturmaßnahmen, die zur Behebung bestimmter Vorfälle und Ereignisse durchgeführt werden können, sowie für einige Ereignisse eine Schaltfläche „Fix It“, damit Sie das Problem sofort beheben können.
- Integriert sich mit OnCommand Workflow Automation , um automatisierte Schutz-Workflows auszuführen.
- Möglichkeit, neue Workloads, wie z. B. eine LUN oder eine Dateifreigabe, direkt aus Unified Manager zu erstellen und ein Performance Service Level zuzuweisen, um die Leistungs- und Speicherziele für die Benutzer zu definieren, die mit diesem Workload auf die Anwendung zugreifen.

Einführung in die Integritätsüberwachung von Active IQ Unified Manager

Active IQ Unified Manager (früher OnCommand Unified Manager) hilft Ihnen, eine große Anzahl von Systemen mit ONTAP -Software über eine zentrale Benutzeroberfläche zu überwachen. Die Unified Manager-Serverinfrastruktur bietet Skalierbarkeit, Supportfähigkeit und erweiterte Überwachungs- und Benachrichtigungsfunktionen.

Zu den wichtigsten Funktionen von Unified Manager gehören Überwachung, Alarmierung, Verwaltung der Verfügbarkeit und Kapazität von Clustern, Verwaltung von Schutzfunktionen sowie Bündelung und Übermittlung von Diagnosedaten an den technischen Support.

Sie können Unified Manager zur Überwachung Ihrer Cluster verwenden. Wenn im Cluster Probleme auftreten, benachrichtigt Sie Unified Manager über die Details dieser Probleme durch Ereignisse. Bei einigen Ereignissen stehen Ihnen auch Abhilfemaßnahmen zur Verfügung, mit denen Sie die Probleme beheben können. Sie können Warnmeldungen für Ereignisse konfigurieren, sodass Sie beim Auftreten von Problemen per E-Mail und SNMP-Traps benachrichtigt werden.

Sie können Unified Manager verwenden, um Speicherobjekte in Ihrer Umgebung zu verwalten, indem Sie sie mit Anmerkungen verknüpfen. Sie können benutzerdefinierte Anmerkungen erstellen und Cluster, virtuelle Speichermaschinen (SVMs) und Volumes mithilfe von Regeln dynamisch mit den Anmerkungen verknüpfen.

Sie können den Speicherbedarf Ihrer Clusterobjekte auch anhand der in den Kapazitäts- und

Integritätsdiagrammen für das jeweilige Clusterobjekt bereitgestellten Informationen planen.

Körperliche und logische Leistungsfähigkeit

Unified Manager nutzt die Konzepte des physischen und logischen Speicherplatzes, die für ONTAP Speicherobjekte verwendet werden.

- **Physische Kapazität:** Physischer Speicherplatz bezieht sich auf die im Datenträger verwendeten physischen Speicherblöcke. Die „physisch genutzte Kapazität“ ist aufgrund der Datenreduzierung durch Speichereffizienzfunktionen (wie Deduplizierung und Komprimierung) normalerweise kleiner als die logisch genutzte Kapazität.
- **Logische Kapazität:** Der logische Speicherplatz bezieht sich auf den nutzbaren Speicherplatz (die logischen Blöcke) in einem Volume. Der logische Speicherplatz bezieht sich darauf, wie der theoretische Speicherplatz genutzt werden kann, ohne die Ergebnisse der Deduplizierung oder Komprimierung zu berücksichtigen. Der „genutzte logische Speicherplatz“ ist der genutzte physische Speicherplatz zuzüglich der Einsparungen durch konfigurierte Speichereffizienzfunktionen (wie Deduplizierung und Komprimierung). Dieser Messwert erscheint häufig größer als die physisch genutzte Kapazität, da er die Datenkomprimierung und andere Reduzierungen des physischen Speicherplatzes nicht berücksichtigt. Daher kann die gesamte logische Kapazität höher sein als der bereitgestellte Speicherplatz.

Kapazitätsmeseinheiten

Unified Manager berechnet die Speicherkapazität basierend auf Binäreinheiten von 1024 (2^{10}) Bytes. In ONTAP 9.10.0 und früher wurden diese Einheiten als KB, MB, GB, TB und PB angezeigt. Ab ONTAP 9.10.1 werden sie im Unified Manager als KiB, MiB, GiB, TiB und PiB angezeigt.



Die für den Durchsatz verwendeten Einheiten sind für alle Versionen von ONTAP weiterhin Kilobyte pro Sekunde (Kbps), Megabyte pro Sekunde (Mbps), Gigabyte pro Sekunde (Gbps) oder Terabyte pro Sekunde (Tbps) usw.

Kapazitätseinheit, die im Unified Manager für ONTAP 9.10.0 und früher angezeigt wird	Kapazitätseinheit, die im Unified Manager für ONTAP 9.10.1 angezeigt wird	Berechnung	Wert in Bytes
KB	KiB	1024	1024 Byte
MB	MiB	$1024 * 1024$	1.048.576 Bytes
GB	GiB	$1024 * 1024 * 1024$	1.073.741.824 Bytes
TB	TiB	$1024 * 1024 * 1024 * 1024$	1.099.511.627.776 Bytes

Einführung in die Leistungsüberwachung von Active IQ Unified Manager

Active IQ Unified Manager (früher OnCommand Unified Manager) bietet Leistungsüberwachungsfunktionen und Ereignisursachenanalyse für Systeme, auf denen NetApp ONTAP -Software ausgeführt wird.

Unified Manager hilft Ihnen, Workloads zu identifizieren, die Clusterkomponenten überbeanspruchen und die

Leistung anderer Workloads im Cluster verringern. Durch die Definition von Richtlinien für Leistungsschwellenwerte können Sie auch Maximalwerte für bestimmte Leistungsindikatoren festlegen, sodass Ereignisse generiert werden, wenn der Schwellenwert überschritten wird. Unified Manager benachrichtigt Sie über diese Leistungsereignisse, sodass Sie Korrekturmaßnahmen ergreifen und die Leistung wieder auf das normale Betriebsniveau bringen können. Sie können Ereignisse in der Unified Manager-Benutzeroberfläche anzeigen und analysieren.

Unified Manager überwacht die Leistung von zwei Arten von Workloads:

- Benutzerdefinierte Workloads

Diese Workloads bestehen aus FlexVol -Volumes und FlexGroup -Volumes, die Sie in Ihrem Cluster erstellt haben.

- Systemdefinierte Workloads

Diese Arbeitslasten bestehen aus internen Systemaktivitäten.

Verwenden Sie Unified Manager REST-APIs

Active IQ Unified Manager bietet Ihnen REST-APIs zum Anzeigen von Informationen zur Überwachung und Verwaltung Ihrer Speicherumgebung. APIs ermöglichen außerdem die Bereitstellung und Verwaltung von Speicherobjekten auf der Grundlage von Richtlinien.

Sie können ONTAP -APIs auch auf allen von ONTAP verwalteten Clustern ausführen, indem Sie das von Unified Manager unterstützte API-Gateway verwenden.

Informationen zu Unified Manager REST-APIs finden Sie unter "[Erste Schritte mit Active IQ Unified Manager REST-APIs](#)".

Was der Unified Manager-Server macht

Die Unified Manager-Serverinfrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Anwendungsserver. Es bietet Infrastrukturdienste wie Erkennung, Überwachung, rollenbasierte Zugriffskontrolle (RBAC), Auditing und Protokollierung.

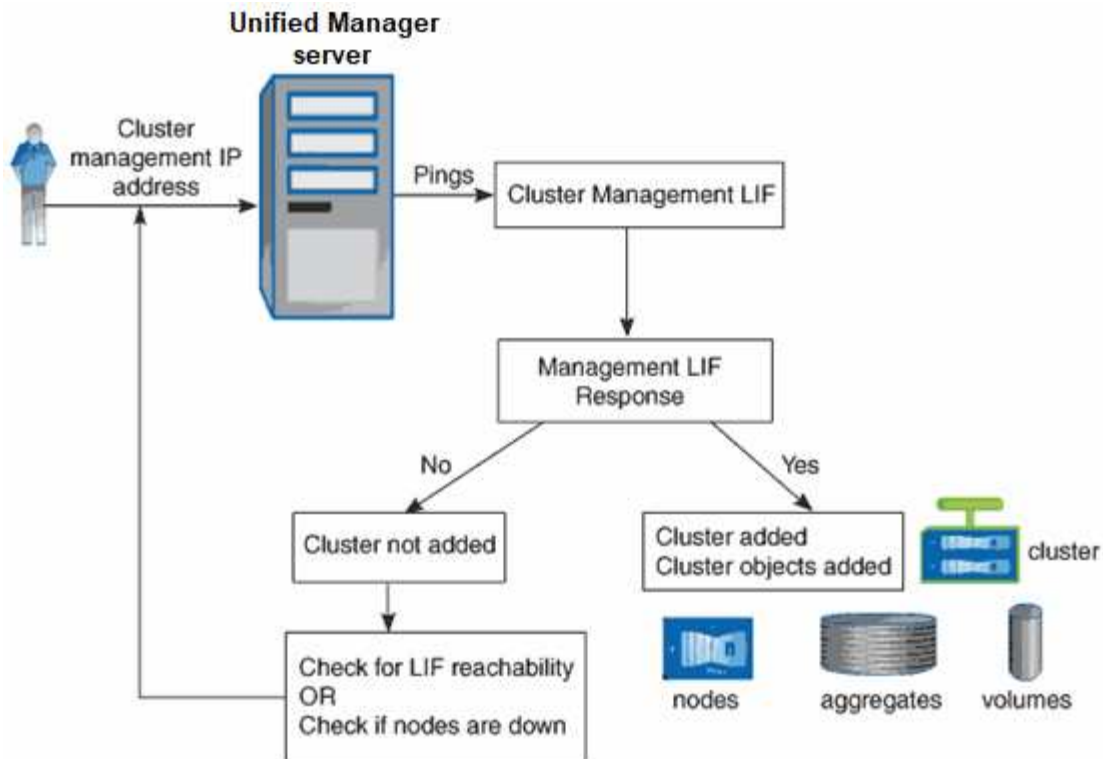
Unified Manager sammelt Clusterinformationen, speichert die Daten in der Datenbank und analysiert die Daten, um festzustellen, ob Clusterprobleme vorliegen.

So funktioniert der Discovery-Prozess

Nachdem Sie den Cluster zu Unified Manager hinzugefügt haben, erkennt der Server die Clusterobjekte und fügt sie seiner Datenbank hinzu. Wenn Sie verstehen, wie der Erkennungsprozess funktioniert, können Sie die Cluster und deren Objekte Ihrer Organisation besser verwalten.

Das Standardüberwachungsintervall beträgt 15 Minuten: Wenn Sie dem Unified Manager-Server einen Cluster hinzugefügt haben, dauert es 15 Minuten, bis die Clusterdetails in der Unified Manager-Benutzeroberfläche angezeigt werden.

Das folgende Bild veranschaulicht den Erkennungsprozess im Active IQ Unified Manager:



Verstehen Sie die Benutzeroberfläche

Die Benutzeroberfläche des Unified Managers besteht hauptsächlich aus einem Dashboard, das eine Übersicht über die überwachten Objekte bietet. Über die Benutzeroberfläche können Sie außerdem alle Clusterobjekte anzeigen.

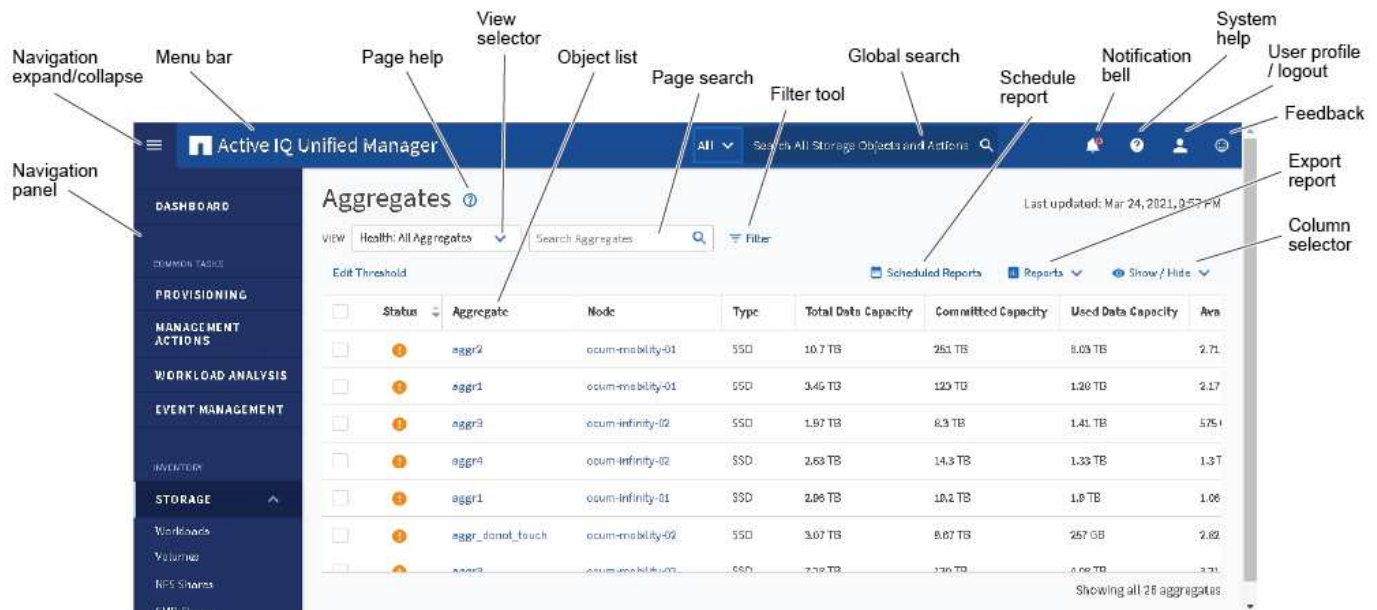
Sie können eine bevorzugte Ansicht auswählen und die Aktionsschaltflächen nach Bedarf verwenden. Ihre Bildschirmkonfiguration wird in einem Arbeitsbereich gespeichert, sodass beim Starten von Unified Manager alle benötigten Funktionen verfügbar sind. Wenn Sie jedoch von einer Ansicht zur anderen und dann zurück navigieren, ist die Ansicht möglicherweise nicht dieselbe.

Typische Fensterlayouts

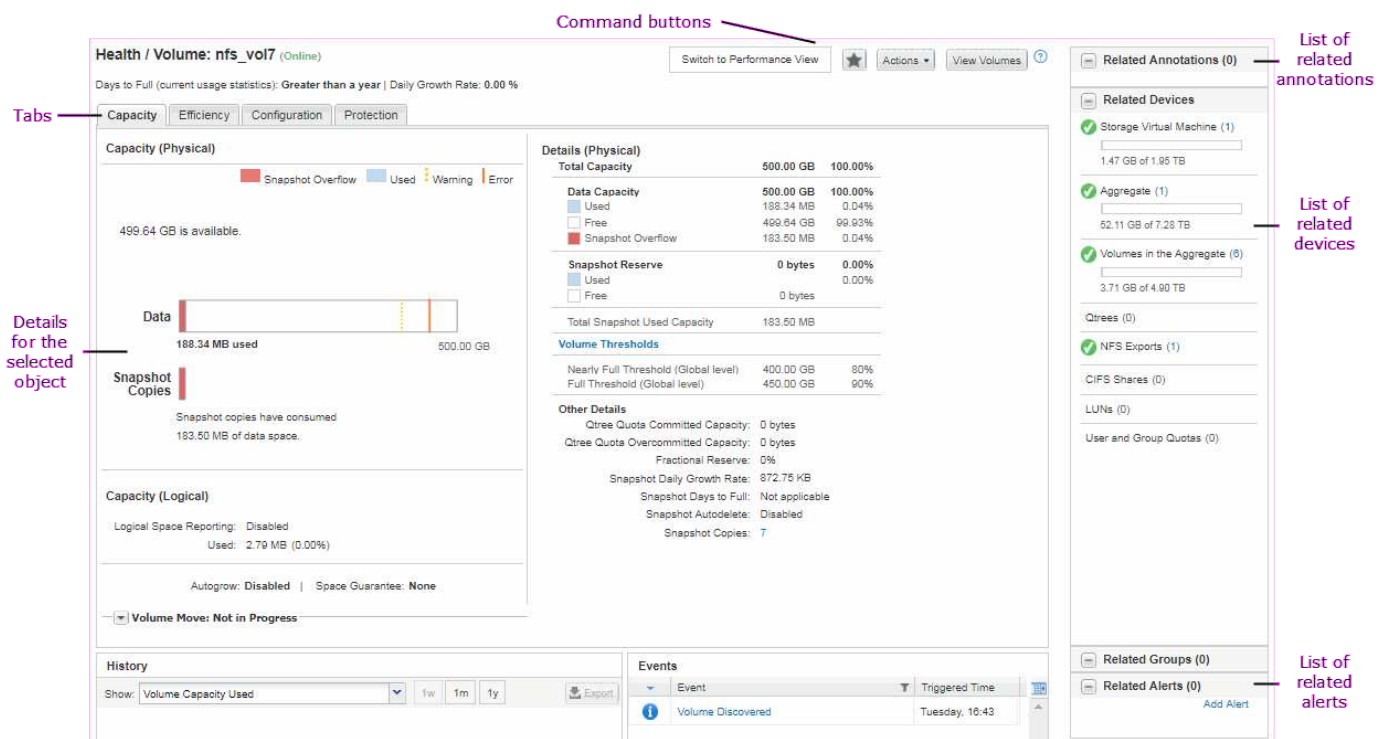
Wenn Sie die typischen Fensterlayouts verstehen, können Sie Active IQ Unified Manager effektiv navigieren und verwenden. Die meisten Unified Manager-Fenster ähneln einem von zwei allgemeinen Layouts: Objektliste oder Details. Die empfohlene Anzeigeeinstellung beträgt mindestens 1280 x 1024 Pixel.

Nicht jedes Fenster enthält jedes Element der folgenden Diagramme.

Layout des Objektlistenfensters



Layout des Fensters „Objektdetails“



Anpassung des Fensterlayouts

Mit Active IQ Unified Manager können Sie das Layout der Informationen auf den Speicher- und Netzwerkobjektseiten anpassen. Durch Anpassen der Fenster können Sie steuern, welche Daten angezeigt werden und wie die Daten angezeigt werden.

• Sortierung

Sie können auf die Spaltenüberschrift klicken, um die Sortierreihenfolge der Spalteneinträge zu ändern.

Wenn Sie auf die Spaltenüberschrift klicken, werden die Sortierpfeile (▲ Und ▼) werden für diese Spalte angezeigt.

- **Filtern**

Sie können auf das Filtersymbol (), um Filter anzuwenden und die Anzeige von Informationen auf den Speicher- und Netzwerkobjektseiten anzupassen, sodass nur die Einträge angezeigt werden, die den angegebenen Bedingungen entsprechen. Sie wenden Filter aus dem Filterbereich an.

Im Filterbereich können Sie die meisten Spalten basierend auf den ausgewählten Optionen filtern. Beispielsweise können Sie in der Ansicht „Integrität: Alle Volumes“ den Bereich „Filter“ verwenden, um alle Volumes anzuzeigen, die offline sind, indem Sie unter „Status“ die entsprechende Filteroption auswählen.

In den kapazitätsbezogenen Spalten einer Liste werden die Kapazitätsdaten immer in den entsprechenden Einheiten angezeigt, die auf zwei Dezimalstellen gerundet sind. Dies gilt auch beim Filtern von Kapazitätsspalten. Wenn Sie beispielsweise den Filter in der Spalte „Gesamtdatenkapazität“ in der Ansicht „Integrität: Alle Aggregate“ verwenden, um Daten größer als 20,45 GB zu filtern, wird die tatsächliche Kapazität von 20,454 GB als 20,45 GB angezeigt. Wenn Sie Daten mit weniger als 20,45 GB filtern, wird die tatsächliche Kapazität von 20,449 GB als 20,45 GB angezeigt.

Wenn Sie den Filter in der Spalte „Verfügbare Daten %“ in der Ansicht „Integrität: Alle Aggregate“ verwenden, um Daten über 20,45 % zu filtern, wird die tatsächliche Kapazität von 20,454 % als 20,45 % angezeigt. Wenn Sie Daten unter 20,45 % filtern, wird die tatsächliche Kapazität von 20,449 % als 20,45 % angezeigt.

- **Spalten ausblenden oder anzeigen**

Sie können auf das Symbol zur Spaltenanzeige (**Einblenden/Ausblenden**) klicken, um auszuwählen, welche Spalten angezeigt werden sollen. Nachdem Sie die entsprechenden Spalten ausgewählt haben, können Sie sie durch Ziehen mit der Maus neu anordnen.

- **Suche**

Sie können das Suchfeld verwenden, um nach bestimmten Objektattributen zu suchen und so die Liste der Artikel auf der Inventarseite zu verfeinern. Sie können beispielsweise „Cloud“ eingeben, um die Liste der Volumes auf der Volume-Inventarseite zu verfeinern und alle Volumes anzuzeigen, die das Wort „Cloud“ enthalten.

- **Daten exportieren**

Sie können auf die Schaltfläche **Berichte** (oder **Exportieren**) klicken, um Daten in eine durch Kommas getrennte Wertedatei zu exportieren. (.csv) Datei, (.pdf) Dokument oder Microsoft Excel (.xlsx) Datei und verwenden Sie die exportierten Daten zum Erstellen von Berichten.

Verwenden Sie die Unified Manager-Hilfe

Die Hilfe enthält Informationen zu allen in Active IQ Unified Manager enthaltenen Funktionen. Über das Inhaltsverzeichnis, den Index oder die Suchfunktion können Sie sich über die Funktionen und deren Verwendung informieren.

Hilfe ist auf jeder Registerkarte und in der Menüleiste der Unified Manager-Benutzeroberfläche verfügbar.

Das Suchtool in der Hilfe funktioniert bei Wortteilen nicht.

- Um mehr über bestimmte Felder oder Parameter zu erfahren, klicken Sie auf  .
- Um alle Hilfeinhalte anzuzeigen, klicken Sie auf  * > **Hilfe/Dokumentation** in der Menüleiste.

Ausführlichere Informationen erhalten Sie, indem Sie einen beliebigen Teil des Inhaltsverzeichnisses im Navigationsbereich erweitern.

- Um die Hilfeinhalte zu durchsuchen, klicken Sie im Navigationsbereich auf die Registerkarte **Suchen**, geben Sie das gewünschte Wort oder die gewünschte Wortfolge ein und klicken Sie auf **Los!**
- Um Hilfethemen auszudrucken, klicken Sie auf das Druckersymbol.

Setzen Sie ein Lesezeichen für Ihre bevorzugten Hilfethemen

Auf der Registerkarte „Hilfefavoriten“ können Sie häufig verwendete Hilfethemen mit einem Lesezeichen versehen. Mithilfe von Lesezeichen können Sie schnell auf Ihre Lieblingsthemen zugreifen.

Schritte

1. Navigieren Sie zu dem Hilfethema, das Sie als Favorit hinzufügen möchten.
2. Klicken Sie auf **Favoriten** und dann auf **Hinzufügen**.

Suche nach Speicherobjekten

Um schnell auf ein bestimmtes Objekt zuzugreifen, können Sie das Feld **Alle Speicherobjekte durchsuchen** oben in der Menüleiste verwenden. Mit dieser Methode der globalen Suche über alle Objekte hinweg können Sie bestimmte Objekte schnell nach Typ finden. Die Suchergebnisse werden nach Speicherobjektyp sortiert und Sie können sie mithilfe des Dropdown-Menüs weiter nach Objekt filtern.

Bevor Sie beginnen

- Zum Ausführen dieser Aufgabe müssen Sie eine der folgenden Rollen innehaben: Operator, Anwendungsadministrator oder Speicheradministrator.
- Eine gültige Suche muss mindestens drei Zeichen enthalten.

Bei Verwendung des Dropdown-Menüwerts „Alle“ zeigt die globale Suche die Gesamtzahl der gefundenen Ergebnisse in allen Objektkategorien an; maximal 25 Suchergebnisse pro Objektkategorie. Sie können einen bestimmten Objektyp aus dem Dropdown-Menü auswählen, um die Suche innerhalb eines bestimmten Objektyps zu verfeinern. In diesem Fall ist die zurückgegebene Liste nicht auf die Top 25 Objekte beschränkt.

Zu den Objekttypen, nach denen Sie suchen können, gehören:

- Cluster
- Nodes
- Speicher-VMs
- Aggregate
- Bände
- Qtrees
- SMB-Aktien

- NFS-Freigaben
- Benutzer- oder Gruppenkontingente
- LUNs
- NVMe-Namespaces
- Initiatorgruppen
- Initiatoren
- Konsistenzgruppe

Durch Eingabe eines Workload-Namens wird die Liste der Workloads unter der entsprechenden Volume- oder LUN-Kategorie zurückgegeben.

Sie können in den Suchergebnissen auf ein beliebiges Objekt klicken, um zur Seite mit den Integritätsdetails für dieses Objekt zu navigieren. Wenn für ein Objekt keine direkte Integritätsseite vorhanden ist, wird die Integritätsseite des übergeordneten Objekts angezeigt. Wenn Sie beispielsweise nach einer bestimmten LUN suchen, wird die SVM-Detailseite angezeigt, auf der sich die LUN befindet.

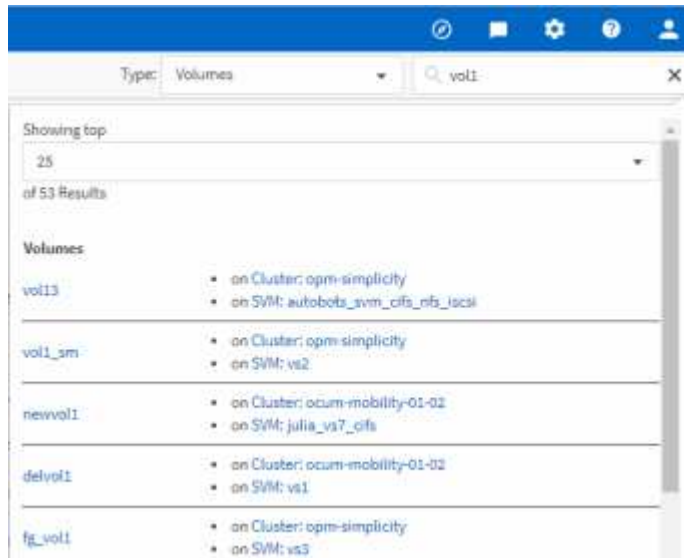


Ports und LIFs können in der globalen Suchleiste nicht durchsucht werden.

Schritte

1. Wählen Sie einen Objekttyp aus dem Menü aus, um die Suchergebnisse auf nur einen einzigen Objekttyp zu verfeinern.
2. Geben Sie mindestens drei Zeichen des Objekttypnamens in das Feld **Alle Speicherobjekte durchsuchen** ein.

In diesem Beispiel ist im Dropdownfeld der Objekttyp „Volumes“ ausgewählt. Wenn Sie „vol1“ in das Feld **Alle Speicherobjekte durchsuchen** eingeben, wird eine Liste aller Volumes angezeigt, deren Namen diese Zeichen enthalten.



Speicherdaten als Berichte exportieren

Sie können Speicherdaten in verschiedenen Ausgabeformaten exportieren und die exportierten Daten dann zum Erstellen von Berichten verwenden. Wenn beispielsweise

10 kritische Ereignisse nicht behoben wurden, können Sie die Daten von der Inventarseite der Ereignisverwaltung exportieren, um einen Bericht zu erstellen, und den Bericht dann an Administratoren senden, die die Probleme beheben können.

