OnCommand Unified Manager Dokumentation

OnCommand Unified Manager 9.5

NetApp
December 20, 2023

This PDF was generated from https://docs.netapp.com/de-de/oncommand-unified-manager-95/index.html on December 20, 2023. Always check docs.netapp.com for the latest.

Inhalt

OnCommand Unified Manager Dokumentation . . . 1
Versionshinweise . . . 2
Los geht's . . . 3
- Schnellstartanleitung für VMware Installationen . . . 3
- Kurzanleitung für Linux-Installationen . . . 4
- Kurzanleitung für Windows-Installationen . . . 5

Installation Von Unified Manager . . . 6
- Einführung in OnCommand Unified Manager . . . 6
- Anforderungen für die Installation von Unified Manager . . . 7
- Installation, Upgrade und Entfernung der Unified Manager Software unter VMware vSphere . . . 18
- Installation, Aktualisierung und Entfernung der Unified Manager Software unter Red hat oder CentOS . . . 27
- Installieren, Aktualisieren und Entfernen der Unified Manager-Software unter Windows . . . 49

Durchführung von Konfigurations- und Administrationsaufgaben . . . 62
- Konfigurieren Von Unified Manager . . . 62

Online-Hilfe . . . 90
- Einführung in OnCommand Unified Manager . . . 90
- Allgemeines zur Benutzeroberfläche . . . 97
- Monitoring des Clusterzustands und der Performance über die Dashboards . . . 105
- Verwalten von Speicherobjekten mit der Option Favoriten . . . 114
- Verwalten von Ereignissen . . . 118
- Verwalten von Meldungen . . . 210
- Verwalten von Skripten . . . 224
- Verwalten von Systemzustandsschwellenwerten . . . 233
- Verwalten von benutzerdefinierten Performance-Schwellenwerten . . . 252
- Analyse von Performance-Ereignissen . . . 268
- Lösen von Leistungsereignissen . . . 284
- Management von Kontingenten . . . 311
- Verwalten und Überwachen der Cluster- und Cluster-Objektintegrität . . . 319
- Verwalten und Überwachen von MetroCluster Konfigurationen . . . 423
- Verwalten von Anmerkungen für Speicherobjekte . . . 432
- Verwalten und Überwachen von Gruppen . . . 451
- Managen und Überwachen von Sicherungsbeziehungen . . . 473
- Ausführen von Sicherungs-Workflows mithilfe von OnCommand Workflow Automation . . . 555
- Performance-Management mithilfe von Performance-Kapazität und verfügbaren IOPS-Informationen . . . 558
- Monitoring der Cluster-Performance über die Startseite des Performance Cluster . . . 567
- Überwachung der Performance mithilfe der Seiten „Performance Inventory“ (Performance-Bestandsaufnahme . . . 572
- Überwachung der Leistung mit den Seiten des Performance Explorers . . . 595
- Anzeigen von Informationen zur Objektkonfiguration . . . 632
- Verstehen und Verwenden der Seite Node Failover Planning . . . 644
- Erfassung von Daten und Monitoring der Workload-Performance . . . 648
- Analyse der Workload-Performance . . . 665
- Verwalten von Berichten . . . 676

Konfiguration von Backup- und Restore-Vorgängen . . . 734
Verwendung von Unified Manager REST-APIs . . . 742
Management und Monitoring von Infinite Volumes . . . 744
Verwalten von Clustern . . . 763
Verwalten des Benutzerzugriffs . . . 772
Verwalten der Authentifizierung . . . 783
Verwalten von Sicherheitszertifikaten . . . 799
Fehlerbehebung . . . 805
Überwachung und Management der Cluster-Performance . . . 817
Einführung in das Performance-Monitoring von OnCommand Unified Manager . . . 817
Navigation in Performance-Workflows in der Unified Manager GUI . . . 821
Allgemeines zu Performance-Ereignissen und Meldungen . . . 833
Verwalten von benutzerdefinierten Performance-Schwellenwerten . . . 843
Monitoring der Cluster-Performance über das Performance-Dashboard . . . 855
Monitoring der Cluster-Performance über die Startseite des Performance Cluster . . . 858
Überwachung der Performance mithilfe der Seiten „Performance Inventory“ (Performance-Bestandsaufnahme . . . 864
Überwachung der Leistung mit den Seiten des Performance Explorers . . . 870
Performance-Management mithilfe von Performance-Kapazität und verfügbaren IOPS-Informationen . . . 893
Verstehen und Verwenden der Seite Node Failover Planning . . . 901
Erfassung von Daten und Monitoring der Workload-Performance . . . 906
Analyse der Workload-Performance . . . 923
Analyse von Performance-Ereignissen . . . 933
Einrichten einer Verbindung zwischen einem Unified Manager-Server und einem externen Datenanbieter 949
Überwachen und managen Sie den Cluster-Zustand . . . 954
Einführung in das Monitoring des Systemzustands von OnCommand Unified Manager . . . 954
Gemeinsame Workflows und Aufgaben im Zusammenhang mit Unified Manager . . . 956
Verwenden der Wartungskonsole . . . 1141
Rechtliche Hinweise . . . 1153
Urheberrecht . . . 1153
Marken . . . 1153
Patente . . . 1153
Datenschutzrichtlinie . . . 1153
Open Source . . . 1153

OnCommand Unified Manager Dokumentation

Versionshinweise

Bietet eine Zusammenfassung der neuen Funktionen, Einschränkungen und bekannten Probleme bei OnCommand Unified Manager 9.5.

Weitere Informationen finden Sie im "Versionshinweise zu OnCommand Unified Manager".

Los geht's

Schnellstartanleitung für VMware Installationen

Systemanforderungen

- Betriebssystem VMware ESXi 5.5, 6.0 und 6.5
- RAM: 12 GB
- CPU: Insgesamt 9572 MHz
- Freier Speicherplatz: 5 GB (Thin Provisioning), 152 GB (Thick Provisioning)

Detaillierte Systemanforderungen finden Sie unter "VMware Software- und Installationsanforderungen" Und "Interoperabilitätsmatrix".

Installation von OnCommand Unified Manager

Laden Sie das Installationsprogramm herunter

1. Laden Sie die herunter `OnCommandUnifiedManager-9.5RC1.ovas` Installationspaket.
2. Speichern Sie die Datei in einem lokalen Verzeichnis oder Netzwerkverzeichnis, auf das Ihr vSphere Client zugreifen kann.

Installation Von Unified Manager

VMware Tools sind nicht im Unified Manager Installationspaket enthalten. Sie müssen ein CD-ROM- oder ISO-Image mounten, um es als Teil des Unified Manager-Installationsprozesses zu installieren.

1. Klicken Sie im vSphere-Client auf **Datei > OVF-Vorlage bereitstellen**.
2. Suchen Sie die OVA-Datei und stellen Sie die virtuelle Appliance mithilfe des Assistenten auf dem ESXi-Server bereit.
3. Füllen Sie auf der Seite Netzwerkkonfiguration auf der Registerkarte Eigenschaften die Felder aus, die für den Installationstyp erforderlich sind, den Sie durchführen:
   - Für eine statische Konfiguration: Geben Sie erforderliche Informationen in alle Felder ein (sekundäre DNS ist nicht erforderlich).
   - Bei DHCP unter Verwendung von IPv4 lassen Sie alle Felder leer.
   - Für DHCP unter Verwendung von IPv6: Aktivieren Sie das Feld „Automatische IPv6-Adresse aktivieren“, und lassen Sie alle anderen Felder leer.
4. Schalten Sie die VM ein.
5. Klicken Sie auf die Registerkarte Konsole, um den anfänglichen Startvorgang anzuzeigen.
6. Folgen Sie der Eingabeaufforderung, um VMware Tools auf der VM zu installieren.
7. Zeitzone konfigurieren.
8. Geben Sie einen Benutzernamen und ein Passwort für die Unified Manager-Wartung ein.

Am Ende der Installation werden die Informationen zur Verbindung mit der Unified Manager Web-Benutzeroberfläche angezeigt.

Kurzanleitung für Linux-Installationen

Systemanforderungen

- Betriebssystem: Red hat Enterprise Linux oder CentOS 64-Bit Version 7.x Architektur, installiert mit der Basisumgebung „Server mit GUI“ aus der Software-Auswahl-Option des OS-Installationsprogramms
- RAM: 12 GB
- CPU: Insgesamt 9572 MHz
- Freier Festplattenspeicher: 100 GB Festplattenspeicher für /opt, 50 GB für die Root-Partition

Detaillierte Systemanforderungen finden Sie unter "Anforderungen an Red hat Enterprise Linux und CentOS Software und Installation" Und das "Interoperabilitätsmatrix".

Installation von OnCommand Unified Manager

Laden Sie das Installationsprogramm herunter

1. Laden Sie die herunter `OnCommandUnifiedManager-rhel7-9.5RC1.zip` Installationspaket.
2. Führen Sie im Verzeichnis, in dem Sie die Installationsdatei heruntergeladen haben, folgende Schritte aus:

```
# unzip OnCommandUnifiedManager-rhel7-9.5RC1.zip
```

Überprüfung der Repository-Konfiguration

Die Vorgehensweisen für die Konfiguration von Red hat Enterprise Linux- oder CentOS-Repositorys sind standortspezifisch. Das im Installationspaket enthaltene Skript pre_install_check.sh kann optional verwendet werden, um zu überprüfen, ob Ihr Betriebssystem korrekt konfiguriert ist. Wenn Ihr System mit dem Internet verbunden ist, erhalten Sie automatisch die Anweisungen zum Einrichten der Red hat Enterprise Linux- und MySQL-Repositories. Informationen zur Installation auf einem System ohne Internetverbindung finden Sie unter "Installation, Aktualisierung und Entfernung der Unified Manager Software unter Red hat oder CentOS".

```
# ./pre_install_check.sh
```

Installation Von Unified Manager

Unified Manager verwendet das `yum` Dienstprogramm zum Installieren der Software und der abhängigen Software. Da es in verschiedenen Organisationen unterschiedliche Bilder von Red hat Enterprise Linux oder CentOS gibt, hängen die installierten Pakete von der Software ab, die in den Bildern vorhanden ist. Der `yum` Das Dienstprogramm bestimmt die abhängigen Softwarepakete für die Installation. Weitere Informationen zu den abhängigen Softwarepaketen finden Sie unter "Installation, Aktualisierung und Entfernung der Unified Manager Software unter Red hat oder CentOS".

Führen Sie als Root-Benutzer oder mit sudo den folgenden Befehl aus dem Verzeichnis aus, in dem die Installationsdatei entpackt wurde:

```
# yum install *.rpm
```

Oder

```
% sudo yum install *.rpms
```

Am Ende der Installation werden die Informationen zur Verbindung mit der Unified Manager Web-Benutzeroberfläche angezeigt. Wenn Sie keine Verbindung zur Web-UI herstellen können, müssen Sie möglicherweise den Whitelist-Port 443 verwenden. Weitere Details erhalten Sie von Ihrem technischen Support-Team.

Kurzanleitung für Windows-Installationen

Systemanforderungen

- Betriebssysteme: Microsoft Windows Server 2012, 2012 R2, 2016 64-Bit Standard und Datacenter Edition
- RAM: 12 GB
- CPU: Insgesamt 9572 MHz
- Freier Speicherplatz: 100 GB Festplattenspeicher für das Installationsverzeichnis, 50 GB Festplattenspeicher für das MySQL-Datenverzeichnis

Detaillierte Systemanforderungen finden Sie unter "Windows Software- und Installationsanforderungen" Und "Interoperabilitätsmatrix".

Installation von OnCommand Unified Manager

Laden Sie das Installationsprogramm herunter

1. Laden Sie die herunter `OnCommandUnifiedManager-9.5RC1.exes` Installationspaket.
2. Kopieren Sie die Installationsdatei in ein Verzeichnis auf dem Zielsystem.

Installation Von Unified Manager

Microsoft .NET 4.5 oder höher muss installiert sein. Unified Manager installiert im Rahmen der Installation weitere erforderliche Pakete von Drittanbietern. Weitere Informationen zu den abhängigen Softwarepaketen finden Sie unter "Installieren, Aktualisieren und Entfernen der Unified Manager-Software unter Windows".

1. Melden Sie sich unter Windows mit dem lokalen Standardkonto an.
2. Klicken Sie in dem Verzeichnis, in dem Sie die Installationsdatei heruntergeladen haben, mit der rechten Maustaste auf die ausführbare Datei Unified Manager (.exe) als Administrator.
3. Geben Sie bei der entsprechenden Aufforderung den Benutzernamen und das Passwort ein, um den Unified Manager-Wartungs-Benutzer zu erstellen.
4. Geben Sie im Datenbankverbindungsassistenten das MySQL-Root-Passwort ein.
5. Befolgen Sie die verbleibenden Anweisungen, um die Installation abzuschließen.
6. Klicken Sie am Ende der Installation auf **Fertig stellen** und die Unified Manager Web-Benutzeroberfläche wird angezeigt.

Installation Von Unified Manager

Einführung in OnCommand Unified Manager

OnCommand Unified Manager ermöglicht das Monitoring und Management des Systemzustands sowie der Performance Ihrer ONTAP Storage-Systeme über eine einheitliche Benutzeroberfläche. Sie können Unified Manager auf einem Linux-Server, auf einem Windows-Server oder als virtuelle Appliance auf einem VMware Host bereitstellen.

Nachdem Sie die Installation abgeschlossen und die Cluster hinzugefügt haben, die Sie verwalten möchten, bietet Unified Manager eine grafische Oberfläche, in der der Kapazitäts-, Verfügbarkeits-, Sicherungs- und Performancestatus der überwachten Speichersysteme angezeigt wird.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Was macht der Unified Manager Server

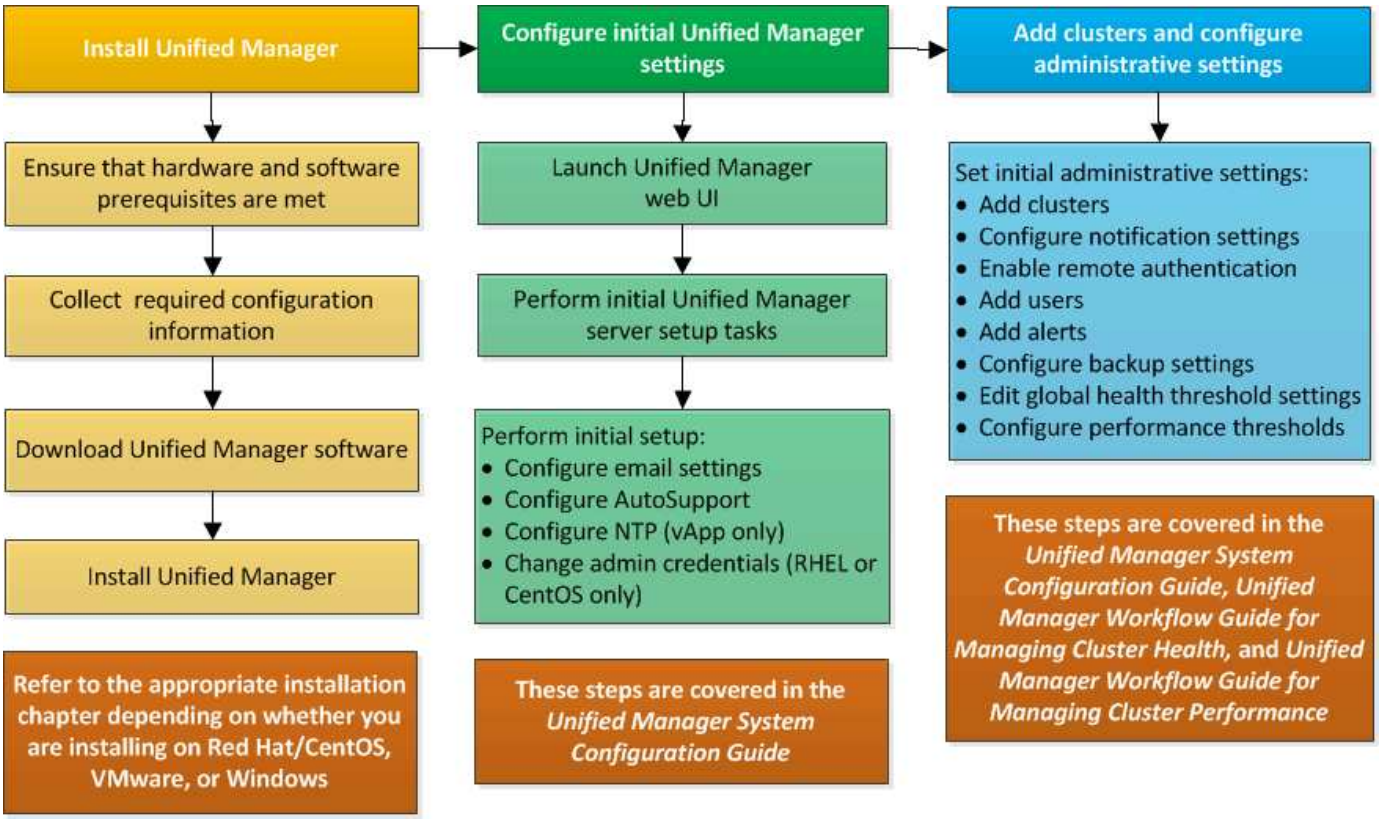
Die Unified Manager Server-Infrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Applikationsserver. Die Lösung bietet Infrastrukturservices wie beispielsweise Discovery, Monitoring, rollenbasierte Zugriffssteuerung (RBAC), Audits und Protokollierungsfunktionen.

Unified Manager sammelt Cluster-Informationen, speichert die Daten in der Datenbank und analysiert die Daten, um zu prüfen, ob es Cluster-Probleme gibt.

Überblick über die Installationsreihenfolge

Im Installations-Workflow werden die Aufgaben beschrieben, die Sie vor der Verwendung von Unified Manager ausführen müssen.

In den Kapiteln dieses Installationsleitfadens werden die Elemente beschrieben, die im folgenden Workflow aufgeführt sind.



Anforderungen für die Installation von Unified Manager

Bevor Sie Unified Manager installieren können, müssen Sie sicherstellen, dass der Server, auf dem Sie Unified Manager installieren möchten, bestimmte Software-, Hardware-, CPU- und Arbeitsspeicheranforderungen erfüllt.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Systemanforderungen für virtuelle Infrastruktur und Hardware

Je nachdem, ob Sie Unified Manager auf einer virtuellen Infrastruktur oder auf einem physischen System installieren, müssen Sie die Mindestanforderungen an Arbeitsspeicher, CPU und Festplattenspeicher erfüllen.

In der folgenden Tabelle werden die Werte angezeigt, die für Speicher-, CPU- und Festplattenspeicherressourcen empfohlen werden. Diese Werte wurden so qualifiziert, dass Unified Manager die akzeptablen Leistungsniveaus erfüllt.