Sie können Daten in eine `.csv` Datei, `.xlsx` Datei oder `.pdf` Dokument von den Inventarseiten **Speicher** und **Netzwerk** und verwenden Sie die exportierten Daten zum Erstellen von Berichten. Es gibt andere Stellen im Produkt, an denen nur `.csv` oder `.pdf` Dateien können generiert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie exportieren möchten...	Machen Sie Folgendes...
Details zum Speicherobjektbestand	Klicken Sie im linken Navigationsmenü auf Speicher oder Netzwerk und wählen Sie dann ein Speicherobjekt aus. Wählen Sie eine der vom System bereitgestellten Ansichten oder eine beliebige benutzerdefinierte Ansicht, die Sie erstellt haben.
Details zur QoS-Richtliniengruppe	Klicken Sie im linken Navigationsmenü auf Speicher > QoS-Richtliniengruppen .
Details zur Speicherkapazität und zum Schutzverlauf	Klicken Sie auf Speicher > Aggregate oder Speicher > Volumes und wählen Sie dann ein einzelnes Aggregat oder Volume aus.
Veranstaltungsdetails	Klicken Sie im linken Navigationsmenü auf Eventverwaltung .
Leistungsdetails der Top 10-Speicherobjekte	Klicken Sie auf Speicher > Cluster > Leistung: Alle Cluster , wählen Sie dann einen Cluster aus und wählen Sie die Registerkarte Top-Performer . Wählen Sie dann ein Speicherobjekt und einen Leistungsindikator aus.

2. Klicken Sie auf die Schaltfläche **Berichte** (oder auf einigen UI-Seiten auf die Schaltfläche **Exportieren**).
3. Klicken Sie auf **CSV herunterladen**, **PDF herunterladen** oder **Excel herunterladen**, um die Exportanforderung zu bestätigen.

Auf der Registerkarte „Top Performers“ können Sie einen Bericht mit den Statistiken für den einzelnen Cluster, den Sie gerade anzeigen, oder für alle Cluster im Rechenzentrum herunterladen.

Die Datei wird heruntergeladen.

4. Öffnen Sie die Datei in der entsprechenden Anwendung.

Verwandte Informationen

["Seite „Integrität/Cluster-Inventar“"](#)

Inhalt der Inventarseite filtern

Sie können die Daten der Inventarseite im Unified Manager filtern, um Daten anhand bestimmter Kriterien schnell zu finden. Mithilfe von Filtern können Sie den Inhalt der Unified Manager-Seiten eingrenzen und nur die Ergebnisse anzeigen, die Sie interessieren. Dies bietet eine sehr effiziente Methode, nur die Daten anzuzeigen, an denen Sie interessiert sind.

Verwenden Sie **Filtern**, um die Rasteransicht Ihren Wünschen entsprechend anzupassen. Die verfügbaren Filteroptionen basieren auf dem Objekttyp, der im Raster angezeigt wird. Wenn derzeit Filter angewendet werden, wird die Anzahl der angewendeten Filter rechts neben der Schaltfläche „Filter“ angezeigt.

Es werden drei Arten von Filterparametern unterstützt.

Parameter	Validierung
Zeichenfolge (Text)	Die Operatoren sind enthält , beginnt mit , endet mit und enthält nicht .
Anzahl	Die Operatoren sind größer als , kleiner als , im letzten und zwischen .
Aufzählung (Text)	Die Operatoren sind ist und ist nicht .

Die Felder „Spalte“, „Operator“ und „Wert“ sind für jeden Filter erforderlich. Die verfügbaren Filter spiegeln die filterbaren Spalten auf der aktuellen Seite wider. Sie können maximal vier Filter anwenden. Gefilterte Ergebnisse basieren auf kombinierten Filterparametern. Gefilterte Ergebnisse gelten für alle Seiten in Ihrer gefilterten Suche, nicht nur für die aktuell angezeigte Seite.

Sie können Filter über das Filterfeld hinzufügen.

1. Klicken Sie oben auf der Seite auf die Schaltfläche **Filter**. Das Filterfeld wird angezeigt.
2. Klicken Sie auf die linke Dropdown-Liste und wählen Sie ein Objekt aus, beispielsweise *Cluster* oder einen Leistungsindikator.
3. Klicken Sie auf die mittlere Dropdown-Liste und wählen Sie den Operator aus, den Sie verwenden möchten.
4. Wählen Sie in der letzten Liste einen Wert aus oder geben Sie ihn ein, um den Filter für dieses Objekt zu vervollständigen.
5. Um einen weiteren Filter hinzuzufügen, klicken Sie auf **+Filter hinzufügen**. Ein zusätzliches Filterfeld wird angezeigt. Vervollständigen Sie diesen Filter mit dem in den vorhergehenden Schritten beschriebenen Verfahren. Beachten Sie, dass nach dem Hinzufügen Ihres vierten Filters die Schaltfläche **+Filter hinzufügen** nicht mehr angezeigt wird.
6. Klicken Sie auf **Filter anwenden**. Die Filteroptionen werden auf das Raster angewendet und die Anzahl der Filter wird rechts neben der Schaltfläche „Filter“ angezeigt.
7. Verwenden Sie das Filterfeld, um einzelne Filter zu entfernen, indem Sie auf das Papierkorbsymbol rechts neben dem zu entfernenden Filter klicken.

8. Um alle Filter zu entfernen, klicken Sie unten im Filterbereich auf **Zurücksetzen**.

Filterbeispiel

Die Abbildung zeigt das Filterbedienfeld mit drei Filtern. Die Schaltfläche **+Filter hinzufügen** wird angezeigt, wenn Sie weniger als die maximal vier Filter haben.

Nachdem Sie auf **Filter anwenden** geklickt haben, wird das Filterfenster geschlossen, Ihre Filter werden angewendet und die Anzahl der angewendeten Filter wird angezeigt ().

Zeigen Sie aktive Ereignisse über die Benachrichtigungsglocke an

Die Benachrichtigungsglocke () in der Menüleiste bietet eine schnelle Möglichkeit, die wichtigsten aktiven Ereignisse anzuzeigen, die Unified Manager verfolgt.

Die Liste der aktiven Ereignisse bietet eine Möglichkeit, die Gesamtzahl der kritischen Ereignisse, Fehler-, Warn- und Upgrade-Ereignisse auf allen Clustern anzuzeigen. Diese Liste enthält Ereignisse der letzten 7 Tage und keine Informationsereignisse. Sie können auf einen Link klicken, um die Liste der Ereignisse anzuzeigen, die Sie am meisten interessieren.

Beachten Sie, dass Unified Manager diese Informationen auf dieser Seite anzeigt, wenn ein Cluster nicht erreichbar ist. Sie können detaillierte Informationen zu einem nicht erreichbaren Cluster anzeigen, indem Sie auf die Schaltfläche **Details** klicken. Diese Aktion öffnet die Seite mit den Veranstaltungsdetails. Auf dieser Seite werden auch Probleme bei der Skalierungsüberwachung angezeigt, beispielsweise zu wenig Speicherplatz oder RAM auf der Verwaltungsstation.

Schritte

1. Klicken Sie in der Menüleiste auf .
2. Um Details zu einem der aktiven Ereignisse anzuzeigen, klicken Sie auf den Ereignistextlink, beispielsweise „2 Kapazität“ oder „4 Leistung“.

Überwachen und verwalten Sie Cluster über das Dashboard

Das Dashboard bietet auf einen Blick kumulative Informationen zum aktuellen Zustand Ihrer überwachten ONTAP Systeme. Das Dashboard bietet „Panels“, mit denen Sie die Gesamtkapazität, Leistung und Sicherheitsintegrität der von Ihnen überwachten Cluster beurteilen können.

Darüber hinaus gibt es bestimmte ONTAP Probleme, die Sie direkt über die Benutzeroberfläche des Unified Managers beheben können, anstatt den ONTAP System Manager oder die ONTAP CLI verwenden zu müssen.

Oben im Dashboard können Sie auswählen, ob die Panels Informationen für alle überwachten Cluster oder für einen einzelnen Cluster anzeigen. Sie können zunächst den Status aller Cluster anzeigen und dann einen Drilldown zu einzelnen Clustern durchführen, wenn Sie detaillierte Informationen anzeigen möchten.



Je nach Ihrer Konfiguration werden einige der unten aufgeführten Bereiche möglicherweise nicht auf der Seite angezeigt.

Paneele	Beschreibung
Verwaltungsmaßnahmen	Wenn Unified Manager ein Problem diagnostizieren und eine einzelne Lösung dafür ermitteln kann, werden diese Lösungen in diesem Bereich mit einer Schaltfläche Fix It angezeigt.
Kapazität	Zeigt die gesamte und genutzte Kapazität für die lokale und die Cloud-Ebene sowie die Anzahl der Tage an, bis die lokale Kapazität die Obergrenze erreicht.
Leistungskapazität	Zeigt den Leistungskapazitätswert für jeden Cluster und die Anzahl der Tage an, bis die Leistungskapazität die Obergrenze erreicht.
Arbeitslast-IOPS	Zeigt die Gesamtzahl der Workloads an, die derzeit in einem bestimmten IOPS-Bereich ausgeführt werden.
Workload-Leistung	Zeigt die Gesamtzahl der konformen und nicht konformen Workloads an, die jedem definierten Performance-Service-Level zugewiesen sind.
Sicherheit	Zeigt die Anzahl der Cluster an, die konform oder nicht konform sind, die Anzahl der SVMs, die konform oder nicht konform sind, und die Anzahl der Volumes, die verschlüsselt oder nicht verschlüsselt sind.
Schutz	Zeigt die Anzahl der Storage-VMs an, die durch eine SVM-DR-Beziehung geschützt sind, die durch eine SnapMirror Beziehung geschützten Volumes, die durch Snapshot geschützten Volumes und die durch MetroCluster geschützten Cluster.
Nutzungsübersicht	Zeigt Cluster sortiert nach höchstem IOPS, höchstem Durchsatz (MBps) oder höchster genutzter physischer Kapazität an.

Dashboard-Seite

Die Dashboard-Seite verfügt über „Panels“, die die allgemeine Kapazität, Leistung und Sicherheitsintegrität der von Ihnen überwachten Cluster anzeigen. Diese Seite enthält außerdem ein Bedienfeld „Verwaltungsaktionen“, in dem Korrekturen aufgelistet sind, die Unified Manager zur Behebung bestimmter Ereignisse vornehmen kann.

Die meisten Panels zeigen auch die Anzahl der aktiven Ereignisse in dieser Kategorie und die Anzahl der in den letzten 24 Stunden hinzugefügten neuen Ereignisse an. Mithilfe dieser Informationen können Sie entscheiden, welche Cluster Sie möglicherweise weiter analysieren müssen, um Ereignisse aufzulösen. Durch Klicken auf die Ereignisse werden die wichtigsten Ereignisse angezeigt und ein Link zur Inventarseite des Ereignismanagements bereitgestellt, die gefiltert ist, um die aktiven Ereignisse in dieser Kategorie anzuzeigen.

Oben im Dashboard können Sie auswählen, ob die Panels Informationen für alle überwachten Cluster („Alle Cluster“) oder für einen einzelnen Cluster anzeigen. Sie können zunächst den Status aller Cluster anzeigen und dann einen Drilldown zu einzelnen Clustern durchführen, wenn Sie detaillierte Informationen anzeigen möchten.



Einige der unten aufgeführten Bedienfelder werden je nach Ihrer Konfiguration auf dem Dashboard angezeigt.

Bereich „Verwaltungsaktionen“

Es gibt bestimmte Probleme, die Unified Manager gründlich diagnostizieren und eine einzige Lösung bereitstellen kann. Sofern verfügbar, werden diese Lösungen in diesem Bereich mit der Schaltfläche **Fix It** oder **Fix All** angezeigt. Sie können diese Probleme sofort über Unified Manager beheben, anstatt ONTAP System Manager oder die ONTAP CLI verwenden zu müssen. Um alle Ausgaben anzuzeigen, klicken Sie auf „Anzeigen“ ["Beheben Sie ONTAP -Probleme direkt vom Unified Manager aus"](#) für weitere Informationen.

Kapazitätspanel

Beim Anzeigen aller Cluster zeigt dieses Fenster die physisch genutzte Kapazität (nach Anwendung der Einsparungen bei der Speichereffizienz) und die physisch verfügbare Kapazität (ohne potenzielle Einsparungen bei der Speichereffizienz) für jeden Cluster, die Anzahl der Tage bis zur voraussichtlichen Volllast der Festplatten und das Datenreduktionsverhältnis (ohne Snapshot-Kopien) basierend auf den konfigurierten ONTAP Einstellungen zur Speichereffizienz an. Außerdem wird die genutzte Kapazität für alle konfigurierten Cloud-Ebenen aufgelistet. Durch Klicken auf das Balkendiagramm gelangen Sie zur Aggregate-Inventarseite für diesen Cluster. Wenn Sie auf den Text „Tage bis zur Volllast“ klicken, wird eine Meldung angezeigt, die das Aggregat mit der geringsten Anzahl verbleibender Kapazitätstage identifiziert. Klicken Sie auf den Aggregatnamen, um weitere Details anzuzeigen.

Beim Anzeigen eines einzelnen Clusters zeigt dieses Fenster die physisch genutzte Kapazität und die physisch verfügbare Kapazität für die Datenaggregate an, sortiert nach den einzelnen Datenträgertypen auf der lokalen Ebene und für die Cloud-Ebene. Wenn Sie auf das Balkendiagramm für einen Datenträgertyp klicken, gelangen Sie zur Volume-Inventarseite für die Volumes, die diesen Datenträgertyp verwenden.

Leistungskapazitätspanel

Beim Anzeigen aller Cluster zeigt dieses Fenster den Leistungskapazitätswert für jeden Cluster (Durchschnittswert der letzten Stunde) und die Anzahl der Tage an, bis die Leistungskapazität die Obergrenze erreicht (basierend auf der täglichen Wachstumsrate). Durch Klicken auf das Balkendiagramm gelangen Sie zur Knotenbestandsseite für diesen Cluster. Beachten Sie, dass auf der Seite „Knoteninventar“ die durchschnittliche Leistungskapazität der letzten 72 Stunden angezeigt wird. Wenn Sie auf den Text „Tage bis zur Volllast“ klicken, wird eine Meldung angezeigt, die den Knoten mit der geringsten Anzahl verbleibender Tage für die Leistungskapazität identifiziert. Klicken Sie auf den Knotennamen, um weitere Details anzuzeigen.

Beim Anzeigen eines einzelnen Clusters zeigt dieses Fenster den Prozentsatz der genutzten Cluster-Leistungskapazität, die Gesamt-IOPS- und Gesamtdurchsatzwerte (MB/s) sowie die Anzahl der Tage an, bis jede dieser drei Kennzahlen voraussichtlich ihre Obergrenze erreicht.

Arbeitslast-IOPS-Panel

Beim Anzeigen eines einzelnen Clusters zeigt dieses Fenster die Gesamtzahl der Workloads an, die derzeit in einem bestimmten IOPS-Bereich ausgeführt werden, und gibt die Anzahl für jeden Datenträgertyp an, wenn Sie mit dem Cursor über das Diagramm fahren.

Bereich „Arbeitslastleistung“

In diesem Bereich wird die Gesamtzahl der konformen und nicht konformen Workloads angezeigt, die jeder Performance Service Level (PSL)-Richtlinie zugewiesen sind. Außerdem wird die Anzahl der Workloads angezeigt, denen keine PSL zugewiesen ist. Durch Klicken auf ein Balkendiagramm gelangen Sie zu den entsprechenden Arbeitslasten, die dieser Richtlinie auf der Seite „Arbeitslasten“ zugewiesen sind. Wenn Sie auf die Zahl hinter dem Balkendiagramm klicken, gelangen Sie zu den konformen und nicht konformen Arbeitslasten, die dieser Richtlinie zugewiesen sind.

Sicherheitspanel

Das Sicherheitsfenster zeigt den allgemeinen Sicherheitsstatus für alle Cluster oder einen einzelnen Cluster an, je nach Ihrer aktuellen Ansicht. Dieses Fenster zeigt Folgendes an:

- eine Liste der in den letzten 24 Stunden empfangenen Sicherheitsereignisse. Klicken Sie auf ein Ereignis, um die Details auf der Seite „Ereignisdetails“ anzuzeigen.
- den Cluster-Sicherheitsstatus (Anzahl der konformen und nicht konformen Cluster)
- der Sicherheitsstatus der Speicher-VM (Anzahl der konformen und nicht konformen Speicher-VMs)
- den Volume-Verschlüsselungsstatus (Anzahl der Volumes, die verschlüsselt oder nicht verschlüsselt sind)
- den Anti-Ransomware-Status des Volumes (Anzahl der Volumes mit aktiviertem oder deaktiviertem Anti-Ransomware-Schutz)

Sie können auf die Balkendiagramme der konformen und nicht konformen Cluster, Speicher-VMs, verschlüsselten und unverschlüsselten Volumes und des Volume-Anti-Ransomware-Status klicken, um zu den entsprechenden Seiten zu gelangen und die Sicherheitsdetails der gefilterten Cluster, Speicher-VMs und Volumes anzuzeigen.

Die Einhaltung basiert auf der ["NetApp Security Hardening Guide für ONTAP 9"](#) . Klicken Sie oben im Bereich auf den Rechtspfeil, um Sicherheitsdetails für alle Cluster auf der Seite „Sicherheit“ anzuzeigen. Weitere Informationen finden Sie unter ["Anzeigen des detaillierten Sicherheitsstatus für Cluster und Storage-VMs"](#) .

Datenschutzpanel

In diesem Bereich wird die Datenschutzzusammenfassung für einen einzelnen oder alle Cluster in einem Rechenzentrum angezeigt. Es zeigt die Gesamtzahl der Datenschutzereignisse, MetroCluster -Ereignisse und die Anzahl der aktiven Ereignisse an, die in den letzten 24 Stunden in ONTAP ausgelöst wurden. Wenn Sie auf den Link jedes dieser Ereignisse klicken, gelangen Sie zur Seite mit den Ereignisdetails. Sie können auf den Link **Alle anzeigen** klicken, um alle aktiven Schutzereignisse auf der Inventarseite der Ereignisverwaltung anzuzeigen. Das Bedienfeld zeigt Folgendes an:

- Die Anzahl der Volumes in einem Cluster oder alle Cluster in einem Rechenzentrum, die durch Snapshot-Kopien geschützt sind.
- Die Anzahl der Volumes in einem Cluster oder alle Cluster in einem Rechenzentrum, die durch SnapMirror -Beziehungen geschützt sind. Bei SnapMirror -Beziehungen wird die Volumeanzahl im Quellcluster berücksichtigt.
- Die Anzahl der Cluster oder alle Cluster in einem Rechenzentrum, die durch die MetroCluster -Konfiguration über IP oder FC geschützt sind.
- Die Anzahl der Volume-Beziehungen mit SnapMirror Recovery Point Objective (RPO)-Verzögerung basierend auf dem Verzögerungsstatus.

Sie können mit der Maus darüberfahren, um die jeweiligen Zählungen und Legenden anzuzeigen. Sie können oben im Bereich auf den rechten Pfeil klicken, um die Details für einen einzelnen oder alle Cluster auf der

Seite „Datenschutz“ anzuzeigen. Sie können auch auf Folgendes klicken:

- Die Balkendiagramme für ungeschützte Volumes und durch Snapshot-Kopien geschützte Volumes ermöglichen es Ihnen, zur Seite „Volumes“ zu gelangen und die Details anzuzeigen.
- Die Balkendiagramme für die durch die MetroCluster -Konfiguration geschützten oder nicht geschützten Cluster, um zur Seite „Cluster“ zu gelangen und die Details anzuzeigen.
- Die Balkendiagramme für alle Beziehungen führen zur Seite „Beziehungen“, wo die Details basierend auf dem Quellcluster gefiltert werden.

Weitere Informationen finden Sie unter ["Anzeigen des Volume-Schutzstatus"](#).

Bedienfeld „Nutzungsübersicht“

Beim Anzeigen aller Cluster können Sie die Cluster nach den höchsten IOPS, dem höchsten Durchsatz (MB/s) oder der höchsten genutzten physischen Kapazität sortiert anzeigen.

Beim Anzeigen eines einzelnen Clusters können Sie die Workloads nach den höchsten IOPS, dem höchsten Durchsatz (MB/s) oder der höchsten genutzten logischen Kapazität sortiert anzeigen.

Verwandte Informationen

["Beheben von Problemen mithilfe automatischer Korrekturen von Unified Manager"](#)

["Anzeigen von Informationen zu Leistungsereignissen"](#)

["Verwalten der Leistung mithilfe von Leistungskapazität und verfügbaren IOPS-Informationen"](#)

["Seite mit den Volumen-/Gesundheitsdetails"](#)

["Analyse und Benachrichtigung von Leistungsereignissen"](#)

["Beschreibung der Ereignisschweregrade"](#)

["Quellen von Leistungsereignissen"](#)

["Verwalten von Cluster-Sicherheitszielen"](#)

["Überwachen Sie die Clusterleistung von der Zielseite des Leistungsclusters aus"](#)

["Überwachen Sie die Leistung mithilfe der Leistungsinventarseiten"](#)

Verwalten Sie ONTAP -Probleme oder -Funktionen direkt vom Unified Manager

Sie können bestimmte ONTAP Probleme beheben oder bestimmte ONTAP Funktionen direkt über die Unified Manager-Benutzeroberfläche verwalten, anstatt den ONTAP System Manager oder die ONTAP CLI verwenden zu müssen. Die Option „Verwaltungsaktionen“ bietet Korrekturen für eine Reihe von ONTAP Problemen, die Unified Manager-Ereignisse ausgelöst haben.

Sie können Probleme direkt auf der Seite „Verwaltungsaktionen“ beheben, indem Sie im linken Navigationsbereich die Option **Verwaltungsaktionen** auswählen. Verwaltungsaktionen sind auch im Bereich „Verwaltungsaktionen“ auf dem Dashboard, auf der Seite mit den Ereignisdetails und in der Auswahl „Arbeitslastanalyse“ im linken Navigationsmenü verfügbar.

Es gibt bestimmte Probleme, die Unified Manager gründlich diagnostizieren und eine einzige Lösung bereitstellen kann. Für bestimmte ONTAP Funktionen, wie z. B. die Anti-Ransomware-Überwachung, führt Unified Manager interne Prüfungen durch und empfiehlt bestimmte Maßnahmen. Sofern verfügbar, werden diese Lösungen in den Verwaltungsaktionen mit der Schaltfläche **Fix It** angezeigt. Klicken Sie auf die Schaltfläche **Fix It**, um das Problem zu beheben. Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Unified Manager sendet ONTAP -Befehle an den Cluster, um die angeforderte Korrektur vorzunehmen. Wenn die Korrektur abgeschlossen ist, ist das Ereignis veraltet.

Einige Verwaltungsaktionen ermöglichen es Ihnen, dasselbe Problem auf mehreren Speicherobjekten mithilfe der Schaltfläche **Alles beheben** zu beheben. Beispielsweise kann es bei 5 Volumes das Ereignis „Volume-Speicherplatz voll“ geben, das durch Klicken auf die Verwaltungsaktion **Alles beheben** für „Volume-Autovergrößerung aktivieren“ behoben werden könnte. Mit einem Klick können Sie dieses Problem auf 5 Volumes beheben.

Informationen zu den ONTAP -Problemen und -Funktionen, die Sie mithilfe der automatischen Behebung verwalten können, finden Sie unter ["Welche Probleme kann Unified Manager beheben?"](#) .

Welche Optionen habe ich, wenn ich die Schaltfläche „Fix It“ oder „Fix All“ sehe?

Auf der Seite „Verwaltungsaktionen“ können Sie mit der Schaltfläche **Beheben** oder **Alles beheben** Probleme beheben, über die Unified Manager durch ein Ereignis benachrichtigt wurde.

Wir empfehlen Ihnen, bei Bedarf auf die Schaltflächen zu klicken, um ein Problem zu beheben. Wenn Sie jedoch nicht sicher sind, ob Sie das Problem wie von Unified Manager empfohlen beheben möchten, können Sie die folgenden Aktionen ausführen:

Was möchten Sie tun?	Aktion
Lassen Sie Unified Manager das Problem bei allen identifizierten Objekten beheben.	Klicken Sie auf die Schaltfläche Alles beheben .
Beheben Sie das Problem für keines der identifizierten Objekte zu diesem Zeitpunkt und verbergen Sie diese Verwaltungsaktion, bis das Ereignis erneut ausgelöst wird.	Klicken Sie auf den Abwärtspfeil und dann auf Alle verwerfen .
Beheben Sie das Problem nur bei einigen der identifizierten Objekte.	Klicken Sie auf den Namen der Verwaltungsaktion, um die Liste zu erweitern und alle einzelnen Fix It -Aktionen anzuzeigen. Folgen Sie dann den Schritten zum Beheben oder Ablehnen einzelner Verwaltungsaktionen.

Was möchten Sie tun?	Aktion
Lassen Sie das Problem von Unified Manager beheben.	Klicken Sie auf die Schaltfläche Fix It .

Was möchten Sie tun?	Aktion
Beheben Sie das Problem zu diesem Zeitpunkt nicht und verbergen Sie diese Verwaltungsaktion, bis das Ereignis erneut ausgelöst wird.	Klicken Sie auf den Abwärtspfeil und dann auf Verwerfen .
Zeigen Sie die Details zu diesem Ereignis an, damit Sie das Problem besser verstehen.	• Klicken Sie auf die Schaltfläche Fix It und überprüfen Sie die Korrektur, die im daraufhin angezeigten Dialogfeld angewendet wird. • Klicken Sie auf den Abwärtspfeil und dann auf Ereignisdetails anzeigen, um die Seite mit den Ereignisdetails anzuzeigen. Klicken Sie dann auf einer der resultierenden Seiten auf Beheben, wenn Sie das Problem beheben möchten.
Zeigen Sie die Details zu diesem Speicherobjekt an, damit Sie das Problem besser verstehen.	Klicken Sie auf den Namen des Speicherobjekts, um Details entweder im Leistungs-Explorer oder auf der Seite „Integritätsdetails“ anzuzeigen.

In einigen Fällen wird die Korrektur in der nächsten 15-minütigen Konfigurationsumfrage angezeigt. In anderen Fällen kann es mehrere Stunden dauern, bis die Konfigurationsänderung verifiziert und das Ereignis verworfen ist.

Um die Liste der abgeschlossenen oder laufenden Verwaltungsaktionen anzuzeigen, klicken Sie auf das Filtersymbol und wählen Sie **Abgeschlossen** oder **In Bearbeitung**.

Fix: Alle Vorgänge werden seriell ausgeführt. Wenn Sie also das Fenster „In Bearbeitung“ anzeigen, haben einige Objekte den Status „In Bearbeitung“, während andere den Status „Geplant“ haben. Dies bedeutet, dass sie noch auf ihre Implementierung warten.

Zeigen Sie den Status der Verwaltungsaktionen an, die Sie beheben möchten

Sie können den Status aller Verwaltungsaktionen, die Sie zur Behebung ausgewählt haben, auf der Seite „Verwaltungsaktionen“ anzeigen. Die meisten Aktionen werden ziemlich schnell als **Abgeschlossen** angezeigt, nachdem Unified Manager den ONTAP-Befehl an den Cluster gesendet hat. Einige Aktionen, beispielsweise das Verschieben eines Volumes, können jedoch länger dauern.

Auf der Seite „Verwaltungsaktionen“ stehen drei Filter zur Verfügung:

- **Abgeschlossen** zeigt sowohl erfolgreich abgeschlossene als auch fehlgeschlagene Verwaltungsaktionen an. **Fehlgeschlagene** Aktionen geben einen Grund für den Fehler an, sodass Sie das Problem manuell beheben können.
- **In Bearbeitung** zeigt sowohl die Verwaltungsmaßnahmen an, die gerade umgesetzt werden, als auch die, deren Umsetzung geplant ist.
- **Empfohlen** zeigt alle Verwaltungsaktionen an, die derzeit für alle überwachten Cluster aktiv sind.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Verwaltungsaktionen**. Alternativ klicken Sie auf  oben im Bereich **Verwaltungsaktionen** auf dem **Dashboard** und wählen Sie die Ansicht aus, die Sie anzeigen möchten.

Die Seite „Verwaltungsaktionen“ wird angezeigt.

2. Sie können auf das Caret-Symbol neben der Verwaltungsaktion im Feld **Beschreibung** klicken, um Details zum Problem und den Befehl anzuzeigen, der zum Beheben des Problems verwendet wird.
3. Um alle **fehlgeschlagenen** Aktionen anzuzeigen, sortieren Sie nach der Spalte **Status** in der Ansicht **Abgeschlossen**. Sie können das **Filter**-Tool für denselben Zweck verwenden.
4. Wenn Sie weitere Informationen zu einer fehlgeschlagenen Verwaltungsaktion anzeigen möchten oder wenn Sie eine empfohlene Verwaltungsaktion korrigieren möchten, können Sie im erweiterten Bereich auf **Ereignisdetails anzeigen** klicken, nachdem Sie auf das Caret-Symbol neben der Verwaltungsaktion geklickt haben. Auf dieser Seite ist eine Schaltfläche „Fix It“ verfügbar.