Hardwarekonfiguration	Empfohlene Einstellungen
RAM	12 GB (Mindestanforderung 8 GB)
Prozessoren	4 CPUs

Hardwarekonfiguration	Empfohlene Einstellungen
CPU-Zykluskapazität	9572 MHz insgesamt (Mindestanforderung 9572 MHz)
Freier Speicherplatz	VMware: • 5 GB (Thin Provisioning) • 152 GB (Thick Provisioning)
Red hat oder CentOS: 150 GB, wobei die Kapazität wie folgt zugewiesen wird: • 50 GB der Root-Partition zugewiesen • 100 GB freier Speicherplatz, der dem zugewiesen ist `/opt/netapp/data` Verzeichnis, das auf einem LVM-Laufwerk oder auf einer separaten lokalen Festplatte installiert ist, die an das Zielsystem angeschlossen ist Der `/tmp` Das Verzeichnis sollte mindestens 10 GB freien Speicherplatz und das haben `/var/log` Das Verzeichnis sollte mindestens 16 GB freien Speicherplatz haben.	Windows: 150 GB, wobei die Kapazität wie folgt zugewiesen wird: • 100 GB Festplattenspeicher für das Installationsverzeichnis • 50 GB Festplattenspeicher für das MySQL-Datenverzeichnis

Unified Manager kann auf Systemen mit wenig Arbeitsspeicher installiert werden. Die empfohlenen 12 GB RAM sorgen jedoch dafür, dass genügend Arbeitsspeicher für eine optimale Leistung zur Verfügung steht und dass das System bei wachsender Konfiguration zusätzliche Cluster und Speicherobjekte aufnehmen kann. Sie dürfen der VM, wo Unified Manager eingesetzt wird, keine Speicherbeschränkungen mehr festlegen und müssen keine Funktionen (z. B. Ballooning) aktivieren, was die Software daran hindert, den im System zugewiesenen Speicher zu nutzen.

Darüber hinaus ist die Anzahl der Nodes begrenzt, die eine einzelne Instanz von Unified Manager überwachen kann, bevor Sie eine zweite Instanz von Unified Manager installieren müssen. Weitere Informationen finden Sie im *Best Practices Guide*.

"Technischer Bericht 4621: Unified Manager Best Practices Guide"

Das Speicher-Page-Swapping beeinträchtigt die Leistung des Systems und der Verwaltungsanwendung negativ. Konkurrenzfähigkeit gegenüber CPU-Ressourcen, die aufgrund der gesamten Host-Auslastung nicht verfügbar sind, kann die Performance beeinträchtigen.

Dedizierte Nutzungsanforderungen

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, muss ausschließlich für Unified Manager verwendet werden und darf nicht mit anderen Applikationen gemeinsam genutzt werden. Andere Applikationen nutzen unter Umständen Systemressourcen und können die Performance von Unified Manager deutlich verringern.

Speicherplatzanforderungen für Backups

Wenn Sie die Backup- und Restore-Funktion von Unified Manager nutzen möchten, müssen Sie zusätzliche Kapazität zuweisen, damit das Verzeichnis „`data`“ oder die Festplatte 150 GB Speicherplatz hat. Ein Backup kann auf ein lokales Ziel oder ein Remote-Ziel geschrieben werden. Als Best Practice empfiehlt es sich, einen Remote-Standort außerhalb des Unified Manager-Hostsystems zu identifizieren, der über mindestens 150 GB Speicherplatz verfügt.

Anforderungen für die Host-Konnektivität

Das physische System oder das virtuelle System, auf dem Sie Unified Manager installieren, müssen so konfiguriert werden, dass es erfolgreich sein kann `ping` Der Hostname des Hosts selbst. Bei einer IPv6-Konfiguration sollten Sie dies überprüfen `ping6` Für den Host-Namen ist erfolgreich, um sicherzustellen, dass die Unified Manager-Installation erfolgreich ist.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Web-Benutzeroberfläche des Produkts zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie einen Namen für den Netzwerk-Host festgelegt. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollten Sie den Hostnamen vom DNS beziehen.

Wenn Sie Benutzern den Zugriff auf Unified Manager über den Kurznamen erlauben möchten, anstatt den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse zu verwenden, muss die Netzwerkkonfiguration diesen Kurznamen einem gültigen FQDN auflösen.

Angehängt `/opt/netapp` Oder `/opt/netapp/data` Anforderungen

Die Montage ist möglich `/opt/netapp` Oder `/opt/netapp/data` Auf einem NAS- oder SAN-Gerät. Beachten Sie, dass die Verwendung von Remote-Bereitstellungspunkten zu Skalierungsproblemen führen kann. Wenn Sie einen Remote-Mount-Punkt verwenden, stellen Sie sicher, dass Ihr SAN- oder NAS-Netzwerk über genügend Kapazität verfügt, um die I/O-Anforderungen von Unified Manager zu erfüllen. Die Kapazität variiert und kann sich je nach Anzahl der von Ihnen überwachten Cluster und Storage-Objekte erhöhen.

Wenn Sie angehängt sind `/opt/netapp` Oder `/opt/netapp/data` Von überall dort, wo das Root-Dateisystem und SELinux in Ihrer Umgebung aktiviert sind, müssen Sie den richtigen Kontext für die gemounteten Verzeichnisse festlegen.

Siehe Thema SELinux Anforderungen zum Mounten von /opt/netapp oder /opt/netapp/Daten auf einer NFS- oder CIFS-Freigabe Weitere Informationen zum Festlegen des richtigen SELinux-Kontexts.

VMware Software- und Installationsanforderungen

Das VMware vSphere System, auf dem Unified Manager installiert wird, erfordert bestimmte Versionen des Betriebssystems und unterstützende Software.

Betriebssystem-Software

Die folgenden Versionen von VMware ESXi werden unterstützt:

- ESXi 5.5, 6.0 und 6.5

Die folgenden Versionen von vSphere werden unterstützt:

- VMware vCenter Server 5.5, 6.0 und 6.5

In der Interoperabilitäts-Matrix finden Sie die vollständige und aktuelle Liste der unterstützten ESXi Versionen.

"mysupport.netapp.com/matrix"

Die Zeit des VMware ESXi-Servers muss mit der NTP-Serverzeit identisch sein, damit die virtuelle Appliance ordnungsgemäß funktioniert. Das Synchronisieren der VMware ESXi Serverzeit mit der NTP-Serverzeit verhindert einen Zeitausfall.

Installationsvoraussetzungen

VMware Hochverfügbarkeit für die virtuelle Unified Manager Appliance wird unterstützt.

Wenn Sie einen NFS-Datastore auf einem Storage-System mit ONTAP Software implementieren, müssen Sie zum Einsatz von Thick Provisioning das NetApp NFS-Plug-in für VMware VAAI verwenden.

Falls die Bereitstellung aufgrund unzureichender Ressourcen nicht in der Umgebung mit hoher Verfügbarkeit funktioniert, müssen Sie die Optionen für virtuelle Clusterfunktionen ändern, indem Sie die Priorität für VM-Neustart deaktivieren und die Host-Isolationsreaktion eingeschaltet lassen.

Anforderungen an Red hat Enterprise Linux und CentOS Software und Installation

Das Linux-System, auf dem Unified Manager installiert wird, erfordert bestimmte Versionen des Betriebssystems und unterstützende Software.

Betriebssystem-Software

Das Linux-System muss die folgenden Versionen des Betriebssystems und die unterstützende Software installiert haben:

- Red hat Enterprise Linux oder CentOS 64-Bit Version 7.x

  Red hat Enterprise Linux 6.x wird ab Unified Manager 9.4 nicht unterstützt.

In der Interoperabilitäts-Matrix finden Sie eine vollständige und aktuelle Liste der unterstützten Red hat Enterprise Linux- und CentOS-Versionen.

"mysupport.netapp.com/matrix"

Folgende Drittanbieterpakete sind erforderlich:

- MySQL Community Edition Version 5.7.23 oder höhere Versionen in der 5.7-Familie (aus dem MySQL-Repository)
- OpenJDK Version 11 (aus dem Red hat Extra Enterprise Linux Server Repository)

  Oracle Java wird ab Unified Manager 9.5 nicht unterstützt.

- P7zip Version 16.02 oder höher (aus dem Red hat Extra Packages for Enterprise Linux Repository)

Wenn Sie nach dem Ausführen von Unified Manager ein Upgrade der Drittanbieter-Software planen, müssen Sie Unified Manager zunächst herunterfahren. Nach Abschluss der Softwareinstallation von Drittanbietern können Sie Unified Manager neu starten.

Anforderungen an die Benutzerautorisierung

Die Installation von Unified Manager auf einem Red hat Enterprise Linux System oder CentOS System kann vom Root-Benutzer oder von nicht-Root-Benutzern mit dem durchgeführt werden `sudo` Befehl.

Installationsvoraussetzungen

Die Best Practices für die Installation von Red hat Enterprise Linux oder CentOS und den damit verbundenen Repositorys auf Ihrem System lauten wie folgt:

- Sie müssen Red hat Enterprise Linux oder CentOS nach Red hat Best Practices installieren, und Sie sollten die folgenden Standardoptionen wählen, die die Auswahl von “SServer mit GUI” erfordern.
- Bei der Installation von Unified Manager auf Red hat Enterprise Linux oder CentOS muss das System Zugriff auf das entsprechende Repository haben, damit das Installationsprogramm auf alle erforderlichen Softwareabhängigkeiten zugreifen und diese installieren kann.
- Für das `yum` Installer um die abhängige Software in den Red hat Enterprise Linux Repositorys zu finden, müssen Sie das System während der Red hat Enterprise Linux Installation oder danach unter Verwendung eines gültigen Red hat Subskriptions registriert haben.

  Informationen zum Red hat Subscription Manager finden Sie in der Red hat Dokumentation.

- Sie müssen das EPEL-Repository (Extra Packages for Enterprise Linux) aktivieren, um die erforderlichen Dienstprogramme von Drittanbietern erfolgreich auf Ihrem System installieren zu können.

  Wenn das EPEL-Repository auf Ihrem System nicht konfiguriert ist, müssen Sie das Repository manuell herunterladen und konfigurieren.

  Manuelles Konfigurieren des EPEL-Repositorys

- Wenn die korrekte Version von MySQL nicht installiert ist, müssen Sie das MySQL-Repository aktivieren, damit die MySQL-Software auf Ihrem System erfolgreich installiert werden kann.

  Wenn das MySQL-Repository nicht auf Ihrem System konfiguriert ist, müssen Sie das Repository manuell herunterladen und konfigurieren.

  Manuelles Konfigurieren des MySQL-Repository

Wenn Ihr System keinen Internetzugang hat und die Repositories nicht von einem mit dem Internet verbundenen System mit dem nicht verbundenen System gespiegelt werden, sollten Sie die Installationsanweisungen befolgen, um die externen Softwareabhängigkeiten Ihres Systems zu bestimmen. Anschließend können Sie die erforderliche Software auf das internetverbundene System herunterladen und die kopieren `.rpm` Dateien auf dem System, auf dem Unified Manager installiert werden soll. Um die Artefakte und Pakete herunterzuladen, müssen Sie das verwenden `yum install` Befehl. Sie müssen sicherstellen, dass auf beiden Systemen die gleiche Betriebssystemversion ausgeführt wird und dass die Abonnementlizenz für die entsprechende Red hat Enterprise Linux- oder CentOS-Version gilt.

Sie dürfen die erforderliche Drittanbietersoftware nicht aus anderen als den hier aufgeführten Repositorys installieren. Die in den Red hat Repositorys installierte Software wurde speziell für Red hat Enterprise Linux entwickelt und entspricht den Best Practices von Red hat (Verzeichnislayouts, Berechtigungen usw.). Software von anderen Standorten folgt möglicherweise nicht diesen Richtlinien. Dies kann dazu führen, dass die Unified Manager-Installation fehlschlägt oder Probleme mit zukünftigen Upgrades verursachen kann.

Port 443 erforderlich

Allgemeine Images von Red hat und CentOS blockieren externen Zugriff auf Port 443. Wenn die Verbindung zwischen Ihrem Browser und Ihrem OnCommand Produkt nicht hergestellt werden kann, ist dies möglicherweise das Problem. Der folgende Befehl ermöglicht den Zugriff auf Port 443 für alle externen Benutzer und Anwendungen: `# firewall-cmd –zone=public –add-port=443/tcp –permanent; firewall-cmd –reload`

Wenden Sie sich vor der Ausführung dieses Befehls an Ihre IT-Abteilung, um zu prüfen, ob für Ihre Sicherheitsrichtlinien ein anderes Verfahren erforderlich ist.

Windows Software- und Installationsanforderungen

Für die erfolgreiche Installation von Unified Manager unter Windows müssen Sie sicherstellen, dass das System, auf dem Unified Manager installiert wird, den Softwareanforderungen entspricht.

Betriebssystem-Software

Unified Manager läuft nur auf einem Windows-Betriebssystem in 64-Bit-Englisch-Sprache. Sie können Unified Manager auf folgenden Windows Plattformen installieren:

- Microsoft Windows Server 2012 Standard und Datacenter Edition
- Microsoft Windows Server 2012 R2 Standard und Datacenter Edition
- Microsoft Windows Server 2016 Standard und Datacenter Edition

Unter Windows Server 2012 R2 muss das Windows Update KB2919355 auf dem Zielsystem installiert sein, da die Installation fehlschlägt.

Beachten Sie, dass Windows Server 2008 nicht wie in früheren Versionen unterstützt wird. In der Interoperabilitäts-Matrix finden Sie die vollständige und aktuelle Liste der unterstützten Windows-Versionen.

"mysupport.netapp.com/matrix"

Der Server sollte für die Ausführung von Unified Manager dediziert sein; es sollten keine anderen Anwendungen auf dem Server installiert sein.

Folgende Drittanbieterpakete sind erforderlich:

- Microsoft Visual C++ 2015 Redistributable Package Version 14.0.24212
- Microsoft Visual C++ weiterverteilbare Pakete für Visual Studio 2013 Version 12.0.40660
- MySQL Community Edition Version 5.7.23, oder höhere Versionen in der 5.7-Familie
- OpenJDK Version 11
- P7zip Version 18.01 oder höher

Wenn diese Drittanbieterpakete nicht installiert sind, installiert Unified Manager sie im Rahmen der Installation.

Ab Unified Manager 9.5 wird OpenJDK im Unified Manager-Installationspaket bereitgestellt und automatisch installiert. Oracle Java wird ab Unified Manager 9.5 nicht unterstützt.

Wenn MySQL vorinstalliert ist, müssen Sie Folgendes sicherstellen:

- Er verwendet den Standardport.
- Die Beispieldatenbanken sind nicht installiert.
- Der Servicename lautet “MYSQL”.

Wenn Sie nach dem Ausführen von Unified Manager ein Upgrade der Drittanbieter-Software planen, müssen Sie Unified Manager zunächst herunterfahren. Nach Abschluss der Softwareinstallation von Drittanbietern können Sie Unified Manager neu starten.

Installationsvoraussetzungen

- Microsoft .NET 4.5 oder höher muss installiert sein.
- Sie müssen 2 GB Speicherplatz für das reservieren `temp` Verzeichnis zum Extrahieren der Installationsdateien.
- Sie müssen 2 GB Festplattenspeicher im Windows-Laufwerk reservieren, um die MSI-Dateien von Unified Manager zwischenzuspeichern.
- Der Microsoft Windows-Server, auf dem Sie Unified Manager installieren möchten, muss mit einem vollständig qualifizierten Domänennamen (FQDN) konfiguriert sein, der diesen entspricht `ping` Die Antworten auf den Hostnamen und FQDN sind erfolgreich.
- Sie müssen den weltweiten Webveröffentlichungsservice von Microsoft IIS deaktivieren und sicherstellen, dass die Ports 80 und 443 frei sind.
- Sie müssen sicherstellen, dass während der Installation die Einstellung für den Host der Remote-Desktopsitzung für „`Windows Installer RDS Compatibility`“ deaktiviert ist.
- UDP-Port 514 muss frei sein und darf nicht von anderen Diensten verwendet werden.

Das Unified Manager-Installationsprogramm konfiguriert die folgenden Ausschlüsse in Windows Defender:

- Datenverzeichnis von Unified Manager (nur Windows Server 2016)
- Unified Manager Installationsverzeichnis vorhanden
- MySQL-Datenverzeichnis

Wenn auf Ihrem Server ein anderer Antiviren-Scanner installiert ist, müssen Sie diese Ausschlüsse manuell konfigurieren.

Unterstützte Browser

Für den Zugriff auf die Unified Manager-Benutzeroberfläche müssen Sie einen unterstützten Browser verwenden.

Unified Manager wurde mit den folgenden Browsern getestet, andere Browser können möglicherweise funktionieren, jedoch nicht qualifiziert sind. Eine vollständige Liste der unterstützten Browser-Versionen finden Sie in der Interoperabilitäts-Matrix.

"mysupport.netapp.com/matrix"

- Mozilla Firefox ESR 60

- Google Chrome Version 68 und 69
- Microsoft Internet Explorer 11

Wenn Sie für alle Browser Popup-Blocker deaktivieren, können Sie sicherstellen, dass die Softwarefunktionen ordnungsgemäß angezeigt werden.

Für Internet Explorer müssen Sie sicherstellen, dass die Kompatibilitätsansicht deaktiviert ist und der Dokumentmodus auf den Standardmodus eingestellt ist. Informationen zu diesen Einstellungen finden Sie in der Microsoft IE-Dokumentation.

Firefox und Chrome sind die bevorzugten Browser, da es einige Fälle gab, in denen komplexe UI-Seiten langsamer laden, wenn Internet Explorer.

Wenn Sie planen, Unified Manager für SAML-Authentifizierung so zu konfigurieren, dass ein Identitäts-Provider (IdP) Benutzer authentifiziert, überprüfen Sie die Liste der vom IdP unterstützten Browser.

Protokoll- und Port-Anforderungen

Durch einen Browser, einen API-Client oder SSH müssen die erforderlichen Ports für die Unified Manager-UI und die Unified-APIs zugänglich sein. Die erforderlichen Ports und Protokolle ermöglichen die Kommunikation zwischen dem Unified Manager Server und den gemanagten Storage-Systemen, Servern und anderen Komponenten.

Verbindungen zum Unified Manager-Server

Bei der Verbindung zur Web-UI von Unified Manager müssen Sie keine Portnummern angeben, da immer Standardports verwendet werden. Da Unified Manager beispielsweise immer auf dem Standardport ausgeführt wird, können Sie eingeben `https://<host>` Statt `https://<host>:443`. Die Standard-Portnummern können nicht geändert werden.

Der Unified Manager Server verwendet spezifische Protokolle für den Zugriff auf folgende Schnittstellen:

Schnittstelle	Protokoll	Port	Beschreibung
Unified Manager Web-UI	HTTP	80	Wird für den Zugriff auf die Web-UI von Unified Manager verwendet; automatische Umleitung zum sicheren Port 443.
Unified Manager Web-UI und -Programme mithilfe von APIs	HTTPS	443	Wird verwendet, um sicher auf die Web-UI von Unified Manager zuzugreifen oder API-Aufrufe durchzuführen. API-Aufrufe können nur über HTTPS erfolgen.

Schnittstelle	Protokoll	Port	Beschreibung
Wartungskonsole	SSH/SFTP	22	Wird verwendet, um auf die Wartungskonsole zuzugreifen und Supportpakete abzurufen.
Linux Befehlszeile	SSH/SFTP	22	Wird verwendet, um auf die Red hat Enterprise Linux oder CentOS Befehlszeile zuzugreifen und Supportpakete abzurufen.
MySQL Datenbank	MySQL	3306	Wird verwendet, um den Zugriff von OnCommand Workflow Automation und OnCommand API Services auf Unified Manager zu aktivieren.
Syslog	UDP	514	Wird verwendet, um auf abonnementbasierte EMS-Nachrichten aus ONTAP-Systemen zuzugreifen und Ereignisse auf der Grundlage der Meldungen zu erstellen.
RUHE	HTTPS	9443	Wird verwendet, um ÜBER authentifizierte ONTAP-Systeme auf Rest-API-basierte EMS-Ereignisse in Echtzeit zuzugreifen.

Verbindungen vom Unified Manager-Server

Sie müssen Ihre Firewall so konfigurieren, dass sie offene Ports ermöglicht, die die Kommunikation zwischen dem Unified Manager-Server und verwalteten Storage-Systemen, Servern und anderen Komponenten ermöglichen. Wenn ein Port nicht geöffnet ist, schlägt die Kommunikation fehl.

Je nach Umgebung können Sie festlegen, welche Ports und Protokolle der Unified Manager-Server für die Verbindung zu bestimmten Zielen verwendet.

Der Unified Manager-Server stellt die Verbindung über folgende Protokolle und Ports zu den gemanagten Storage-Systemen, Servern und anderen Komponenten her:

Ziel	Protokoll	Port	Beschreibung
Storage-System	HTTPS	443/TCP	Dient zum Überwachen und Managen von Storage-Systemen.
Storage-System	NDMP	10000/TCP	Wird für bestimmte Snapshot-Restore-Vorgänge verwendet.
AutoSupport Server	HTTPS	443	Wird zum Senden von AutoSupport-Informationen verwendet. Für diese Funktion ist ein Internetzugang erforderlich.
Authentifizierungsserver	LDAP	389	Wird zur Erstellung von Authentifizierungsanforderungen sowie von Benutzer- und Gruppenabfragen verwendet.
LDAPS	636	Wird für sichere LDAP-Kommunikation verwendet.	Mailserver
SMTP	25	Wird zum Senden von Benachrichtigungs-E-Mails verwendet.	SNMP-Trap-Absender
SNMPv1 oder SNMPv3	162/UDP	Wird zum Senden von SNMP-Traps für Warnmeldungen verwendet.	Server für externen Datenprovider
TCP	2003	Dient zum Senden von Performance-Daten an einen externen Datenanbieter wie Graphite.	NTP-Server

Füllen Sie das Arbeitsblatt aus

Vor der Installation und Konfiguration von Unified Manager sollten konkrete Informationen über die Umgebung sofort zur Verfügung stehen. Sie können die Informationen im Arbeitsblatt aufzeichnen.

Informationen zur Installation von Unified Manager

Die zur Installation von Unified Manager erforderlichen Details

System, auf dem Software bereitgestellt wird	Ihr Wert
ESXi-Server-IP-Adresse (nur VMware)	
Vollständig qualifizierter Domain-Name des Hosts	
Host-IP-Adresse	
Netzwerkmaske	
Gateway-IP-Adresse	
Primäre DNS-Adresse	
Sekundäre DNS-Adresse	
Domänen durchsuchen	
Wartungs-Benutzername	
Wartungs-Benutzer-Passwort	

Informationen zur Unified Manager-Konfiguration

Die Details zum Konfigurieren von Unified Manager nach der Installation. Je nach Konfiguration sind einige Werte optional.

Einstellung	Ihr Wert
Wartungs-Benutzer-E-Mail-Adresse	
NTP-Server (nur VMware)	
Hostname oder IP-Adresse des SMTP-Servers	
SMTP-Benutzername	
SMTP-Passwort	
SMTP-Port	25 (Standardwert)
E-Mail, von der aus Benachrichtigungen gesendet werden	

Einstellung	Ihr Wert
Hostname oder IP-Adresse des Authentifizierungsservers	
Active Directory-Administratorname oder LDAP-BIND-Distinguished Name	
Active Directory-Kennwort oder LDAP-Bindekennwort	
Authentifizierungsserverbasis mit Distinguished Name	
ID-Provider (IdP)-URL	
Metadaten des Identitäts-Providers (IdP)	
IP-Adresse des SNMP-Trap-Zielhosts	
SNMP-Port	

Cluster-Informationen

Die Details für die Storage-Systeme, die Sie mit Unified Manager managen möchten.

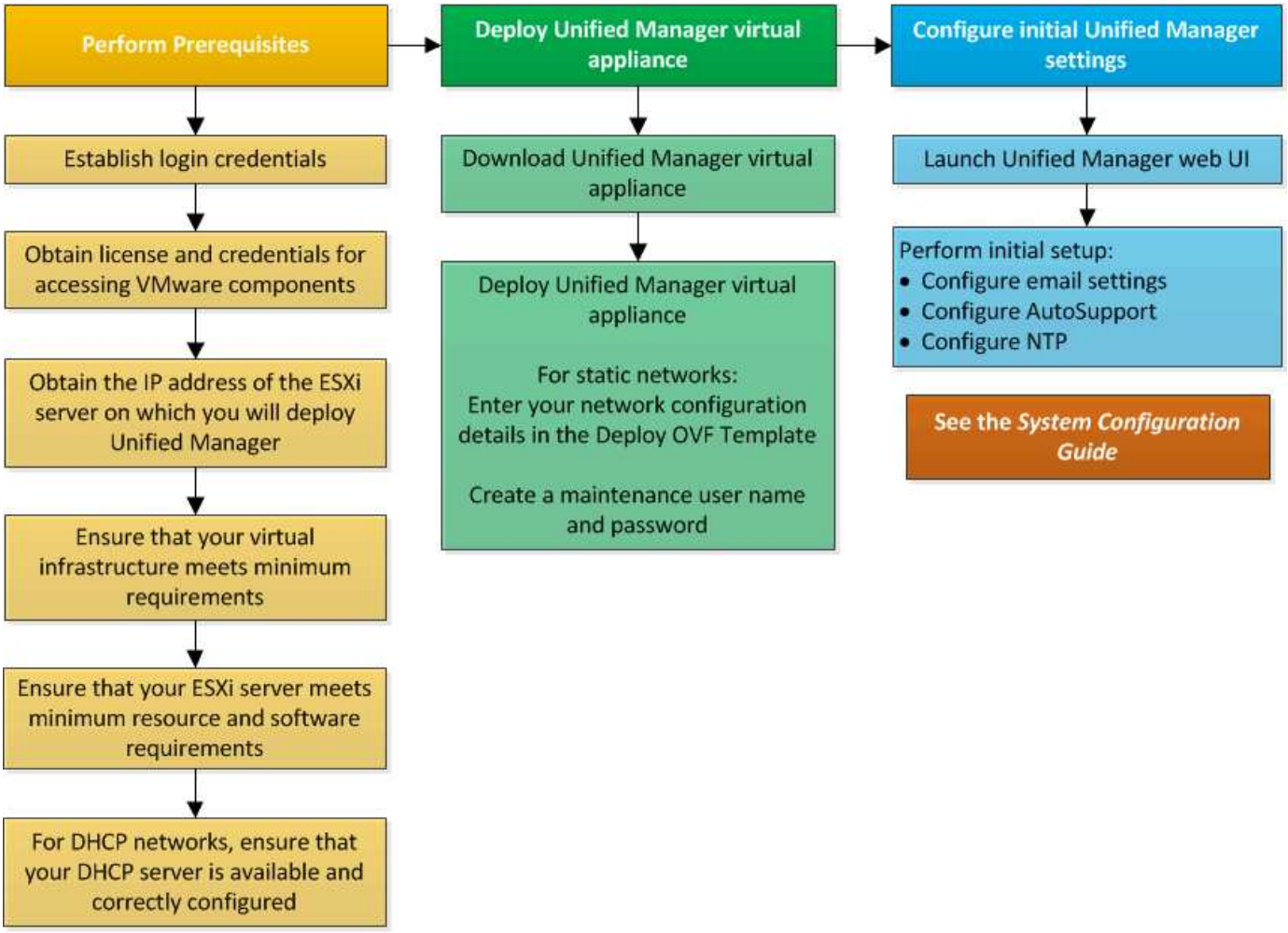
Cluster 1 von N	Ihr Wert
Host-Name oder Cluster-Management-IP-Adresse	
Benutzername des ONTAP-Administrators Dem Administrator muss die Rolle „`admin`“ zugewiesen worden sein.	
ONTAP-Administratorpasswort	
Protokoll (HTTP oder HTTPS)	

Installation, Upgrade und Entfernung der Unified Manager Software unter VMware vSphere

Auf VMware vSphere Systemen können Sie die Unified Manager Software installieren, ein Upgrade auf eine neuere Softwareversion durchführen oder die virtuelle Unified Manager Appliance entfernen.

Überblick über den Implementierungsprozess auf VMware

Der Bereitstellungs-Workflow beschreibt die Aufgaben, die Sie ausführen müssen, bevor Sie Unified Manager verwenden können.



Einführung Von Unified Manager

Die Bereitstellung von Unified Manager umfasst das Herunterladen von Software, die Bereitstellung der virtuellen Appliance, das Erstellen eines Benutzernamens und Kennworts für die Wartung und das Durchführen der ersten Einrichtung in der Web-Benutzeroberfläche.

Bevor Sie beginnen

- Sie müssen die Systemanforderungen für die Implementierung abgeschlossen haben.

  Systemanforderungen

- Sie müssen die folgenden Informationen haben:
  - Anmeldedaten für die NetApp Support-Website
  - Zugangsdaten für den Zugriff auf VMware vCenter Server und vSphere Web Client (für vSphere Version 6.5) oder vSphere Client (für vSphere Version 5.5 oder 6.0)

- IP-Adresse des ESXi-Servers, auf dem Sie die virtuelle Unified Manager-Appliance bereitstellen
- Details zum Datacenter, z. B. Speicherplatz im Datenspeicher und Speicheranforderungen
- IPv6 muss auf dem Host aktiviert sein, wenn Sie IPv6-Adressen verwenden möchten.
- CD-ROM- oder ISO-Image der VMware Tools

Über diese Aufgabe

Sie können Unified Manager als virtuelle Appliance auf einem VMware ESXi Server bereitstellen.

Sie müssen über die VMware Konsole auf die Wartungskonsole zugreifen, nicht über SSH.

VMware Tools sind nicht im Unified Manager enthalten `.ova` Datei und muss separat installiert werden.

Nachdem Sie fertig sind

Nachdem Sie die Implementierung und das Setup abgeschlossen haben, können Sie entweder Cluster hinzufügen oder zusätzliche Netzwerkeinstellungen in der Wartungskonsole konfigurieren und anschließend auf die Web-Benutzeroberfläche zugreifen.

Die OVA-Datei von Unified Manager wird heruntergeladen

Sie müssen Unified Manager herunterladen `.ova` Datei von der NetApp Support Site, um Unified Manager als virtuelle Appliance zu implementieren.

Bevor Sie beginnen

Sie müssen Anmeldedaten für die NetApp Support-Website besitzen.

Über diese Aufgabe

Der `.ova` Die Datei enthält die in einer virtuellen Appliance konfigurierte Unified Manager Software.

Schritte

1. Melden Sie sich bei der NetApp Support Site an und navigieren Sie zur Download-Seite, um Unified Manager auf VMware vSphere zu installieren.

   "NetApp Downloads: Software"

2. Laden Sie herunter, und speichern Sie die `.ova` Datei in ein lokales Verzeichnis oder Netzwerkverzeichnis, auf das Ihr vSphere Client zugreifen kann.
3. Überprüfen Sie die Prüfsumme, um sicherzustellen, dass die Software ordnungsgemäß heruntergeladen wurde.

Implementieren der virtuellen Unified Manager Appliance

Sie können die virtuelle Unified Manager-Appliance bereitstellen, nachdem Sie den heruntergeladen haben `.ova` Datei von der NetApp Support Site Sie müssen vSphere Web Client (für vSphere Version 6.5) oder vSphere Client (für vSphere Version 5.5 oder 6.0) verwenden, um die virtuelle Appliance auf einem ESXi-Server bereitzustellen. Wenn Sie die virtuelle Appliance bereitstellen, wird eine virtuelle Maschine erstellt.

Bevor Sie beginnen

Sie müssen die Systemanforderungen geprüft haben. Wenn Änderungen zur Erfüllung der Systemanforderungen erforderlich sind, müssen Sie die Änderungen vor der Bereitstellung der virtuellen Unified Manager Appliance implementieren.

Anforderungen an die virtuelle Infrastruktur

VMware Software- und Installationsanforderungen

Wenn Sie DHCP verwenden, müssen Sie sicherstellen, dass der DHCP-Server verfügbar ist und die Konfigurationen der DHCP- und VM-Netzwerkadapter korrekt sind. Standardmäßig ist DHCP konfiguriert.

Wenn Sie eine statische Netzwerkkonfiguration verwenden, müssen Sie sicherstellen, dass die IP-Adresse nicht im selben Subnetz dupliziert wird und dass die entsprechenden DNS-Servereinträge konfiguriert wurden.

Vor der Bereitstellung der virtuellen Appliance müssen Sie folgende Informationen haben:

- Zugangsdaten für den Zugriff auf VMware vCenter Server und vSphere Web Client (für vSphere Version 6.5) oder vSphere Client (für vSphere Version 5.5 oder 6.0)
- IP-Adresse des ESXi-Servers, auf dem Sie die virtuelle Unified Manager-Appliance bereitstellen
- Details zum Datacenter, wie zum Beispiel die Verfügbarkeit von Speicherplatz
- Wenn Sie DHCP nicht verwenden, müssen Sie über die IPv4- oder IPv6-Adressen für die Netzwerkgeräte verfügen, mit denen Sie eine Verbindung herstellen möchten:
  - Vollständig qualifizierter Domänenname (FQDN) des Hosts
  - IP-Adresse des Hosts
  - Netzwerkmaske
  - IP-Adresse des Standard-Gateways
  - Primäre und sekundäre DNS-Adressen
  - Domänen durchsuchen
- CD-ROM- oder ISO-Image für die VMware Tools

Über diese Aufgabe

VMware-Tools sind nicht in enthalten `.ova` Datei: Sie müssen die VMware Tools separat installieren.

Bei der Bereitstellung der virtuellen Appliance wird ein eigensigniertes Zertifikat für HTTPS-Zugriff generiert. Beim Zugriff auf die Web-Benutzeroberfläche von Unified Manager wird möglicherweise eine Browserwarnung über nicht vertrauenswürdige Zertifikate angezeigt.

VMware Hochverfügbarkeit für die virtuelle Unified Manager Appliance wird unterstützt.

Schritte

1. Klicken Sie im vSphere-Client auf **Datei** > **OVF-Vorlage bereitstellen**.
2. Schließen Sie den Assistenten * OVF-Vorlage bereitstellen* aus, um die virtuelle Unified Manager-Appliance bereitzustellen.

   Auf der Seite Netzwerkkonfiguration:

- Lassen Sie alle Felder leer, wenn Sie DHCP- und IPv4-Adressen verwenden.
- Aktivieren Sie das Kontrollkästchen „`Auto IPv6 Addressing`“, und lassen Sie alle anderen Felder leer, wenn Sie DHCP- und IPv6-Adressen verwenden.
- Wenn Sie eine statische Netzwerkkonfiguration verwenden möchten, können Sie die Felder auf dieser Seite ausfüllen und diese Einstellungen werden während der Bereitstellung angewendet. Sie müssen sicherstellen, dass die IP-Adresse für den Host, auf dem sie bereitgestellt wird, eindeutig ist, dass sie nicht bereits verwendet wird und dass er über einen gültigen DNS-Eintrag verfügt.

3. Nachdem die virtuelle Unified Manager-Appliance auf dem ESXi-Server bereitgestellt wurde, schalten Sie die VM ein, indem Sie mit der rechten Maustaste auf die VM klicken und anschließend **Power on** wählen.

   Wenn der Einschaltvorgang aufgrund unzureichender Ressourcen fehlschlägt, müssen Sie Ressourcen hinzufügen und die Installation dann wiederholen.

4. Klicken Sie auf die Registerkarte **Konsole**.

   Der erste Bootvorgang dauert einige Minuten.

5. Folgen Sie der Eingabeaufforderung, um die VMware Tools auf der VM zu installieren.

   Bei Verwendung des vSphere Web Client mit vSphere 6.5 müssen Sie das ISO-Image von VMware Tools manuell mounten. Wählen Sie in der VM **Einstellungen bearbeiten** > **virtuelle Hardware** > **CD/DVD-Laufwerk x** > **Datastore ISO-Datei** und klicken Sie dann auf **Durchsuchen**, um die Datei auszuwählen `linux.iso` Als Mount-Bild.

6. Um Ihre Zeitzone zu konfigurieren, geben Sie Ihren geografischen Bereich und Ihre Stadt oder Region wie im Fenster VM **Konsole** aufgefordert ein.

   Alle angezeigten Datumsangaben verwenden die für Unified Manager konfigurierte Zeitzone, unabhängig von der Zeitzone auf Ihren verwalteten Geräten. Dies sollten Sie beim Vergleich von Zeitstempel beachten. Wenn Ihre Speichersysteme und der Management-Server mit demselben NTP-Server konfiguriert sind, verweisen sie sofort auf den gleichen, auch wenn sie anders aussehen. Wenn Sie beispielsweise eine Snapshot Kopie mit einem Gerät erstellen, das mit einer anderen Zeitzone als der des Management-Servers konfiguriert ist, wird die im Zeitstempel widergespiegelte Zeit die Zeit des Management-Servers verwendet.

7. Wenn keine DHCP-Dienste verfügbar sind oder wenn in den Details für die statische Netzwerkkonfiguration ein Fehler aufgetreten ist, wählen Sie eine der folgenden Optionen aus:

Verwenden Sie…	Dann tun Sie das…
DHCP	Wählen Sie **DHCP wiederholen**. Wenn Sie DHCP verwenden möchten, sollten Sie sicherstellen, dass es korrekt konfiguriert ist. Wenn Sie ein DHCP-fähiges Netzwerk verwenden, werden die Einträge FQDN und DNS-Server automatisch der virtuellen Appliance zugewiesen. Wenn DHCP nicht ordnungsgemäß mit DNS konfiguriert ist, wird der Hostname „`OnCommand`“ automatisch zugewiesen und dem Sicherheitszertifikat zugeordnet. Wenn Sie kein DHCP-fähiges Netzwerk eingerichtet haben, müssen Sie die Netzwerkkonfigurationsinformationen manuell eingeben.
Eine statische Netzwerkkonfiguration	a. Wählen Sie **Geben Sie die Details für die statische Netzwerkkonfiguration** ein. Die Konfiguration dauert einige Minuten. b. Bestätigen Sie die eingegebenen Werte und wählen Sie **Y** aus.

8. Geben Sie an der Eingabeaufforderung einen Benutzernamen für die Wartung ein, und klicken Sie auf **Enter**.

   Der Wartungsbenutzername muss mit einem Buchstaben von a-z beginnen, gefolgt von einer beliebigen Kombination aus -, a-z oder 0-9.

9. Geben Sie an der Eingabeaufforderung ein Passwort ein und klicken Sie auf **Enter**.

   Die VM-Konsole zeigt die URL der Web-UI von Unified Manager an.

Nachdem Sie fertig sind

Sie können auf die Web-UI zugreifen, um die Ersteinrichtung von Unified Manager durchzuführen, wie im *OnCommand Unified Manager System Configuration Guide* beschrieben.

Upgrade von Unified Manager auf VMware

Sie können ein Upgrade auf Unified Manager Version 9.5 nur von Instanzen von Unified Manager 7.3 oder 9.4 durchführen.

Über diese Aufgabe

Während des Upgrades ist Unified Manager nicht verfügbar. Vor dem Upgrade von Unified Manager sollten alle laufenden Vorgänge abgeschlossen werden.

Wenn Unified Manager mit einer Instanz von OnCommand Workflow Automation gekoppelt ist und für beide

Produkte neue Versionen der Software zur Verfügung stehen, müssen Sie die beiden Produkte trennen und anschließend eine neue Workflow-Automatisierungsverbindung einrichten, nachdem Sie die Upgrades durchgeführt haben. Wenn Sie ein Upgrade auf nur eines der Produkte durchführen, müssen Sie sich nach dem Upgrade bei Workflow Automation anmelden und überprüfen, ob noch Daten von Unified Manager erfasst werden.

Herunterladen des Unified Manager ISO-Images

Vor dem Upgrade von Unified Manager müssen Sie das Unified Manager ISO Image von der NetApp Support Site herunterladen.

Bevor Sie beginnen

Sie müssen Anmeldedaten für die NetApp Support-Website besitzen.