Welche Probleme kann Unified Manager beheben?

Mithilfe der automatischen Korrekturfunktion von Active IQ Unified Manager können Sie bestimmte ONTAP Probleme beheben oder bestimmte ONTAP Funktionen, wie z. B. die Anti-Ransomware-Überwachung, effektiv über Unified Manager verwalten.

Diese Tabelle beschreibt diese ONTAP Probleme oder -Funktionen, die Sie direkt über die Schaltfläche **Fix It** oder **Fix All** auf der Unified Manager-Web-Benutzeroberfläche verwalten können.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
Volume-Speicherplatz voll Der Speicherplatz des Datenträgers ist fast erschöpft und die Kapazitätsgrenze wurde überschritten. Dieser Schwellenwert ist standardmäßig auf 90 % der Volumegröße eingestellt.	Automatisches Volume-Vergrößern aktivieren	Unified Manager stellt fest, dass die automatische Volumevergrößerung für dieses Volume nicht konfiguriert ist, und aktiviert diese Funktion, damit die Kapazität des Volumes bei Bedarf vergrößert wird.
Inodes voll Dieses Volume hat keine Inodes mehr und kann keine neuen Dateien aufnehmen.	Erhöhen Sie die Anzahl der Inodes auf dem Volume	Erhöht die Anzahl der Inodes auf dem Volume um 2 Prozent.
Nichtübereinstimmung der Speicherebenenrichtlinie erkannt Das Volume enthält viele inaktive Daten und die aktuelle Tiering-Richtlinie ist auf „Nur Snapshot“ oder „Keine“ eingestellt.	Aktivieren Sie das automatische Cloud-Tiering	Da sich das Volume bereits auf einem FabricPool befindet, wird die Tiering-Richtlinie auf „Auto“ geändert, sodass inaktive Daten in die kostengünstigere Cloud-Stufe verschoben werden.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
Speicherebenen-Nichtübereinstimmung erkannt Das Volume enthält viele inaktive Daten, befindet sich jedoch nicht auf einer Cloud-fähigen Speicherebene (FabricPool).	Ändern der Speicherebene des Volumes	Verschiebt das Volume in die Cloud-fähige Speicherebene und setzt die Tiering-Richtlinie auf „Auto“, um inaktive Daten in die Cloud-Ebene zu verschieben.
Überwachungsprotokoll deaktiviert Das Überwachungsprotokoll ist für die Speicher-VM nicht aktiviert	Aktivieren Sie die Überwachungsprotokollierung für die Speicher-VM	Aktiviert die Audit-Protokollierung auf der Speicher-VM. Beachten Sie, dass für die Speicher-VM bereits ein lokaler oder Remote-Speicherort für das Überwachungsprotokoll konfiguriert sein muss.
Login-Banner deaktiviert Das Anmeldebanner für den Cluster sollte aktiviert werden, um die Sicherheit durch deutliche Kennzeichnung der Zugriffsbeschränkungen zu erhöhen.	Anmeldebanner für den Cluster festlegen	Setzt das Cluster-Anmeldebanner auf „Zugriff auf autorisierte Benutzer beschränkt“.
Login-Banner deaktiviert Das Anmeldebanner für die Speicher-VM sollte aktiviert werden, um die Sicherheit durch deutliche Kennzeichnung der Zugriffsbeschränkungen zu erhöhen.	Anmeldebanner für die Speicher-VM festlegen	Legt das Anmeldebanner der Speicher-VM auf „Zugriff auf autorisierte Benutzer beschränkt“ fest.
SSH verwendet unsichere Chiffren Chiffren mit dem Suffix „-cbc“ gelten als unsicher.	Entfernen Sie unsichere Chiffren aus dem Cluster	Entfernt die unsicheren Chiffren – wie z. B. aes192-cbc und aes128-cbc – aus dem Cluster.
SSH verwendet unsichere Chiffren Chiffren mit dem Suffix „-cbc“ gelten als unsicher.	Entfernen unsicherer Chiffren aus der Speicher-VM	Entfernt die unsicheren Chiffren – wie z. B. aes192-cbc und aes128-cbc – aus der Speicher-VM.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
AutoSupport HTTPS-Transport deaktiviert Das zum Senden von AutoSupport -Nachrichten an den technischen Support verwendete Transportprotokoll sollte verschlüsselt sein.	Legen Sie HTTPS als Transportprotokoll für AutoSupport -Nachrichten fest	Legt HTTPS als Transportprotokoll für AutoSupport -Nachrichten im Cluster fest.
Schwellenwert für Cluster-Lastungleichgewicht überschritten Zeigt an, dass die Last zwischen den Knoten im Cluster unausgewogen ist. Dieses Ereignis wird generiert, wenn die Abweichung der genutzten Leistungskapazität zwischen den Knoten mehr als 30 % beträgt.	Ausbalancieren der Cluster-Workloads	Unified Manager ermittelt das Volume, das sich am besten von einem Knoten zum anderen verschieben lässt, um das Ungleichgewicht zu verringern, und verschiebt dann das Volume.
Schwellenwert für Cluster-Kapazitätsungleichgewicht überschritten Zeigt an, dass die Kapazität zwischen den Aggregaten im Cluster unausgewogen ist. Dieses Ereignis wird generiert, wenn die Abweichung der genutzten Kapazität zwischen Aggregaten mehr als 70 % beträgt.	Clusterkapazität ausgleichen	Unified Manager ermittelt das beste Volume zum Verschieben von einem Aggregat zu einem anderen, um das Ungleichgewicht zu reduzieren, und verschiebt dann das Volume.
Schwellenwert für genutzte Leistungskapazität überschritten Zeigt an, dass die Last auf dem Knoten überbeansprucht werden könnte, wenn Sie die Auslastung durch eine oder mehrere hochaktive Workloads nicht reduzieren. Dieses Ereignis wird generiert, wenn der Wert für die genutzte Knotenleistungskapazität länger als 12 Stunden über 100 % liegt.	Begrenzen Sie die hohe Belastung des Knotens	Unified Manager identifiziert das Volume mit den höchsten IOPS und wendet eine QoS-Richtlinie an, die die erwarteten und maximalen IOPS-Werte des Verlaufs verwendet, um die Belastung des Knotens zu reduzieren.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
Warnschwelle für dynamische Ereignisse überschritten Zeigt an, dass der Knoten aufgrund der ungewöhnlich hohen Belastung einiger Workloads bereits in einem überlasteten Zustand arbeitet.	Reduzieren Sie die Überlastung im Knoten	Unified Manager identifiziert das Volume mit den höchsten IOPS und wendet eine QoS-Richtlinie an, die die erwarteten und maximalen IOPS-Werte des Verlaufs verwendet, um die Belastung des Knotens zu reduzieren.
Übernahme nicht möglich Failover ist derzeit deaktiviert, sodass der Zugriff auf die Ressourcen des Knotens während eines Ausfalls oder Neustarts verloren geht, bis der Knoten wieder verfügbar ist.	Knoten-Failover aktivieren	Unified Manager sendet den entsprechenden Befehl, um das Failover auf allen Knoten im Cluster zu aktivieren.
Option Cf.takeover.on_panic ist deaktiviert Die Node-Shell-Option „cf.takeover.on_panic“ ist auf Aus gesetzt, was auf HA-konfigurierten Systemen zu einem Problem führen könnte.	Übernahme bei Panik aktivieren	Unified Manager sendet den entsprechenden Befehl an den Cluster, um diese Einstellung auf Ein zu ändern.
Deaktivieren Sie die NodeShell-Option snapmirror.enable Die alte NodeShell-Option „snapmirror.enable“ ist auf on eingestellt, was nach dem Upgrade auf ONTAP 9.3 oder höher zu Problemen beim Booten führen kann.	Setzen Sie die Option snapmirror.enable auf „Aus“	Unified Manager sendet den entsprechenden Befehl an den Cluster, um diese Einstellung auf Aus zu ändern.
Telnet aktiviert Weist auf ein potenzielles Sicherheitsproblem hin, da Telnet unsicher ist und Daten unverschlüsselt überträgt.	Telnet deaktivieren	Unified Manager sendet den entsprechenden Befehl an den Cluster, um Telnet zu deaktivieren.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
Konfigurieren des Anti-Ransomware-Lernens für Speicher-VMs Überprüft regelmäßig, ob Cluster mit Lizenzen für die Anti-Ransomware-Überwachung vorhanden sind. Überprüft, ob eine Speicher-VM in einem solchen Cluster nur NFS- oder SMB-Volumes unterstützt.	Platzieren Sie Speicher-VMs in einem <code>learning</code> Modus der Anti-Ransomware-Überwachung	Unified Manager setzt Anti-Ransomware-Überwachung auf <code>learning</code> Status für die Speicher-VMs über die Cluster-Verwaltungskonsole. Die Anti-Ransomware-Überwachung aller neuen Volumes, die auf der Speicher-VM erstellt werden, wird automatisch in einen Lernmodus versetzt. Durch diese Aktivierung kann ONTAP das Aktivitätsmuster auf den Volumes erlernen und Anomalien aufgrund potenzieller böswilliger Angriffe erkennen.
Konfigurieren des Volume-Anti-Ransomware-Lernens Überprüft regelmäßig, ob Cluster mit Lizenzen für die Anti-Ransomware-Überwachung vorhanden sind. Überprüft, ob ein Volume in einem solchen Cluster nur NFS- oder SMB-Dienste unterstützt.	Legen Sie Bänder in <code>learning</code> Modus der Anti-Ransomware-Überwachung	Unified Manager setzt Anti-Ransomware-Überwachung auf <code>learning</code> Status für die Volumes über die Cluster-Verwaltungskonsole. Durch diese Aktivierung kann ONTAP das Aktivitätsmuster auf den Volumes erlernen und Anomalien aufgrund potenzieller böswilliger Angriffe erkennen.
Aktivieren Sie den Volume-Anti-Ransomware Überprüft regelmäßig, ob Cluster mit Lizenzen für die Anti-Ransomware-Überwachung vorhanden sind. Erkennt, ob die Volumes im <code>learning</code> Modus der Anti-Ransomware-Überwachung für mehr als 45 Tage und ermittelt die Aussicht, sie in den aktiven Modus zu versetzen.	Legen Sie Bänder in <code>active</code> Modus der Anti-Ransomware-Überwachung	Unified Manager setzt Anti-Ransomware-Überwachung auf <code>active</code> auf den Volumes über die Cluster-Verwaltungskonsole. Durch diese Aktivierung kann ONTAP das Aktivitätsmuster auf den Volumes erlernen, Anomalien aufgrund potenzieller böswilliger Angriffe erkennen und Warnmeldungen für Datenschutzmaßnahmen erstellen.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
Volume-Anti-Ransomware deaktivieren Überprüft regelmäßig, ob Cluster mit Lizenzen für die Anti-Ransomware-Überwachung vorhanden sind. Erkennt wiederholte Benachrichtigungen während der aktiven Anti-Ransomware-Überwachung auf den Volumes (z. B. werden über einen Zeitraum von 30 Tagen mehrere Warnungen vor potenziellen Ransomware-Angriffen zurückgegeben).	Deaktivieren Sie die Anti-Ransomware-Überwachung auf Volumes	Unified Manager deaktiviert die Anti-Ransomware-Überwachung auf den Volumes über die Cluster-Verwaltungskonsolle.

Überschreiben von Verwaltungsaktionen durch Skripte

Sie können benutzerdefinierte Skripte erstellen und sie mit Warnungen verknüpfen, um bei bestimmten Ereignissen bestimmte Aktionen auszuführen, und müssen sich nicht für die standardmäßigen Verwaltungsaktionen entscheiden, die auf der Seite „Verwaltungsaktionen“ oder im Unified Manager-Dashboard dafür verfügbar sind.

Wenn Sie bestimmte Aktionen für einen Ereignistyp ausführen möchten und diese nicht als Teil der von Unified Manager bereitgestellten Verwaltungsaktionsfunktion beheben möchten, können Sie ein benutzerdefiniertes Skript für die bestimmte Aktion konfigurieren. Sie können das Skript dann mit einer Warnung für diesen Ereignistyp verknüpfen und sich einzeln um solche Ereignisse kümmern. In diesem Fall werden für diesen bestimmten Ereignistyp keine Verwaltungsaktionen auf der Seite „Verwaltungsaktionen“ oder im Unified Manager-Dashboard generiert.

Verwalten von Clustern

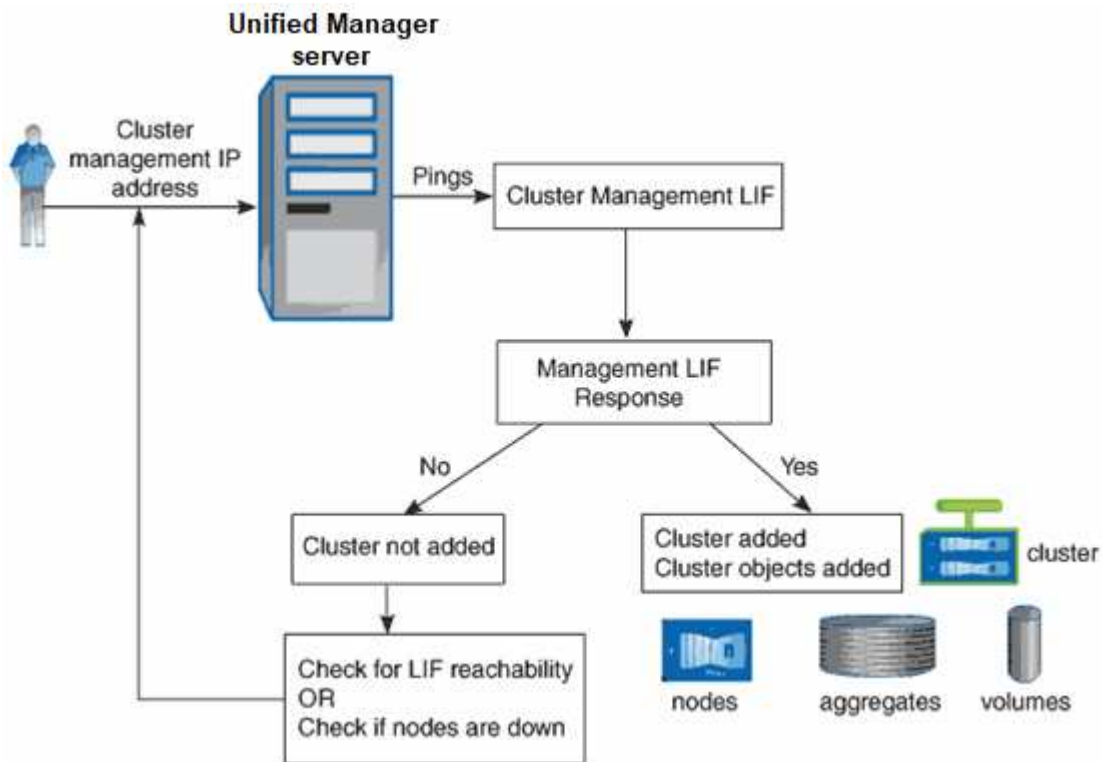
Sie können die ONTAP Cluster verwalten, indem Sie Unified Manager zum Überwachen, Hinzufügen, Bearbeiten und Entfernen von Clustern verwenden.

So funktioniert der Cluster-Erkennungsprozess

Nachdem Sie Unified Manager einen Cluster hinzugefügt haben, erkennt der Server die Clusterobjekte und fügt sie seiner Datenbank hinzu. Wenn Sie verstehen, wie der Erkennungsprozess funktioniert, können Sie die Cluster und deren Objekte Ihrer Organisation besser verwalten.

Das Überwachungsintervall zum Sammeln von Clusterkonfigurationsinformationen beträgt 15 Minuten. Nachdem Sie beispielsweise einen Cluster hinzugefügt haben, dauert es 15 Minuten, bis die Clusterobjekte in der Unified Manager-Benutzeroberfläche angezeigt werden. Dieser Zeitrahmen gilt auch für Änderungen an einem Cluster. Wenn Sie beispielsweise einem SVM in einem Cluster zwei neue Volumes hinzufügen, werden Ihnen diese neuen Objekte nach dem nächsten Abfrageintervall, das bis zu 15 Minuten dauern kann, in der Benutzeroberfläche angezeigt.

Das folgende Bild veranschaulicht den Erkennungsprozess:



Nachdem alle Objekte für einen neuen Cluster erkannt wurden, beginnt Unified Manager mit der Erfassung historischer Leistungsdaten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Datenkontinuitätserfassung erfasst. Mit dieser Funktion erhalten Sie unmittelbar nach dem Hinzufügen eines Clusters Leistungsinformationen für mehr als zwei Wochen. Nachdem der Datenkontinuitätserfassungszyklus abgeschlossen ist, werden standardmäßig alle fünf Minuten Echtzeitdaten zur Clusterleistung erfasst.



Da die Erfassung von 15 Tagen Leistungsdaten CPU-intensiv ist, wird empfohlen, das Hinzufügen neuer Cluster zu staffeln, damit Abfragen zur Datenkontinuitätserfassung nicht auf zu vielen Clustern gleichzeitig ausgeführt werden.

Liste der überwachten Cluster anzeigen

Auf der Seite „Cluster-Setup“ können Sie Ihren Clusterbestand anzeigen. Sie können Details zu den Clustern anzeigen, beispielsweise deren Namen oder IP-Adresse und Kommunikationsstatus.

Bevor Sie beginnen

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

Schritt

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung > Cluster-Setup**.

Alle von Unified Manager verwalteten Cluster in Ihrer Speicherumgebung werden angezeigt. Die Liste der Cluster ist nach der Spalte mit dem Schweregrad des Erfassungsstatus sortiert. Sie können auf eine Spaltenüberschrift klicken, um die Cluster nach verschiedenen Spalten zu sortieren.

Cluster hinzufügen

Sie können Active IQ Unified Manager einen Cluster hinzufügen, damit Sie den Cluster überwachen können. Dazu gehört die Möglichkeit, Clusterinformationen wie Zustand, Kapazität, Leistung und Konfiguration des Clusters abzurufen, sodass Sie eventuell auftretende Probleme finden und beheben können.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen über die folgenden Informationen verfügen:
 - Unified Manager unterstützt lokale ONTAP -Cluster, ONTAP Select und Cloud Volumes ONTAP.
 - Sie müssen über den Hostnamen oder die Cluster-Verwaltungs-IP-Adresse (IPv4 oder IPv6) für den Cluster verfügen.

Bei Verwendung des Hostnamens muss dieser in die Cluster-Management-IP-Adresse für das Cluster-Management-LIF aufgelöst werden. Wenn Sie ein Knotenverwaltungs-LIF verwenden, schlägt der Vorgang fehl.

- Sie müssen über den Benutzernamen und das Kennwort verfügen, um auf den Cluster zugreifen zu können.

Dieses Konto muss über die Rolle *admin* verfügen und der Anwendungszugriff muss auf *ontapi*, *console* und *http* eingestellt sein.

- Sie müssen die Portnummer kennen, um über das HTTPS-Protokoll eine Verbindung zum Cluster herzustellen (normalerweise Port 443).
- Auf dem Cluster muss die ONTAP Softwareversion 9.9 oder höher ausgeführt werden.
- Sie müssen über ausreichend Speicherplatz auf dem Unified Manager-Server verfügen. Sie können dem Server keinen Cluster hinzufügen, wenn bereits mehr als 90 % des Speicherplatzes belegt sind.
- Sie verfügen über die erforderlichen Zertifikate:

SSL (HTTPS)-Zertifikat: Dieses Zertifikat ist Eigentum von Unified Manager. Bei einer Neuinstallation von Unified Manager wird ein standardmäßiges selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt, zur besseren Sicherheit ein Upgrade auf ein CA-signiertes Zertifikat durchzuführen. Wenn das Serverzertifikat abläuft, sollten Sie es neu generieren und Unified Manager neu starten, damit die Dienste das neue Zertifikat integrieren. Weitere Informationen zum Neugenerieren von SSL-Zertifikaten finden Sie unter ["Generieren eines HTTPS-Sicherheitszertifikats"](#).

EMS-Zertifikat: Dieses Zertifikat ist Eigentum von Unified Manager. Es wird während der Authentifizierung für von ONTAP empfangene EMS-Benachrichtigungen verwendet.

Zertifikate für gegenseitige TLS-Kommunikation: Wird während der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatsbasierte Authentifizierung ist für einen Cluster basierend auf der ONTAP -Version aktiviert. Wenn auf dem Cluster eine niedrigere ONTAP Version als 9.5 ausgeführt wird, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

Die zertifikatbasierte Authentifizierung wird für einen Cluster nicht automatisch aktiviert, wenn Sie eine ältere Version von Unified Manager aktualisieren. Sie können es jedoch aktivieren, indem Sie die Clusterdetails ändern und speichern. Wenn das Zertifikat abläuft, sollten Sie es neu generieren, um das neue Zertifikat zu integrieren. Weitere Informationen zum Anzeigen und Neugenerieren des

Zertifikats finden Sie unter "[Cluster bearbeiten](#)".



- Sie können einen Cluster über die Web-Benutzeroberfläche hinzufügen und die zertifikatbasierte Authentifizierung wird automatisch aktiviert.
- Sie können einen Cluster über die Unified Manager CLI hinzufügen. Die zertifikatbasierte Authentifizierung ist standardmäßig nicht aktiviert. Wenn Sie einen Cluster mithilfe der Unified Manager-CLI hinzufügen, müssen Sie den Cluster mithilfe der Unified Manager-Benutzeroberfläche bearbeiten. Sie können sehen "[Unterstützte Unified Manager CLI-Befehle](#)" um einen Cluster mithilfe der Unified Manager CLI hinzuzufügen.
- Wenn die zertifikatbasierte Authentifizierung für einen Cluster aktiviert ist und Sie die Sicherung von Unified Manager von einem Server nehmen und auf einem anderen Unified Manager-Server wiederherstellen, auf dem der Hostname oder die IP-Adresse geändert wurde, kann die Überwachung des Clusters fehlschlagen. Um den Fehler zu vermeiden, bearbeiten und speichern Sie die Clusterdetails. Weitere Informationen zum Bearbeiten von Clusterdetails finden Sie unter "[Cluster bearbeiten](#)".
- Auf Clusterebene fügt die Active IQ Schnittstelle zwei neue Benutzergruppeneinträge für die Authentifizierungsmethode „cert“ hinzu.

+ **Cluster-Zertifikate:** Dieses Zertifikat ist Eigentum von ONTAP. Sie können Unified Manager keinen Cluster mit einem abgelaufenen Zertifikat hinzufügen. Wenn das Zertifikat bereits abgelaufen ist, sollten Sie es vor dem Hinzufügen des Clusters neu generieren. Informationen zur Zertifikatsgenerierung finden Sie im Knowledge Base-Artikel (KB). "[So erneuern Sie ein selbstsigniertes ONTAP -Zertifikat in der System Manager-Benutzeroberfläche](#)".

- Eine einzelne Instanz von Unified Manager kann eine bestimmte Anzahl von Knoten unterstützen. Wenn Sie eine Umgebung überwachen müssen, die die unterstützte Knotenanzahl überschreitet, müssen Sie eine zusätzliche Instanz von Unified Manager installieren, um einige der Cluster zu überwachen. Eine Liste der unterstützten Knotenanzahl finden Sie im "[Leitfaden zu Best Practices für Unified Manager](#)".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung > Cluster-Setup**.
2. Klicken Sie auf der Seite „Cluster-Setup“ auf **Hinzufügen**.
3. Geben Sie im Dialogfeld „Cluster hinzufügen“ die erforderlichen Werte an und klicken Sie dann auf **Senden**.
4. Klicken Sie im Dialogfeld „Host autorisieren“ auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.
5. Klicken Sie auf **Ja**.

Nachdem Sie die Clusterdetails gespeichert haben, können Sie das Zertifikat für die gegenseitige TLS-Kommunikation für einen Cluster sehen.

Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, überprüft Unified Manager das Zertifikat nur, wenn der Cluster zum ersten Mal hinzugefügt wird. Unified Manager überprüft das Zertifikat nicht bei jedem API-Aufruf an ONTAP.

Nachdem alle Objekte für einen neuen Cluster erkannt wurden, beginnt Unified Manager mit der Erfassung historischer Leistungsdaten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Datenkontinuitätserfassung erfasst. Mit dieser Funktion erhalten Sie unmittelbar nach dem Hinzufügen eines Clusters Leistungsdaten für mehr als zwei Wochen. Nachdem der Datenkontinuitätserfassungszyklus

abgeschlossen ist, werden standardmäßig alle fünf Minuten Echtzeitdaten zur Clusterleistung erfasst.



- Die Erfassung von Leistungsdaten für 15 Tage ist CPU-intensiv. NetApp empfiehlt, das Hinzufügen neuer Cluster zeitlich zu staffeln, damit die Abfragen zur Datenkontinuitätserfassung nicht auf zu vielen Clustern gleichzeitig ausgeführt werden. Wenn Sie Unified Manager während des Datenkontinuitätserfassungszeitraums neu starten, wird die Erfassung angehalten und Sie sehen Lücken in den Leistungsdiagrammen für den fehlenden Zeitraum.
- Wenn Sie einen ONTAP Cluster mit Version 9.14.1 oder höher hinzufügen, erfolgt die Kommunikation über die Cloud-Agent-Funktion. ONTAP erstellt automatisch einen internen Servicekontob Benutzer mit schreibgeschützten Berechtigungen (z. B. `clus-agent-xxxx`). Unified Manager stoppt die Datenerfassung aus diesen Clustern, wenn `clus-agent` Benutzer wird gelöscht.

Wenn Sie eine Fehlermeldung erhalten, dass Sie den Cluster nicht hinzufügen können, überprüfen Sie, ob die folgenden Probleme vorliegen:



- Wenn die Uhren auf den beiden Systemen nicht synchronisiert sind und das Startdatum des Unified Manager-HTTPS-Zertifikats nach dem Datum auf dem Cluster liegt. Sie müssen sicherstellen, dass die Uhren über NTP oder einen ähnlichen Dienst synchronisiert werden.
- Wenn der Cluster die maximale Anzahl an EMS-Benachrichtigungszielen erreicht hat, kann die Unified Manager-Adresse nicht hinzugefügt werden. Standardmäßig können auf dem Cluster nur 20 EMS-Benachrichtigungsziele definiert werden.

Verwandte Informationen

["Benutzer hinzufügen"](#)

["Anzeigen der Clusterliste und Details"](#)

["Installieren eines von einer Zertifizierungsstelle signierten und zurückgegebenen HTTPS-Zertifikats"](#)

Cluster bearbeiten

Sie können die Einstellungen eines vorhandenen Clusters, wie etwa Hostname oder IP-Adresse, Benutzername, Kennwort und Port, mithilfe des Dialogfelds „Cluster bearbeiten“ ändern.

Bevor Sie beginnen

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



Ab Unified Manager 9.7 können Cluster nur noch über HTTPS hinzugefügt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung > Cluster-Setup**.
2. Wählen Sie auf der Seite **Cluster-Setup** den Cluster aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Cluster bearbeiten** die Werte nach Bedarf. + Wenn Sie die Details für einen zu Unified Manager hinzugefügten Cluster geändert haben, können Sie die Zertifikatsdetails für die gegenseitige TLS-Kommunikation basierend auf der ONTAP Version anzeigen. Weitere Informationen zur

ONTAP -Version finden Sie unter ["Zertifikate für die gegenseitige TLS-Kommunikation"](#) . + Sie können die Zertifikatsdetails anzeigen, indem Sie auf **Zertifikatsdetails** klicken. Wenn das Zertifikat abgelaufen ist, klicken Sie auf die Schaltfläche **Neu generieren**, um das neue Zertifikat einzubinden.

4. Klicken Sie auf **Senden**.
5. Klicken Sie im Dialogfeld „Host autorisieren“ auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.
6. Klicken Sie auf **Ja**.

Verwandte Informationen

["Benutzer hinzufügen"](#)

["Anzeigen der Clusterliste und Details"](#)

Cluster entfernen

Sie können einen Cluster über die Seite „Cluster-Setup“ aus Unified Manager entfernen. Sie können beispielsweise einen Cluster entfernen, wenn die Clustererkennung fehlschlägt oder wenn Sie ein Speichersystem außer Betrieb nehmen möchten.