Schritte

1. Loggen Sie sich auf der NetApp Support Site ein und öffnen Sie die Seite zum Software Download.
2. Laden Sie herunter, und speichern Sie die `.iso` Bilddatei in ein lokales Verzeichnis oder Netzwerkverzeichnis, auf das Ihr vSphere Client zugreifen kann.
3. Überprüfen Sie die Prüfsumme, um sicherzustellen, dass die Software ordnungsgemäß heruntergeladen wurde.

Verwandte Informationen

"NetApp Support"

Aktualisieren der virtuellen Unified Manager Appliance

Sie können ein Upgrade von Unified Manager Version 7.3 oder 9.4 auf Unified Manager 9.5 durchführen.

Bevor Sie beginnen

- Sie müssen das heruntergeladen haben `.iso` Datei von der NetApp Support Site
- Das System, auf dem Unified Manager aktualisiert wird, muss die System- und Software-Anforderungen erfüllen.

  Anforderungen an die virtuelle Infrastruktur

  VMware Software- und Installationsanforderungen

- Für vSphere 6.5-Benutzer müssen Sie die VMware Remote Console (VMRC) installiert haben.
- Sie müssen die folgenden Informationen haben:
  - Anmeldedaten für die NetApp Support-Website
  - Zugangsdaten für den Zugriff auf VMware vCenter Server und vSphere Web Client (für vSphere Version 6.5) oder vSphere Client (für vSphere Version 5.5 oder 6.0)
  - Anmeldedaten für den Unified Manager-Wartungsbenutzer

Über diese Aufgabe

Während des Upgrades ist Unified Manager nicht verfügbar. Vor dem Upgrade von Unified Manager sollten alle laufenden Vorgänge abgeschlossen werden.

Wenn Workflow Automation und Unified Manager gekoppelt sind, müssen Sie den Hostnamen in Workflow Automation manuell aktualisieren.

Schritte

1. Klicken Sie im vSphere Client auf **Startseite** > **Inventar** > **VMs und Vorlagen**.
2. Wählen Sie die virtuelle Maschine (VM) aus, auf der die virtuelle Unified Manager Appliance installiert ist.
3. Wenn die Unified Manager-VM ausgeführt wird, navigieren Sie zu **Zusammenfassung** > **Befehle** > **Herunterfahren Gast**.
4. Erstellen Sie eine Backup-Kopie wie beispielsweise einen Snapshot oder Klon der Unified Manager VM, um ein applikationskonsistentes Backup zu erstellen.
5. Schalten Sie über vSphere Client die Unified Manager VM ein.
6. Wählen Sie das Unified Manager Upgrade-Image aus:

Sie verwenden…	Dann tun Sie das…
VSphere 5.5 oder 6.0	a. Klicken Sie auf das Symbol * CD/DVD Drive* und wählen Sie auf der lokalen Festplatte * * * die Option mit ISO-Image verbinden. b. Wählen Sie die aus `OnCommandUnifiedManager-9.5-virtual-update.iso` Datei und klicken Sie auf **Öffnen**.
VSphere 6.5	a. Starten Sie die VMware Remote Console. b. Klicken Sie auf das Symbol **CD-ROM** und wählen Sie **mit der Datenträgerbilddatei verbinden (.iso)** aus. c. Wählen Sie die aus `OnCommandUnifiedManager-9.5-virtual-update.iso` Datei und klicken Sie auf **Öffnen**.

7. Klicken Sie auf die Registerkarte **Konsole**.
8. Melden Sie sich bei der Wartungskonsole von Unified Manager an.
9. Wählen Sie im Hauptmenü * die Option **Upgrade**.

   Es wird eine Meldung angezeigt, dass Unified Manager während des Aktualisierungsvorgangs nicht verfügbar ist und nach Abschluss wieder aufgenommen wird.

10. Typ `y` Um fortzufahren.

    Es wird eine Warnung angezeigt, die Sie daran erinnert, die virtuelle Maschine zu sichern, auf der sich das virtuelle Gerät befindet.

11. Typ `y` Um fortzufahren.

    Der Upgrade-Prozess und der Neustart von Unified Manager Services können mehrere Minuten dauern.

12. Drücken Sie eine beliebige Taste, um fortzufahren.

    Sie werden automatisch von der Wartungskonsole abgemeldet.

13. Loggen Sie sich bei der Wartungskonsole ein und überprüfen Sie die Version von Unified Manager.

Nachdem Sie fertig sind

Sie können sich bei der Web-Benutzeroberfläche anmelden, um die aktualisierte Version von Unified Manager zu verwenden. Beachten Sie, dass Sie warten müssen, bis der Erkennungsvorgang abgeschlossen ist, bevor Sie eine Aufgabe in der Benutzeroberfläche ausführen.

Starten Sie die Virtual Machine von Unified Manager neu

Sie können die virtuelle Maschine (VM) von Unified Manager von der Wartungskonsole aus neu starten. Sie müssen die VM nach dem Generieren eines neuen Sicherheitszertifikats neu starten oder wenn Probleme mit der VM auftreten.

Bevor Sie beginnen

- Die virtuelle Appliance muss eingeschaltet sein.
- Sie müssen als Wartungbenutzer bei der Unified Manager Wartungskonsole angemeldet sein.

Über diese Aufgabe

Sie können die virtuelle Maschine auch von vSphere mit der Option VMware **Neustart Gast** neu starten.

Schritte

1. Wählen Sie in der Wartungskonsole **Systemkonfiguration** > **virtuelle Maschine neu starten** aus.
2. Starten Sie in Ihrem Browser die grafische Benutzeroberfläche von Unified Manager (GUI), und melden Sie sich an.

Verwandte Informationen

"VMware vSphere PowerCLI cmdlets Referenz: Neustart-VMGuest"

Entfernen von Unified Manager aus VMware

Sie können Unified Manager deinstallieren, indem Sie die virtuelle Appliance zerstören, auf der die Unified Manager-Software installiert ist.

Bevor Sie beginnen

- Sie benötigen Zugangsdaten für den Zugriff auf VMware vCenter Server und vSphere Web Client (für vSphere Version 6.5) oder vSphere Client (für vSphere Version 5.5 oder 6.0).
- Der Unified Manager-Server darf keine aktive Verbindung zu einem externen Datenanbieter haben.

Wenn eine aktive Verbindung besteht, müssen Sie die Verbindung über die Unified ManagerMaintenance-Konsole löschen.

- Der Unified Manager-Server darf keine aktive Verbindung zu einem Workflow Automation-Server haben.

  Wenn eine aktive Verbindung besteht, müssen Sie die Verbindung über das Menü Administration löschen.

- Alle Cluster (Datenquellen) müssen vom Unified Manager-Server entfernt werden, bevor Sie die virtuelle Maschine (VM) löschen.

Schritte

1. Überprüfen Sie mithilfe der Unified ManagerMaintenance-Konsole, ob der Unified Manager-Server keine aktive Verbindung zu einem externen Datenanbieter hat.
2. Klicken Sie im vSphere Client auf **Startseite** > **Inventar** > **VMs und Vorlagen**.
3. Wählen Sie die VM aus, die Sie zerstören möchten, und klicken Sie auf die Registerkarte **Zusammenfassung**.
4. Wenn die VM ausgeführt wird, klicken Sie auf **Power** > **Herunterfahren Gast**.
5. Klicken Sie mit der rechten Maustaste auf die VM, die Sie zerstören möchten, und klicken Sie auf **von Festplatte löschen**.

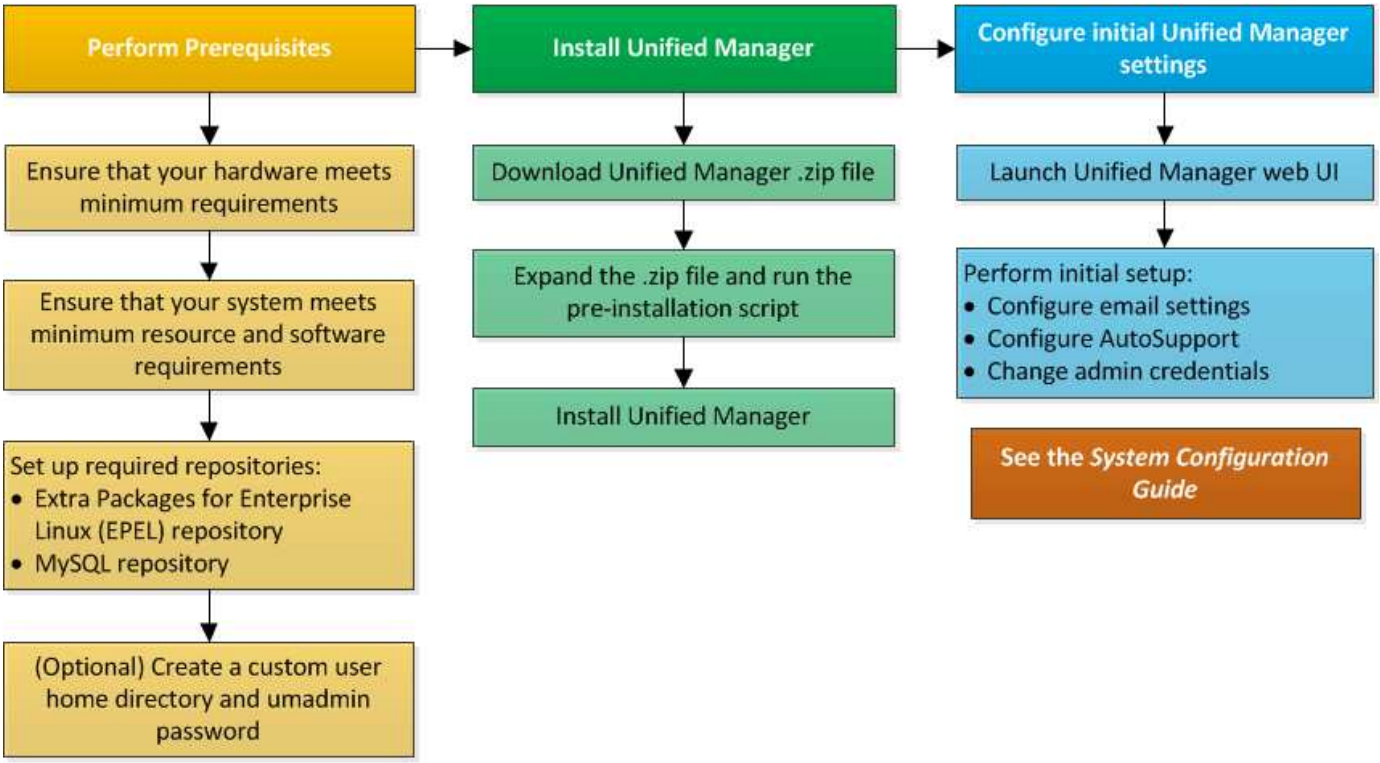
Installation, Aktualisierung und Entfernung der Unified Manager Software unter Red hat oder CentOS

Unter Linux-Systemen können Sie Unified Manager installieren, auf eine neuere Softwareversion aktualisieren oder Unified Manager entfernen.

Unified Manager kann auf Red hat Enterprise Linux oder CentOS Servern installiert werden. Der Linux-Server, auf dem Unified Manager installiert wird, kann entweder auf einem physischen Rechner oder auf einer virtuellen Maschine ausgeführt werden, die auf VMware ESXi, Microsoft Hyper-V oder Citrix XenServer ausgeführt wird.

Überblick über den Installationsprozess auf Red hat oder CentOS

Im Installations-Workflow werden die Aufgaben beschrieben, die Sie vor der Verwendung von Unified Manager ausführen müssen.



Einrichten der erforderlichen Software-Repositorys

Das System muss Zugriff auf bestimmte Repositories haben, damit das Installationsprogramm alle erforderlichen Softwareabhängigkeiten aufrufen und installieren kann.

Manuelles Konfigurieren des EPEL-Repositorys

Wenn das System, auf dem Sie Unified Manager installieren, keinen Zugriff auf das EPEL-Repository (Extra Packages for Enterprise Linux) hat, müssen Sie das Repository manuell herunterladen und für eine erfolgreiche Installation konfigurieren.

Über diese Aufgabe

Das EPEL-Repository bietet Zugriff auf die erforderlichen Drittanbieter-Dienstprogramme, die auf Ihrem System installiert werden müssen. Sie verwenden das EPEL-Repository, unabhängig davon, ob Sie Unified Manager auf einem Red hat oder CentOS-System installieren.

Schritte

1. Laden Sie das EPEL-Repository für Ihre Installation herunter: `wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm`
2. EPEL-Repository konfigurieren: `yum install epel-release-latest-7.noarch.rpm`

Manuelles Konfigurieren des MySQL-Repository

Wenn das System, auf dem Sie Unified Manager installieren, keinen Zugriff auf das MySQL Community Edition Repository hat, müssen Sie das Repository manuell

herunterladen und konfigurieren, damit eine erfolgreiche Installation durchgeführt werden kann.

Über diese Aufgabe

Das MySQL-Repository bietet Zugriff auf die erforderliche MySQL-Software, die auf Ihrem System installiert werden muss.

> Diese Aufgabe schlägt fehl, wenn das System keine Internetverbindung hat. Beachten Sie die MySQL-Dokumentation, wenn das System, auf dem Sie Unified Manager installieren, keinen Internetzugang hat.

Schritte

1. Laden Sie das entsprechende MySQL-Repository für Ihre Installation herunter: `wget http://repo.mysql.com/yum/mysql-5.7-community/el/7/x86_64/mysql57-community-release-el7-7.noarch.rpm`
2. Konfigurieren Sie das MySQL-Repository: `yum install mysql57-community-release-el7-7.noarch.rpm`

SELinux Anforderungen zum Mounten von /opt/netapp oder /opt/netapp/Daten auf einer NFS- oder CIFS-Freigabe

Wenn Sie die Montage planen `/opt/netapp` Oder `/opt/netapp/data` Auf einem NAS- oder SAN-Gerät, und SELinux ist aktiviert, müssen Sie die folgenden Überlegungen beachten.

Über diese Aufgabe

Wenn planen, zu montieren `/opt/netapp` Oder `/opt/netapp/data` Von überall dort, wo das Root-Dateisystem und SELinux in Ihrer Umgebung aktiviert sind, müssen Sie den richtigen Kontext für die gemounteten Verzeichnisse festlegen. Befolgen Sie diese beiden Schritte, um den richtigen SELinux-Kontext zu setzen und zu bestätigen.

- Konfigurieren Sie SELinux-Kontext, wenn `/opt/netapp/data` Angehängt ist
- Konfigurieren Sie SELinux-Kontext, wenn `/opt/netapp` Angehängt ist

Konfigurieren des SELinux-Kontexts Wann `/opt/netapp/data` Ist montiert

Wenn Sie angehängt sind `/opt/netapp/data` In Ihrem System und SELinux ist auf festgelegt `Enforcing`, Stellen Sie sicher, dass der SELinux-Kontexttyp für `/opt/netapp/data` Ist auf festgelegt `mysqld_db_t`, Das ist das Standard-Kontextelement für den Speicherort der Datenbankdateien.

1. Führen Sie diesen Befehl aus, um den Kontext zu überprüfen: `ls -dZ /opt/netapp/data`

   Beispielausgabe:

   ```
   drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0
   /opt/netapp/data
   ```

In dieser Ausgabe ist der Kontext `default_t` Das muss in geändert werden `mysqld_db_t`.

2. Führen Sie diese Schritte aus, um den Kontext basierend auf der Art und Weise festzulegen, wie Sie angehängt haben `/opt/netapp/data`.
   a. Führen Sie die folgenden Befehle aus, um den Kontext auf einzustellen `mysqld_db_t`: `semanage fcontext -a -t mysql_db_t "/opt/netapp/data"``restorecon -R -v /opt/netapp/data`
   b. Wenn Sie konfiguriert haben `/opt/netapp/data` In `/etc/fstab`, Sie müssen die bearbeiten `/etc/fstab` Datei: Für das `/opt/netapp/data/` Mount-Option, fügen Sie die MySQL-Bezeichnung wie folgt hinzu: `context=system_u:object_r:mysqld_db_t:s0`
   c. Heben Sie die Bereitstellung ab und montieren Sie sie wieder `/opt/netapp/data/` Zum Aktivieren des Kontexts.
   d. Wenn Sie über einen direkten NFS-Mount verfügen, führen Sie den folgenden Befehl aus, um den Kontext auf festzulegen `mysql_db_t`: `mount <nfsshare>:/<mountpoint> /opt/netapp/data -o context=system_u:object_r:mysql_db_t:s0`
3. Überprüfen Sie, ob der Kontext richtig eingestellt ist: `ls -dZ /opt/netapp/data/`

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/
```

Konfigurieren des SELinux-Kontexts Wann `/opt/netapp` Ist montiert

Nachdem Sie den richtigen Kontext für festgelegt haben `/opt/netapp/data/`, Stellen Sie sicher, dass das übergeordnete Verzeichnis `/opt/netapp` Der SELinux-Kontext ist nicht auf festgelegt `file_t`.

1. Führen Sie diesen Befehl aus, um den Kontext zu überprüfen: `ls -dZ /opt/netapp`

   Beispielausgabe:

```
drwxr-xr-x. mysql root unconfined_u:object_r:file_t:s0 /opt/netapp
```

   In dieser Ausgabe ist der Kontext `file_t` Das muss geändert werden. Mit den folgenden Befehlen wird der Kontext auf festgelegt `usr_t`. Sie können den Kontext auf einen anderen Wert als einstellen `file_t` Basierend auf Ihren Sicherheitsanforderungen

2. Führen Sie diese Schritte aus, um den Kontext basierend auf der Art und Weise festzulegen, wie Sie angehängt haben `/opt/netapp`.
   a. Führen Sie die folgenden Befehle aus, um den Kontext festzulegen: `semanage fcontext -a -t usr_t "/opt/netapp"``restorecon -v /opt/netapp`
   b. Wenn Sie konfiguriert haben `/opt/netapp` In `/etc/fstab`, Sie müssen die bearbeiten `/etc/fstab` Datei: Für das `/opt/netapp` Mount-Option, fügen Sie die MySQL-Bezeichnung wie folgt hinzu: `context=system_u:object_r:usr_t:s0`
   c. Heben Sie die Bereitstellung ab und montieren Sie sie wieder `/opt/netapp` Zum Aktivieren des Kontexts.

d. Wenn Sie über einen direkten NFS-Mount verfügen, führen Sie den folgenden Befehl aus, um den Kontext festzulegen: `mount <nfsshare>:/<mountpoint> /opt/netapp -o context=system_u:object_r:usr_t:s0`

3. Überprüfen Sie, ob der Kontext richtig eingestellt ist: `ls -dZ /opt/netapp`