Bevor Sie beginnen

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

Diese Aufgabe entfernt den ausgewählten Cluster aus Unified Manager. Nachdem ein Cluster entfernt wurde, wird er nicht mehr überwacht. Die beim entfernten Cluster registrierte Instanz von Unified Manager wird ebenfalls vom Cluster abgemeldet.

Durch das Entfernen eines Clusters werden auch alle zugehörigen Speicherobjekte, Verlaufsdaten, Speicherdienste und alle zugehörigen Ereignisse aus Unified Manager gelöscht. Diese Änderungen werden nach dem nächsten Datenerfassungszyklus auf den Inventarseiten und den Detailseiten angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung > Cluster-Setup**.
2. Wählen Sie auf der Seite „Cluster-Setup“ den Cluster aus, den Sie entfernen möchten, und klicken Sie auf **Entfernen**.
3. Klicken Sie im Meldungsdialogfeld **Datenquelle entfernen** auf **Entfernen**, um die Entfernanforderung zu bestätigen.

Verwandte Informationen

["Benutzer hinzufügen"](#)

["Anzeigen der Clusterliste und Details"](#)

Cluster neu entdecken

Sie können einen Cluster manuell über die Seite „Cluster-Setup“ erneut erkennen, um die neuesten Informationen zum Zustand, Überwachungsstatus und Leistungsstatus des Clusters zu erhalten.

Sie können einen Cluster manuell erneut erkennen, wenn Sie ihn aktualisieren möchten – etwa durch Erhöhen

der Größe eines Aggregats, wenn nicht genügend Speicherplatz vorhanden ist – und Unified Manager die von Ihnen vorgenommenen Änderungen erkennen soll.

Wenn Unified Manager mit OnCommand Workflow Automation (WFA) gekoppelt wird, löst die Kopplung die erneute Erfassung der von WFA zwischengespeicherten Daten aus.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung > Cluster-Setup**.
2. Klicken Sie auf der Seite **Cluster-Setup** auf **Neu erkennen**.

Unified Manager erkennt den ausgewählten Cluster erneut und zeigt den neuesten Integritäts- und Leistungsstatus an.

Verwandte Informationen

["Anzeigen der Clusterliste und Details"](#)

Überwachen Sie die virtuelle VMware-Infrastruktur

Active IQ Unified Manager bietet Einblick in die virtuellen Maschinen (VMs) in Ihrer virtuellen Infrastruktur und ermöglicht die Überwachung und Fehlerbehebung bei Speicher- und Leistungsproblemen in Ihrer virtuellen Umgebung. Sie können diese Funktion verwenden, um Latenzprobleme in Ihrer Speicherumgebung zu ermitteln oder wenn ein Leistungsereignis auf Ihrem vCenter Server gemeldet wird.

Eine typische Bereitstellung einer virtuellen Infrastruktur auf ONTAP umfasst verschiedene Komponenten, die über die Rechen-, Netzwerk- und Speicherebenen verteilt sind. Leistungsverzögerungen in einer VM-Anwendung können durch eine Kombination von Latenzen entstehen, denen die verschiedenen Komponenten auf den jeweiligen Ebenen ausgesetzt sind. Diese Funktion ist nützlich für Speicher- und vCenter Server-Administratoren und IT-Generalisten, die ein Leistungsproblem in einer virtuellen Umgebung analysieren und herausfinden müssen, in welcher Komponente das Problem aufgetreten ist.

Sie können jetzt über das vCenter-Menü des VMware-Bereichs auf den vCenter-Server zugreifen. Die Vorschau jeder aufgelisteten virtuellen Maschine verfügt über den Link **VCENTER SERVER** in der TOPOLOGIE-ANSICHT, der den vCenter Server in einem neuen Browser startet. Sie können auch die Schaltfläche **Topologie erweitern** verwenden, um den vCenter Server zu starten, und auf die Schaltfläche **In vCenter anzeigen** klicken, um die Datenspeicher im vCenter Server anzuzeigen.

Unified Manager stellt das zugrunde liegende Subsystem einer virtuellen Umgebung in einer topologischen Ansicht dar, um festzustellen, ob im Rechenknoten, Netzwerk oder Speicher ein Latenzproblem aufgetreten ist. Die Ansicht hebt außerdem das spezifische Objekt hervor, das die Leistungsverzögerung verursacht, damit Abhilfemaßnahmen ergriffen und das zugrunde liegende Problem behoben werden kann.

Eine auf ONTAP -Speicher bereitgestellte virtuelle Infrastruktur umfasst die folgenden Objekte:

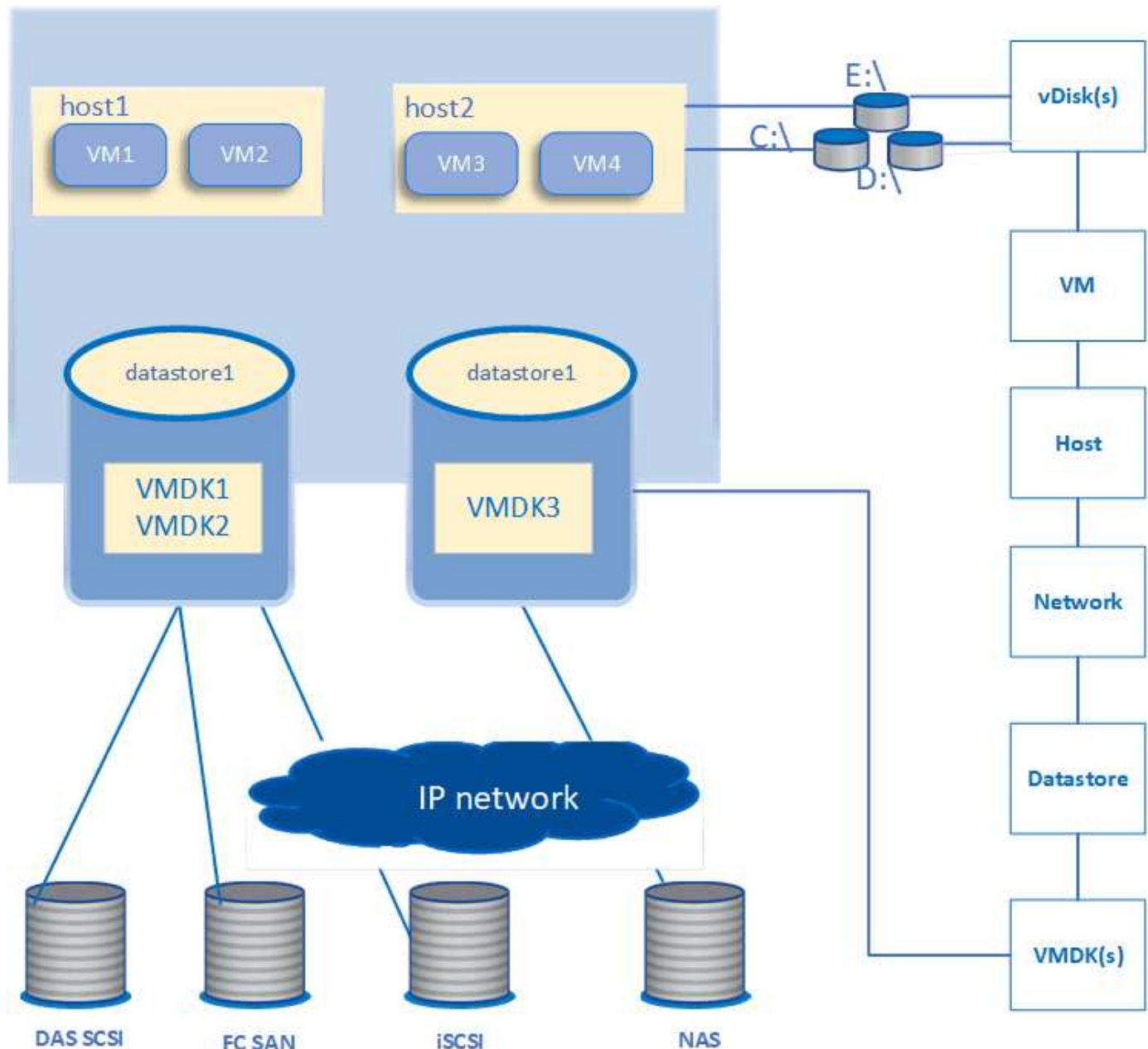
- vCenter Server: Eine zentrale Steuerungsebene zum Verwalten der VMware-VMs, ESXi-Hosts und aller zugehörigen Komponenten in einer virtuellen Umgebung. Weitere Informationen zu vCenter Server finden Sie in der VMware-Dokumentation.
- Host: Ein physisches oder virtuelles System, auf dem ESXi, die Virtualisierungssoftware von VMware, ausgeführt wird und das die VM hostet.
- Datenspeicher: Datenspeicher sind virtuelle Speicherobjekte, die mit den ESXi-Hosts verbunden sind.

Datenspeicher sind verwaltbare Speichereinheiten von ONTAP, wie LUNs oder Volumes, die als Repository für VM-Dateien wie Protokolldateien, Skripts, Konfigurationsdateien und virtuelle Datenträger verwendet werden. Sie sind über eine SAN- oder IP-Netzwerkverbindung mit den Hosts in der Umgebung verbunden. Datenspeicher außerhalb von ONTAP, die vCenter Server zugeordnet sind, werden im Unified Manager nicht unterstützt oder angezeigt.

- VM: Eine virtuelle VMware-Maschine.
- Virtuelle Datenträger: Die virtuellen Datenträger auf den Datenspeichern der VMs, die die Erweiterung VMDK haben. Daten von einer virtuellen Festplatte werden auf der entsprechenden VMDK gespeichert.
- VMDK: Eine virtuelle Maschinenfestplatte im Datenspeicher, die Speicherplatz für virtuelle Festplatten bereitstellt. Für jede virtuelle Festplatte gibt es ein entsprechendes VMDK.

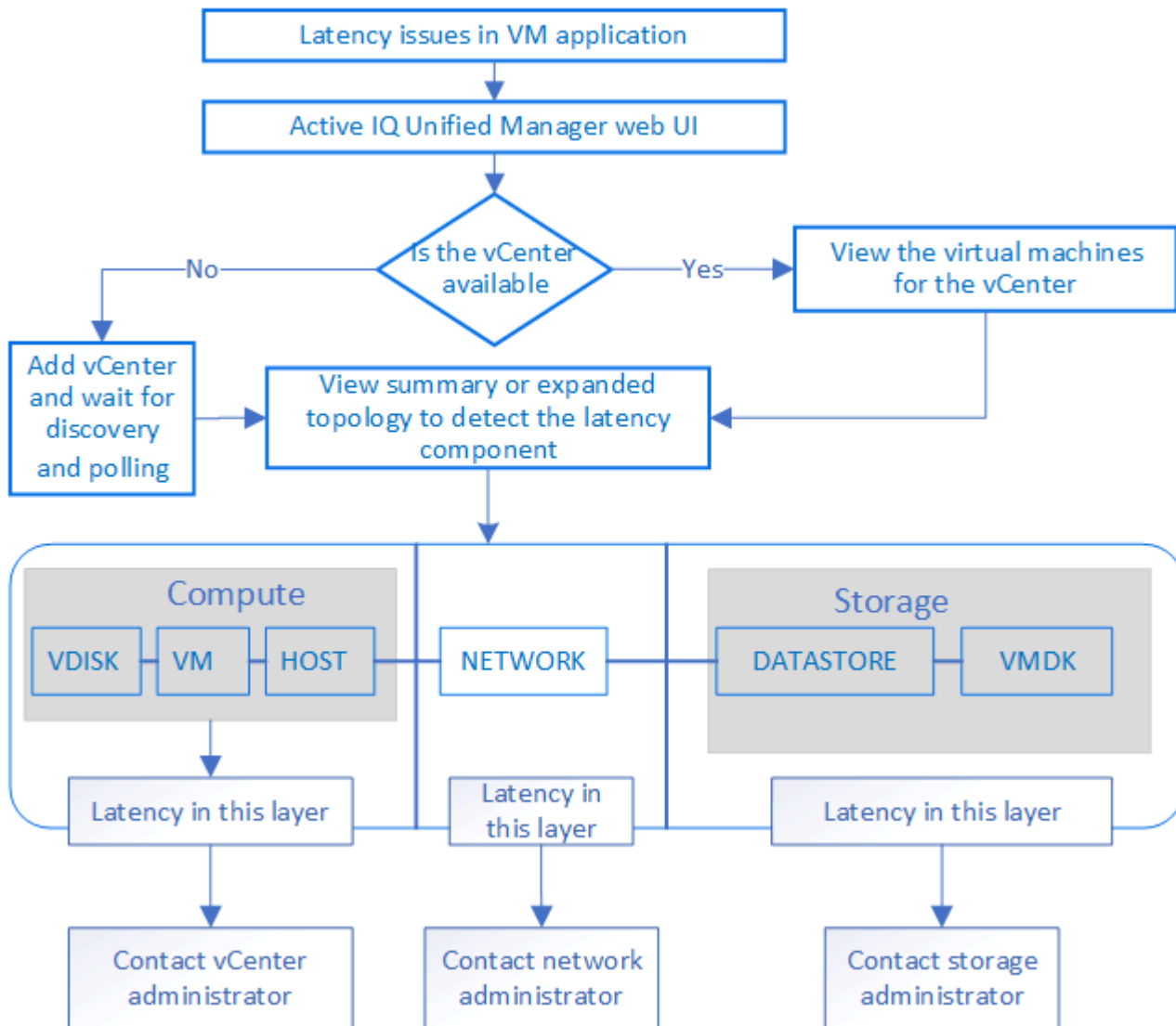
Diese Objekte werden in einer VM-Topologieansicht dargestellt.

VMware-Virtualisierung auf ONTAP



Benutzer-Workflow

Das folgende Diagramm zeigt einen typischen Anwendungsfall für die Verwendung der VM-Topologieansicht:



Was wird nicht unterstützt?

- Datenspeicher außerhalb von ONTAP, die den vCenter Server-Instanzen zugeordnet sind, werden von Unified Manager nicht unterstützt. VMs mit virtuellen Datenträgern auf diesen Datenspeichern werden ebenfalls nicht unterstützt.
- Ein Datenspeicher, der sich über mehrere LUNs erstreckt, wird nicht unterstützt.
- Datenspeicher, die Network Address Translation (NAT) zum Zuordnen von Daten-LIF (Zugriffsendpunkt) verwenden, werden nicht unterstützt.
- Das Exportieren von Volumes oder LUNs als Datenspeicher auf verschiedenen Clustern mit denselben IP-Adressen in einer Konfiguration mit mehreren LIFs wird nicht unterstützt, da Unified Manager nicht erkennen kann, welcher Datenspeicher zu welchem Cluster gehört.

Beispiel: Angenommen, Cluster A hat Datenspeicher A. Datenspeicher A wird über Daten-LIF mit derselben IP-Adresse xxxx exportiert und VM A wird auf diesem Datenspeicher erstellt. Ebenso hat Cluster B den Datenspeicher B. Der Datenspeicher B wird über Daten-LIF mit derselben IP-Adresse xxxx exportiert und VM B wird auf dem Datenspeicher B erstellt. UM kann weder den Datenspeicher A für die

Topologie von VM A dem entsprechenden ONTAP Volume/LUN zuordnen noch VM B zuordnen.

- Als Datenspeicher werden nur NAS- und SAN-Volumes (iSCSI und FCP für VMFS) unterstützt, virtuelle Volumes (vVols) werden nicht unterstützt.
- Es werden nur virtuelle iSCSI-Festplatten unterstützt. Virtuelle Festplatten vom Typ NVMe und SATA werden nicht unterstützt.
- Die Ansichten ermöglichen nicht die Erstellung von Berichten zur Analyse der Leistung der verschiedenen Komponenten.
- Für die Notfallwiederherstellung (DR) der Storage Virtual Machine (Storage VM), die nur für virtuelle Infrastrukturen auf Unified Manager unterstützt wird, muss die Konfiguration in vCenter Server manuell geändert werden, um in Switchover- und Switchback-Szenarien auf die aktiven LUNs zu verweisen. Ohne manuelles Eingreifen sind ihre Datenspeicher nicht mehr zugänglich.

Anzeigen und Hinzufügen von vCenter Server

Um die Leistung der virtuellen Maschinen (VMs) anzuzeigen und Fehler zu beheben, müssen die zugehörigen vCenter-Server zu Ihrer Active IQ Unified Manager Instanz hinzugefügt werden.

Bevor Sie beginnen

Stellen Sie vor dem Hinzufügen oder Anzeigen von vCenter-Servern Folgendes sicher:

- Sie kennen die Namen der vCenter-Server.
- Sie kennen die IP-Adresse des vCenter Servers und verfügen über die erforderlichen Anmeldeinformationen. Die Anmeldeinformationen müssen von einem vCenter Server-Administrator oder einem Root-Benutzer mit schreibgeschütztem Zugriff auf vCenter Server stammen.
- Auf dem vCenter Server, den Sie hinzufügen möchten, wird vSphere 6.5 oder höher ausgeführt.



Der Support von Unified Manager für VMware ESXi und vCenter Server ist in englischer und japanischer Sprache verfügbar.

- Die Datenerfassungseinstellung in vCenter Server ist auf die Statistikebene von *Level 3*, wodurch das erforderliche Maß an Metrikerfassung für alle überwachten Objekte sichergestellt wird. Die Intervalldauer sollte *5 minutes* und der Speicherzeitraum sollte *1 day*.

Weitere Informationen finden Sie im Abschnitt „Datenerfassungsebenen“ des vSphere-Überwachungs- und Leistungshandbuchs in der VMware-Dokumentation.

- Für eine erfolgreiche Berechnung der Latenzwerte werden die Latenzwerte im vCenter Server in Millisekunden und nicht in Mikrosekunden konfiguriert.
- Beim Hinzufügen des Datenspeichers zu vCenter Server können Sie sowohl die IP-Adresse des Hosts als auch den vollqualifizierten Domännennamen (FQDN) verwenden. Wenn Sie FQDN hinzufügen, stellen Sie sicher, dass der Domänenname vom Unified Manager-Server aufgelöst werden kann. Stellen Sie beispielsweise bei einer Linux-Installation sicher, dass der Domänenname in der `/etc/resolv.conf` Datei.
- Die aktuelle Uhrzeit des vCenter Servers ist mit der Zeitzone des vCenter Servers synchronisiert.
- vCenter Server ist für eine erfolgreiche Erkennung erreichbar.
- Sie haben Lesezugriff auf das VMware SDK, wenn Sie den vCenter Server zu Unified Manager hinzufügen. Dies ist für die Konfigurationsabfrage erforderlich.

Für jeden hinzugefügten und erkannten vCenter Server sammelt Unified Manager die Konfigurationsdaten, z. B. die vCenter Server- und ESXi-Serverdetails, die ONTAP Zuordnung, Datenspeicherdetails und die Anzahl der gehosteten VMs. Darüber hinaus werden die Leistungskennzahlen der Komponenten erfasst.

Schritte

1. Gehen Sie zu **VMWARE > vCenter** und prüfen Sie, ob Ihr vCenter Server in der Liste verfügbar ist.



Wenn Ihr vCenter Server nicht verfügbar ist, müssen Sie vCenter Server hinzufügen.

- a. Klicken Sie auf **Hinzufügen**.
- b. Fügen Sie die richtige IP-Adresse für vCenter Server hinzu und stellen Sie sicher, dass das Gerät erreichbar ist.
- c. Fügen Sie den Benutzernamen und das Kennwort des Administrators oder Root-Benutzers mit schreibgeschütztem Zugriff auf vCenter Server hinzu.
- d. Fügen Sie die benutzerdefinierte Portnummer hinzu, wenn Sie einen anderen Port als den Standardport 443 verwenden.
- e. Klicken Sie auf **Speichern**.

Nach erfolgreicher Erkennung wird Ihnen ein Serverzertifikat angezeigt, das Sie akzeptieren müssen.

Wenn Sie das Zertifikat akzeptieren, wird vCenter Server zur Liste der verfügbaren vCenter Server hinzugefügt. Das Hinzufügen des Geräts führt nicht zur Datenerfassung für die zugehörigen VMs und die Erfassung erfolgt in den geplanten Intervallen.

2. Wenn Ihr vCenter Server auf der Seite **vCenters** verfügbar ist, überprüfen Sie seinen Status, indem Sie mit der Maus über das Feld **Status** fahren, um anzuzeigen, ob Ihr vCenter Server wie erwartet funktioniert oder ob eine Warnung oder ein Fehler vorliegt.



Durch das Hinzufügen von vCenter Server können Sie die folgenden Status anzeigen. Es kann jedoch bis zu einer Stunde dauern, bis die Leistungs- und Latenzdaten der entsprechenden VMs nach dem Hinzufügen von vCenter Server korrekt wiedergegeben werden.

- Grün: „Normal“, was bedeutet, dass vCenter Server erkannt wurde und Leistungsmetriken erfolgreich erfasst wurden
 - Gelb: „Warnung“ (z. B. wenn die Statistikebene für vCenter Server nicht auf 3 oder höher eingestellt wurde, um Statistiken für jedes Objekt zu erhalten)
 - Orange: „Fehler“ (weist auf interne Fehler hin, z. B. Ausnahme, Fehler bei der Konfigurationsdatenerfassung oder Nichterreichbarkeit des vCenter-Servers). Sie können auf das Spaltenanzeigesymbol (**Einblenden/Ausblenden**) klicken, um die Statusmeldung für einen vCenter-Server-Status anzuzeigen und das Problem zu beheben.
3. Falls der vCenter-Server nicht erreichbar ist oder sich die Anmeldeinformationen geändert haben, bearbeiten Sie die vCenter-Serverdetails, indem Sie **vCenter > Bearbeiten** auswählen.
 4. Nehmen Sie die erforderlichen Änderungen auf der Seite **VMware vCenter Server bearbeiten** vor.
 5. Klicken Sie auf **Speichern**.

Die Datenerfassung auf vCenter Server beginnt

vCenter Server sammelt in Echtzeit 20-sekündige Leistungsdatenproben und fasst sie zu 5-Minuten-Proben

zusammen. Der Zeitplan für die Leistungsdatenerfassung von Unified Manager basiert auf den Standardeinstellungen von vCenter Server. Unified Manager verarbeitet die vom vCenter Server erhaltenen 5-Minuten-Beispiele und berechnet einen stündlichen Durchschnitt der IOPS und Latenz für die virtuellen Festplatten, VMs und Hosts. Für Datenspeicher berechnet Unified Manager einen stündlichen Durchschnitt der IOPS und Latenz aus von ONTAP erhaltenen Beispielen. Diese Werte stehen zu jeder vollen Stunde zur Verfügung. Die Leistungsmetriken sind nicht sofort nach dem Hinzufügen von vCenter Server verfügbar, sondern erst zu Beginn der nächsten Stunde. Die Abfrage der Leistungsdaten beginnt nach Abschluss eines Zyklus der Konfigurationsdatenerfassung.

Zum Abfragen von vCenter Server-Konfigurationsdaten folgt Unified Manager demselben Zeitplan wie zum Erfassen von Cluster-Konfigurationsdaten. Informationen zur Konfiguration von vCenter Server und zum Zeitplan für die Leistungsdatenerfassung finden Sie unter „Clusterkonfiguration und Aktivität zur Leistungsdatenerfassung“.

Verwandte Informationen

["Clusterkonfiguration und Leistungsdatenerfassungsaktivität"](#)

Entfernen von vCenter Server

Sie können vCenter-Server aus Ihrer Active IQ Unified Manager Instanz entfernen. Sie können beispielsweise einen vCenter Server entfernen, wenn die vCenter Server-Erkennung fehlschlägt oder wenn er nicht mehr benötigt wird.

Durch das Entfernen eines vCenter-Servers werden auch alle auf diesem vCenter gehosteten virtuellen Maschinen (VMs) und deren Konfigurationsdaten gelöscht. Nachdem der vCenter Server entfernt wurde, wird er zusammen mit den zugehörigen Objekten und Verlaufsdaten nicht mehr überwacht. Diese Änderungen werden auf den Inventarseiten von vCenter und virtuellen Maschinen angezeigt.

Bevor Sie beginnen

Stellen Sie vor dem Entfernen von vCenter-Servern Folgendes sicher:

- Sie verfügen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“.
- Sie sollten die Namen der vCenter-Server und die jeweiligen zugehörigen IP-Adressen kennen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **VMWARE>vCenter**.
2. Wählen Sie auf der vCenters-Seite den vCenter Server aus, den Sie entfernen möchten, und klicken Sie auf **Entfernen**.
3. Klicken Sie im Meldungsdialogfeld **vCenter entfernen** auf **OK**, um die Entfernungsanforderung zu bestätigen.

Überwachen virtueller Maschinen

Bei Latenzproblemen bei den Anwendungen der virtuellen Maschine (VM) müssen Sie möglicherweise die VMs überwachen, um die Ursache zu analysieren und zu beheben. Die VMs sind verfügbar, wenn ihr vCenter Server und die ONTAP Cluster, die den VM-Speicher hosten, zu Unified Manager hinzugefügt werden.

Die Details der VMs sehen Sie auf der Seite **VMWARE > > Virtuelle Maschinen**. Es werden Informationen wie Verfügbarkeit, Status, genutzte und zugewiesene Kapazität, Netzwerklatenz sowie IOPS und Latenz der VM,

des Datenspeichers und des Hosts angezeigt. Bei einer VM, die mehrere Datenspeicher unterstützt, zeigt das Raster die Metriken des Datenspeichers mit der schlechtesten Latenz an, wobei ein Sternchensymbol (*) zusätzliche Datenspeicher anzeigt. Wenn Sie auf das Symbol klicken, werden die Metriken des zusätzlichen Datenspeichers angezeigt. Einige dieser Spalten stehen zum Sortieren und Filtern nicht zur Verfügung.



Zum Anzeigen einer VM und ihrer Details muss die Erkennung (Polling oder Metrikerfassung) des ONTAP Clusters abgeschlossen sein. Wenn der Cluster aus Unified Manager entfernt wird, ist die VM nach dem nächsten Erkennungszyklus nicht mehr verfügbar.

Auf dieser Seite können Sie auch die detaillierte Topologie einer VM anzeigen und die Komponenten anzeigen, mit denen die VM verbunden ist, beispielsweise den Host, die virtuelle Festplatte und den damit verbundenen Datenspeicher. Die Topologieansicht zeigt die zugrunde liegenden Komponenten in ihren spezifischen Ebenen in der folgenden Reihenfolge an: **Virtuelle Festplatte > VM > Host > Netzwerk > Datenspeicher > VMDK**.

Sie können den E/A-Pfad und die Latenzen auf Komponentenebene aus topologischer Sicht bestimmen und feststellen, ob der Speicher die Ursache des Leistungsproblems ist. Die Übersichtsansicht der Topologie zeigt den E/A-Pfad an und hebt die Komponente mit IOPS- und Latenzproblemen hervor, damit Sie über die Schritte zur Fehlerbehebung entscheiden können. Sie können auch eine erweiterte Ansicht der Topologie erhalten, die jede Komponente separat zusammen mit der Latenz dieser Komponente darstellt. Sie können eine Komponente auswählen, um den durch die Ebenen hervorgehobenen E/A-Pfad zu bestimmen.

Anzeigen der Übersichtstopologie

So ermitteln Sie Leistungsprobleme, indem Sie die VMs in einer Übersichtstopologie anzeigen:

1. Gehen Sie zu **VMWARE > Virtuelle Maschinen**.
2. Suchen Sie nach Ihrer VM, indem Sie ihren Namen in das Suchfeld eingeben. Sie können Ihre Suchergebnisse auch nach bestimmten Kriterien filtern, indem Sie auf die Schaltfläche **Filter** klicken. Wenn Sie Ihre VM jedoch nicht finden können, stellen Sie sicher, dass der entsprechende vCenter Server hinzugefügt und erkannt wurde.



vCenter Server erlauben Sonderzeichen (wie %, &, *, \$, #, @, !, \, /, :, *, ?, ", <, >, |, ;, ') in den Namen von vSphere-Entitäten wie VM, Cluster, Datenspeicher, Ordner oder Datei. Der VMware vCenter Server und der ESX/ESXi-Server maskieren Sonderzeichen, die in den Anzeigenamen verwendet werden, nicht. Wenn der Name jedoch im Unified Manager verarbeitet wird, wird er anders angezeigt. Beispielsweise eine VM mit dem Namen %\$VC_AIQUM_clone_191124% in vCenter Server wird angezeigt als %25\$VC_AIQUM_clone_191124%25 im Unified Manager. Sie müssen dieses Problem beachten, wenn Sie eine VM abfragen, deren Name Sonderzeichen enthält.

3. Überprüfen Sie den Status der VM. Die VM-Status werden vom vCenter Server abgerufen. Die folgenden Status sind verfügbar. Weitere Informationen zu diesen Status finden Sie in der VMware-Dokumentation.
 - Normal
 - Warnung
 - Alarm
 - Nicht überwacht
 - Unbekannt
4. Klicken Sie auf den Abwärtspfeil neben der VM, um die Übersichtsansicht der Topologie der Komponenten auf den Compute-, Netzwerk- und Speicherebenen anzuzeigen. Der Knoten mit Latenzproblemen wird hervorgehoben. Die Übersichtsansicht zeigt die schlechteste Latenz der Komponenten. Wenn eine VM

beispielsweise über mehr als eine virtuelle Festplatte verfügt, wird in dieser Ansicht die virtuelle Festplatte mit der schlechtesten Latenz aller virtuellen Festplatten angezeigt.

5. Um die Latenz und den Durchsatz des Datenspeichers über einen bestimmten Zeitraum zu analysieren, klicken Sie auf die Schaltfläche **Workload Analyzer** über dem Symbol des Datenspeicherobjekts. Sie gelangen zur Seite „Workload-Analyse“, wo Sie einen Zeitraum auswählen und die Leistungsdiagramme des Datenspeichers anzeigen können. Weitere Informationen zum Workload-Analyzer finden Sie unter *Fehlerbehebung bei Workloads mit dem Workload-Analyzer*.

Erweiterte Topologie anzeigen

Sie können zu jeder Komponente einzeln einen Drilldown durchführen, indem Sie die erweiterte Topologie der VM anzeigen.

Schritte

1. Klicken Sie in der Übersichtsansicht der Topologie auf **Topologie erweitern**. Sie können die detaillierte Topologie jeder Komponente separat mit den Latenzzahlen für jedes Objekt anzeigen. Wenn in einer Kategorie mehrere Knoten vorhanden sind, beispielsweise mehrere Knoten im Datenspeicher oder VMDK, wird der Knoten mit der schlimmsten Latenz rot hervorgehoben.
2. Um den E/A-Pfad eines bestimmten Objekts zu überprüfen, klicken Sie auf das Objekt, um den E/A-Pfad und die entsprechende Zuordnung anzuzeigen. Um beispielsweise die Zuordnung einer virtuellen Festplatte anzuzeigen, klicken Sie auf die virtuelle Festplatte, um ihre hervorgehobene Zuordnung zum jeweiligen VMDK anzuzeigen. Im Falle einer Leistungsverzögerung dieser Komponenten können Sie weitere Daten von ONTAP sammeln und das Problem beheben.



Für VMDKs werden keine Metriken gemeldet. In der Topologie werden nur die VMDK-Namen und keine Metriken angezeigt.

Verwandte Informationen

["Fehlerbehebung bei Workloads mit dem Workload Analyzer"](#)

Anzeigen der virtuellen Infrastruktur in einem Disaster Recovery-Setup

Sie können die Konfigurations- und Leistungsmetriken der in einer MetroCluster -Konfiguration oder einem Disaster Recovery-Setup (SVM DR) einer Storage Virtual Machine (Storage VM) gehosteten Datenspeicher anzeigen.

Auf Unified Manager können Sie die NAS-Volumes oder LUNs in einer MetroCluster -Konfiguration anzeigen, die als Datenspeicher in vCenter Server angeschlossen sind. Die in einer MetroCluster -Konfiguration gehosteten Datenspeicher werden in derselben topologischen Ansicht dargestellt wie ein Datenspeicher in einer Standardumgebung.

Sie können auch die NAS-Volumes oder LUNs in einer Speicher-VM-Notfallwiederherstellungskonfiguration anzeigen, die den Datenspeichern in vCenter Server zugeordnet sind.

Anzeigen von Datenspeichern in der MetroCluster -Konfiguration

Beachten Sie die folgenden Voraussetzungen, bevor Sie Datenspeicher in einer MetroCluster -Konfiguration anzeigen:

- Im Falle eines Switchovers und Switchbacks sollte die Erkennung der primären und sekundären Cluster des HA-Paares und der vCenter-Server abgeschlossen sein.

- Die primären und sekundären Cluster des HA-Paares und die vCenter-Server müssen von Unified Manager verwaltet werden.
- Die erforderliche Einrichtung muss auf ONTAP und vCenter Server abgeschlossen werden. Weitere Informationen finden Sie in der ONTAP und vCenter-Dokumentation.

["ONTAP 9 Dokumentationscenter"](#)

Führen Sie die folgenden Schritte aus, um Datenspeicher anzuzeigen:

1. Klicken Sie auf der Seite **VMWARE > Virtuelle Maschinen** auf die VM, die den Datenspeicher hostet. Klicken Sie auf den **Workload Analyzer** oder den Datastore-Objektlink. Im Standardszenario, wenn der primäre Standort, der das Volume oder die LUN hostet, wie erwartet funktioniert, können Sie die vServer-Clusterdetails des primären Standorts sehen.
2. Im Falle einer Katastrophe und einer anschließenden Umschaltung auf den sekundären Standort verweist der Datastore-Link auf die Leistungsmetriken des Volumes oder LUN im sekundären Cluster. Dies wird nach Abschluss des nächsten Cluster-Zyklus und der vServer-Erkennung (Erfassung) widergespiegelt.
3. Nach einem erfolgreichen Switchback spiegelt die Datenspeicherverknüpfung wieder die Leistungsmetriken des Volumes oder LUN im primären Cluster wider. Dies wird nach Abschluss des nächsten Cluster-Zyklus und der vServer-Erkennung angezeigt.

Anzeigen von Datenspeichern in der Konfiguration zur Notfallwiederherstellung von Speicher-VMs

Beachten Sie die folgenden Voraussetzungen, bevor Sie Datenspeicher in einer Storage-VM-Notfallwiederherstellungskonfiguration anzeigen:

- Im Falle eines Switchovers und Switchbacks sollte die Erkennung der primären und sekundären Cluster des HA-Paares und der vCenter-Server abgeschlossen sein.
- Sowohl der Quell- als auch der Zielcluster und die Speicher-VM-Peers sollten von Unified Manager verwaltet werden.
- Die erforderliche Einrichtung muss auf ONTAP und vCenter Server abgeschlossen werden.
 - Bei NAS-Datenspeichern (NFS und VMFS) umfassen die Schritte im Katastrophenfall das Hochfahren der sekundären Speicher-VM, das Überprüfen der Daten-LIFs und -Routen, das Herstellen verlorener Verbindungen auf vCenter Server und das Starten der VMs.

Für eine Umschaltung zurück zum primären Standort sollten die Daten zwischen den Volumes synchronisiert werden, bevor der primäre Standort mit der Bereitstellung der Daten beginnt.

- Für SAN-Datenspeicher (iSCSI und FC für VMFS) formatiert vCenter Server die gemountete LUN in einem VMFS-Format. Im Katastrophenfall umfassen die Schritte das Hochfahren der sekundären Speicher-VM und die Überprüfung der Daten-LIFs und -Routen. Wenn sich die iSCSI-Ziel-IPs von den primären LIFs unterscheiden, müssen sie manuell hinzugefügt werden. Die neuen LUNs sollten als Geräte unter dem iSCSI-Adapter des Speicheradapters des Hosts verfügbar sein. Anschließend sollten neue VMFS-Datenspeicher mit den neuen LUNs erstellt und die alten VMs mit neuen Namen registriert werden. Die VMs müssen betriebsbereit sein.

Im Falle einer Wiederherstellung sollten die Daten zwischen den Volumes synchronisiert werden. Neue VMFS-Datenspeicher sollten erneut unter Verwendung der LUNs erstellt und die alten VMs mit neuen Namen registriert werden.

Informationen zum Setup finden Sie in der ONTAP und vCenter Server-Dokumentation.

Führen Sie die folgenden Schritte aus, um Datenspeicher anzuzeigen:

1. Klicken Sie auf der Seite **VMWARE > Virtuelle Maschinen** auf das VM-Inventar, das den Datenspeicher hostet. Klicken Sie auf den Link zum Datenspeicherobjekt. Im Standardszenario können Sie die Leistungsdaten der Volumes und LUNs in der primären Storage-VM sehen.
2. Im Falle einer Katastrophe und einer anschließenden Umschaltung auf die sekundäre Speicher-VM verweist der Datenspeicher-Link auf die Leistungsmetriken des Volumes oder LUN in der sekundären Speicher-VM. Dies wird nach Abschluss des nächsten Cluster-Zyklus und der vServer-Erkennung (Erfassung) widergespiegelt.
3. Nach einem erfolgreichen Switchback spiegelt die Datenspeicherverknüpfung wieder die Leistungsmetriken des Volumes oder LUN in der primären Speicher-VM wider. Dies wird nach Abschluss des nächsten Cluster-Zyklus und der vServer-Erkennung angezeigt.

Nicht unterstützte Szenarien

- Beachten Sie bei einer MetroCluster -Konfiguration die folgenden Einschränkungen:
 - Cluster nur in der **NORMAL** Und **SWITCHOVER** Staaten werden aufgenommen. Andere Staaten, wie z. **PARTIAL_SWITCHOVER**, **PARTIAL_SWITCHBACK** , Und **NOT_REACHABLE** werden nicht unterstützt.
 - Sofern die automatische Umschaltung (ASO) nicht aktiviert ist, kann der sekundäre Cluster beim Ausfall des primären Clusters nicht erkannt werden und die Topologie verweist weiterhin auf das Volume oder die LUN im primären Cluster.
- Beachten Sie bei einer Storage-VM-Notfallwiederherstellungskonfiguration die folgende Einschränkung:
 - Eine Konfiguration mit aktiviertem Site Recovery Manager (SRM) oder Storage Replication Adapter (SRA) für eine SAN-Speicherumgebung wird nicht unterstützt.

Bereitstellen und Verwalten von Workloads

Die aktive Verwaltungsfunktion von Active IQ Unified Manager bietet Leistungsservicelevel, Speichereffizienzrichtlinien und Speicheranbieter-APIs für die Bereitstellung, Überwachung und Verwaltung von Speicher-Workloads in einem Rechenzentrum.



Unified Manager bietet diese Funktionalität standardmäßig. Sie können es unter **Speicherverwaltung > Funktionseinstellungen** deaktivieren, wenn Sie diese Funktion nicht verwenden möchten.

Wenn diese Option aktiviert ist, können Sie Workloads auf den ONTAP Clustern bereitstellen, die von Ihrer Instanz von Unified Manager verwaltet werden. Sie können den Workloads auch Richtlinien wie Leistungsservicelevel und Speichereffizienzrichtlinien zuweisen und Ihre Speicherumgebung basierend auf diesen Richtlinien verwalten.

Diese Funktion ermöglicht die folgenden Funktionen:

- Automatische Erkennung von Speicher-Workloads auf den hinzugefügten Clustern, was eine einfache Auswertung und Bereitstellung von Speicher-Workloads ermöglicht
- Bereitstellung von NAS-Workloads mit Unterstützung der Protokolle NFS und CIFS

- Bereitstellung von SAN-Workloads mit Unterstützung der iSCSI- und FCP-Protokolle
- Unterstützung für NFS- und CIFS-Protokolle auf derselben Dateifreigabe
- Verwaltung von Leistungsservicelevels und Speichereffizienzrichtlinien
- Zuweisen von Leistungsservicelevels und Speichereffizienzrichtlinien zu Speicher-Workloads

Mit den Optionen **Bereitstellung**, **Speicher > Workloads** und **Richtlinien** im linken Bereich der Benutzeroberfläche können Sie verschiedene Konfigurationen ändern.

Mit diesen Optionen können Sie die folgenden Funktionen ausführen:

- Zeigen Sie Speicher-Workloads auf der Seite **Speicher > Workloads** an.
- Erstellen Sie Speicher-Workloads auf der Seite „Workload bereitstellen“
- Erstellen und Verwalten von Leistungsservicelevels anhand von Richtlinien
- Erstellen und Verwalten von Speichereffizienzrichtlinien aus Richtlinien
- Weisen Sie Speicher-Workloads Richtlinien auf der Seite „Workloads“ zu.

Verwandte Informationen

["Richtlinienbasierte Speicherverwaltung"](#)

Übersicht über Workloads

Eine Arbeitslast stellt die Eingabe-/Ausgabevorgänge (E/A) eines Speicherobjekts dar, beispielsweise eines Volumes oder einer LUN. Die Art und Weise der Speicherbereitstellung basiert auf den erwarteten Arbeitslastanforderungen. Workload-Statistiken werden von Active IQ Unified Manager erst verfolgt, wenn Datenverkehr zum und vom Speicherobjekt stattfindet. Beispielsweise sind die IOPS- und Latenzwerte der Arbeitslast verfügbar, nachdem Benutzer mit der Verwendung einer Datenbank- oder E-Mail-Anwendung begonnen haben.

Auf der Seite „Workloads“ wird eine Zusammenfassung der Speicher-Workloads der von Unified Manager verwalteten ONTAP Cluster angezeigt. Es bietet auf einen Blick kumulative Informationen zu den Speicher-Workloads, die dem Performance Service Level entsprechen, sowie zu den nicht konformen Speicher-Workloads. Darüber hinaus können Sie die gesamte, verfügbare und genutzte Kapazität und Leistung (IOPS) der Cluster in Ihrem Rechenzentrum beurteilen.



Es wird empfohlen, die Anzahl der Speicher-Workloads zu ermitteln, die nicht konform, nicht verfügbar oder von keinem Performance Service Level verwaltet werden, und die erforderlichen Maßnahmen zu ergreifen, um ihre Konformität, Kapazitätsnutzung und IOPS sicherzustellen.

Die Seite „Workloads“ enthält die folgenden zwei Abschnitte:

- **Übersicht über Workloads:** Bietet eine Übersicht über die Anzahl der Speicher-Workloads auf den von Unified Manager verwalteten ONTAP Clustern.
- **Rechenzentrumsübersicht:** Bietet eine Übersicht über die Kapazität und IOPS der Speicher-Workloads im Rechenzentrum. Die relevanten Daten werden auf Rechenzentrumsebene und für einzelne angezeigt.

Abschnitt „Workloads – Übersicht“

Der Abschnitt „Workloadsübersicht“ bietet auf einen Blick zusammengefasste Informationen zu den Speicher-Workloads. Der Status der Speicher-Workloads wird basierend auf zugewiesenen und nicht zugewiesenen Performance-Service-Levels angezeigt.

- **Zugewiesen:** Für Speicher-Workloads, denen Performance-Service-Level zugewiesen wurden, werden die folgenden Status gemeldet:
 - **Konform:** Die Leistung von Speicher-Workloads basiert auf den ihnen zugewiesenen Performance Service Levels. Wenn die Speicher-Workloads innerhalb der in den zugehörigen Performance Service Levels definierten Schwellenlatenz liegen, werden sie als „konform“ gekennzeichnet. Die konformen Arbeitslasten sind blau markiert.
 - **Nicht konform:** Während der Leistungsüberwachung werden Speicher-Workloads als „nicht konform“ markiert, wenn die Latenz der Speicher-Workloads die im zugehörigen Leistungs-Servicelevel definierte Schwellenlatenz überschreitet. Die nicht konformen Arbeitslasten sind orange markiert.
 - **Nicht verfügbar:** Speicher-Workloads werden als „nicht verfügbar“ markiert, wenn sie offline sind oder der entsprechende Cluster nicht erreichbar ist. Die nicht verfügbaren Workloads sind rot markiert.
- **Nicht zugewiesen:** Speicher-Workloads, denen kein Performance-Service-Level zugewiesen ist, werden als „nicht zugewiesen“ gemeldet. Die Nummer wird durch das Informationssymbol übermittelt.

Die Gesamtzahl der Arbeitslasten ist die Summe der zugewiesenen und nicht zugewiesenen Arbeitslasten.

Sie können auf die Gesamtzahl der in diesem Abschnitt angezeigten Workloads klicken und sie auf der Seite „Workloads“ anzeigen.

Der Unterabschnitt „Konformität nach Leistungsserviceleveln“ zeigt die Gesamtzahl der verfügbaren Speicherarbeitslasten an:

- Konform mit jedem Typ von Performance Service Level
- Bei denen eine Diskrepanz zwischen den zugewiesenen und den empfohlenen Performance Service Levels besteht

Abschnitt „Übersicht über das Rechenzentrum“

Der Abschnitt „Rechenzentrumsübersicht“ stellt die verfügbare und genutzte Kapazität sowie die IOPS für alle Cluster im Rechenzentrum grafisch dar. Mithilfe dieser Daten sollten Sie die Kapazität und IOPS der Speicher-Workloads verwalten. Der Abschnitt zeigt außerdem die folgenden Informationen zu den Speicherarbeitslasten aller Cluster an:

- Die gesamte, verfügbare und genutzte Kapazität für alle Cluster in Ihrem Rechenzentrum
- Die gesamten, verfügbaren und verwendeten IOPS für alle Cluster in Ihrem Rechenzentrum
- Die verfügbare und genutzte Kapazität basierend auf jedem Performance Service Level
- Die verfügbaren und genutzten IOPS basierend auf jedem Performance Service Level
- Der gesamte Speicherplatz und die IOPS, die von den Workloads verwendet werden, denen kein Performance Service Level zugewiesen ist

Wie die Kapazität und Leistung von Rechenzentren basierend auf Performance Service Levels berechnet wird

Die genutzte Kapazität und die IOPS werden im Hinblick auf die insgesamt genutzte Kapazität und Leistung aller Speicher-Workloads in den Clustern abgerufen.

Die verfügbaren IOPS werden basierend auf der erwarteten Latenz und den empfohlenen Leistungsserviceleveln auf den Knoten berechnet. Es umfasst die verfügbaren IOPS für alle Performance-Service-Levels, deren erwartete Latenz kleiner oder gleich ihrer eigenen erwarteten Latenz ist.

Die verfügbare Kapazität wird basierend auf der erwarteten Latenz und den empfohlenen Leistungsserviceleveln für Aggregate berechnet. Es umfasst die verfügbare Kapazität für alle Performance-Service-Levels, deren erwartete Latenz kleiner oder gleich ihrer eigenen erwarteten Latenz ist.

Arbeitslasten anzeigen

Wenn Sie Cluster zu Unified Manager hinzufügen, werden die Speicher-Workloads auf jedem Cluster automatisch erkannt und auf der Seite „Workloads“ angezeigt.

Unified Manager beginnt erst mit der Analyse der Workloads für Empfehlungen (empfohlene PSLs), nachdem die E/A-Vorgänge für die Speicher-Workloads gestartet wurden.

FlexGroup Volumina und ihre Bestandteile sind ausgeschlossen.

Übersicht über Workloads

Auf der Seite „Workloads-Übersicht“ wird die Übersicht über die Workloads im Rechenzentrum sowie die Speicherplatz- und Leistungsübersicht des Rechenzentrums angezeigt.

- **Arbeitslastübersicht**-Bereich: Zeigt die Gesamtzahl der Arbeitslasten und die Anzahl der Arbeitslasten mit oder ohne zugewiesene PSLs an. Außerdem wird die Aufschlüsselung der Arbeitslastanzahl für jede PSL angezeigt. Durch Klicken auf die Zählungen gelangen Sie zur Ansicht **Alle Workloads** mit den gefilterten Workloads. Sie können auch die Anzahl der Workloads anzeigen, die nicht der Systemempfehlung entsprechen, und ihnen die vom System empfohlenen PSLs zuweisen, indem Sie auf die Schaltfläche **Vom System empfohlene PSLs zuweisen** klicken.
- **Rechenzentrumsübersicht**-Bereich: Zeigt den verfügbaren und genutzten Speicherplatz (TiB) und die Leistung (IOPS) des Rechenzentrums an. Außerdem wird eine Aufschlüsselung des verfügbaren und verwendeten Speicherplatzes (TiB) und der Leistung (IOPS) aller Workloads unter jeder PSL angezeigt.

Ansicht „Alle Workloads“

Auf der Seite **Speicher > Workloads > Alle Workloads** werden die Speicher-Workloads aufgelistet, die mit den von Unified Manager verwalteten ONTAP Clustern verknüpft sind.

Für die neu erkannten Speicher-Workloads, bei denen keine E/A-Vorgänge stattgefunden haben, lautet der Status „Warten auf E/A“. Nachdem die E/A-Vorgänge für die Speicher-Workloads begonnen haben, beginnt Unified Manager mit der Analyse und der Workload-Status ändert sich in „Lernen ...“. Nach Abschluss der Analyse (innerhalb von 24 Stunden nach Beginn der E/A-Vorgänge) werden die empfohlenen PSLs für die Speicher-Workloads angezeigt.

Auf der Seite können Sie Speicher-Workloads auch Storage Efficiency Policies (SEPs) und Performance Service Levels (PSLs) zuweisen. Sie können mehrere Aufgaben ausführen:

- Hinzufügen oder Bereitstellen von Speicherworkloads
- Anzeigen und Filtern der Liste der Workloads
- Zuweisen von PSLs zu Speicher-Workloads
- Bewerten Sie vom System empfohlene PSLs und weisen Sie sie Arbeitslasten zu
- Zuweisen von SEPs zu Speicher-Workloads

Hinzufügen oder Bereitstellen von Speicher-Workloads

Sie können die Speicher-Workloads zu unterstützten LUNs (die sowohl iSCSI- als auch FCP-Protokolle unterstützen), NFS-Dateifreigaben und SMB-Freigaben hinzufügen oder bereitstellen.

Schritte

1. Klicken Sie auf **Speicher > Workloads > Alle Workloads > Erstellen**.
2. Erstellen Sie Arbeitslasten. Weitere Informationen finden Sie unter "[Bereitstellung und Verwaltung von Workloads](#)".

Anzeigen und Filtern von Workloads

Auf dem Bildschirm „Alle Workloads“ können Sie alle Workloads in Ihrem Rechenzentrum anzeigen oder anhand ihrer PSLs oder Namen nach bestimmten Speicher-Workloads suchen. Über das Filtersymbol können Sie bestimmte Bedingungen für Ihre Suche eingeben. Sie können nach verschiedenen Filterbedingungen suchen, beispielsweise nach dem Hostcluster oder der Speicher-VM. Die Option **Gesamtkapazität** ermöglicht das Filtern nach der Gesamtkapazität der Workloads (in MB). In diesem Fall kann die Anzahl der zurückgegebenen Workloads jedoch variieren, da die Gesamtkapazität auf Byte-Ebene verglichen wird.

Für jede Arbeitslast werden Informationen wie Hostcluster und Speicher-VM zusammen mit den zugewiesenen PSL und SEP angezeigt.

Auf der Seite können Sie auch die Leistungsdetails einer Arbeitslast anzeigen. Sie können detaillierte Informationen zu IOPS, Kapazität und Latenz der Arbeitslast anzeigen, indem Sie auf die Schaltfläche **Spalten auswählen/sortieren** klicken und bestimmte Spalten zur Anzeige auswählen. In der Spalte „Leistungsansicht“ werden die durchschnittlichen und Spitzen-IOPS für eine Arbeitslast angezeigt. Sie können auf das Symbol des Arbeitslastanalysators klicken, um die detaillierte IOPS-Analyse anzuzeigen.

Analysieren von Leistungs- und Kapazitätskriterien für eine Workload

Über die Schaltfläche **Arbeitslast analysieren** im Popup-Fenster **IOPS-Analyse** gelangen Sie zur Seite „Arbeitslastanalyse“, auf der Sie einen Zeitraum auswählen und die Latenz-, Durchsatz- und Kapazitätstrends für die ausgewählte Arbeitslast anzeigen können. Weitere Informationen zum Workload-Analyzer finden Sie unter "[Fehlerbehebung bei Workloads mit dem Workload-Analyzer](#)".

Sie können Leistungsinformationen zu einer Arbeitslast anzeigen, um die Fehlerbehebung zu erleichtern, indem Sie in der Spalte **Leistungsansicht** auf das Balkendiagrammsymbol klicken. Um Leistungs- und Kapazitätsdiagramme auf der Seite „Arbeitslastanalyse“ anzuzeigen und das Objekt zu analysieren, klicken Sie auf die Schaltfläche **Arbeitslast analysieren**.

Weitere Informationen finden Sie unter "[Welche Daten zeigt der Workload Analyzer an](#)".

Zuweisen von Richtlinien zu Workloads

Sie können Speicher-Effizienzrichtlinien (SEPs) und Performance Service Levels (PSLs) mithilfe der verschiedenen Navigationsoptionen von der Seite „Alle Workloads“ aus Speicher-Workloads zuweisen.

Zuweisen von Richtlinien zu einer einzelnen Arbeitslast

Sie können einer einzelnen Arbeitslast entweder eine PSL oder eine SEP oder beides zuweisen. Gehen Sie folgendermaßen vor:

1. Wählen Sie die Arbeitslast aus.
2. Klicken Sie auf das Bearbeitungssymbol neben der Zeile und dann auf **Bearbeiten**.

Die Felder **Zugewiesenes Leistungsservicelevel** und **Speichereffizienzrichtlinie** sind aktiviert.

3. Wählen Sie die gewünschte PSL oder SEP oder beides aus.
4. Klicken Sie auf das Häkchensymbol, um die Änderungen zu übernehmen.



Sie können auch eine Arbeitslast auswählen und auf **Weitere Aktionen** klicken, um die Richtlinien zuzuweisen.

Zuweisen von Richtlinien zu mehreren Speicher-Workloads

Sie können mehreren Speicher-Workloads gleichzeitig eine PSL oder ein SEP zuweisen. Gehen Sie folgendermaßen vor:

1. Aktivieren Sie die Kontrollkästchen für die Workloads, denen Sie die Richtlinie zuweisen möchten, oder wählen Sie alle Workloads in Ihrem Rechenzentrum aus.
2. Klicken Sie auf **Weitere Aktionen**.
3. Wählen Sie zum Zuweisen eines PSL **Performance Service Level zuweisen**. Wählen Sie zum Zuweisen eines SEP **Speichereffizienzrichtlinie zuweisen**. Es wird ein Popup angezeigt, in dem Sie die Richtlinie auswählen können.
4. Wählen Sie die entsprechende Richtlinie aus und klicken Sie auf **Übernehmen**. Die Anzahl der Workloads, denen die Richtlinien zugewiesen sind, wird angezeigt. Die Workloads, denen die Richtlinien nicht zugewiesen sind, werden ebenfalls mit der Ursache aufgelistet.



Das Anwenden von Richtlinien auf Workloads in großen Mengen kann je nach Anzahl der ausgewählten Workloads einige Zeit in Anspruch nehmen. Sie können auf die Schaltfläche **Im Hintergrund ausführen** klicken und mit anderen Aufgaben fortfahren, während der Vorgang im Hintergrund ausgeführt wird. Wenn die Massenzuweisung abgeschlossen ist, können Sie den Abschlussstatus anzeigen. Wenn Sie eine PSL auf mehrere Workloads anwenden, können Sie keine weitere Anfrage auslösen, während der vorherige Job der Massenzuweisung ausgeführt wird.

Zuweisen von vom System empfohlenen PSLs zu Workloads

Sie können den Speicherarbeitslasten in einem Rechenzentrum, denen keine PSLs zugewiesen sind oder die nicht mit der Systemempfehlung übereinstimmen, vom System empfohlene PSLs zuweisen. Um diese Funktion zu verwenden, klicken Sie auf die Schaltfläche **Vom System empfohlene PSLs zuweisen**. Sie müssen keine bestimmten Workloads auswählen.

Die Empfehlung wird intern durch Systemanalysen ermittelt und für Workloads übersprungen, deren IOPS und andere Parameter nicht mit den Definitionen eines verfügbaren PSL übereinstimmen. Speicher-Workloads mit `Waiting for I/O` und Lernstatus sind ebenfalls ausgeschlossen.