```
drwxr-xr-x. mysql root unconfined_u:object_r:usr_t:s0 /opt/netapp
```

Installation von Unified Manager unter Red hat Enterprise Linux oder CentOS

Sie müssen wissen, dass die Schritte zum Herunterladen und Installieren von Unified Manager je nach Installationsszenario unterschiedlich sind. Bevor Sie Unified Manager auf Red hat Enterprise Linux oder CentOS installieren, können Sie entscheiden, ob Sie Unified Manager für Hochverfügbarkeit konfigurieren möchten.

Erstellen eines benutzerdefinierten Home-Verzeichnisses für Benutzer und eines umadmin-Passworts vor der Installation

Sie können ein benutzerdefiniertes Home-Verzeichnis erstellen und Ihr eigenes umadmin-Benutzerpasswort vor der Installation von Unified Manager definieren. Diese Aufgabe ist optional, aber einige Standorte benötigen möglicherweise die Flexibilität, die Standardeinstellungen für die Unified Manager-Installation zu überschreiben.

Bevor Sie beginnen

- Das System muss die in beschriebenen Anforderungen erfüllen Hardwaresystemanforderungen.
- Sie müssen sich als Root-Benutzer beim Red hat Enterprise Linux oder CentOS System anmelden können.

Über diese Aufgabe

Die Standardinstallation von Unified Manager führt die folgenden Aufgaben aus:

- Erstellt den umadmin-Benutzer mit `/home/umadmin` Als Home Directory damit füllt.
- Weist dem umadmin-Benutzer das Standardpasswort „`admin`“ zu.

Weil einige Installationsumgebungen den Zugriff auf beschränken `/home`, Die Installation schlägt fehl. Sie müssen das Home-Verzeichnis an einem anderen Speicherort erstellen. Darüber hinaus können auf einigen Websites Regeln über die Komplexität von Passwörtern oder die Festlegung von Passwörtern durch lokale Administratoren statt durch das Installationsprogramm festgelegt werden.

Wenn in Ihrer Installationsumgebung die Standardeinstellungen dieser Installation außer Kraft gesetzt werden müssen, führen Sie die folgenden Schritte aus, um ein benutzerdefiniertes Home-Verzeichnis zu erstellen und das Kennwort des umadmin-Benutzers zu definieren.

Wenn diese Informationen vor der Installation definiert werden, erkennt das Installationsskript diese Einstellungen und verwendet die definierten Werte anstatt die Standardeinstellungen der Installation zu verwenden.

Darüber hinaus enthält die standardmäßige Unified Manager-Installation den umadmin-Benutzer in den

Sudoers-Dateien (`ocum_sudoers` Und `ocie_sudoers`) Im `/etc/sudoers.d/` Verzeichnis. Wenn Sie diesen Inhalt aufgrund von Sicherheitsrichtlinien aus Ihrer Umgebung entfernen oder aufgrund eines Tools zur Sicherheitsüberwachung wieder hinzufügen müssen. Sie müssen die sudoers-Konfiguration beibehalten, da für einige Unified Manager-Vorgänge diese sudo-Berechtigungen erforderlich sind.

Schritte

1. Melden Sie sich als Root-Benutzer beim Server an.
2. Erstellen Sie das umadmin Gruppenkonto mit dem Namen “maintual”:`groupadd maintenance`
3. Erstellen Sie das Benutzerkonto „`umadmin`“ in der Wartungsgruppe unter einem Home-Verzeichnis Ihrer Wahl:`adduser --home <home_directory\> -g maintenance umadmin`
4. Definieren Sie das umadmin-Passwort:`passwd umadmin`

   Das System fordert Sie zur Eingabe einer neuen Passwort-Zeichenfolge für den umadmin-Benutzer auf.

Nachdem Sie fertig sind

Nachdem Sie Unified Manager installiert haben, müssen Sie die Anmeldungs-Shell für den umadmin-Benutzer angeben.

Herunterladen von Unified Manager für Red hat Enterprise Linux oder CentOS

Sie müssen Unified Manager herunterladen `.zip` Datei von der NetApp Support Site zur Installation von Unified Manager.

Bevor Sie beginnen

Sie müssen Anmeldedaten für die NetApp Support-Website besitzen.

Über diese Aufgabe

Sowohl für Red hat Enterprise Linux als auch für CentOS Systeme laden Sie das gleiche Unified Manager Installationspaket herunter.

Schritte

1. Melden Sie sich auf der NetApp Support Site an und navigieren Sie zur Download-Seite, um Unified Manager auf der Red hat Enterprise Linux Plattform zu installieren.

   "NetApp Downloads: Software"

2. Laden Sie Unified Manager herunter `.zip` Datei in ein Verzeichnis auf dem Zielsystem.
3. Überprüfen Sie die Prüfsumme, um sicherzustellen, dass die Software ordnungsgemäß heruntergeladen wurde.

Installation von Unified Manager unter Red hat Enterprise Linux oder CentOS

Sie können Unified Manager auf einer physischen oder virtuellen Red hat Enterprise Linux oder CentOS Plattform installieren.

Bevor Sie beginnen

- Das System, auf dem Unified Manager installiert werden soll, muss die System- und Softwareanforderungen erfüllen.

  Hardwaresystemanforderungen

  Anforderungen an Red hat und CentOS Software und Installation

- Sie müssen Unified Manager heruntergeladen haben `.zip` Datei von der NetApp Support Site auf das Zielsystem
- Sie benötigen einen unterstützten Webbrowser.
- Die Terminalemulationssoftware muss ScRollback aktiviert haben.

Über diese Aufgabe

Das Red hat Enterprise Linux oder CentOS System kann alle erforderlichen Versionen der erforderlichen Hilfssoftware (Java, MySQL, zusätzliche Utilities) installiert haben, oder es kann nur einige der erforderlichen Software installiert haben, oder es kann ein neu installiertes System mit keiner der erforderlichen Software installiert sein.

Schritte

1. Melden Sie sich beim Server an, auf dem Sie Unified Manager installieren.
2. Geben Sie die entsprechenden Befehle ein, um zu ermitteln, welche Software möglicherweise eine Installation oder ein Upgrade auf dem Zielsystem erforderlich ist, um die Installation zu unterstützen:

Erforderliche Software und Mindestversion	Befehl zum Überprüfen der Software und der Version
OpenJDK Version 11	`java -version`
MySQL 5.7.23 Community Edition	`rpm -qa
grep -i mysql`	P7zip 9.20.1
`rpm -qa	grep p7zip`

3. Wenn eine beliebige Version der aufgeführten Software vor der erforderlichen Version liegt, geben Sie den entsprechenden Befehl ein, um das Modul zu deinstallieren:

Zu deinstallierenden Software	Befehl zum Deinstallieren der Software
MySQL Deinstallieren Sie alle Versionen, die nicht MySQL 5.7.23 Community Edition oder höher sind.	`rpm -e <mysql_package_name>` Wenn Sie Abhängigkeitsfehler erhalten, müssen Sie das hinzufügen `--nodeps` Option zum Deinstallieren der Komponente.

Zu deinstallierenden Software	Befehl zum Deinstallieren der Software
Alle anderen Module	`yum remove module_name`

4. Navigieren Sie zum Verzeichnis, in dem Sie die Installation heruntergeladen haben `.zip` Datei und Erweiterung des Unified Manager Bundles: `unzip OnCommandUnifiedManager-rhel7-9.5.zip`

   Erforderlich `.rpm` Module für Unified Manager werden in das Zielverzeichnis entpackt.

5. Stellen Sie sicher, dass die folgenden Module im Verzeichnis verfügbar sind: `ls *.rpm`
   - `ocie-au-<version>.x86_64.rpm`
   - `ocie-server-<version>.x86_64.rpm`
   - `ocie-serverbase-<version>.x86_64.rpm`
   - `netapp-application-server-<version>.x86_64.rpm`
   - `netapp-platform-base-<version>.x86_64.rpm`
   - `netapp-ocum-<version>.x86_64.rpm`
6. Führen Sie das Skript vor der Installation aus, um sicherzustellen, dass keine Systemkonfigurationseinstellungen oder installierte Software vorhanden sind, die mit der Installation von Unified Manager in Konflikt geraten: `pre_install_check.sh`

   Das Skript vor der Installation überprüft, ob das System über ein gültiges Red hat-Abonnement verfügt und dass es Zugriff auf die erforderlichen Software-Repositorys hat. Wenn das Skript Probleme erkennt, müssen Sie die Probleme vor der Installation von Unified Manager beheben.

   ⓘ Sie müssen Schritt 7 *Only* ausführen, wenn Sie die für Ihre Installation erforderlichen Pakete manuell herunterladen müssen. Wenn Ihr System über einen Internetzugang verfügt und alle erforderlichen Pakete verfügbar sind, fahren Sie mit Schritt 8 fort.

7. Bei Systemen, die nicht mit dem Internet verbunden sind oder die Red hat Enterprise Linux-Repositories nicht verwenden, führen Sie die folgenden Schritte aus, um festzustellen, ob erforderliche Pakete fehlen und diese Pakete anschließend herunterladen:
   a. Zeigen Sie auf dem System, auf dem Sie Unified Manager installieren, die Liste der verfügbaren und nicht verfügbaren Pakete an: `yum install *.rpm --assumeno`

      Die Elemente im Abschnitt „`Installieren:`“ sind die Pakete, die im aktuellen Verzeichnis verfügbar sind, und die Elemente im Abschnitt „`Installieren für Abhängigkeiten:`“ sind die Pakete, die auf Ihrem System fehlen.

   b. Laden Sie auf einem System mit Internetzugang die fehlenden Pakete herunter: `yum install <package_name\> --downloadonly --downloaddir=.`

      ⓘ Da das Plug-in “yum-Plugin-downloadonly” nicht immer auf Red hat Enterprise Linux-Systemen aktiviert ist, müssen Sie möglicherweise die Funktionalität zum Herunterladen eines Pakets ohne Installation aktivieren: `yum install yum-plugin-downloadonly`

   c. Kopieren Sie die fehlenden Pakete aus dem mit dem Internet verbundenen System auf Ihr

Installationssystem.

8. Installieren der Software: `yum install *.rpm`

   Mit diesem Befehl wird der installiert `.rpm` Pakete, alle anderen erforderlichen unterstützende Software sowie die Unified Manager Software.

   > Versuchen Sie nicht, die Installation mithilfe alternativer Befehle (z. B. `rpm -ivh ...`). Für die erfolgreiche Installation von Unified Manager auf einem Red hat Enterprise Linux- oder CentOS-System müssen alle Unified Manager-Dateien und zugehörigen Dateien in einer bestimmten Reihenfolge in eine bestimmte Verzeichnisstruktur installiert werden, die automatisch von der erzwungen wird `yum install *.rpm` Befehl.

9. Ignorieren Sie die E-Mail-Benachrichtigung, die sofort nach den Installationsmeldungen angezeigt wird.

   Die E-Mail informiert den Root-Benutzer über einen anfänglichen cron-Job-Fehler, der sich nicht nachteilig auf die Installation auswirkt.

10. Nach Abschluss der Installationsmeldungen blättern Sie zurück zu den Meldungen, bis die Meldung angezeigt wird, in der das System eine IP-Adresse oder URL für die Web-UI von Unified Manager, den Wartungs-Benutzernamen (umadmin) und ein Standardpasswort anzeigt.

    Die Meldung ähnelt der folgenden:

    ```
    OnCommand Unified Manager installed successfully.
    Use a web browser and one of the following URL(s) to configure and
    access the Unified Manager GUI.
    https://default_ip_address/    (if using IPv4)
    https://[default_ip_address]/  (if using IPv6)
    https://fully_qualified_domain_name/

    Log in to Unified Manager in a web browser by using following details:
      username: umadmin
      password: admin
    ```

11. Notieren Sie die IP-Adresse oder URL, den zugewiesenen Benutzernamen (umadmin) und das aktuelle Passwort.
12. Wenn Sie vor der Installation von Unified Manager ein umadmin-Benutzerkonto mit einem benutzerdefinierten Home-Verzeichnis erstellt haben, müssen Sie die Anmeldungs-Shell für umadmin-Benutzer angeben:`usermod -s /bin/maintenance-user-shell.sh umadmin`

Nachdem Sie fertig sind

Sie können auf die Web-UI zugreifen, um die Ersteinrichtung von Unified Manager durchzuführen, wie im *OnCommand Unified Manager System Configuration Guide* beschrieben.

Benutzer, die während der Unified Manager-Installation erstellt wurden

Wenn Sie Unified Manager auf Red hat Enterprise Linux oder CentOS installieren, werden die folgenden Benutzer von Unified Manager und Dienstprogrammen von

Drittanbietern erstellt: Umadmin, jboss und mysql.

- **Umadmin**

  Wird zur ersten Anmeldung bei Unified Manager verwendet. Diesem Benutzer wird eine Benutzerrolle „`OnCommand Administrator`“ zugewiesen und als Typ „`MWartung Benutzer`“ konfiguriert. Dieser Benutzer wird von Unified Manager erstellt.

- **jboss**

  Wird zum Ausführen von Unified Manager-Services im Zusammenhang mit dem JBoss-Dienstprogramm verwendet. Dieser Benutzer wird von Unified Manager erstellt.

- * Mysql*

  Führt MySQL-Datenbankabfragen von Unified Manager aus. Dieser Benutzer wird vom externen Dienstprogramm MySQL erstellt.

Zusätzlich zu diesen Benutzern erstellt Unified Manager auch entsprechende Gruppen: Maintenance, jboss und mysql. Die Wartungs- und jboss-Gruppen werden von Unified Manager erstellt, während die mysql-Gruppe von einem externen Dienstprogramm erstellt wird.

Wenn Sie vor der Installation von Unified Manager ein benutzerdefiniertes Home-Verzeichnis erstellt und Ihr eigenes umadmin-Benutzerpasswort festgelegt haben, wird die Wartungsgruppe oder der Benutzer umadmin nicht neu erstellt.

Ändern des JBoss-Passworts

Sie können ein neues, benutzerdefiniertes JBoss-Kennwort erstellen, um das bei der Installation festgelegte Standardpasswort zu überschreiben. Diese Aufgabe ist optional, aber an einigen Standorten muss diese Sicherheitsfunktion möglicherweise die Standardeinstellung für die Unified Manager-Installation außer Kraft setzen. Dieser Vorgang ändert auch das Passwort, das JBoss zum Zugriff auf MySQL verwendet.

Bevor Sie beginnen

- Sie müssen Root-Zugriff auf das Red hat Enterprise Linux oder CentOS System haben, auf dem Unified Manager installiert ist.
- Sie müssen auf die von NetApp bereitgestellte Lösung zugreifen können `password.sh` Skript im Verzeichnis `/opt/netapp/essentials/bin`.

Schritte

1. Melden Sie sich als Root-Benutzer auf dem System an.
2. Beenden Sie die Unified Manager Services, indem Sie die folgenden Befehle in der angezeigten Reihenfolge eingeben: `service ocieau stop``service ocie stop`

   Beenden Sie die zugehörige MySQL-Software nicht.

3. Geben Sie den folgenden Befehl ein, um den Passwortänderungsprozess zu starten: `/opt/netapp/essentials/bin/password.sh resetJBossPassword`

4. Geben Sie bei Aufforderung das alte JBoss-Passwort ein.

   Das Standardpasswort lautet `D11h1aMu@79%`.

5. Geben Sie bei entsprechender Aufforderung das neue JBoss-Passwort ein und bestätigen Sie es anschließend erneut.
6. Starten Sie nach Abschluss des Skripts die Unified Manager Services, indem Sie in der angezeigten Reihenfolge die folgenden Befehle eingeben: `service ocie start``service ocieau start`
7. Nachdem alle Services gestartet wurden, können Sie sich in der UI von Unified Manager einloggen.

Einrichtung von Unified Manager für Hochverfügbarkeit

Mithilfe des Veritas Cluster Server (VCS) können Sie eine Konfiguration mit hoher Verfügbarkeit erstellen. Das Hochverfügbarkeits-Setup bietet Failover-Funktionen und hilft bei Disaster Recovery.

In einer Hochverfügbarkeitseinrichtung bleibt jeweils nur ein Node aktiv. Wenn ein Node ausfällt, erkennt der VCS-Service dieses Ereignis und überträgt sofort die Kontrolle auf den anderen Node. Der zweite Node im Setup wird aktiv und beginnt mit der Bereitstellung von Services. Der Failover-Prozess erfolgt automatisch.

Ein VCS Cluster, der mit dem Unified Manager Server konfiguriert ist, besteht aus zwei Knoten, wobei jeder Knoten dieselbe Version des Unified Manager ausführt. Alle Unified Manager-Serverdaten müssen für den Zugriff von einer gemeinsam genutzten Datenfestplatte konfiguriert werden.

Nach der Installation von Unified Manager in VCS müssen Sie Unified Manager konfigurieren, um in der VCS-Umgebung arbeiten zu können. Über Konfigurationsskripte kann Unified Manager für die Arbeit in VCS Umgebungen eingerichtet werden.

Anforderungen an Unified Manager in VCS

Vor der Installation von Unified Manager in einer Veritas Cluster Server (VCS) Umgebung müssen Sie sicherstellen, dass die Clusterknoten ordnungsgemäß konfiguriert sind, um Unified Manager zu unterstützen.

Sie müssen sicherstellen, dass die VCS-Konfiguration die folgenden Anforderungen erfüllt:

- Auf beiden Cluster-Nodes muss eine unterstützte Betriebssystemversion ausgeführt werden.
- Die gleiche Version von Unified Manager muss auf beiden Cluster-Nodes mithilfe des gleichen Pfads installiert werden.
- Der MySQL-Benutzer auf beiden Knoten muss die gleiche Benutzer-ID und Gruppen-ID haben.
- Es müssen native ext3-, ext4-Dateisysteme und LVM (Logical Volume Manager) verwendet werden.
- Unified Manager muss über Fibre Channel (FC) oder iSCSI mit dem Storage-System verbunden sein.

  Sie müssen außerdem sicherstellen, dass die FC-Verbindung aktiv ist und dass die auf den Storage-Systemen erstellten LUNs beiden Cluster-Nodes zugänglich sind.

- Die gemeinsam genutzte Datenfestplatte muss über ausreichend Speicherplatz (mindestens 80 GB) für die Unified Manager-Datenbank, Berichte, Zertifikate und Skript-Plug-in-Ordner verfügen.
- Auf jedem System müssen mindestens zwei Netzwerkschnittstellen eingerichtet sein: Eine für die Node-zu-Node-Kommunikation und die andere für die Node-to-Client-Kommunikation.

Der Name der für die Kommunikation zwischen Nodes und Clients verwendeten Netzwerkschnittstelle muss auf beiden Systemen identisch sein.

- Zwischen den Cluster-Nodes muss eine separate Heartbeat-Verbindung hergestellt werden. Andernfalls wird die Netzwerkschnittstelle für die Kommunikation zwischen den Cluster-Nodes verwendet.
- Optional: SnapDrive für UNIX sollte verwendet werden, um einen freigegebenen Speicherort zu erstellen, der beiden Knoten in einem hochverfügbaren Setup zugänglich ist.

  Informationen zum Installieren und Erstellen eines gemeinsam genutzten Speicherorts finden Sie im Handbuch *SnapDrive for UNIX Installation and Administration*. Sie können auch LUNs über SnapDrive oder die Befehlszeilenschnittstelle des Storage-Systems verwalten. Weitere Informationen finden Sie in der Kompatibilitätsmatrix für SnapDrive für UNIX.

- Für die SnapDrive- und VCS-Anwendungen muss zusätzlicher RAM verfügbar sein.

Installieren von Unified Manager auf VCS

Zur Konfiguration der Hochverfügbarkeit müssen Sie Unified Manager auf beiden Cluster-Knoten von VCS installieren.

Bevor Sie beginnen

- VCS muss auf beiden Knoten des Clusters installiert und konfiguriert sein.

  Weitere Informationen zur Installation von VCS finden Sie in der Anleitung zum *Veritas Cluster Server 6.2.1 Installation Guide*.

- Sie müssen über klare Root-Berechtigungen verfügen, um sich bei der Unified Manager-Serverkonsole anzumelden.

Über diese Aufgabe

Sie müssen beide Instanzen von Unified Manager konfigurieren, um dieselbe Datenbank zu verwenden und denselben Satz Nodes zu überwachen.

Schritte

1. Melden Sie sich beim ersten Node des Clusters an.
2. Installation von Unified Manager auf dem ersten Node

   Installation von Unified Manager unter Red hat Enterprise Linux oder CentOS

3. Wiederholen Sie die Schritte 1 und 2 auf dem zweiten Node des Clusters.
4. Melden Sie sich bei der zweiten Instanz von Unified Manager als Root-Benutzer beim Red hat Enterprise Linux oder CentOS Server an und geben Sie das gleiche umadmin Passwort ein, das Sie in der ersten Instanz von Unified Manager festgelegt haben.`passwd umadmin`

Konfiguration von Unified Manager mit VCS mithilfe von Konfigurationsskripten

Sie können Unified Manager mit Veritas Cluster Server (VCS) mit Konfigurationsskripten konfigurieren.

Bevor Sie beginnen

- Unified Manager muss auf beiden Knoten in der VCS Setup installiert sein.
- Das XML: LibXML-Modul muss mit Perl gebündelt werden, damit VCS-Skripte funktionieren können.
- Sie müssen eine gemeinsame LUN mit ausreichender Größe erstellt haben, um den Quell-Unified Manager-Daten gerecht zu werden.
- Sie müssen den absoluten Mount-Pfad angegeben haben, damit das Skript funktioniert.

  Das Skript funktioniert nicht, wenn Sie einen Ordner im Mount-Pfad erstellen.

- Sie müssen das heruntergeladen haben `ha_setup.pl` Skript an `/opt/netapp/ocum/scripts`.

Über diese Aufgabe

Im VCS-Setup ist der Knoten, für den die virtuelle IP-Schnittstelle und der Mount Point aktiv sind, der erste Knoten. Der andere Node ist der zweite Node.

Schritte

1. Melden Sie sich beim ersten Node des Clusters an.

   Im Hochverfügbarkeitseinstellungen müssen Sie alle Unified Manager-Services auf dem zweiten Node angehalten haben.

2. Fügen Sie das VCS-Installationsverzeichnis hinzu `/opt/VRTSvcs/bin` Zum PFAD Umgebungsvariable.
3. Wenn Sie eine vorhandene Unified Manager Einrichtung konfigurieren, erstellen Sie ein Unified Manager Backup und erstellen Sie das Support Bundle.
4. Führen Sie die aus `ha_setup.pl` Skript: `perl ha_setup.pl --first -t vcs -g group_name -e eth_name -i cluster_ip -m net_mask -n fully_qualified_cluster_name -f mount_path -v volume_group -d disk_group -l install_dir -u user_name -p password`

   ```
   perl \ha_setup.pl --first -t vcs -g umgroup -e eth0 -i 10.11.12.13 -m
   255.255.255.0 -n cluster.eng.company.com -f /mnt/ocumdb -v ocumdb_SdHv -d
   ocumdb_SdDg -l /opt/netapp/ -u admin -p wx17yz
   ```

5. Überprüfen Sie mithilfe der Veritas Operations Manager Webkonsole oder VCS Cluster Manager, ob eine Failover-Gruppe erstellt wird und ob die Unified Manager Serverdienste, Bereitstellungspunkt, virtuelle IP, Netzwerkschnittstellenkarte (NIC) und Volume-Gruppe der Cluster-Gruppe hinzugefügt werden.
6. Verschieben Sie die Unified Manager Service-Gruppe manuell zum sekundären Node und überprüfen Sie, ob ein Cluster-Failover funktioniert.
7. Überprüfen Sie, ob VCS auf den zweiten Knoten des Clusters umgeschaltet wurde.

   Vergewissern Sie sich, dass der Datenmounten, die virtuelle IP, die Volume-Gruppe und die NIC auf dem zweiten Node des Clusters online sind.

8. Beenden Sie Unified Manager mit Veritas Operations Manager.
9. Führen Sie die aus `perl ha_setup.pl --join -t vcs -f``mount_path` Befehl im zweiten Node des Clusters, sodass der Unified Manager Server auf die LUN verweist.
10. Überprüfen Sie, ob die Unified Manager Server Services auf dem zweiten Knoten des Clusters

ordnungsgemäß gestartet werden.

11. Generieren Sie das Unified Manager-Zertifikat erneut, nachdem Sie die Konfigurationsskripte ausgeführt haben, um die globale IP-Adresse abzurufen.

    a. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Setup** auf **HTTPS-Zertifikat**.

    b. Klicken Sie auf **HTTPS-Zertifikat erneut erstellen**.

    Das neu erstellte Zertifikat enthält nur die Cluster-IP-Adresse, nicht den vollqualifizierten Domänennamen (FQDN). Zur Einrichtung von Unified Manager für Hochverfügbarkeit müssen Sie die globale IP-Adresse verwenden.

12. Greifen Sie über folgende Ressourcen auf die Unified Manager-UI zu: `https://<FQDN of Global IP>`

Nachdem Sie fertig sind

Nach der Konfiguration der Hochverfügbarkeit müssen Sie einen freigegebenen Backup-Speicherort erstellen. Der freigegebene Speicherort ist erforderlich, um die Backups zu enthalten, die Sie vor und nach dem Failover erstellen. Die beiden Nodes in der Hochverfügbarkeitseinrichtung müssen auf den gemeinsamen Speicherort zugreifen können.

Unified Manager Service-Ressourcen für VCS Konfiguration

Sie müssen die Cluster Service Ressourcen von Unified Manager zu Veritas Cluster Server (VCS) hinzufügen. Diese Cluster-Serviceressourcen werden für verschiedene Zwecke eingesetzt, beispielsweise für das Monitoring von Storage-Systemen, die Planung von Jobs, Verarbeitungsereignisse und das Monitoring aller anderen Unified Manager Services.

Die folgende Tabelle enthält die Kategorie aller Unified Manager Services:

Kategorie	Services
Speicherressource	• `vol` • `mount`
Datenbankressource	• `mysqld`
Netzwerkressource	• `nic` • `vip`
Unified Manager Ressource	• `ocie` • `ocieau`

Aktualisierung einer vorhandenen Unified Manager-Einrichtung für hohe Verfügbarkeit

Sie können Ihre vorhandene Unified Manager Installation aktualisieren und Ihre Setup-Umgebung auf hohe Verfügbarkeit konfigurieren.

Bevor Sie beginnen

- Sie müssen ein Backup- und Support-Bundle Ihrer vorhandenen Daten erstellt haben.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen dem Cluster einen zweiten Knoten hinzugefügt und Veritas Cluster Server (VCS) auf dem zweiten Knoten installiert haben.

  Siehe *Veritas Cluster Server 6.2.1 Installation Guide*.

- Der neu hinzugefügte Node muss konfiguriert werden, um auf denselben freigegebenen Speicherort wie den des bestehenden Nodes im Hochverfügbarkeitsaufbau zuzugreifen.

Schritte

1. Melden Sie sich bei dem neuen Node des Clusters an.
2. Installation von Unified Manager auf dem Knoten

   Installation von Unified Manager unter Red hat Enterprise Linux oder CentOS

3. Konfigurieren Sie den Unified Manager-Server mithilfe von Konfigurationsskripten auf dem bestehenden Node mit Daten.
4. Initiieren Sie ein manuelles Failover auf den zweiten Node.
5. Führen Sie die aus `perl ha_setup.pl --join -t vcs -f``mount_path` Befehl auf dem zweiten Node des Clusters, sodass der Unified Manager Server Daten auf die Shared LUN verweist.
6. Wenn OnCommand Workflow Automation (WFA) für Unified Manager konfiguriert ist, deaktivieren Sie die WFA Verbindung und konfigurieren Sie sie dann neu.
7. Wenn SnapProtect mit Unified Manager konfiguriert ist, konfigurieren Sie SnapProtect mit einer neuen Cluster-IP-Adresse und den vorhandenen Storage-Richtlinien neu.
8. Generieren Sie die benutzerdefinierten Berichte erneut, und fügen Sie diese Berichte mit der neuen Cluster-IP-Adresse zu Unified Manager hinzu.

Upgrade von Unified Manager auf Red hat Enterprise Linux oder CentOS

Sie können ein Upgrade von Unified Manager durchführen, wenn eine neue Softwareversion verfügbar ist.

Patch-Releases der Unified Manager Software werden bei der Bereitstellung durch NetApp anhand des gleichen Verfahrens wie bei neuen Releases installiert.

Wenn Unified Manager mit einer Instanz von OnCommand Workflow Automation gekoppelt ist und für beide Produkte neue Versionen der Software zur Verfügung stehen, müssen Sie die beiden Produkte trennen und anschließend eine neue Workflow-Automatisierungsverbindung einrichten, nachdem Sie die Upgrades durchgeführt haben. Wenn Sie ein Upgrade auf nur eines der Produkte durchführen, müssen Sie sich nach dem Upgrade bei Workflow Automation anmelden und überprüfen, ob noch Daten von Unified Manager erfasst werden.

Upgrade von Unified Manager auf Red hat Enterprise Linux oder CentOS

Sie können ein Upgrade von Unified Manager Version 7.3 oder 9.4 auf Unified Manager 9.5 durchführen, indem Sie die Installationsdatei auf der Red hat Plattform herunterladen

und ausführen.

Bevor Sie beginnen

- Das System, auf dem Unified Manager aktualisiert wird, muss die System- und Software-Anforderungen erfüllen.

  Hardwaresystemanforderungen

  Anforderungen an Red hat und CentOS Software und Installation

- Ab Unified Manager 9.4 wird Red hat Enterprise Linux 6.x nicht mehr unterstützt. Wenn Sie RHEL 6 verwenden, müssen Sie Ihre Instanz von RHEL auf Version 7.x aktualisieren, bevor Sie auf Unified Manager 9.5 aktualisieren.
- Ab Unified Manager 9.5 wird Oracle Java nicht mehr unterstützt. Die korrekte Version von OpenJDK muss vor dem Upgrade auf Unified Manager 9.5 installiert werden.
- Sie müssen über ein Abonnement für den Red hat Enterprise Linux Subscription Manager verfügen.
- Um Datenverlust zu vermeiden, müssen Sie ein Backup der Unified Manager-Datenbank erstellt haben, falls während des Upgrades ein Problem auftritt. Es wird auch empfohlen, die Sicherungsdatei aus dem zu verschieben `/opt/netapp/data` Verzeichnis zu einem externen Speicherort.
- Sie sollten alle laufenden Vorgänge abgeschlossen haben, da Unified Manager während des Upgrades nicht verfügbar ist.

Über diese Aufgabe

Diese Schritte enthalten Informationen zu Systemen, die für Hochverfügbarkeit mit Veritas Operation Manager konfiguriert sind. Wenn Ihr System nicht für hohe Verfügbarkeit konfiguriert ist, ignorieren Sie diese zusätzlichen Schritte.

Schritte

1. Melden Sie sich beim Red hat Enterprise Linux- oder CentOS-Zielserver an.
2. Laden Sie das Unified Manager Bundle auf den Server herunter.

   Herunterladen von Unified Manager für Red hat oder CentOS

3. Navigieren Sie zum Zielverzeichnis und erweitern Sie das Unified Manager Bundle: `unzip OnCommandUnifiedManager-rhel7-9.5.zip`

   Die erforderlichen RPM-Module für Unified Manager werden in das Zielverzeichnis entpackt.

4. Bestätigen Sie das Vorhandensein der aufgeführten Module: `ls *.rpm`

   Die folgenden RPM-Module sind aufgelistet:

   - `ocie-au-<version>.x86_64.rpm`
   - `ocie-server-<version>.x86_64.rpm`
   - `ocie-serverbase-<version>.x86_64.rpm`
   - `netapp-application-server-<version>.x86_64.rpm`

- netapp-platform-base-<version>.x86_64.rpm
- netapp-ocum-<version>.x86_64.rpm

5. Bei Systemen, die nicht mit dem Internet verbunden sind oder die RHEL-Repositorys nicht nutzen, führen Sie die folgenden Schritte aus, um festzustellen, ob erforderliche Pakete fehlen und diese Pakete heruntergeladen werden können:

   a. Die Liste der verfügbaren und nicht verfügbaren Pakete anzeigen: `yum install *.rpm --assumeno`

      Die Elemente im Abschnitt „`Installieren:`“ sind die Pakete, die im aktuellen Verzeichnis verfügbar sind, und die Elemente im Abschnitt „`Installieren für Abhängigkeiten:`“ sind die Pakete, die auf Ihrem System fehlen.

   b. Laden Sie die fehlenden Pakete auf einem anderen System mit Internetzugang herunter: `yum install package_name --downloadonly --downloaddir=.`

      Da das Plug-in “yum-Plugin-downloadonly” nicht immer auf Red hat Enterprise Linux-Systemen aktiviert ist, müssen Sie möglicherweise die Funktionalität zum Herunterladen eines Pakets ohne Installation aktivieren: `yum install yum-plugin-downloadonly`

   c. Kopieren Sie die fehlenden Pakete aus dem mit dem Internet verbundenen System auf Ihr Installationssystem.

6. Wenn Unified Manager für Hochverfügbarkeit konfiguriert ist, beenden Sie alle Unified Manager Services auf dem ersten Knoten mit Veritas Operations Manager.

7. Aktualisieren Sie Unified Manager mithilfe des folgenden Skripts: `upgrade.sh`

   Dieses Skript führt automatisch die RPM-Module aus, aktualisiert die erforderliche unterstützende Software und die darauf ausgeführten Unified Manager-Module. Außerdem prüft das Upgrade-Skript, ob es Systemkonfigurationseinstellungen oder installierte Software gibt, die mit dem Upgrade von Unified Manager in Konflikt geraten. Wenn das Skript Probleme erkennt, müssen Sie die Probleme vor dem Upgrade von Unified Manager beheben.

   Versuchen Sie nicht, ein Upgrade mit alternativen Befehlen wie z. B. durchzuführen `rpm -Uvh ...`). Für ein erfolgreiches Upgrade müssen alle Unified Manager-Dateien und zugehörigen Dateien in einer bestimmten Reihenfolge auf eine bestimmte Verzeichnisstruktur aktualisiert werden, die vom Skript automatisch ausgeführt und konfiguriert wird.

8. Beenden Sie bei Hochverfügbarkeitsinstallationen alle Unified Manager-Dienste auf dem zweiten Knoten mit Veritas Operations Manager.

9. Bei Hochverfügbarkeitsinstallationen wechseln Sie die Service-Gruppe beim Hochverfügbarkeits-Setup auf den zweiten Node und aktualisieren Unified Manager auf dem zweiten Node.

10. Nach Abschluss des Upgrades blättern Sie zurück durch die Meldungen, bis die Meldung eine IP-Adresse oder URL für die Web-UI von Unified Manager, den Wartungs-Benutzernamen (umadmin) und das Standardpasswort angezeigt wird.

    Die Meldung ähnelt der folgenden:

```
OnCommand Unified Manager upgraded successfully.
Use a web browser and one of the following URLs to access the OnCommand
Unified Manager GUI:

https://default_ip_address/    (if using IPv4)
https://[default_ip_address]/  (if using IPv6)
https://fully_qualified_domain_name/
```

Nachdem Sie fertig sind

Geben Sie die angegebene IP-Adresse oder URL in einen unterstützten Webbrowser ein, um die Unified Manager Web-UI zu starten, und melden Sie sich anschließend mit demselben Wartungs-Benutzernamen (umadmin) und Kennwort an, das Sie zuvor festgelegt haben.

Aktualisieren des Host-Betriebssystems von Red hat Enterprise Linux 6.x auf 7.x

Wenn Sie bereits Unified Manager auf einem Red hat Enterprise Linux 6.x-System installiert haben und jetzt ein Upgrade auf Red hat Enterprise Linux 7.x durchführen müssen, müssen Sie eines der in diesem Thema aufgeführten Verfahren befolgen. In beiden Fällen müssen Sie eine Sicherung von Unified Manager auf dem Red hat Enterprise Linux 6.x-System erstellen und anschließend die Sicherung auf einem Red hat Enterprise Linux 7.x-System wiederherstellen.

Über diese Aufgabe

Der Unterschied zwischen den beiden unten aufgeführten Optionen besteht darin, dass Sie in einem Fall die Wiederherstellung von Unified Manager auf einem neuen RHEL 7.x-Server durchführen und in dem anderen Fall die Wiederherstellung auf demselben Server durchführen.

Da diese Aufgabe erfordert, dass Sie auf dem Red hat Enterprise Linux 6.x-System ein Backup von Unified Manager erstellen, sollten Sie das Backup nur dann erstellen, wenn Sie bereit sind, den gesamten Upgrade-Prozess abzuschließen, sodass Unified Manager für den kürzesten Zeitraum offline ist. In der Unified Manager-Benutzeroberfläche werden Lücken in gesammelten Daten für den Zeitraum angezeigt, in dem das Red hat Enterprise Linux 6.x-System heruntergefahren wird, und bevor das neue Red hat Enterprise Linux 7.x gestartet wird.

Weitere Informationen zu den Backup- und Wiederherstellungsprozessen finden Sie in der Online-Hilfe des *Unified Manager*.

Aktualisieren des Host-Betriebssystems mit einem neuen Server

Führen Sie diese Schritte aus, wenn Sie ein Ersatzsystem haben, auf dem Sie RHEL 7.x-Software installieren können, so dass Sie die Unified Manager-Wiederherstellung auf diesem System durchführen können, während das RHEL 6.x-System weiterhin verfügbar ist.

1. Installieren und konfigurieren Sie einen neuen Server mit der Red hat Enterprise Linux 7.x-Software.

   Red hat Software und Installationsanforderungen

2. Installieren Sie auf dem Red hat Enterprise Linux 7.x-System dieselbe Version der Unified Manager-

Software, die Sie auf dem vorhandenen Red hat Enterprise Linux 6.x-System verwenden.

Installation von Unified Manager auf Red hat Enterprise Linux

Starten Sie die UI nicht, und konfigurieren Sie keine Cluster-, Benutzer- oder Authentifizierungseinstellungen, wenn die Installation abgeschlossen ist. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.

3. Erstellen Sie auf dem Red hat Enterprise Linux 6.x-System aus dem Menü Administration in der Web-Benutzeroberfläche ein Unified Manager-Backup und kopieren Sie die Sicherungsdatei anschließend an einen externen Speicherort.
4. Fahren Sie auf dem Red hat Enterprise Linux 6.x-System Unified Manager herunter.
5. Kopieren Sie auf dem Red hat Enterprise Linux 7.x-System die Sicherungsdatei vom externen Speicherort nach `/data/ocum-backup/`, Und geben Sie dann den folgenden Befehl ein, um die Unified Manager-Datenbank aus der Sicherungsdatei wiederherzustellen:`um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>`
6. Geben Sie die IP-Adresse oder URL in einem unterstützten Webbrowser ein, um die Unified Manager Web-UI zu starten, und melden Sie sich anschließend beim System an.

Sobald Sie überprüft haben, ob das System ordnungsgemäß funktioniert, können Sie Unified Manager vom Red hat Enterprise Linux 6.x-System entfernen.

Aktualisierung des Host-Betriebssystems auf demselben Server

Befolgen Sie diese Schritte, wenn Sie kein Ersatzsystem haben, auf dem Sie RHEL 7.x Software installieren können.

1. Erstellen Sie im Menü Administration in der Web UI ein Backup von Unified Manager und kopieren Sie die Sicherungsdatei anschließend an einen externen Speicherort.
2. Entfernen Sie das Red hat Enterprise Linux 6.x-Image aus dem System, und löschen Sie das System vollständig.
3. Installation und Konfiguration der Red hat Enterprise Linux 7.x-Software auf demselben System

   Red hat Software und Installationsanforderungen

4. Installieren Sie auf dem Red hat Enterprise Linux 7.x-System dieselbe Version der Unified Manager-Software, die Sie auf dem Red hat Enterprise Linux 6.x-System hatten.

   Installation von Unified Manager auf Red hat Enterprise Linux

   Starten Sie die UI nicht, und konfigurieren Sie keine Cluster-, Benutzer- oder Authentifizierungseinstellungen, wenn die Installation abgeschlossen ist. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.

5. Kopieren Sie die Sicherungsdatei vom externen Speicherort nach `/data/ocum-backup/`, Und geben Sie dann den folgenden Befehl ein, um die Unified Manager-Datenbank aus der Sicherungsdatei wiederherzustellen:`um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>`
6. Geben Sie die IP-Adresse oder URL in einem unterstützten Webbrowser ein, um die Unified Manager Web-UI zu starten, und melden Sie sich anschließend beim System an.

Upgrade von Drittanbieterprodukten auf Linux

Sie können Produkte von Drittanbietern wie JRE und MySQL auf Unified Manager aktualisieren, wenn sie auf Linux-Systemen installiert sind.

Die Unternehmen, die diese Drittanbieterprodukte entwickeln, melden regelmäßig Sicherheitsschwachstellen. Sie können ein Upgrade auf neuere Versionen dieser Software nach Ihrem eigenen Zeitplan durchführen.

Aktualisieren von JRE auf Linux

Sie können auf eine neuere Version der Java Runtime Environment (JRE) auf dem Linux-Server, auf dem Unified Manager installiert ist, aktualisieren, um die Behebung von Sicherheitsschwachstellen zu erhalten.

Bevor Sie beginnen

Sie müssen über Root-Rechte für das Linux-System verfügen, auf dem Unified Manager installiert ist.

Schritte

1. Melden Sie sich als Root-Benutzer auf dem Unified Manager-Hostcomputer an.
2. Laden Sie die entsprechende Version von Java (64-Bit) auf das Zielsystem herunter.
3. Beenden Sie die Unified Manager Services: `service ocieau stop``service ocie stop`
4. Installieren Sie die neueste JRE auf dem System.
5. Starten Sie die Unified Manager Services: `service ocie start``service ocieau start`

Aktualisieren von MySQL auf Linux

Sie können auf eine neuere Version von MySQL auf dem Linux-Server aktualisieren, auf dem Unified Manager installiert ist, um Korrekturen für Sicherheitslücken zu erhalten.

Bevor Sie beginnen

Sie müssen über Root-Rechte für das Linux-System verfügen, auf dem Unified Manager installiert ist.

Über diese Aufgabe

Sie können nur ein Upgrade auf kleinere Updates von MySQL 5.7 durchführen, zum Beispiel 5.7.1 bis 5.7.2 . Sie können kein Upgrade auf die Hauptversionen von MySQL durchführen, z. B. Version 5.8.

Schritte

1. Melden Sie sich als Root-Benutzer auf dem Unified Manager-Hostcomputer an.
2. Laden Sie den neuesten MySQL Community Server herunter `.rpm` Auf dem Zielsystem bündeln.
3. Enttar das Paket in ein Verzeichnis auf dem Zielsystem.
4. Sie erhalten mehrere `.rpm` Pakete im Verzeichnis nach dem Entrieten des Bundles, aber Unified Manager benötigt nur die folgenden rpm-Pakete:
   - mysql-Community-Client-5.7.x

- mysql-Community-libs-5.7.x
- mysql-Community-Server-5.7.x
- mysql-Community-common-5.7.x
- mysql-Community-libs-compat-5.7.x Alle anderen löschen `.rpm` Pakete. Die Installation aller Pakete in einem rpm-Paket verursacht keine Probleme.

5. Beenden Sie den Unified Manager-Service und die zugehörige MySQL-Software in der folgenden Reihenfolge:
6. Rufen Sie das Upgrade von MySQL mit dem folgenden Befehl auf: `yum install *.rpm`

   `*.rpm` Bezieht sich auf das `.rpm` Pakete in dem Verzeichnis, in dem Sie die neuere Version von MySQL heruntergeladen haben.

7. Starten Sie Unified Manager in der angezeigten Reihenfolge:

Neustart von Unified Manager in Red hat Enterprise Linux oder CentOS

Möglicherweise müssen Sie Unified Manager neu starten, nachdem Sie die Konfigurationsänderungen vorgenommen haben.

Bevor Sie beginnen

Sie müssen Root-Benutzerzugriff auf Red hat Enterprise Linux oder CentOS Server haben, auf dem Unified Manager installiert ist.

Schritte

1. Melden Sie sich als Root-Benutzer an dem Server an, auf dem Sie den Unified Manager-Service neu starten möchten.
2. Beenden Sie den Unified Manager-Service und die zugehörige MySQL-Software in der folgenden Reihenfolge:

   Beenden Sie bei der Installation in einer Hochverfügbarkeits-Einrichtung den Unified Manager Service mithilfe von VCS Operations Manager oder VCS Befehlen.

3. Starten Sie Unified Manager in der angezeigten Reihenfolge:

   Starten Sie bei der Installation in einer hochverfügbaren Einrichtung den Unified Manager Service über VCS Operations Manager oder VCS Befehle.

Entfernen von Unified Manager aus dem Red hat Enterprise Linux- oder CentOS-Host

Wenn Sie Unified Manager aus Red hat Enterprise Linux oder CentOS Host entfernen müssen, können Sie Unified Manager mit einem einzigen Befehl anhalten und deinstallieren.

Bevor Sie beginnen

- Sie müssen über Root-Benutzerzugriff auf den Server verfügen, von dem Sie Unified Manager entfernen

möchten.

- Security-Enhanced Linux (SELinux) muss auf dem Red hat-Rechner deaktiviert werden. Ändern Sie den SELinux-Laufzeitmodus in „`permissiv`“, indem Sie das verwenden `setenforce 0` Befehl.
- Alle Cluster (Datenquellen) müssen vor dem Entfernen der Software vom Unified Manager-Server entfernt werden.
- Der Unified Manager-Server darf keine aktive Verbindung zu einem externen Datenanbieter wie Graphite haben.

  In diesem Fall müssen Sie die Verbindung über die Unified ManagerMaintenance-Konsole löschen.

Über diese Aufgabe

Diese Schritte enthalten Informationen zu Systemen, die für Hochverfügbarkeit mit Veritas Operation Manager konfiguriert sind. Wenn Ihr System nicht für hohe Verfügbarkeit konfiguriert ist, ignorieren Sie diese zusätzlichen Schritte.

Schritte

1. Melden Sie sich als Root-Benutzer an dem Cluster-Node an, der die Cluster-Ressourcen besitzt, auf denen Sie Unified Manager entfernen möchten.
2. Beenden Sie alle Unified Manager Services mit VCS Operations Manager oder VCS Befehlen.
3. Beenden Sie Unified Manager, und entfernen Sie ihn vom Server: `rpm -e netapp-ocum ocie-au ocie-server netapp-platform-base netapp-application-server ocie-serverbase`

   In diesem Schritt werden alle zugehörigen NetApp RPM Pakete entfernt. Die erforderlichen Softwaremodule wie Java, MySQL und p7zip werden nicht entfernt.
4. Wechseln Sie mit dem VCS Operations Manager zum anderen Knoten.
5. Melden Sie sich bei dem zweiten Node des Clusters an.
6. Beenden Sie alle Services, und entfernen Sie Unified Manager aus dem zweiten Node: `rpm -e netapp-ocum ocie-au ocie-server netapp-platform-base netapp-application-server ocie-serverbase`
7. Verhindern Sie, dass die Service-Gruppe VCS Operations Manager oder VCS-Befehle verwendet.
8. Entfernen Sie gegebenenfalls die zugehörigen Softwaremodule wie Java, MySQL und p7zip: `rpm -e p7zip mysql-community-client mysql-community-server mysql-community-common mysql-community-libs java-x.y`

Ergebnisse

Nach Abschluss dieses Vorgangs wird die Software entfernt, MySQL-Daten werden jedoch nicht gelöscht. Alle Daten aus dem `/opt/netapp/data` Verzeichnis wird in verschoben `/opt/netapp/data/BACKUP` Ordner nach der Deinstallation.

Entfernen des benutzerdefinierten umadmin-Benutzers und der Wartungsgruppe

Wenn Sie vor der Installation von Unified Manager ein benutzerdefiniertes Home-Verzeichnis erstellt haben, um Ihr eigenes umadmin-Benutzer- und Wartungskonto zu definieren, sollten Sie diese Elemente nach der Deinstallation von Unified Manager

entfernen.

Über diese Aufgabe

Bei der standardmäßigen Deinstallation von Unified Manager werden keine benutzerdefinierten umadmin-Benutzer und ein Maintenance-Konto entfernt. Sie müssen diese Elemente manuell löschen.

Schritte

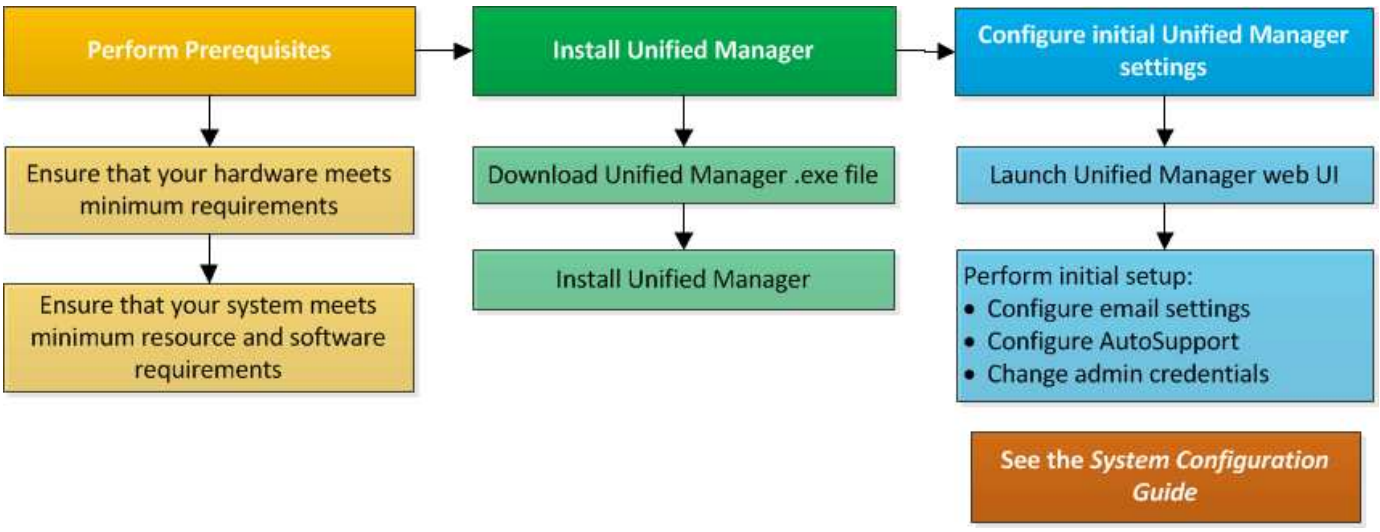
1. Melden Sie sich als Root-Benutzer beim Red hat Enterprise Linux-Server an.
2. Löschen Sie den umadmin-Benutzer:`userdel umadmin`
3. Löschen Sie die Wartungsgruppe:`groupdel maintenance`

Installieren, Aktualisieren und Entfernen der Unified Manager-Software unter Windows

Auf Windows-Systemen können Sie Unified Manager installieren, auf eine neuere Softwareversion aktualisieren oder die Unified Manager-Anwendung entfernen.

Überblick über die Installation unter Windows

Im Installations-Workflow werden die Aufgaben beschrieben, die Sie vor der Verwendung von Unified Manager ausführen müssen.



Installation von Unified Manager unter Windows

Es ist wichtig, dass Sie die Schritte kennen, um Unified Manager unter Windows herunterzuladen und zu installieren. Vor der Installation von Unified Manager unter Windows können Sie entscheiden, ob Sie Unified Manager für hohe Verfügbarkeit konfigurieren möchten.

Installation von Unified Manager auf einem Windows System

Sie können Unified Manager auf Windows installieren, um Probleme hinsichtlich Kapazität, Verfügbarkeit, Performance und Sicherung Ihres Storage zu überwachen und zu beheben.

Bevor Sie beginnen

- Das System, auf dem Unified Manager installiert werden soll, muss die System- und Software-Anforderungen erfüllen.

  Hardwaresystemanforderungen

  Windows Software- und Installationsanforderungen

  > Ab Unified Manager 9.5 wird OpenJDK im Unified Manager-Installationspaket bereitgestellt und automatisch installiert. Oracle Java wird ab Unified Manager 9.5 nicht unterstützt.

- Sie müssen über Administratorrechte für Windows verfügen.
- Sie benötigen einen unterstützten Webbrowser.
- Das Unified Manager-Wartungsbenutzerkennwort muss zwischen 8 und 20 Zeichen lang sein und darf Groß-/Kleinschreibung- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten.
- Die folgenden Sonderzeichen sind in der Kennwortzeichenfolge für den Wartungbenutzer oder für den MySQL-Root-Benutzer nicht zulässig: " ' ` % , = & < > ^ \ / ( ) [ ] ;

  Folgende Sonderzeichen sind erlaubt: ~ ! @ # * - ? . : + { }

Schritte

1. Melden Sie sich unter Windows mit dem lokalen Standardkonto an.
2. Loggen Sie sich auf der NetApp Support Site ein und suchen Sie die Download-Seite zur Installation von Unified Manager auf der Windows-Plattform.

   "NetApp Downloads: Software"

3. Laden Sie die Unified Manager Windows Installationsdatei von der NetApp Support Site in ein Zielverzeichnis im Windows System herunter.
4. Navigieren Sie zum Verzeichnis, in dem sich die Installationsdatei befindet.
5. Klicken Sie mit der rechten Maustaste, und führen Sie die ausführbare Datei für das Unified Manager-Installationsprogramm aus (`.exe`) Datei als Administrator.

   Unified Manager erkennt fehlende oder vorinstallierte Pakete von Drittanbietern und listet sie auf. Wenn die erforderlichen Drittanbieterpakete nicht im System installiert sind, installiert Unified Manager diese im Rahmen der Installation.

6. Klicken Sie Auf **Weiter**.
7. Geben Sie den Benutzernamen und das Kennwort ein, um den Wartungbenutzer zu erstellen.
8. Geben Sie im Assistenten * Datenbankverbindung* das MySQL-Root-Passwort ein.
9. Klicken Sie auf **Ändern**, um einen neuen Speicherort für das Installationsverzeichnis von Unified Manager

und das MySQL-Datenverzeichnis anzugeben.

Wenn Sie das Installationsverzeichnis nicht ändern, wird Unified Manager im Standardinstallationsverzeichnis installiert.

10. Klicken Sie Auf **Weiter**.
11. Klicken Sie im Assistenten * Ready to Install Shield* auf **Install**.
12. Klicken Sie nach Abschluss der Installation auf **Fertig stellen**.

Ergebnisse

Die Installation erstellt mehrere Verzeichnisse:

- Installationsverzeichnis vorhanden

  Dies ist das Stammverzeichnis für Unified Manager, das Sie während der Installation angegeben haben. Beispiel: `C:\Program Files\NetApp\`

- MySQL-Datenverzeichnis

  Dies ist das Verzeichnis, in dem die MySQL-Datenbanken gespeichert werden, die Sie während der Installation angegeben haben. Beispiel: `C:\ProgramData\MySQL\MySQLServerData\`

- Java-Verzeichnis

  Dies ist das Verzeichnis, in dem OpenJDK installiert wird. Beispiel: `C:\Program Files\NetApp\JDK\`

- Verzeichnis der Applikationsdaten von Unified Manager (AppDataDir)

  Dies ist das Verzeichnis, in dem alle applikationsgenerierten Daten gespeichert werden. Dazu zählen Protokolle, Support-Bundles, Backup und alle anderen zusätzlichen Daten. Beispiel: `C:\ProgramData\NetApp\OnCommandAppData\`

Nachdem Sie fertig sind

Sie können auf die Web-Benutzeroberfläche zugreifen, um die Ersteinrichtung von Unified Manager durchzuführen, wie unter beschrieben "Konfigurieren Von Unified Manager".

Durchführen einer unbeaufsichtigten Installation von Unified Manager

Sie können Unified Manager ohne Eingriff des Benutzers über die Befehlszeilenschnittstelle installieren. Sie können die unbeaufsichtigte Installation abschließen, indem Sie die Parameter in Schlüsselwert-Paaren übergeben.

Schritte

1. Melden Sie sich mit dem lokalen Standardkonto an der Windows-Befehlszeilenschnittstelle an.
2. Navigieren Sie zu dem Speicherort, an dem Unified Manager installiert werden soll, und wählen Sie eine der folgenden Optionen:

Option	Anweisungen

Falls Pakete von Drittanbietern vorinstalliert sind	`OnCommandUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qn /l*v CompletePathForLogFile"`
	
	Beispiel:
	
	`OnCommandUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:\ProgramData\MYSQL\MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qn /l*v C:\install.log"`

Falls Pakete von Drittanbietern nicht installiert sind	`OnCommandUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qr /l*v CompletePathForLogFile"`
	
	Beispiel:
	
	`OnCommandUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:\ProgramData\MYSQL\MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qr /l*v C:\install.log"`

Der `/qr` Option aktiviert den leisen Modus mit einer reduzierten Benutzeroberfläche. Es wird eine grundlegende Benutzeroberfläche angezeigt, die den Installationsfortschritt anzeigt. Sie werden nicht nach Eingaben gefragt. Wenn Pakete von Drittanbietern wie JRE, MySQL und 7zip nicht vorinstalliert sind, müssen Sie das verwenden `/qr` Option. Die Installation schlägt fehl, wenn der `/qn` Option wird auf einem Server verwendet, auf dem keine Pakete von Drittanbietern installiert sind.

Der `/qn` Option aktiviert den stillen Modus ohne Benutzeroberfläche. Während der Installation werden keine Benutzeroberfläche oder Details angezeigt. Sie dürfen das nicht verwenden `/qn` Option, wenn Pakete von Drittanbietern nicht installiert sind.

3. Melden Sie sich über die folgende URL bei der Web-Benutzeroberfläche von Unified Manager an:

   `https://IP address`

Einrichtung von Unified Manager in einer Failover-Clustering-Umgebung