Es gibt spezielle Schlüsselwörter, nach denen Unified Manager im Workload-Namen sucht, um die Systemanalyse zu überschreiben und eine andere PSL für den Workload zu empfehlen. Wenn der Name der Arbeitslast die Buchstaben „ora“ enthält, wird die **Extreme Performance** PSL empfohlen. Und wenn der Workload die Buchstaben „vm“ im Namen hat, wird die **Performance** PSL empfohlen.

Siehe auch den Knowledge Base (KB)-Artikel "[ActiveIQ Unified Manager „Empfohlene Leistungsserviceebene des Systems zuweisen“ ist nicht anpassungsfähig an eine stark variable Arbeitslast](#)"

Bereitstellen von Dateifreigabevolumes

Sie können auf der Seite „Workload bereitstellen“ Dateifreigabevolumes erstellen, die CIFS/SMB- und NFS-Protokolle auf einem vorhandenen Cluster und einer Storage Virtual Machine (Storage-VM) unterstützen.

Bevor Sie beginnen

- Die Speicher-VM muss über Speicherplatz für die Bereitstellung des Dateifreigabevolumes verfügen.
- Einer oder beide der SMB- und NFS-Dienste sollten auf Ihrer Speicher-VM aktiviert sein.
- Um den Performance Service Level (PSL) und die Storage Efficiency Policy (SEP) für die Arbeitslast auszuwählen und zuzuweisen, müssen die Richtlinien erstellt worden sein, bevor Sie mit der Erstellung der Arbeitslast beginnen.

Schritte

1. Fügen Sie auf der Seite **Workload bereitstellen** den Namen der Workload hinzu, die Sie erstellen möchten, und wählen Sie dann den Cluster aus der verfügbaren Liste aus.
2. Basierend auf dem von Ihnen ausgewählten Cluster filtert das Feld **STORAGE VM** die verfügbaren Speicher-VMs für diesen Cluster. Wählen Sie die erforderliche Speicher-VM aus der Liste aus.

Basierend auf den auf der Speicher-VM unterstützten SMB- und NFS-Diensten wird die NAS-Option im Abschnitt „Hostinformationen“ aktiviert.

3. Weisen Sie im Abschnitt „Speicher und Optimierung“ die Speicherkapazität und PSL sowie optional einen SEP für die Arbeitslast zu.

Die Spezifikationen für das SEP werden der LUN zugewiesen und die Definitionen für das PSL werden beim Erstellen auf die Arbeitslast angewendet.

4. Aktivieren Sie das Kontrollkästchen **Leistungsgrenzen erzwingen**, wenn Sie die PSL erzwingen möchten, die Sie der Arbeitslast zugewiesen haben.

Durch die Zuweisung einer PSL zu einer Arbeitslast wird sichergestellt, dass das Aggregat, auf dem die Arbeitslast erstellt wird, die in der jeweiligen Richtlinie definierten Leistungs- und Kapazitätsziele unterstützen kann. Wenn beispielsweise einer Arbeitslast die PSL „Extreme Performance“ zugewiesen wird, sollte das Aggregat, auf dem die Arbeitslast bereitgestellt werden soll, in der Lage sein, die Leistungs- und Kapazitätsziele der Richtlinie „Extreme Performance“ zu unterstützen, beispielsweise SSD-Speicher.



Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird die PSL nicht auf die Arbeitslast angewendet und der Status der Arbeitslast wird auf dem Dashboard als „Nicht zugewiesen“ angezeigt.

5. Wählen Sie die Option **NAS**.

Wenn die Option **NAS** nicht aktiviert ist, überprüfen Sie, ob die von Ihnen ausgewählte Speicher-VM SMB oder NFS oder beides unterstützt.



Wenn Ihre Speicher-VM sowohl für SMB- als auch für NFS-Dienste aktiviert ist, können Sie die Kontrollkästchen **Freigabe über NFS** und **Freigabe über SMB** aktivieren und eine Dateifreigabe erstellen, die sowohl NFS- als auch SMB-Protokolle unterstützt. Wenn Sie entweder eine SMB- oder eine CIFS-Freigabe erstellen möchten, aktivieren Sie nur das jeweilige Kontrollkästchen.

6. Geben Sie für NFS-Dateifreigabevolumes die IP-Adresse des Hosts oder Netzwerks an, um auf das Dateifreigabevolume zuzugreifen. Sie können durch Kommas getrennte Werte für mehrere Hosts eingeben.

Beim Hinzufügen der Host-IP-Adresse wird eine interne Prüfung ausgeführt, um die Hostdetails mit der Speicher-VM abzugleichen, und die Exportrichtlinie für diesen Host wird erstellt oder, falls eine vorhandene Richtlinie vorhanden ist, wird sie wiederverwendet. Wenn mehrere NFS-Freigaben für denselben Host erstellt werden, wird eine verfügbare Exportrichtlinie für denselben Host mit übereinstimmenden Regeln für alle Dateifreigaben wiederverwendet. Die Funktion zum Festlegen von Regeln einzelner Richtlinien oder zum Wiederverwenden von Richtlinien durch die Bereitstellung bestimmter Richtlinienschlüssel ist verfügbar, wenn Sie die NFS-Freigabe mithilfe von APIs bereitstellen.

7. Geben Sie für eine SMB-Freigabe an, welche Benutzer oder Benutzergruppen auf die SMB-Freigabe zugreifen können, und weisen Sie die erforderlichen Berechtigungen zu. Für jede Benutzergruppe wird während der Erstellung der Dateifreigabe eine neue Zugriffskontrollliste (ACL) generiert.
8. Klicken Sie auf **Speichern**.

Die Arbeitslast wird der Liste der Speicherarbeitslasten hinzugefügt.

Bereitstellen von LUNs

Sie können auf der Seite „Workload bereitstellen“ LUNs erstellen, die CIFS/SMB- und NFS-Protokolle auf einem vorhandenen Cluster und einer Storage Virtual Machine (Storage-VM) unterstützen.

Bevor Sie beginnen

- Die Speicher-VM muss über Speicherplatz für die Bereitstellung der LUN verfügen.
- Sowohl iSCSI als auch FCP müssen auf der Speicher-VM aktiviert sein, auf der Sie die LUN erstellen.
- Um den Performance Service Level (PSL) und die Storage Efficiency Policy (SEP) für die Arbeitslast auszuwählen und zuzuweisen, müssen die Richtlinien erstellt worden sein, bevor Sie mit der Erstellung der Arbeitslast beginnen.

Schritte

1. Fügen Sie auf der Seite **Workload bereitstellen** den Namen der Workload hinzu, die Sie erstellen möchten, und wählen Sie dann den Cluster aus der verfügbaren Liste aus.

Basierend auf dem von Ihnen ausgewählten Cluster filtert das Feld **STORAGE VM** die verfügbaren Speicher-VMs für diesen Cluster.

2. Wählen Sie aus der Liste die Speicher-VM aus, die die iSCSI- und FCP-Dienste unterstützt.

Basierend auf Ihrer Auswahl wird die SAN-Option im Abschnitt „Hostinformationen“ aktiviert.

3. Weisen Sie im Abschnitt **Speicher und Optimierung** die Speicherkapazität und PSL sowie optional den SEP für die Arbeitslast zu.

Die Spezifikationen für das SEP werden der LUN zugewiesen und die Definitionen für das PSL werden beim Erstellen auf die Arbeitslast angewendet.

4. Aktivieren Sie das Kontrollkästchen **Leistungsgrenzen erzwingen**, wenn Sie die zugewiesene PSL für die Arbeitslast erzwingen möchten.

Durch die Zuweisung einer PSL zu einer Arbeitslast wird sichergestellt, dass das Aggregat, auf dem die Arbeitslast erstellt wird, die in der jeweiligen Richtlinie definierten Leistungs- und Kapazitätsziele unterstützen kann. Wenn beispielsweise einer Arbeitslast die PSL „Extreme Leistung“ zugewiesen wird, sollte das Aggregat, auf dem die Arbeitslast bereitgestellt werden soll, in der Lage sein, die Leistungs- und Kapazitätsziele der Richtlinie „Extreme Leistung“ zu unterstützen, beispielsweise SSD-Speicher.



Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird die PSL nicht auf die Arbeitslast angewendet und der Status der Arbeitslast wird auf dem Dashboard als `unassigned`.

5. Wählen Sie die Option **SAN**. Wenn die Option **SAN** nicht aktiviert ist, überprüfen Sie, ob die von Ihnen ausgewählte Speicher-VM iSCSI und FCP unterstützt.
6. Wählen Sie das Host-Betriebssystem aus.
7. Geben Sie die Hostzuordnung an, um den Zugriff der Initiatoren auf die LUN zu steuern. Sie können vorhandene Initiatorgruppen (igroups) zuweisen oder neue igroups definieren und zuordnen.



Wenn Sie beim Bereitstellen der LUN eine neue igroup erstellen, müssen Sie bis zum nächsten Erkennungszyklus (bis zu 15 Minuten) warten, bevor Sie sie verwenden können. Es wird daher empfohlen, eine vorhandene Igroup aus der Liste der verfügbaren Igroups zu verwenden.

Wenn Sie eine neue Igroup erstellen möchten, wählen Sie die Schaltfläche **Neue Initiatorgruppe erstellen** und geben Sie die Informationen für die Igroup ein.

8. Klicken Sie auf **Speichern**.

Die LUN wird der Liste der Speicher-Workloads hinzugefügt.

Leistungsservice-Levels

Mit einem Performance Service Level (PSL) können Sie die Leistungs- und Speicherziele für eine Arbeitslast definieren. Sie können einer Arbeitslast beim ersten Erstellen der Arbeitslast oder später durch Bearbeiten der Arbeitslast eine PSL zuweisen.

Die Verwaltung und Überwachung von Speicherressourcen basieren auf Service Level Objectives (SLOs). SLOs werden durch Service Level Agreements definiert, die auf der erforderlichen Leistung und Kapazität basieren. In Unified Manager beziehen sich SLOs auf die PSL-Definitionen der Anwendungen, die auf NetApp-Speicher ausgeführt werden. Speicherdienste unterscheiden sich anhand der Leistung und Nutzung der zugrunde liegenden Ressourcen. Eine PSL ist eine Beschreibung der Speicherdienstziele. Ein PSL ermöglicht dem Speicheranbieter, die Leistungs- und Kapazitätsziele für die Arbeitslast anzugeben. Wenn Sie einer Workload eine PSL zuweisen, wird die entsprechende Workload auf ONTAP anhand ihrer Leistungs- und Kapazitätsziele verwaltet. Jeder PSL wird durch Spitzen-, erwartete und absolute Mindest-IOPs sowie die erwartete Latenz bestimmt.

Unified Manager verfügt über die folgenden PSL-Typen:

- **Systemdefiniert:** Unified Manager bietet einige vorgefertigte Richtlinien, die nicht geändert werden können. Diese vordefinierten PSLs sind:

- Extreme Leistung
- Performance
- Wert

Die PSLs „Extreme Performance“, „Performance“ und „Value“ sind für die meisten gängigen Speicher-Workloads in einem Rechenzentrum anwendbar.

Unified Manager bietet außerdem drei Performance Service Levels für Datenbankanwendungen. Dabei handelt es sich um PSLs mit extrem hoher Leistung, die Burst-IOPS unterstützen und für Datenbankanwendungen mit den höchsten Durchsatzanforderungen geeignet sind.

- Extreme für Datenbankprotokolle
- Extreme für gemeinsam genutzte Datenbankdaten
- Extreme für Datenbankdaten
- **Benutzerdefiniert:** Wenn die vordefinierten Performance Service Levels Ihren Anforderungen nicht entsprechen, können Sie neue PSLs erstellen, die Ihren Anforderungen entsprechen. Weitere Informationen finden Sie unter ["Erstellen und Bearbeiten von Performance-Service-Levels"](#).
- **Beyond Extreme:** Die Beyond Extreme PSLs sind die vom System empfohlenen PSLs, die für Arbeitslasten vorgeschlagen werden, die höhere IOPS als Extreme erfordern. Die Workloads werden intern anhand ihrer IOPS, Kapazität und Latenz analysiert und für jeden dieser Workloads wird auf dem Bildschirm **Speicher > Workloads > Alle Workloads** ein Beyond Extreme PSL empfohlen. Sie können die PSLs auf die Workloads anwenden, um eine optimale Leistung sicherzustellen.

Die IOPS-Parameter für die Workloads werden dynamisch generiert, abhängig vom Workload-Verhalten, und an den Namen der Beyond Extreme PSL im Format angehängt `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`. Wenn das System beispielsweise eine Arbeitslast ermittelt, die die Spitzen- und erwarteten IOPS aufweist, 106345 Und 37929 bzw. die für die Arbeitslast generierte Beyond Extreme PSL wird wie folgt benannt: `Beyond Extreme 106345 37929`. Obwohl diese PSLs vom System empfohlen werden, werden sie bei der Zuweisung zu Workloads als gekennzeichnet. `User-defined` im Typ.

Verwalten Sie Arbeitslasten durch die Zuweisung von PSLs

Sie können auf PSLs über die Seite **Richtlinien > Leistungs-Servicelevel** und mithilfe der APIs des Speicheranbieters zugreifen. Die Verwaltung von Speicher-Workloads durch die Zuweisung von PSLs ist praktisch, da Sie die Speicher-Workloads nicht einzeln verwalten müssen. Alle Änderungen können auch durch die Neuzuweisung einer anderen PSL verwaltet werden, anstatt sie einzeln zu verwalten. Unified Manager hilft Ihnen, Ihren Arbeitslasten PSLs basierend auf internen Bewertungen und Empfehlungen zuzuweisen.

Informationen zum Zuweisen systemseitig empfohlener PSLs zu Workloads finden Sie unter ["Zuweisen von vom System empfohlenen PSLs zu Workloads"](#)

Auf der Seite „Performance Service Levels“ werden die verfügbaren PSL-Richtlinien aufgelistet und Sie können diese hinzufügen, bearbeiten und löschen.



Sie können keine PSL ändern, die systemdefiniert ist oder die derzeit einer Arbeitslast zugewiesen ist. Sie können keine PSL löschen, die einer Arbeitslast zugewiesen ist oder die einzige verfügbare PSL ist.

Auf dieser Seite werden die folgenden Informationen angezeigt:

Feld	Beschreibung
Name	Name der PSL.
Typ	Ob die Richtlinie systemdefiniert oder benutzerdefiniert ist.
Erwartete IOPS/TB	Mindestanzahl an IOPS, die eine Anwendung voraussichtlich auf einer LUN oder Dateifreigabe ausführen kann. „Erwartete IOPS“ gibt die minimal erwarteten zugewiesenen IOPS basierend auf der zugewiesenen Größe des Speicherobjekts an.
Spitzen-IOPS/TB	Maximale Anzahl von IOPS, die eine Anwendung auf einer LUN oder Dateifreigabe ausführen kann. Peak IOPS gibt die maximal möglichen zugewiesenen IOPS an, basierend auf der Größe des zugewiesenen Speicherobjekts oder der Größe des verwendeten Speicherobjekts. Spitzen-IOPS basieren auf einer Zuweisungsrichtlinie. Die Zuweisungsrichtlinie lautet entweder „zugewiesener Speicherplatz“ oder „verwendeter Speicherplatz“. Wenn die Zuweisungsrichtlinie auf „zugewiesener Speicherplatz“ eingestellt ist, wird der Spitzen-IOPS basierend auf der Größe des Speicherobjekts berechnet. Wenn die Zuweisungsrichtlinie auf „Verwendeter Speicherplatz“ eingestellt ist, wird der Spitzen-IOPS basierend auf der im Speicherobjekt gespeicherten Datenmenge berechnet, wobei die Speichereffizienz berücksichtigt wird. Standardmäßig ist die Zuweisungsrichtlinie auf „genutzter Speicherplatz“ eingestellt.

Feld	Beschreibung
Absolutes Minimum an IOPS	Der absolute Mindest-IOPS-Wert wird als Überschreitung verwendet, wenn der erwartete IOPS-Wert unter diesem Wert liegt. Die Standardwerte der systemdefinierten PSLs sind die folgenden: • Extreme Leistung: Wenn erwartete IOPS $\geq 6144/\text{TB}$, dann absolutes Minimum an IOPS = 1000 • Leistung: Wenn erwartete IOPS $\geq 2048/\text{TB}$ und $< 6144/\text{TB}$, dann absolutes Minimum an IOPS = 500 • Wert: Wenn die erwarteten IOPS $\geq 128/\text{TB}$ und $< 2048/\text{TB}$ sind, dann ist der absolute Mindest-IOPS = 75 Die Standardwerte der systemdefinierten Datenbank-PSLs sind die folgenden: • Extrem für Datenbankprotokolle: Wenn erwartete IOPS ≥ 22528, dann absolutes Minimum an IOPS = 4000 • Extrem für gemeinsam genutzte Datenbankdaten: Wenn erwartete IOPS ≥ 16384, dann absolutes Minimum an IOPS = 2000 • Extrem für Datenbankdaten: Wenn erwartete IOPS ≥ 12288, dann absolutes Minimum an IOPS = 2000 Der höhere Wert des absoluten IOPS-Mindestwerts für benutzerdefinierte PSLs kann maximal 75.000 betragen. Der niedrigere Wert berechnet sich wie folgt: $1000/\text{erwartete Latenz}$
Erwartete Latenz	Erwartete Latenz für Speicher-IOPS in Millisekunden pro Vorgang (ms/op).
Kapazität	Gesamte verfügbare und genutzte Kapazität in den Clustern.
Arbeitslasten	Anzahl der Speicher-Workloads, denen die PSL zugewiesen wurde.

Informationen dazu, wie die Spitzen-IOPS und die erwarteten IOPS dazu beitragen, eine konsistente differenzierte Leistung auf ONTAP Clustern zu erzielen, finden Sie im folgenden KB-Artikel: https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F["Was ist Performance Budgeting?"]

Ereignisse, die für Workloads generiert werden, die den durch PSLs definierten Schwellenwert überschreiten

Beachten Sie, dass Unified Manager eines der folgenden Ereignisse generiert, um Sie auf ein potenzielles Leistungsproblem hinzuweisen, wenn die Arbeitslasten in der letzten Stunde 30 % der Zeit den erwarteten Latenzwert überschritten haben:

- Latenzschwelle für Workload-Volumen überschritten, wie in der Service-Level-Richtlinie für die Leistung definiert
- Der in der Service-Level-Richtlinie für die Leistung definierte Schwellenwert für die Arbeitslast-LUN-Latenz wurde überschritten.

Möglicherweise möchten Sie die Arbeitslast analysieren, um herauszufinden, was die höheren Latenzwerte verursacht.

Weitere Informationen finden Sie unter den folgenden Links:

- ["Volumenereignisse"](#)
- ["Was passiert, wenn eine Leistungsschwellenrichtlinie verletzt wird?"](#)
- ["So nutzt Unified Manager die Workload-Latenz, um Leistungsprobleme zu identifizieren"](#)
- ["Was sind Performance-Ereignisse"](#)

Systemdefinierte PSLs

Die folgende Tabelle enthält Informationen zu den systemdefinierten PSLs:

Leistungsservicelevel	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/op)	Spitzen-IOPS	Erwartete IOPS	Absolutes Minimum an IOPS
Extreme Leistung	Bietet extrem hohen Durchsatz bei sehr geringer Latenz Ideal für latenzempfindliche Anwendungen	1	12288	6144	1000
Performance	Bietet hohen Durchsatz bei geringer Latenz Ideal für Datenbank- und virtualisierte Anwendungen	2	4096	2048	500

Leistungsservicelevel	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/op)	Spitzen-IOPS	Erwartete IOPS	Absolutes Minimum an IOPS
Wert	Bietet hohe Speicherkapazität und moderate Latenz Ideal für Anwendungen mit hoher Kapazität wie E-Mail, Webinhalte, Dateifreigaben und Sicherungsziele	17	512	128	75
Extreme für Datenbankprotokolle	Bietet maximalen Durchsatz bei niedrigster Latenz. Ideal für Datenbankanwendungen, die Datenbankprotokolle unterstützen. Diese PSL bietet den höchsten Durchsatz, da Datenbankprotokolle extrem stoßweise auftreten und die Protokollierung ständig erforderlich ist.	1	45056	22528	4000

Leistungsservicelevel	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/op)	Spitzen-IOPS	Erwartete IOPS	Absolutes Minimum an IOPS
Extreme für gemeinsam genutzte Datenbankdaten	Bietet einen sehr hohen Durchsatz bei geringster Latenz. Ideal für Datenbankanwendungen: Daten, die in einem gemeinsamen Datenspeicher gespeichert, aber datenbankübergreifend genutzt werden.	1	32768	16384	2000
Extreme für Datenbankdaten	Bietet hohen Durchsatz bei geringster Latenz. Ideal für Daten aus Datenbankanwendungen, wie Datenbanktabelleninformationen und Metadaten.	1	24576	12288	2000

Erstellen und Bearbeiten von Performance Service Levels

Wenn die systemdefinierten Performance-Service-Levels nicht Ihren Workload-Anforderungen entsprechen, können Sie Ihre eigenen Performance-Service-Levels erstellen, die für Ihre Workloads optimiert sind.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.
- Der Name des Performance Service Level muss eindeutig sein und Sie dürfen die folgenden reservierten Schlüsselwörter nicht verwenden:

Prime, Extreme , Performance , Value , Unassigned , Learning , Idle , Default , Und None .

Sie erstellen und bearbeiten benutzerdefinierte Performance-Service-Levels auf der Seite „Performance-Service-Levels“, indem Sie die Service-Level-Ziele definieren, die Sie für die Anwendungen benötigen, die auf den Speicher zugreifen.



Sie können einen Performance-Servicelevel nicht ändern, wenn er aktuell einer Arbeitslast zugewiesen ist.

Schritte

1. Wählen Sie im linken Navigationsbereich unter **Einstellungen Richtlinien > Leistungsservicelevel** aus.
2. Klicken Sie auf der Seite **Performance-Service-Levels** auf die entsprechende Schaltfläche, je nachdem, ob Sie ein neues Performance-Service-Level erstellen oder ein vorhandenes Performance-Service-Level bearbeiten möchten.

Zu...	Befolgen Sie diese Schritte...
Erstellen eines neuen Performance-Service-Levels	Klicken Sie auf Hinzufügen .
Bearbeiten eines vorhandenen Performance-Service-Levels	Wählen Sie ein vorhandenes Performance-Service-Level aus und klicken Sie dann auf Bearbeiten .

Die Seite zum Hinzufügen oder Bearbeiten eines Performance-Service-Levels wird angezeigt.

3. Passen Sie das Performance-Service-Level an, indem Sie die Leistungsziele angeben, und klicken Sie dann auf **Senden**, um das Performance-Service-Level zu speichern.

Sie können das neue oder geänderte Performance-Service-Level auf Workloads (LUNs, NFS-Dateifreigaben, CIFS-Freigaben) von der Seite „Workloads“ oder beim Bereitstellen eines neuen Workloads anwenden.

Verwalten von Speichereffizienzrichtlinien

Mit einer Storage Efficiency Policy (SEP) können Sie die Speichereffizienzmerkmale einer Arbeitslast definieren. Sie können einer Arbeitslast beim ersten Erstellen der Arbeitslast oder später durch Bearbeiten der Arbeitslast einen SEP zuweisen.

Zur Speichereffizienz gehört der Einsatz von Technologien wie Thin Provisioning, Deduplizierung und Datenkomprimierung, die die Speicherauslastung erhöhen und die Speicherkosten senken. Beim Erstellen von SEPs können Sie diese platzsparenden Technologien entweder einzeln oder zusammen verwenden, um maximale Speichereffizienz zu erreichen. Wenn Sie die Richtlinien mit Ihren Speicher-Workloads verknüpfen, werden ihnen die angegebenen Richtlinieneinstellungen zugewiesen. Mit Unified Manager können Sie systemdefinierte und benutzerdefinierte SEPs zuweisen, um die Speicherressourcen in Ihrem Rechenzentrum zu optimieren.

Unified Manager bietet zwei systemdefinierte SEPs: High und Low. Diese SEPs sind auf die meisten Speicher-Workloads in einem Rechenzentrum anwendbar. Sie können jedoch Ihre eigenen Richtlinien erstellen, wenn die systemdefinierten SEPs Ihren Anforderungen nicht entsprechen.

Sie können einen SEP, der systemdefiniert ist oder derzeit einer Arbeitslast zugewiesen ist, nicht ändern. Sie können keinen SEP löschen, der einer Arbeitslast zugewiesen ist oder der einzige verfügbare SEP ist.

Auf der Seite „Speichereffizienzrichtlinien“ werden die verfügbaren SEPs aufgelistet und Sie können benutzerdefinierte SEPs hinzufügen, bearbeiten und löschen. Auf dieser Seite werden die folgenden Informationen angezeigt:

Feld	Beschreibung
Name	Name des SEP.
Typ	Ob die Richtlinie systemdefiniert oder benutzerdefiniert ist.
Platzreserve	Ob das Volume Thin Provisioning oder Thick Provisioning ist.
Deduplizierung	Ob die Deduplizierung für die Arbeitslast aktiviert ist: • Inline: Die Deduplizierung erfolgt während des Schreibens auf die Arbeitslast • Hintergrund: Deduplizierung erfolgt im Workload • Deaktivieren: Die Deduplizierung ist für die Arbeitslast deaktiviert
Komprimierung	Ob die Datenkomprimierung für die Arbeitslast aktiviert ist: • Inline: Die Datenkomprimierung erfolgt während des Schreibens in die Arbeitslast • Hintergrund: Die Datenkomprimierung erfolgt im Workload • Deaktivieren: Die Datenkomprimierung ist für die Arbeitslast deaktiviert
Arbeitslasten	Anzahl der Speicher-Workloads, denen das SEP zugewiesen wurde

Richtlinien zum Erstellen einer benutzerdefinierten Speichereffizienzrichtlinie

Wenn die vorhandenen SEPs die Richtlinienanforderungen für Ihre Speicher-Workloads nicht erfüllen, können Sie ein benutzerdefiniertes SEP erstellen. Es wird jedoch empfohlen, dass Sie versuchen, die systemdefinierten SEPs für Ihre Speicher-Workloads zu verwenden und nur bei Bedarf benutzerdefinierte SEPs zu erstellen.

Sie können den den Workloads zugewiesenen SEP auf der Seite „Alle Workloads“ und auf der Seite „Volume-/Integritätsdetails“ anzeigen. Sie können das Datenreduktionsverhältnis auf Clusterebene (ohne Snapshot-Kopien) basierend auf diesen Speichereffizienzen im Kapazitätsbereich auf dem Dashboard und in der Ansicht „Kapazität: Alle Cluster“ anzeigen.

Erstellen und Bearbeiten von Speichereffizienzrichtlinien

Wenn die systemdefinierten Speichereffizienzrichtlinien nicht Ihren Workload-Anforderungen entsprechen, können Sie Ihre eigenen Speichereffizienzrichtlinien erstellen, die für Ihre Workloads optimiert sind.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.
- Der Name der Speichereffizienzrichtlinie muss eindeutig sein und Sie können die folgenden reservierten Schlüsselwörter nicht verwenden:

High, Low, Unassigned, Learning, Idle, Default, Und None.

Sie erstellen und bearbeiten benutzerdefinierte Speichereffizienzrichtlinien auf der Seite „Speichereffizienzrichtlinien“, indem Sie die Speichereffizienzmerkmale definieren, die Sie für die Anwendungen benötigen, die auf den Speicher zugreifen.



Sie können eine Speichereffizienzrichtlinie nicht ändern, wenn sie derzeit einer Arbeitslast zugewiesen ist.

Schritte

1. Wählen Sie im linken Navigationsbereich unter **Einstellungen Richtlinien > Speichereffizienz** aus.
2. Klicken Sie auf der Seite **Speichereffizienzrichtlinien** auf die entsprechende Schaltfläche, je nachdem, ob Sie eine neue Speichereffizienzrichtlinie erstellen oder eine vorhandene Speichereffizienzrichtlinie bearbeiten möchten.

Zu...	Befolgen Sie diese Schritte...
Erstellen einer neuen Speichereffizienzrichtlinie	Klicken Sie auf Hinzufügen
Bearbeiten einer vorhandenen Speichereffizienzrichtlinie	Wählen Sie eine vorhandene Speichereffizienzrichtlinie aus und klicken Sie auf Bearbeiten

Die Seite zum Hinzufügen oder Bearbeiten einer Speichereffizienzrichtlinie wird angezeigt.

3. Passen Sie die Speichereffizienzrichtlinie an, indem Sie die Speichereffizienzmerkmale angeben, und klicken Sie dann auf **Senden**, um die Speichereffizienzrichtlinie zu speichern.

Sie können die neue oder geänderte Speichereffizienzrichtlinie auf Workloads (LUNs, NFS-Dateifreigaben, CIFS-Freigaben) von der Seite „Workloads“ oder beim Bereitstellen eines neuen Workloads anwenden.

Verwalten und Überwachen von MetroCluster -Konfigurationen

Die Überwachungsunterstützung für MetroCluster -Konfigurationen in der Unified Manager-Web-Benutzeroberfläche ermöglicht es Ihnen, Ihre MetroCluster Konfigurationen über FC und IP auf Verbindungsprobleme zu überprüfen. Durch die frühzeitige Erkennung eines Konnektivitätsproblems können Sie Ihre MetroCluster -Konfigurationen effektiv verwalten.

Lautstärkeverhalten beim Umschalten und Zurückschalten

Ereignisse, die ein Switchover oder Switchback auslösen, führen dazu, dass aktive

Volumes von einem Cluster in den anderen Cluster in der Disaster Recovery-Gruppe verschoben werden. Die Volumes auf dem Cluster, die aktiv waren und Daten an Clients übermittelt haben, werden gestoppt, und die Volumes auf dem anderen Cluster werden aktiviert und beginnen mit der Datenübermittlung. Unified Manager überwacht nur die Volumes, die aktiv und aktiv sind.

Da Volumes von einem Cluster in einen anderen verschoben werden, wird empfohlen, beide Cluster zu überwachen. Eine einzelne Instanz von Unified Manager kann beide Cluster in einer MetroCluster-Konfiguration überwachen, aber manchmal erfordert die Entfernung zwischen den beiden Standorten die Verwendung von zwei Unified Manager-Instanzen zur Überwachung beider Cluster. Die folgende Abbildung zeigt eine einzelne Instanz von Unified Manager:

Die Volumes mit p im Namen geben die primären Volumes an, und die Volumes mit b im Namen sind gespiegelte Sicherungsvolumes, die von SnapMirror erstellt werden.

Während des Normalbetriebs:

- Cluster A hat zwei aktive Volumes: Vol1p und Vol2p.
- Cluster B hat zwei aktive Volumes: Vol3p und Vol4p.
- Cluster A hat zwei inaktive Volumes: Vol3b und Vol4b.
- Cluster B hat zwei inaktive Volumes: Vol1b und Vol2b.

Informationen zu jedem der aktiven Volumes (Statistiken, Ereignisse usw.) werden von Unified Manager gesammelt. Vol1p- und Vol2p-Statistiken werden von Cluster A und Vol3p- und Vol4p-Statistiken von Cluster B gesammelt.

Nach einem katastrophalen Fehler kommt es zu einer Umschaltung der aktiven Volumes von Cluster B zu Cluster A:

- Cluster A hat vier aktive Volumes: Vol1p, Vol2p, Vol3b und Vol4b.
- Cluster B hat vier inaktive Volumes: Vol3p, Vol4p, Vol1b und Vol2b.

Wie im Normalbetrieb werden Informationen zu jedem der aktiven Volumes vom Unified Manager erfasst. In diesem Fall werden die Statistiken zu Vol1p und Vol2p jedoch von Cluster A erfasst, und die Statistiken zu Vol3b und Vol4b werden ebenfalls von Cluster A erfasst.

Beachten Sie, dass Vol3p und Vol3b nicht dieselben Volumes sind, da sie sich auf unterschiedlichen Clustern befinden. Die Informationen im Unified Manager für Vol3p sind nicht dieselben wie für Vol3b:

- Während der Umstellung auf Cluster A sind Vol3p-Statistiken und -Ereignisse nicht sichtbar.
- Beim allerersten Umschalten sieht Vol3b wie ein neuer Band ohne historische Informationen aus.

Wenn Cluster B repariert ist und ein Switchback durchgeführt wird, ist Vol3p auf Cluster B wieder aktiv, mit den historischen Statistiken und einer Statistiklücke für den Zeitraum während der Umschaltung. Vol3b kann von Cluster A aus erst angezeigt werden, wenn eine weitere Umschaltung erfolgt:



- Inaktive MetroCluster Volumes, beispielsweise Vol3b auf Cluster A nach dem Switchback, werden mit der Meldung „Dieses Volume wurde gelöscht“ gekennzeichnet. Das Volume wird nicht wirklich gelöscht, wird aber derzeit nicht von Unified Manager überwacht, da es nicht das aktive Volume ist.
- Wenn ein einzelner Unified Manager beide Cluster in einer MetroCluster -Konfiguration überwacht, gibt die Volume-Suche Informationen zu dem Volume zurück, das zu diesem Zeitpunkt aktiv ist. Beispielsweise würde eine Suche nach „Vol3“ Statistiken und Ereignisse für Vol3b auf Cluster A zurückgeben, wenn eine Umschaltung stattgefunden hat und Vol3 auf Cluster A aktiv geworden ist.

Cluster-Konnektivitätsstatusdefinitionen für die MetroCluster über-FC-Konfiguration

Die Konnektivität zwischen den Clustern in einer MetroCluster -über-FC-Konfiguration kann einen der folgenden Status aufweisen: Optimal, Beeinträchtigt oder Ausgefallen. Wenn Sie den Verbindungsstatus verstehen, können Sie Ihre MetroCluster -Konfigurationen effektiv verwalten.

Verbindungsstatus	Beschreibung	Angezeigtes Symbol
Optimal	Die Konnektivität zwischen den Clustern in der MetroCluster -Konfiguration ist normal.	
Betroffen	Ein oder mehrere Fehler beeinträchtigen den Status der Failover-Verfügbarkeit; beide Cluster in der MetroCluster -Konfiguration sind jedoch noch aktiv. Zum Beispiel, wenn die ISL-Verbindung ausgefallen ist, wenn die IP-Verbindung zwischen den Clustern ausgefallen ist oder wenn der Partnercluster nicht erreichbar ist.	
Runter	Die Konnektivität zwischen den Clustern in der MetroCluster -Konfiguration ist unterbrochen, weil einer oder beide Cluster ausgefallen sind oder sich die Cluster im Failover-Modus befinden. Beispielsweise, wenn der Partnercluster aufgrund einer Katastrophe ausfällt oder wenn eine Umstellung zu Testzwecken geplant ist.	Umschaltung mit Fehlern:  Umschaltung erfolgreich: 

Datenspiegelungsstatusdefinitionen für MetroCluster über FC

MetroCluster über FC-Konfigurationen bieten Datenspiegelung und die zusätzliche Möglichkeit, ein Failover einzuleiten, wenn ein ganzer Standort nicht verfügbar ist. Der Status der Datenspiegelung zwischen den Clustern in einer MetroCluster über-FC-Konfiguration kann entweder „Normal“ oder „Spiegelung nicht verfügbar“ sein. Wenn Sie den Status kennen, können Sie Ihre MetroCluster -Konfigurationen effektiv verwalten.

Datenspiegelungsstatus	Beschreibung	Angezeigtes Symbol
Normal	Die Datenspiegelung zwischen den Clustern in der MetroCluster -Konfiguration ist normal.	
Spiegelung nicht verfügbar	Die Datenspiegelung zwischen den Clustern in der MetroCluster -Konfiguration ist aufgrund einer Umschaltung nicht verfügbar. Beispielsweise, wenn der Partnercluster aufgrund einer Katastrophe ausfällt oder wenn eine Umstellung zu Testzwecken geplant ist.	Umschaltung mit Fehlern:  Umschaltung erfolgreich: 

Überwachen Sie MetroCluster -Konfigurationen

Sie können Konnektivitätsprobleme in Ihrer MetroCluster -Konfiguration überwachen. Zu den Details gehören der Status der Komponenten und der Konnektivität innerhalb eines Clusters sowie der Konnektivitätsstatus zwischen den Clustern in der MetroCluster -Konfiguration. Hier erfahren Sie, wie Sie Konnektivitätsprobleme in Clustern überwachen, die durch MetroCluster over FC- und MetroCluster over IP-Konfigurationen geschützt sind.

Sie können die MetroCluster -Konfigurationen aus den folgenden Ansichten im linken Navigationsbereich des Active IQ Unified Manager überwachen:

- **Speicher > Cluster > Schutz: MetroCluster** anzeigen
- **Schutz > Beziehungen > Beziehung: MetroCluster** anzeigen

Unified Manager verwendet Systemzustandswarnungen, um den Status der Komponenten und der Konnektivität in der MetroCluster -Konfiguration anzuzeigen.

Bevor Sie beginnen

- Sowohl die lokalen als auch die Remote-Cluster in einer MetroCluster -Konfiguration müssen zu Active IQ Unified Manager hinzugefügt werden.

- Wenn in einer MetroCluster -over-IP-Konfiguration ein Mediator unterstützt werden soll, muss der Mediator konfiguriert und über die entsprechende API zum Cluster hinzugefügt werden.
- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Überwachen Sie Konnektivitätsprobleme in der MetroCluster über-FC-Konfiguration

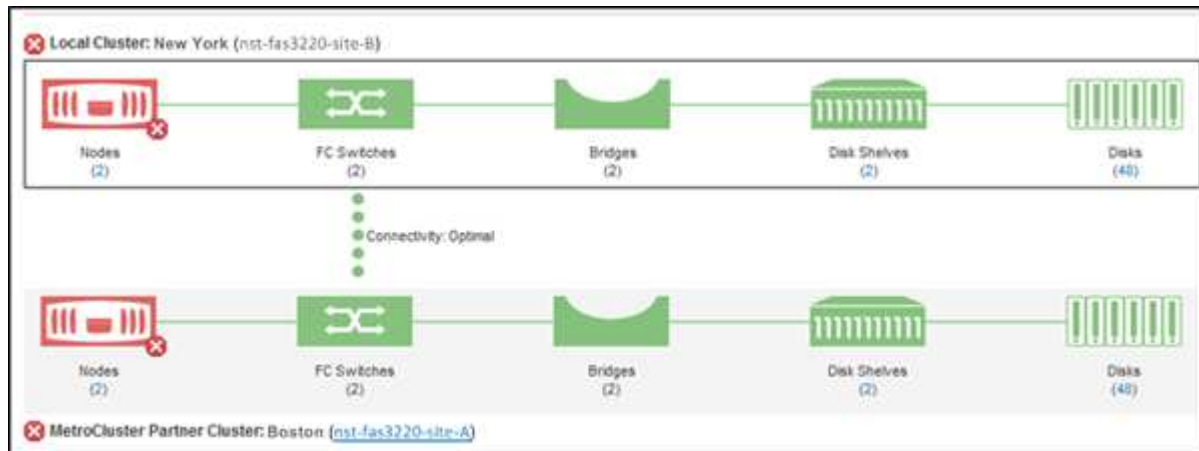
Für Cluster in einer MetroCluster -über-FC-Konfiguration werden die Konnektivitätsdiagramme auf der Detailseite **Cluster/Integrität** angezeigt. Befolgen Sie diese Schritte.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher > Cluster**.

Es wird eine Liste aller überwachten Cluster angezeigt.

2. Klicken Sie in der Ansicht **Schutz: MetroCluster** auf den Namen des Clusters, für den Sie die Konfigurationsdetails von MetroCluster über FC anzeigen möchten. Alternativ können Sie in einer MetroCluster -Konfiguration nach Clustern filtern.
3. Klicken Sie auf der Detailseite **Cluster/Integrität** auf die Registerkarte * MetroCluster -Konnektivität*. Die Registerkarte * MetroCluster -Konnektivität* ist nur für MetroCluster über-FC-Konfigurationen verfügbar.



Die Topologie der MetroCluster -Konfiguration wird im entsprechenden Cluster-Objektbereich angezeigt. Sie können die auf der Seite „Cluster-/Integritätsdetails“ angezeigten Informationen verwenden, um etwaige Verbindungsprobleme zu beheben. Wenn beispielsweise die Verbindung zwischen dem Knoten und dem Switch in einem Cluster unterbrochen ist, wird das folgende Symbol angezeigt:



Wenn Sie den Zeiger über das Symbol bewegen, können Sie detaillierte Informationen zum generierten Ereignis anzeigen.

Wenn Sie Konnektivitätsprobleme in Ihrer MetroCluster -Konfiguration feststellen, müssen Sie sich beim System Manager anmelden oder auf die ONTAP CLI zugreifen, um die Probleme zu beheben.

Weitere Informationen zum Bestimmen der Clusterintegrität finden Sie unter ["Bestimmen Sie die Clusterintegrität in der MetroCluster -über-FC-Konfiguration"](#).

Überwachen Sie Konnektivitätsprobleme in der MetroCluster -over-IP-Konfiguration

Für Cluster in einer MetroCluster -over-IP-Konfiguration werden die Konnektivitätsdiagramme auf der Seite **Cluster** angezeigt. Befolgen Sie diese Schritte.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher > Cluster**.

Es wird eine Liste aller überwachten Cluster angezeigt.

2. Klicken Sie in der Ansicht **Schutz: MetroClusters** auf den Namen des Clusters, für den Sie die Konfigurationsdetails von MetroCluster over IP anzeigen möchten. Alternativ können Sie in einer MetroCluster -Konfiguration nach Clustern filtern.
3. Erweitern Sie die Zeile, indem Sie auf das Caret-Symbol klicken ▾ Symbol. Das Caret-Symbol wird nur für einen Cluster angezeigt, der durch die MetroCluster over-IP-Konfiguration geschützt ist.

Sie können die Topologie der Quell- und Spiegelsites sowie den Mediator (sofern vorhanden) anzeigen, der für die Verbindung verwendet wird. Sie können die folgenden Informationen anzeigen:

- Konnektivität zwischen den Standorten
- Gesundheits- und Verfügbarkeitsprobleme, falls vorhanden, auf beiden Websites
- Mediatorbezogene Probleme
- Replikationsbezogene Probleme.



Die folgenden Status werden gemeldet: Kritisch (❌), Fehler (⚠️) oder Normal (✅). Sie können auch den aggregierten Datenreplikationsstatus der Primär- und Spiegeldaten in derselben Topologie anzeigen.

Im folgenden Diagramm können Sie sehen, dass die standortübergreifende Konnektivität zwischen den Quell- und Zielclustern nicht verfügbar ist und der Mediator zwischen ihnen nicht konfiguriert ist.



4. Klicken Sie auf das Statussymbol. Es wird eine Meldung mit der Fehlerdefinition angezeigt. Wenn für das Problem in Ihrer MetroCluster over IP-Konfiguration ein Ereignis ausgelöst wurde, können Sie in der Nachricht auf die Schaltfläche **Ereignis anzeigen** klicken und die Ereignisdetails anzeigen. Wenn Sie das

Problem und das Ereignis behoben haben, wechselt das Statussymbol in dieser Topologie zu „Normal“ (✓).

5. Weitere Konfigurationsdetails können Sie in den Abschnitten * MetroCluster -Übersicht* und **Schutz** auf der Registerkarte **Konfiguration** der Detailseite **Cluster/Integrität** anzeigen.



Nur bei einer MetroCluster -over-IP-Konfiguration können Sie die Clustertopologie auf der Seite **Cluster** anzeigen. Für Cluster in einer MetroCluster über-FC-Konfiguration wird die Topologie auf der Registerkarte * MetroCluster Konnektivität* auf der Detailseite **Cluster/Integrität** angezeigt.

Verwandte Informationen

- ["Cluster-/Integritätsdetailseite"](#)
- Informationen zur Ansicht **Relationship: MetroCluster** finden Sie unter ["Überwachen Sie MetroCluster -Konfigurationen"](#) .
- Informationen zur Ansicht **Beziehung: Transferstatus des letzten Monats** finden Sie unter ["Beziehung: Ansicht des Übertragungsstatus des letzten Monats"](#) .
- Informationen zur Ansicht **Beziehung: Übertragungsrate des letzten Monats** finden Sie unter ["Beziehung: Ansicht der Übertragungsrate des letzten Monats"](#) .
- Informationen zur Ansicht **Beziehung: Alle Beziehungen** finden Sie unter ["Beziehung: Ansicht „Alle Beziehungen“"](#) .

Überwachen der MetroCluster -Replikation

Sie können den Gesamtzustand der logischen Verbindungen überwachen und diagnostizieren, während Sie die Daten spiegeln. Sie können die Probleme oder Risiken identifizieren, die die Spiegelung von Clusterkomponenten wie Aggregaten, Knoten und virtuellen Speichermaschinen unterbrechen.

Unified Manager verwendet Systemzustandswarnungen, um den Status der Komponenten und der Konnektivität in der MetroCluster -Konfiguration zu überwachen.

Bevor Sie beginnen

Sowohl der lokale als auch der Remote-Cluster in der MetroCluster -Konfiguration müssen zu Unified Manager hinzugefügt werden

Anzeigen der Replikation für MetroCluster über IP-Konfigurationen

Bei MetroCluster over IP-Konfigurationen wird der Datenreplikationsstatus in der Topologie-Vorschauansicht für einen durch MetroCluster over IP geschützten Cluster aus den folgenden Ansichten im linken Navigationsbereich des Unified Manager angezeigt:

- **Speicher > Cluster > Schutz: MetroCluster** anzeigen
- **Schutz > Beziehungen > Beziehung: MetroCluster** anzeigen

Weitere Informationen finden Sie unter ["Überwachen Sie Konnektivitätsprobleme in MetroCluster über IP"](#) .

Anzeigen der Replikation für MetroCluster über FC-Konfigurationen

Befolgen Sie diese Schritte, um etwaige Probleme bei der Datenreplikation für die MetroCluster über-FC-

Konfiguration zu ermitteln.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher > Cluster**.

Es wird eine Liste der überwachten Cluster angezeigt.

2. Klicken Sie in der Ansicht **Health: All Clusters** auf den Namen des Clusters, für den Sie die MetroCluster Replikationsdetails anzeigen möchten. Klicken Sie auf der Seite **Cluster-/Integritätsdetails** auf die Registerkarte * MetroCluster -Replikation*.

Die Topologie der zu replizierenden MetroCluster Konfiguration wird am lokalen Standort im entsprechenden Cluster-Objektbereich mit den Informationen zum Remote-Standort angezeigt, an dem die Daten gespiegelt werden. Wenn Sie den Zeiger über das Symbol bewegen, können Sie detaillierte Informationen zum generierten Ereignis anzeigen.

Sie können die auf der Seite „Cluster-/Integritätsdetails“ angezeigten Informationen verwenden, um etwaige Replikationsprobleme zu beheben. Wenn Sie Spiegelungsprobleme in Ihrer MetroCluster -Konfiguration feststellen, müssen Sie sich beim System Manager anmelden oder auf die ONTAP CLI zugreifen, um die Probleme zu beheben.

Verwandte Informationen

["Cluster-/Integritätsdetailseite"](#)

Verwalten von Kontingenten

Mithilfe von Benutzer- und Gruppenkontingenten können Sie den Speicherplatz oder die Anzahl der Dateien begrenzen, die ein Benutzer oder eine Benutzergruppe verwenden kann. Sie können Kontingentinformationen zu Benutzern und Benutzergruppen anzeigen, beispielsweise die Festplatten- und Dateinutzung und die verschiedenen für Festplatten festgelegten Beschränkungen.

Welche Kontingentgrenzen gibt es

Benutzerkontingentgrenzen sind Werte, die der Unified Manager-Server verwendet, um zu bewerten, ob sich der Speicherplatzverbrauch eines Benutzers der Grenze nähert oder die durch die Benutzerkontingentgrenze festgelegte Grenze erreicht hat. Wenn das weiche Limit überschritten oder das harte Limit erreicht wird, generiert der Unified Manager-Server Benutzerkontingentereignisse.

Standardmäßig sendet der Unified Manager-Server eine Benachrichtigungs-E-Mail an Benutzer, die das weiche Kontingentlimit überschritten oder das harte Kontingentlimit erreicht haben und für die Benutzerkontingentereignisse konfiguriert sind. Benutzer mit der Rolle „Anwendungsadministrator“ können Warnmeldungen konfigurieren, die die angegebenen Empfänger über Benutzer- oder Benutzergruppenkontingentereignisse benachrichtigen.

Sie können Kontingentgrenzen entweder mit dem ONTAP System Manager oder der ONTAP CLI festlegen.

Anzeigen von Benutzer- und Benutzergruppenkontingenten

Auf der Seite „Storage VM / Health Details“ werden Informationen zu den Benutzer- und Benutzergruppenkontingenten angezeigt, die auf der SVM konfiguriert sind. Sie können den Namen des Benutzers oder der Benutzergruppe, die für die Datenträger und Dateien festgelegten Beschränkungen, den verwendeten Datenträger- und Dateispeicherplatz sowie die E-Mail-Adresse für Benachrichtigungen anzeigen.

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher > Speicher-VMs**.
2. Wählen Sie in der Ansicht **Integrität: Alle Storage-VMs** eine Storage-VM aus und klicken Sie dann auf die Registerkarte **Benutzer- und Gruppenkontingente**.

Verwandte Informationen

["Benutzer hinzufügen"](#)

Erstellen Sie Regeln zum Generieren von E-Mail-Adressen

Sie können Regeln erstellen, um die E-Mail-Adresse basierend auf dem Benutzerkontingent anzugeben, das Clustern, virtuellen Speichermaschinen (SVMs), Volumes, Qtrees, Benutzern oder Benutzergruppen zugeordnet ist. Bei einer Quotenüberschreitung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Richtlinien auf der Seite „Regeln zum Generieren von E-Mail-Adressen für Benutzer- und Gruppenkontingente“ gelesen haben.

Sie müssen die Regeln für Kontingent-E-Mail-Adressen definieren und sie in der Reihenfolge eingeben, in der Sie sie ausführen möchten. Wenn Sie beispielsweise die E-Mail-Adresse [abc@xyz.com](#) verwenden möchten, um Benachrichtigungen über Kontingentverletzungen für abc zu erhalten, und die E-Mail-Adresse dl-\$GROUP@\$DOMAIN für alle anderen Gruppen verwenden möchten, müssen die Regeln in der folgenden Reihenfolge aufgeführt werden:

- wenn (\$USER == 'abc') dann [abc@xyz.com](#)
- wenn (\$GROUP == *) dann dl-\$GROUP@\$DOMAIN

Wenn keines der Kriterien der von Ihnen angegebenen Regeln erfüllt ist, wird die Standardregel verwendet:

wenn (\$USER_OR_GROUP == *) dann \$USER_OR_GROUP@\$DOMAIN

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein > Kontingent-E-Mail-Regeln**.
2. Geben Sie die Regel basierend auf Ihren Kriterien ein.

3. Klicken Sie auf **Validieren**, um die Syntax der Regel zu validieren.

Wenn die Syntax der Regel falsch ist, wird eine Fehlermeldung angezeigt. Sie müssen die Syntax korrigieren und erneut auf **Validieren** klicken.

4. Klicken Sie auf **Speichern**.
5. Überprüfen Sie, ob die von Ihnen erstellte E-Mail-Adresse auf der Registerkarte „Benutzer- und Gruppenkontingente“ der Detailseite „Speicher-VM/Integrität“ angezeigt wird.

Erstellen Sie ein E-Mail-Benachrichtigungsformat für Benutzer- und Benutzergruppenkontingente

Sie können ein Benachrichtigungsformat für die E-Mails erstellen, die an einen Benutzer oder eine Benutzergruppe gesendet werden, wenn ein kontingentbezogenes Problem vorliegt (weiches Limit überschritten oder hartes Limit erreicht).

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein > Kontingent-E-Mail-Format**.
2. Geben Sie die Details in den Feldern **Von**, **Betreff** und **E-Mail-Details** ein oder ändern Sie sie.
3. Klicken Sie auf **Vorschau**, um eine Vorschau der E-Mail-Benachrichtigung anzuzeigen.
4. Klicken Sie auf **Schließen**, um das Vorschaufenster zu schließen.
5. Ändern Sie bei Bedarf den Inhalt der E-Mail-Benachrichtigung.
6. Klicken Sie auf **Speichern**.

Bearbeiten Sie die E-Mail-Adressen der Benutzer- und Gruppenkontingente

Sie können die E-Mail-Adressen basierend auf dem Benutzerkontingent ändern, das Clustern, virtuellen Speichermaschinen (SVMs), Volumes, Qtrees, Benutzern oder Benutzergruppen zugeordnet ist. Sie können die E-Mail-Adresse ändern, wenn Sie die E-Mail-Adresse überschreiben möchten, die durch die im Dialogfeld „Regeln zum Generieren von E-Mail-Adressen für Benutzer- und Gruppenkontingente“ angegebenen Regeln generiert wurde.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die [Richtlinien zum Erstellen von Regeln](#) .

Wenn Sie eine E-Mail-Adresse bearbeiten, gelten die Regeln zum Generieren der E-Mail-Adressen für Benutzer- und Gruppenkontingente nicht mehr für das Kontingent. Damit Benachrichtigungen an die durch die angegebenen Regeln generierte E-Mail-Adresse gesendet werden, müssen Sie die E-Mail-Adresse löschen und die Änderung speichern.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher > SVMs**.

2. Wählen Sie in der Ansicht **Health: All Storage VMs** eine SVM aus und klicken Sie dann auf die Registerkarte **User and Group Quotas**.
3. Klicken Sie unterhalb der Registerkartenreihe auf **E-Mail-Adresse bearbeiten**.
4. Führen Sie im Dialogfeld **E-Mail-Adresse bearbeiten** die entsprechende Aktion aus:

Wenn...	Dann...
Sie möchten, dass Benachrichtigungen an die E-Mail-Adresse gesendet werden, die durch die angegebenen Regeln generiert wurde	a. Löschen Sie die E-Mail-Adresse im Feld E-Mail-Adresse. b. Klicken Sie auf Speichern. c. Aktualisieren Sie den Browser, indem Sie F5 drücken, um das Dialogfeld „E-Mail-Adresse bearbeiten“ neu zu laden. Die von der angegebenen Regel generierte E-Mail-Adresse wird im Feld E-Mail-Adresse angezeigt.
Sie möchten, dass Benachrichtigungen an eine bestimmte E-Mail-Adresse gesendet werden	a. Ändern Sie die E-Mail-Adresse im Feld E-Mail-Adresse. b. Klicken Sie auf Speichern. Die Regeln zum Generieren der E-Mail-Adressen für Benutzer- und Gruppenkontingente sind auf das Kontingent nicht mehr anwendbar.

Erfahren Sie mehr über Quoten

Wenn Sie die Konzepte zu Kontingenten verstehen, können Sie Ihre Benutzerkontingente und Benutzergruppenkontingente effizient verwalten.

Überblick über den Quotenprozess

Quoten können weich oder hart sein. Weiche Kontingente veranlassen ONTAP , eine Benachrichtigung zu senden, wenn bestimmte Grenzwerte überschritten werden, und harte Kontingente verhindern, dass ein Schreibvorgang erfolgreich ist, wenn bestimmte Grenzwerte überschritten werden.

Wenn ONTAP von einem Benutzer oder einer Benutzergruppe eine Anforderung zum Schreiben auf ein FlexVol volume erhält, prüft es, ob auf diesem Volume Kontingente für den Benutzer oder die Benutzergruppe aktiviert sind, und ermittelt Folgendes:

- Ob die harte Grenze erreicht wird

Wenn ja, schlägt der Schreibvorgang fehl, wenn das harte Limit erreicht ist und die Benachrichtigung zum harten Kontingent gesendet wird.

- Ob das Soft-Limit überschritten wird

Wenn ja, ist der Schreibvorgang erfolgreich, wenn das Soft-Limit überschritten wird und die Soft-Quota-Benachrichtigung gesendet wird.

- Ob ein Schreibvorgang das Soft-Limit nicht überschreitet

Wenn ja, ist der Schreibvorgang erfolgreich und es wird keine Benachrichtigung gesendet.

Informationen zu Kontingenten

Kontingente bieten eine Möglichkeit, den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien einzuschränken oder zu verfolgen. Sie legen Quoten fest, indem Sie `/etc/quotas` Datei. Kontingente werden auf ein bestimmtes Volume oder einen bestimmten Qtree angewendet.

Warum Sie Kontingente verwenden

Sie können Kontingente verwenden, um die Ressourcennutzung in FlexVol -Volumes zu begrenzen, eine Benachrichtigung zu senden, wenn die Ressourcennutzung bestimmte Werte erreicht, oder um die Ressourcennutzung zu verfolgen.

Sie legen aus folgenden Gründen ein Kontingent fest:

- Um den Speicherplatz oder die Anzahl der Dateien zu begrenzen, die von einem Benutzer oder einer Gruppe verwendet werden können oder die in einem Qtree enthalten sein können
- Um den Speicherplatz oder die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien zu verfolgen, ohne eine Begrenzung festzulegen
- Um Benutzer zu warnen, wenn ihre Festplatten- oder Dateinutzung hoch ist

Beschreibung der Kontingentdialogfelder

Sie können die entsprechende Option auf der Registerkarte „Benutzer- und Gruppenkontingente“ in der Ansicht „Integrität: Alle Speicher-VMs“ verwenden, um das Format der E-Mail-Benachrichtigung zu konfigurieren, die gesendet wird, wenn ein kontingentbezogenes Problem auftritt, und um Regeln zum Angeben von E-Mail-Adressen basierend auf dem Benutzerkontingent zu konfigurieren.

Seite „E-Mail-Benachrichtigungsformat“

Auf der Seite „E-Mail-Benachrichtigungsformat“ werden die Regeln der E-Mail angezeigt, die an einen Benutzer oder eine Benutzergruppe gesendet wird, wenn ein kontingentbezogenes Problem vorliegt (weiches Limit überschritten oder hartes Limit erreicht).

Die E-Mail-Benachrichtigung wird nur gesendet, wenn die folgenden Benutzer- oder Benutzergruppenkontingentereignisse generiert werden: Weiches Limit für Speicherplatz des Benutzer- oder Gruppenkontingents überschritten, Weiches Limit für Dateianzahl des Benutzer- oder Gruppenkontingents überschritten, Hartes Limit für Speicherplatz des Benutzer- oder Gruppenkontingents erreicht oder Hartes Limit für Dateianzahl des Benutzer- oder Gruppenkontingents erreicht.

- **Aus**

Zeigt die E-Mail-Adresse an, von der die E-Mail gesendet wird. Sie können diese Adresse ändern.

Standardmäßig ist dies die auf der Benachrichtigungsseite angegebene E-Mail-Adresse.

- **Thema**

Zeigt den Betreff der Benachrichtigungs-E-Mail an.

- **E-Mail-Details**

Zeigt den Text der Benachrichtigungs-E-Mail an. Sie können den Text Ihren Anforderungen entsprechend ändern. Sie können beispielsweise Informationen zu den Quotenattributen bereitstellen und die Anzahl der Schlüsselwörter reduzieren. Sie sollten die Schlüsselwörter jedoch nicht ändern.

Gültige Schlüsselwörter sind wie folgt:

- **\$EVENT_NAME**

Gibt den Ereignisnamen an, der die E-Mail-Benachrichtigung verursacht hat.

- **\$QUOTA_TARGET**

Gibt den Qtree oder das Volume an, auf das das Kontingent anwendbar ist.

- **\$QUOTA_USED_PERCENT**

Gibt den Prozentsatz des Festplatten-Hardlimits, des Festplatten-Softlimits, des Datei-Hardlimits oder des Datei-Softlimits an, der vom Benutzer oder der Benutzergruppe verwendet wird.

- **\$QUOTA_LIMIT**

Gibt das Festplattenlimit oder das Dateilimit an, das vom Benutzer oder der Benutzergruppe erreicht wird. Dabei wird eines der folgenden Ereignisse generiert:

- Hartes Limit für Benutzer- oder Gruppenkontingentspeicherplatz erreicht
- Soft-Limit für Benutzer- oder Gruppenkontingent-Festplattenspeicher erreicht
- Festes Limit für die Anzahl der Benutzer- oder Gruppenkontingentedateien erreicht
- Soft-Limit für die Anzahl der Benutzer- oder Gruppenkontingentedateien erreicht

- **\$QUOTA_USED**

Gibt den belegten Speicherplatz oder die Anzahl der vom Benutzer oder der Benutzergruppe erstellten Dateien an.

- **\$QUOTA_USER**

Gibt den Benutzer- oder Benutzergruppennamen an.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die am E-Mail-Benachrichtigungsformat vorgenommenen Änderungen in der Vorschau anzeigen, speichern oder abbrechen:

- **Vorschau**

Zeigt eine Vorschau der Benachrichtigungs-E-Mail an.

- **Auf Werkseinstellungen zurücksetzen**

Ermöglicht Ihnen, das Benachrichtigungsformat auf die werkseitigen Standardwerte zurückzusetzen.

- **Speichern**

Speichert die am Benachrichtigungsformat vorgenommenen Änderungen.

Regeln zum Generieren der Seite „Benutzer- und Gruppenkontingent-E-Mail-Adressen“

Auf der Seite „Regeln zum Generieren von E-Mail-Adressen mit Benutzer- und Gruppenkontingenten“ können Sie Regeln zum Angeben von E-Mail-Adressen basierend auf dem mit Clustern, SVMs, Volumes, Qtrees, Benutzern oder Benutzergruppen verknüpften Benutzerkontingent erstellen. Bei einer Quotenüberschreitung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

Regelbereich

Sie müssen die Regeln für eine Kontingent-E-Mail-Adresse definieren. Sie können auch Kommentare hinzufügen, um die Regeln zu erläutern.

So definieren Sie Regeln

Sie müssen die Regeln in der Reihenfolge eingeben, in der Sie sie ausführen möchten. Wenn das Kriterium der ersten Regel erfüllt ist, wird die E-Mail-Adresse basierend auf dieser Regel generiert. Wenn das Kriterium nicht erfüllt ist, wird das Kriterium für die nächste Regel berücksichtigt und so weiter. Jede Zeile listet eine separate Regel auf. Die Standardregel ist die letzte Regel in der Liste. Sie können die Prioritätsreihenfolge der Regeln ändern. Sie können die Reihenfolge der Standardregel jedoch nicht ändern.

Wenn Sie beispielsweise die E-Mail-Adresse qtree1@xyz.com verwenden möchten, um Benachrichtigungen über Kontingentverletzungen für qtree1 zu erhalten, und die E-Mail-Adresse admin@xyz.com für alle anderen qtrees verwenden möchten, müssen die Regeln in der folgenden Reihenfolge aufgeführt werden:

- wenn (\$QTREE == 'qtree1') dann qtree1@xyz.com
- wenn (\$QTREE == *) dann admin@xyz.com

Wenn keines der Kriterien der von Ihnen angegebenen Regeln erfüllt ist, wird die Standardregel verwendet:

wenn (\$USER_OR_GROUP == *) dann \$USER_OR_GROUP@\$DOMAIN

Wenn mehrere Benutzer über dasselbe Kontingent verfügen, werden die Namen der Benutzer als durch Kommas getrennte Werte angezeigt und die Regeln gelten nicht für das Kontingent.

So fügen Sie Kommentare hinzu

Sie können Kommentare hinzufügen, um die Regeln zu erläutern. Sie sollten am Anfang jedes Kommentars # verwenden und jede Zeile einen separaten Kommentar auflisten.

Regelsyntax

Die Syntax der Regel muss eine der folgenden sein:

- Wenn (valid variableoperator *) Dann email ID@domain name

if ist ein Schlüsselwort und wird in Kleinbuchstaben geschrieben. Der Operator ist ==. Die E-Mail-ID kann beliebige Zeichen, die gültigen Variablen \$USER_OR_GROUP, \$USER oder \$GROUP oder eine Kombination aus beliebigen Zeichen und den gültigen Variablen \$USER_OR_GROUP, \$USER oder \$GROUP enthalten. Der Domänenname kann ein beliebiges Zeichen, die gültige Variable \$DOMAIN oder eine Kombination aus einem beliebigen Zeichen und der gültigen Variable \$DOMAIN enthalten. Gültige Variablen können in Groß- oder Kleinbuchstaben geschrieben sein, dürfen aber keine Kombination aus beiden sein. Beispielsweise sind \$domain und \$DOMAIN gültig, aber \$Domain ist keine gültige Variable.

- Wenn (valid variableoperator `string`) Dann email ID@domain name

if ist ein Schlüsselwort und wird in Kleinbuchstaben geschrieben. Der Operator kann „enthält“ oder „==“ sein. Die E-Mail-ID kann ein beliebiges Zeichen, die gültigen Variablen \$USER_OR_GROUP, \$USER oder \$GROUP oder eine Kombination aus einem beliebigen Zeichen und den gültigen Variablen \$USER_OR_GROUP, \$USER oder \$GROUP enthalten. Der Domänenname kann ein beliebiges Zeichen, die gültige Variable \$DOMAIN oder eine Kombination aus einem beliebigen Zeichen und der gültigen Variable \$DOMAIN enthalten. Gültige Variablen können in Groß- oder Kleinbuchstaben geschrieben sein, dürfen aber keine Kombination aus beiden sein. Beispielsweise sind \$domain und \$DOMAIN gültig, aber \$Domain ist keine gültige Variable.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die erstellten Regeln speichern, bestätigen oder abbrechen:

- **Bestätigen**

Validiert die Syntax der erstellten Regel. Wenn bei der Validierung Fehler auftreten, wird die Regel, die den Fehler erzeugt, zusammen mit einer Fehlermeldung angezeigt.

- **Auf Werkseinstellungen zurücksetzen**

Ermöglicht Ihnen, die Adressregeln auf die werkseitigen Standardwerte zurückzusetzen.

- **Speichern**

Überprüft die Syntax der Regel und speichert die Regel, wenn keine Fehler vorliegen. Wenn bei der Validierung Fehler auftreten, wird die Regel, die den Fehler generiert, zusammen mit einer Fehlermeldung angezeigt.

Fehlerbehebung

Informationen zur Fehlerbehebung helfen Ihnen, Probleme zu identifizieren und zu lösen, die bei der Verwendung von Unified Manager auftreten.

Fügen Sie dem Unified Manager-Datenbankverzeichnis Speicherplatz hinzu

Das Unified Manager-Datenbankverzeichnis enthält alle von ONTAP -Systemen erfassten Integritäts- und Leistungsdaten. Unter bestimmten Umständen kann es erforderlich sein, dass Sie die Größe des Datenbankverzeichnisses erhöhen.

Beispielsweise kann das Datenbankverzeichnis voll werden, wenn Unified Manager Daten aus einer großen Anzahl von Clustern sammelt, wobei jeder Cluster viele Knoten hat. Sie erhalten ein Warnereignis, wenn das Datenbankverzeichnis zu 90 % voll ist, und ein kritisches Ereignis, wenn das Verzeichnis zu 95 % voll ist.



Wenn das Verzeichnis zu 95 % gefüllt ist, werden keine weiteren Daten mehr aus den Clustern erfasst.

Die zum Hinzufügen von Kapazität zum Datenverzeichnis erforderlichen Schritte unterscheiden sich, je nachdem, ob Unified Manager auf einem VMware ESXi-Server, einem Red Hat Linux-Server oder einem Microsoft Windows-Server ausgeführt wird.

Fügen Sie Speicherplatz zur Datenfestplatte der virtuellen VMware-Maschine hinzu

Wenn Sie den Speicherplatz auf der Datenfestplatte für die Unified Manager-Datenbank erhöhen müssen, können Sie nach der Installation Kapazität hinzufügen, indem Sie den Speicherplatz mithilfe der Unified Manager-Wartungskonsole erhöhen.

Bevor Sie beginnen

- Sie müssen Zugriff auf den vSphere-Client haben.
- Auf der virtuellen Maschine dürfen keine Snapshots lokal gespeichert sein.
- Sie müssen über die Anmeldeinformationen des Wartungsbenutzers verfügen.

Wir empfehlen Ihnen, Ihre virtuelle Maschine zu sichern, bevor Sie die Größe virtueller Festplatten erhöhen.

Schritte

1. Wählen Sie im vSphere-Client die virtuelle Maschine Unified Manager aus und fügen Sie dann mehr Festplattenkapazität zu Daten hinzu `disk 3`. Weitere Informationen finden Sie in der VMware-Dokumentation.

In einigen seltenen Fällen verwendet die Unified Manager-Bereitstellung „Festplatte 2“ für die Datenfestplatte anstelle von „Festplatte 3“. Wenn dies bei Ihrer Bereitstellung der Fall ist, erhöhen Sie den Speicherplatz auf der größeren Festplatte. Auf der Datenfestplatte ist immer mehr Speicherplatz vorhanden als auf der anderen Festplatte.

2. Wählen Sie im vSphere-Client die virtuelle Maschine Unified Manager und dann die Registerkarte **Konsole** aus.
3. Klicken Sie in das Konsolenfenster und melden Sie sich dann mit Ihrem Benutzernamen und Kennwort bei der Wartungskonsole an.
4. Geben Sie im **Hauptmenü** die Nummer für die Option **Systemkonfiguration** ein.
5. Geben Sie im **Systemkonfigurationsmenü** die Zahl für die Option **Datenträgergröße erhöhen** ein.

Fügen Sie dem Datenverzeichnis des Linux-Hosts Speicherplatz hinzu

Wenn Sie nicht genügend Speicherplatz für die `/opt/netapp/data` Verzeichnis zur Unterstützung von Unified Manager, wenn Sie den Linux-Host ursprünglich eingerichtet und dann Unified Manager installiert haben, können Sie nach der Installation Speicherplatz hinzufügen, indem Sie den Speicherplatz auf dem `/opt/netapp/data` Verzeichnis.

Bevor Sie beginnen

Sie müssen über Root-Benutzerzugriff auf die Red Hat Enterprise Linux-Maschine verfügen, auf der Unified Manager installiert ist.

Wir empfehlen, dass Sie die Unified Manager-Datenbank sichern, bevor Sie die Größe des Datenverzeichnisses erhöhen.

Schritte

1. Melden Sie sich als Root-Benutzer bei der Linux-Maschine an, auf der Sie Speicherplatz hinzufügen möchten.
2. Stoppen Sie den Unified Manager-Dienst und die zugehörige MySQL-Software in der angezeigten Reihenfolge: `systemctl stop ocieau ocie mysqld`
3. Erstellen Sie einen temporären Sicherungsordner (z. B. `/backup-data`) mit ausreichend Speicherplatz, um die Daten im aktuellen `/opt/netapp/data` Verzeichnis.
4. Kopieren Sie den Inhalt und die Berechtigungskonfiguration des bestehenden `/opt/netapp/data` Verzeichnis in das Sicherungsdatenverzeichnis:

```
cp -arp /opt/netapp/data/* /backup-data
```

5. Wenn SE Linux aktiviert ist:

- a. Holen Sie sich den SE Linux-Typ für Ordner auf vorhandenen `/opt/netapp/data` Ordner:

```
se_type=`ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1
```

Das System gibt eine Bestätigung ähnlich der folgenden zurück:

```
echo $se_type  
mysqld_db_t
```

- a. Führen Sie den `chcon` Befehl zum Festlegen des SE Linux-Typs für das Sicherungsverzeichnis:

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Entfernen Sie den Inhalt des `/opt/netapp/data` Verzeichnis:

- a. `cd /opt/netapp/data`
- b. `rm -rf *`

7. Erweitern Sie die Größe des `/opt/netapp/data` Verzeichnis auf mindestens 150 GB durch LVM-Befehle oder durch Hinzufügen zusätzlicher Festplatten.



Wenn Sie erstellt haben `/opt/netapp/data` von einer Festplatte, dann sollten Sie nicht versuchen, zu mounten `/opt/netapp/data` als NFS- oder CIFS-Freigabe. Denn in diesem Fall, wenn Sie versuchen, den Speicherplatz zu erweitern, einige LVM-Befehle, wie zum Beispiel `resize` Und `extend` funktioniert möglicherweise nicht wie erwartet.

8. Bestätigen Sie, dass die `/opt/netapp/data` Verzeichnisbesitzer (mysql) und Gruppe (root) bleiben unverändert:

```
ls -ltr /opt/netapp/ | grep data
```

Das System gibt eine Bestätigung ähnlich der folgenden zurück:

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. Wenn SE Linux aktiviert ist, bestätigen Sie, dass der Kontext für die `/opt/netapp/data` Verzeichnis ist immer noch auf `mysql_d_b_t` eingestellt:

- a. `touch /opt/netapp/data/abc`
- b. `ls -Z /opt/netapp/data/abc`

Das System gibt eine Bestätigung ähnlich der folgenden zurück:

```
-rw-r--r--. root root unconfined_u:object_r:mysql_d_b_t:s0  
/opt/netapp/data/abc
```

10. Löschen Sie die Datei `abc` damit diese überflüssige Datei in Zukunft keinen Datenbankfehler verursacht.
11. Kopieren Sie den Inhalt von `backup-data` zurück zur erweiterten `/opt/netapp/data` Verzeichnis:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. Wenn SE Linux aktiviert ist, führen Sie den folgenden Befehl aus:

```
chcon -R --type=mysql_d_b_t /opt/netapp/data
```

13. Starten Sie den MySQL-Dienst:

```
systemctl start mysqld
```

14. Nachdem der MySQL-Dienst gestartet wurde, starten Sie die Dienste `ocie` und `ocieau` in der angezeigten Reihenfolge:

```
systemctl start ocie ocieau
```

15. Nachdem alle Dienste gestartet sind, löschen Sie den Sicherungsordner `/backup-data`:

```
rm -rf /backup-data
```

Fügen Sie dem logischen Laufwerk des Microsoft Windows-Servers Speicherplatz hinzu

Wenn Sie den Speicherplatz für die Unified Manager-Datenbank erhöhen müssen, können Sie die Kapazität des logischen Laufwerks erhöhen, auf dem Unified Manager installiert ist.

Bevor Sie beginnen

Sie müssen über Windows-Administratorrechte verfügen.

Wir empfehlen Ihnen, die Unified Manager-Datenbank zu sichern, bevor Sie Speicherplatz hinzufügen.

Schritte

1. Melden Sie sich als Administrator bei dem Windows-Server an, auf dem Sie Speicherplatz hinzufügen möchten.
2. Führen Sie den Schritt aus, der der Methode entspricht, mit der Sie mehr Speicherplatz hinzufügen möchten:

Option	Beschreibung
Erhöhen Sie auf einem physischen Server die Kapazität des logischen Laufwerks, auf dem der Unified Manager-Server installiert ist.	Befolgen Sie die Schritte im Microsoft-Thema: "Erweitern eines Basisvolumes"
Fügen Sie auf einem physischen Server ein Festplattenlaufwerk hinzu.	Befolgen Sie die Schritte im Microsoft-Thema: "Hinzufügen von Festplattenlaufwerken"
Erhöhen Sie auf einer virtuellen Maschine die Größe einer Festplattenpartition.	Befolgen Sie die Schritte im VMware-Thema: "Erhöhen der Größe einer Festplattenpartition"

Ändern des Erfassungsintervalls für Leistungsstatistiken

Das Standarderfassungsintervall für Leistungsstatistiken beträgt 5 Minuten. Sie können dieses Intervall auf 10 oder 15 Minuten ändern, wenn Sie feststellen, dass Sammlungen aus großen Clustern nicht innerhalb der Standardzeit abgeschlossen werden. Diese Einstellung wirkt sich auf die Erfassung von Statistiken aus allen Clustern aus, die diese Instanz von Unified Manager überwacht.

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.

Das Problem, dass die Erfassung von Leistungsstatistiken nicht rechtzeitig abgeschlossen wird, wird durch die Bannermeldungen angezeigt `Unable to consistently collect from cluster <cluster_name>` or `Data collection is taking too long on cluster <cluster_name>`.

Sie sollten das Erfassungsintervall nur ändern, wenn dies aufgrund eines Problems bei der Statistikerfassung erforderlich ist. Ändern Sie diese Einstellung aus keinem anderen Grund.



Das Ändern dieses Werts von der Standardeinstellung von 5 Minuten kann sich auf die Anzahl und Häufigkeit der von Unified Manager gemeldeten Leistungsereignisse auswirken. Beispielsweise lösen systemdefinierte Leistungsschwellenwerte Ereignisse aus, wenn die Richtlinie 30 Minuten lang überschritten wird. Bei der Verwendung von 5-Minuten-Sammlungen muss die Richtlinie bei sechs aufeinanderfolgenden Sammlungen überschritten werden. Bei 15-Minuten-Abholungen darf die Richtlinie nur für zwei Abholperioden überschritten werden.

Eine Meldung unten auf der Seite „Cluster-Setup“ gibt das aktuelle Intervall zur Erfassung statistischer Daten an.

Schritte

1. Melden Sie sich per SSH als Wartungsbenutzer beim Unified Manager-Host an.

Die Eingabeaufforderungen der Unified Manager-Wartungskonsole werden angezeigt.

2. Geben Sie die Nummer der Menüoption mit der Bezeichnung **Konfiguration des Leistungsabfrageintervalls** ein und drücken Sie dann die Eingabetaste.
3. Geben Sie bei entsprechender Aufforderung das Wartungsbenutzerkennwort erneut ein.
4. Geben Sie die Zahl für das neue Abfrageintervall ein, das Sie festlegen möchten, und drücken Sie dann die Eingabetaste.

Wenn Sie das Erfassungsintervall des Unified Managers auf 10 oder 15 Minuten geändert haben und über eine aktuelle Verbindung zu einem externen Datenanbieter (z. B. Graphite) verfügen, müssen Sie das Übertragungsintervall des Datenanbieters so ändern, dass es gleich oder größer als das Erfassungsintervall des Unified Managers ist.

Ändern Sie die Dauer, für die Unified Manager Ereignis- und Leistungsdaten speichert

Standardmäßig speichert Unified Manager Ereignisdaten und Leistungsdaten für alle überwachten Cluster 6 Monate lang. Nach Ablauf dieser Zeit werden ältere Daten automatisch gelöscht, um Platz für neue Daten zu schaffen. Dieser Standardzeitrahmen funktioniert für die meisten Konfigurationen gut, aber bei sehr großen Konfigurationen mit vielen Clustern und Knoten muss der Aufbewahrungszeitraum möglicherweise verkürzt werden, damit Unified Manager optimal funktioniert.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Sie können die Aufbewahrungszeiträume für diese beiden Datentypen auf der Seite „Datenaufbewahrung“ ändern. Diese Einstellungen wirken sich auf die Aufbewahrung von Daten aus allen Clustern aus, die diese Instanz von Unified Manager überwacht.



Unified Manager sammelt alle 5 Minuten Leistungsstatistiken. Jeden Tag werden die 5-Minuten-Statistiken zu stündlichen Leistungsstatistiken zusammengefasst. Es speichert 30 Tage lang 5-minütige historische Leistungsdaten und 6 Monate lang stündlich zusammengefasste Leistungsdaten (standardmäßig).

Sie sollten die Aufbewahrungsfrist nur dann verkürzen, wenn der Speicherplatz knapp wird oder die Sicherung und andere Vorgänge sehr lange dauern. Die Verkürzung der Aufbewahrungsfrist hat folgende Auswirkungen:

- Alte Leistungsdaten werden nach Mitternacht aus der Unified Manager-Datenbank gelöscht.
- Alte Ereignisdaten werden sofort aus der Unified Manager-Datenbank gelöscht.
- Ereignisse vor Ablauf der Aufbewahrungsfrist können in der Benutzeroberfläche nicht mehr angezeigt werden.
- Stellen in der Benutzeroberfläche, an denen stündliche Leistungsstatistiken angezeigt werden, sind vor Ablauf der Aufbewahrungsfrist leer.
- Wenn die Aufbewahrungsdauer des Ereignisses die Aufbewahrungsdauer der Leistungsdaten überschreitet, wird unter dem Leistungsschieberegler eine Meldung angezeigt, die darauf hinweist, dass für ältere Leistungsereignisse möglicherweise keine Hintergrunddaten in den zugehörigen Diagrammen vorhanden sind.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Richtlinien > Datenaufbewahrung**.
2. Wählen Sie auf der Seite **Datenaufbewahrung** das Schieberegler-Tool im Bereich „Ereignisaufbewahrung“ oder „Aufbewahrung von Leistungsdaten“ aus, verschieben Sie es auf die Anzahl der Monate, für die die Daten aufbewahrt werden sollen, und klicken Sie auf **Speichern**.

Unbekannter Authentifizierungsfehler

Wenn Sie einen authentifizierungsbezogenen Vorgang ausführen, z. B. Remotebenutzer oder -gruppen hinzufügen, bearbeiten, löschen oder testen, wird möglicherweise die folgende Fehlermeldung angezeigt: `Unknown authentication error`.

Ursache

Dieses Problem kann auftreten, wenn Sie für die folgenden Optionen einen falschen Wert festgelegt haben:

- Administratorname des Active Directory-Authentifizierungsdienstes
- Bind Distinguished Name des OpenLDAP-Authentifizierungsdienstes

Korrekturmaßnahme

1. Klicken Sie im linken Navigationsbereich auf **Allgemein > Remote-Authentifizierung**.
2. Geben Sie basierend auf dem von Ihnen ausgewählten Authentifizierungsdienst die entsprechenden Informationen für den Administratornamen oder den Bind Distinguished Name ein.
3. Klicken Sie auf **Authentifizierung testen**, um die Authentifizierung mit den von Ihnen angegebenen Details zu testen.
4. Klicken Sie auf **Speichern**.

Benutzer nicht gefunden

Wenn Sie einen authentifizierungsbezogenen Vorgang ausführen, z. B. Remotebenutzer oder -gruppen hinzufügen, bearbeiten, löschen oder testen, wird die folgende Fehlermeldung angezeigt: `User not found`.

Ursache

Dieses Problem kann auftreten, wenn der Benutzer auf dem AD-Server oder LDAP-Server vorhanden ist und Sie den Basis-Distinguished Name auf einen falschen Wert festgelegt haben.

Korrekturmaßnahme

1. Klicken Sie im linken Navigationsbereich auf **Allgemein > Remote-Authentifizierung**.
2. Geben Sie die entsprechenden Informationen für den Basis-Distinguished Name ein.
3. Klicken Sie auf **Speichern**.

Problem beim Hinzufügen von LDAP mithilfe anderer Authentifizierungsdienste

Wenn Sie „Andere“ als Authentifizierungsdienst auswählen, behalten die Benutzer- und Gruppenobjektklassen die Werte aus der zuvor ausgewählten Vorlage bei. Wenn der

LDAP-Server nicht dieselben Werte verwendet, kann der Vorgang fehlschlagen.

Ursache

Die Benutzer sind in OpenLDAP nicht richtig konfiguriert.

Korrekturmaßnahme

Sie können dieses Problem manuell beheben, indem Sie eine der folgenden Problemumgehungen verwenden.

Wenn Ihre LDAP-Benutzerobjektklasse und Gruppenobjektklasse „Benutzer“ bzw. „Gruppe“ sind, führen Sie die folgenden Schritte aus:

1. Klicken Sie im linken Navigationsbereich auf **Allgemein > Remote-Authentifizierung**.
2. Wählen Sie im Dropdown-Menü **Authentifizierungsdienst** die Option **Active Directory** und dann **Andere** aus.
3. Füllen Sie die Textfelder aus.

Wenn Ihre LDAP-Benutzerobjektklasse und Gruppenobjektklasse „posixAccount“ bzw. „posixGroup“ sind, führen Sie die folgenden Schritte aus:

1. Klicken Sie im linken Navigationsbereich auf **Allgemein > Remote-Authentifizierung**.
2. Wählen Sie im Dropdown-Menü **Authentifizierungsdienst** die Option **OpenLDAP** und dann **Andere** aus.
3. Füllen Sie die Textfelder aus.

Wenn die ersten beiden Workarounds nicht funktionieren, rufen Sie den `option-set` API und legen Sie die `auth.ldap.userObjectClass` Und `auth.ldap.groupObjectClass` Optionen auf die richtigen Werte.

Problem mit der Protokollrotation des NetApp Manageability SDK auf Windows-Systemen

Nachdem Sie einen ONTAPI API-basierten Cluster zu Unified Manager auf einem Windows-Betriebssystem hinzugefügt haben, `nmsdk.log` Die Dateigröße nimmt zu und überschreitet die Größenbeschränkung von 10 MB.

Ursache

Dieses Problem kann auftreten, wenn keine Protokollrotation stattfindet.

Korrekturmaßnahme

1. Stoppen Sie Unified Manager.
2. Wenn Sie Unified Manager unter Windows installieren, installieren Sie Logrotate Version 0.0.0.18. Weitere Informationen finden Sie im ["Leitfaden zur Sicherheitshärtung für den technischen Bericht zum NetApp Manageability SDK"](#) .
3. Starten Sie Unified Manager.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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