Mithilfe von Failover Clustering lässt sich die Hochverfügbarkeit für Unified Manager konfigurieren. Das Hochverfügbarkeitseinrichtung ermöglicht Failover-Funktionen.

Bei diesem Setup besitzt nur ein Node alle Cluster-Ressourcen. Wenn ein Node ausfällt oder eine der konfigurierten Services nicht online geschaltet werden kann, erkennt der Failover-Cluster-Service dieses Ereignis und überträgt sofort die Kontrolle auf den anderen Node. Der zweite Node im Setup wird aktiv und beginnt mit der Bereitstellung von Services. Der Failover-Prozess erfolgt automatisch, und Sie müssen keine Aktionen durchführen.

Ein mit dem Unified Manager-Server konfiguriertes Failover-Cluster besteht aus zwei Knoten, auf denen jeder Node dieselbe Version des Unified Manager-Servers ausführt. Alle Unified Manager-Serverdaten müssen für den Zugriff von einer gemeinsam genutzten Datenfestplatte konfiguriert werden.

Anforderungen für Unified Manager in einer Failover Clustering-Umgebung

Vor dem Installieren von Unified Manager in einer Failover-Clustering-Umgebung müssen Sie sicherstellen, dass die Cluster-Nodes ordnungsgemäß konfiguriert sind, um Unified Manager zu unterstützen.

Sie müssen sicherstellen, dass die Failover-Cluster-Konfiguration die folgenden Anforderungen erfüllt:

- Beide Clusterknoten müssen dieselbe Version von Microsoft Windows Server ausführen.
- Die gleiche Version von Unified Manager muss auf beiden Cluster-Nodes mithilfe des gleichen Pfads installiert werden.
- Das Failover Clustering muss auf beiden Nodes installiert und aktiviert sein.

  Anweisungen hierzu finden Sie in der Microsoft-Dokumentation.

- Zum Erstellen gemeinsam genutzter Datenfestplatten müssen Sie Fibre Channel Switched Fabric oder iSCSI-basierten Storage als Storage Back-End verwenden
- Optional: Bei Verwendung von SnapDrive für Windows muss ein gemeinsamer Speicherort erstellt werden, der für beide Knoten im Hochverfügbarkeitseinrichtung zugänglich ist.

  Informationen zum Installieren und Erstellen eines gemeinsam genutzten Speicherorts finden Sie im Installationshandbuch *SnapDrive for Windows*.

  Sie können auch LUNs über die Befehlszeilenschnittstelle des Storage-Systems verwalten. Weitere Informationen finden Sie in der SnapDrive for Windows Compatibility Matrix.

- Sie müssen Perl installiert haben `XML::LibXML` Und `File::chdir` Module für Skripte zu funktionieren.
- Die Cluster-Einrichtung muss nur zwei Nodes enthalten.
- Der Quorumtyp „`Node und Disk Majority`“ muss für das Failover Clustering verwendet werden.
- Sie müssen eine freigegebene IP-Adresse mit einem entsprechenden FQDN konfiguriert haben, damit sie als globale Cluster-IP-Adresse für den Zugriff auf Unified Manager verwendet werden kann.

- Das Passwort für den Unified Manager-Wartungsbenutzer muss auf beiden Nodes identisch sein.
- Sie müssen nur IPv4-IP-Adresse verwendet haben.

Installation von Unified Manager auf MSCS

Zur Konfiguration der Hochverfügbarkeit müssen Sie Unified Manager auf beiden Microsoft Cluster Server (MSCS) Cluster Knoten installieren.

Schritte

1. Melden Sie sich als Domänenbenutzer auf beiden Knoten des Clusters an.
2. Sorgen Sie für Hochverfügbarkeit, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Konfigurieren Sie für eine vorhandene Unified Manager-Installation die Hochverfügbarkeit	Fügen Sie einen weiteren Server hinzu, der mit dem vorhandenen Server gekoppelt werden soll: a. Aktualisieren Sie den vorhandenen Unified Manager-Server auf die neueste Softwareversion. b. Erstellen Sie ein Backup der vorhandenen Unified Manager-Installation, und speichern Sie das Backup auf einer gemounteten LUN. c. Installation von Unified Manager auf dem zweiten Node Installation von Unified Manager auf einem Windows System d. Stellen Sie das Backup der vorhandenen Unified Manager-Installation auf dem zweiten Knoten wieder her.
Konfigurieren Sie Hochverfügbarkeit bei einer neuen Unified Manager-Installation	Installation von Unified Manager auf beiden Knoten Installation von Unified Manager auf einem Windows System

Konfiguration des Unified Manager Servers mit MSCS mithilfe von Konfigurationsskripten

Nach der Installation von Unified Manager auf beiden Cluster-Knoten können Sie Unified Manager mit Failover Cluster Manager mithilfe von Konfigurationsskripten konfigurieren.

Bevor Sie beginnen

Sie müssen eine freigegebene LUN erstellt haben, die ausreichend groß ist, um den Unified Manager-Quelldaten gerecht zu werden.

Schritte

1. Melden Sie sich beim ersten Node des Clusters an.
2. Erstellen Sie eine Rolle in Windows 2012 oder Windows 2016 mit Failover Cluster Manager:
   a. Starten Sie Failover Cluster Manager.
   b. Erstellen Sie die leere Rolle, indem Sie auf **Rollen** > **leere Rolle erstellen** klicken.
   c. Fügen Sie die globale IP-Adresse der Rolle hinzu, indem Sie mit der rechten Maustaste auf **Role** > **Ressourcen hinzufügen** > **Weitere Ressourcen** > **IP-Adresse** klicken.

      Beide Knoten müssen diese IP-Adresse anpingen können, da Unified Manager über diese IP-Adresse gestartet wird, nachdem die Hochverfügbarkeit konfiguriert ist.

   d. Fügen Sie die Datenfestplatte zur Rolle hinzu, indem Sie mit der rechten Maustaste auf **Role** > **Add Storage** klicken.
3. Führen Sie die aus `ha_setup.pl` Skript auf dem ersten Knoten: `perl ha_setup.pl --first -t mscs -g group_name -i ip address -n fully_qualified_domain_cluster_name -f shared_location_path -k data_disk -u user_name -p password`

   ```
   C:\Program Files\NetApp\ocum\bin>perl .\ha_setup.pl --first -t mscs -g umgroup -i "IP Address" -n spr38457002.eng.company.com -k "Cluster Disk 2" -f E:\ -u admin -p wx17yz
   ```

   Das Skript ist unter verfügbar `Install_Dir\NetApp\ocum\bin`.

   - Sie können den Wert des erhalten `-g`, `-k`, und `-i` Optionen mit dem `cluster res` Befehl.
   - Der `-n` Die Option muss der FQDN der globalen IP-Adresse sein, die von beiden Knoten aus angepingt werden kann.
4. Überprüfen Sie mithilfe der Failover Cluster Manager Webkonsole, ob die Unified Manager-Serverdienste, die Datenfestplatte und die Cluster-IP-Adresse der Cluster-Gruppe hinzugefügt werden.
5. Stoppen Sie alle Unified Manager Server Services (MySQL, ocie und ocieau), indem Sie die verwenden `services.msc` Befehl.
6. Wechseln Sie die Service-Gruppe in Failover Cluster Manager auf den zweiten Knoten.
7. Führen Sie den Befehl aus `perl ha_setup.pl --join -t mscs -f``shared_location_path` Auf dem zweiten Node des Clusters, um auf die Daten des Unified Manager Servers auf die LUN zu verweisen.

   ```
   perl ha_setup.pl --join -t mscs -f E:\
   ```

8. Stellen Sie mit Failover Cluster Manager alle Unified Manager-Services online.
9. Wechseln Sie manuell zum anderen Knoten des Microsoft Cluster Servers.
10. Überprüfen Sie, ob die Unified Manager-Serverdienste auf dem anderen Knoten des Clusters ordnungsgemäß gestartet werden.
11. Generieren Sie das Unified Manager-Zertifikat erneut, nachdem Sie Konfigurationsskripte ausgeführt haben, um die globale IP-Adresse zu erhalten.
    a. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Setup** auf **HTTPS-Zertifikat**.
    b. Klicken Sie auf **HTTPS-Zertifikat erneut erstellen**.

Das neu erstellte Zertifikat stellt die Cluster-IP-Adresse und nicht den vollqualifizierten Domänennamen (FQDN) bereit. Zur Einrichtung von Unified Manager für Hochverfügbarkeit müssen Sie die globale IP-Adresse verwenden.

12. Greifen Sie über folgende Ressourcen auf die Unified Manager-UI zu: `https://<FQDN of Global IP>`

Nachdem Sie fertig sind

Nach der Konfiguration der Hochverfügbarkeit müssen Sie einen freigegebenen Backup-Speicherort erstellen. Der gemeinsam genutzte Speicherort ist erforderlich, um die Backups vor und nach dem Failover zu enthalten. Beide Nodes in der Hochverfügbarkeitseinrichtung müssen auf den gemeinsamen Speicherort zugreifen können.

Upgrade von Unified Manager auf Windows

Sie können ein Upgrade von Unified Manager 7.3 oder 9.4 auf Unified Manager 9.5 durchführen, indem Sie die Installationsdatei auf der Windows-Plattform herunterladen und ausführen.

Bevor Sie beginnen

- Das System, auf dem Unified Manager aktualisiert wird, muss die System- und Software-Anforderungen erfüllen.

  Hardwaresystemanforderungen

  Windows Software- und Installationsanforderungen

  Ab Unified Manager 9.5 wird OpenJDK im Unified Manager-Installationspaket bereitgestellt und automatisch installiert. Oracle Java wird ab Unified Manager 9.5 nicht unterstützt.

  Ab Unified Manager 9.4 ist Microsoft .NET 4.5.2 oder höher erforderlich. Stellen Sie sicher, dass Sie die richtige Version von .NET installiert haben, bevor Sie das Upgrade starten.

- Sie müssen über Administratorrechte für Windows verfügen.
- Zur Anmeldung auf der NetApp Support Site müssen Sie über gültige Zugangsdaten verfügen.
- Um Datenverlust zu vermeiden, müssen Sie ein Backup des Unified Manager-Rechners erstellt haben, falls während des Upgrades ein Problem auftritt.
- Sie müssen über ausreichend Speicherplatz verfügen, um das Upgrade durchführen zu können.

  Der verfügbare Speicherplatz auf dem Installationslaufwerk muss 2.5 GB größer sein als die Größe des Datenverzeichnisses. Das Upgrade wird angehalten und es wird eine Fehlermeldung angezeigt, die angibt, wie viel Speicherplatz hinzugefügt werden soll, wenn nicht genügend freier Speicherplatz vorhanden ist.

Über diese Aufgabe

Während des Upgrades ist Unified Manager nicht verfügbar. Vor dem Upgrade von Unified Manager sollten alle laufenden Vorgänge abgeschlossen werden.

Wenn Unified Manager mit einer Instanz von OnCommand Workflow Automation gekoppelt ist und für beide Produkte neue Versionen der Software zur Verfügung stehen, müssen Sie die beiden Produkte trennen und

anschließend eine neue Workflow-Automatisierungsverbindung einrichten, nachdem Sie die Upgrades durchgeführt haben. Wenn Sie ein Upgrade auf nur eines der Produkte durchführen, müssen Sie sich nach dem Upgrade bei Workflow Automation anmelden und überprüfen, ob noch Daten von Unified Manager erfasst werden.

Schritte

1. Loggen Sie sich auf der NetApp Support Site ein und suchen Sie die Download-Seite zur Installation von Unified Manager auf der Windows-Plattform.

   "NetApp Downloads: Software"

2. Laden Sie die Windows-Installationsdatei von Unified Manager in ein Zielverzeichnis im Windows-System herunter.
3. Wenn Unified Manager für Hochverfügbarkeit konfiguriert ist, beenden Sie alle Unified Manager Services auf dem ersten Node mithilfe von Microsoft Cluster Server, und starten Sie dann den MySQL Service ab `services.msc`.
4. Klicken Sie mit der rechten Maustaste, und führen Sie die ausführbare Datei für das Unified Manager-Installationsprogramm aus `(.exe)` Datei als Administrator ausführen.

   Unified Manager fordert Sie zur folgenden Meldung auf:

   ```
   This setup will perform an upgrade of 'OnCommand Unified Manager'. Do
   you want to continue?
   ```

5. Klicken Sie auf **Ja** und dann auf **Weiter**.
6. Geben Sie das während der Installation festgelegte MySQL-Root-Passwort ein, und klicken Sie auf **Weiter**.
7. Wenn das Upgrade erfolgreich durchgeführt wurde, starten Sie, wenn das System für Hochverfügbarkeit konfiguriert ist, alle Unified Manager Services vom Failover Cluster Manager und befolgen Sie die verbleibenden Aufgaben.
8. Führen Sie an der Eingabeaufforderung den aus `ha_setup.pl` Skript zum Konfigurieren der neuen Dienste im Failover-Cluster und der Dateien, die sich am freigegebenen Speicherort befinden.

   ```
   C:\Program Files\NetApp\ocum\bin> perl .\ha_setup.pl --upgrade --first -t mscs
   -g kjaggrp -i "New IP Address1" -n scs8003.englab.company.com -k "Cluster Disk
   2" -f E:\ -u user -p userpass
   ```

9. Beenden Sie alle Unified Manager-Services (ocie, ocieau und MySQL) auf dem ersten Knoten, indem Sie Microsoft Cluster Server verwenden.
10. Starten Sie den MySQL-Service auf dem zweiten Knoten von `services.msc`.
11. Schalten Sie die Service-Gruppe in der Hochverfügbarkeitseinrichtung auf den zweiten Node um.
12. Aktualisieren von Unified Manager auf dem zweiten Node
13. Geben Sie an der Eingabeaufforderung ein `Y` Um fortzufahren, oder geben Sie ein anderes Zeichen ein, das abgebrochen werden soll.

    Die Upgrade- und Neustartprozesse der Unified Manager Services dauern möglicherweise mehrere Minuten.

14. Starten Sie alle Unified Manager-Dienste auf beiden Knoten mit Microsoft Cluster Server.
15. Führen Sie an der Eingabeaufforderung den aus `ha_setup.pl` Skript mit dem `--upgrade` Option.

    ```
    perl ha_setup.pl --upgrade --join -t mscs -f E:\
    ```

16. Melden Sie sich in der Web-UI von Unified Manager an und überprüfen Sie die Versionsnummer.

Nachdem Sie fertig sind

Führen Sie den folgenden Befehl aus, um eine stille Aktualisierung von Unified Manager durchzuführen: `OnCommandUnifiedManager-9.5.exe /s /v"MYSQL_PASSWORD=netapp21! /qn /l*v C:\install.log`

Aktualisieren von Drittanbieterprodukten auf Windows

Sie können Produkte von Drittanbietern wie JRE und MySQL auf Unified Manager aktualisieren, wenn sie auf Windows-Systemen installiert sind.

Die Unternehmen, die diese Drittanbieterprodukte entwickeln, melden regelmäßig Sicherheitsschwachstellen. Sie können ein Upgrade auf neuere Versionen dieser Software nach Ihrem eigenen Zeitplan durchführen.

Aktualisieren von JRE unter Windows

Sie können auf eine neuere Version der Java Runtime Environment (JRE) auf dem Windows-Server aktualisieren, auf dem Unified Manager installiert ist, um die Behebung von Sicherheitsschwachstellen zu erhalten.

Bevor Sie beginnen

Sie müssen über Windows-Administratorrechte für das System verfügen, auf dem Unified Manager installiert ist.

Schritte

1. Melden Sie sich als Admin-Benutzer auf der Unified Manager-Host-Maschine an.
2. Laden Sie die entsprechende Version von Java (64-Bit) von der JDK-Site auf das Zielsystem herunter.

   Beispiel: Download `openjdk-11_windows-x64_bin.zip` Von `http://jdk.java.net/11/`.

3. Beenden Sie mithilfe der Windows Services-Konsole die folgenden Unified Manager-Services:
   - Übernahme von NetApp OCIE (Ocie-au)
   - NetApp OnCommand Applikations-Server (OnCommandsvc)
4. Erweitern Sie den `zip` Datei:
5. Kopieren Sie die Verzeichnisse und Dateien aus dem Ergebnis `jdk` Verzeichnis (z. B. `jdk-11.0.1` An den Speicherort, an dem Java installiert ist. Beispiel: `C:\Program Files\NetApp\JDK\`
6. Starten Sie die Unified Manager-Dienste über die Windows Services-Konsole:
   - NetApp OnCommand Applikations-Server (OnCommandsvc)

◦ Übernahme von NetApp OCIE (Ocie-au)

Aktualisieren von MySQL unter Windows

Sie können auf eine neuere Version von MySQL auf dem Windows-Server aktualisieren, auf dem Unified Manager installiert ist, um Korrekturen für Sicherheitslücken zu erhalten.

Bevor Sie beginnen

- Sie müssen über Windows-Administratorrechte für das System verfügen, auf dem Unified Manager installiert ist.
- Sie müssen das Passwort für den MySQL-Root-Benutzer besitzen.

Schritte

1. Melden Sie sich als Admin-Benutzer auf der Unified Manager-Host-Maschine an.
2. Laden Sie die entsprechende Version von MySQL auf das Zielsystem herunter.
3. Beenden Sie mithilfe der Windows Services-Konsole die folgenden Unified Manager-Services:
   ◦ Übernahme von NetApp OCIE (Ocie-au)
   ◦ NetApp OnCommand Applikations-Server (OnCommandsvc)
   ◦ MYSQL
4. Klicken Sie auf das `.msi` Paket zum Aufrufen des Upgrades von MySQL und befolgen Sie die Anweisungen auf dem Bildschirm, um das Upgrade abzuschließen.
5. Starten Sie die Unified Manager-Dienste über die Windows Services-Konsole:
   ◦ MYSQL
   ◦ NetApp OnCommand Applikations-Server (OnCommandsvc)
   ◦ Übernahme von NetApp OCIE (Ocie-au)

Neustart von Unified Manager unter Windows

Möglicherweise müssen Sie Unified Manager neu starten, nachdem Sie die Konfigurationsänderungen vorgenommen haben.

Bevor Sie beginnen

Sie müssen über Administratorrechte für Windows verfügen.

Schritte

1. Melden Sie sich unter Windows mit dem lokalen Standardkonto an.
2. Beenden Sie die Unified Manager Services:

Von der…	Stoppen Sie die Dienste in folgender Reihenfolge…
Kommandozeile	a. `sc stop ocie-au` b. `sc stop Oncommandsvc`
Microsoft Service Manager	a. Übernahme von NetApp OCIE (Ocie-au) b. NetApp OnCommand Applikations-Server (OnCommandsvc)

Beenden Sie bei der Installation in einer Hochverfügbarkeits-Einrichtung den Unified Manager Service entweder über Microsoft Service Manager oder über die Befehlszeile.

3. Starten Sie die Unified Manager Services:

Von der…	Starten Sie die Dienste in folgender Reihenfolge…
Kommandozeile	a. `sc start Oncommandsvc` b. `sc start ocie-au`
Microsoft Service Manager	a. NetApp OnCommand Applikations-Server (OnCommandsvc) b. Übernahme von NetApp OCIE (Ocie-au)

Starten Sie bei der Installation in einer Hochverfügbarkeitseinrichtung den Unified Manager-Service entweder über Microsoft Service Manager oder über die Befehlszeile.

Deinstallieren von Unified Manager von Windows

Sie können Unified Manager von Windows deinstallieren, indem Sie den Assistenten Programme und Funktionen verwenden oder eine unbeaufsichtigte Deinstallation von der Befehlszeilenschnittstelle durchführen.

Bevor Sie beginnen

- Sie müssen über Administratorrechte für Windows verfügen.
- Alle Cluster (Datenquellen) müssen vom Unified Manager-Server entfernt werden, bevor die Software deinstalliert wird.
- Der Unified Manager-Server darf keine aktive Verbindung zu einem externen Datenanbieter wie Graphite haben.

  In diesem Fall müssen Sie die Verbindung über die Unified ManagerMaintenance-Konsole löschen.

Schritte

1. Bei der Installation in einem Hochverfügbarkeitssetup sollten die Ressourcen der HA-Servicegruppe entfernt und die HA-Servicegruppe gelöscht werden, bevor Unified Manager von beiden Nodes deinstalliert wird.
2. Deinstallieren Sie Unified Manager, indem Sie eine der folgenden Optionen auswählen:

So deinstallieren Sie Unified Manager über…	Dann…
Assistent Programme und Funktionen	a. Navigieren Sie zu **Systemsteuerung** > **Programm und Funktionen**. b. Wählen Sie OnCommand Unified Manager und klicken Sie auf **Deinstallieren**.
Kommandozeile	a. Melden Sie sich mit Administratorrechten an der Windows-Befehlszeile an. b. Navigieren Sie zum Verzeichnis OnCommand Unified Manager, und führen Sie den folgenden Befehl aus: `msiexec /x {A78760DB-7EC0-4305-97DB-E4A89CDFF4E1} /qn /l*v %systemdrive%\UmUnInstall.log`

   Wenn die Benutzerkontensteuerung (UAC) auf dem Server aktiviert ist und Sie als Domänenbenutzer angemeldet sind, müssen Sie die Methode zur Deinstallation der Befehlszeile verwenden.

   Unified Manager wird von Ihrem System deinstalliert.

3. Deinstallieren Sie die folgenden Pakete und Daten von Drittanbietern, die während der Deinstallation von Unified Manager nicht entfernt werden:
   - Pakete von Drittanbietern: JRE, MySQL, Microsoft Visual C++ 2015 Redistributable und 7zip
   - MySQL Applikationsdaten von Unified Manager
   - Anwendungsprotokolle und Inhalt des Applikationsdatenverzeichnisses

Durchführung von Konfigurations- und Administrationsaufgaben

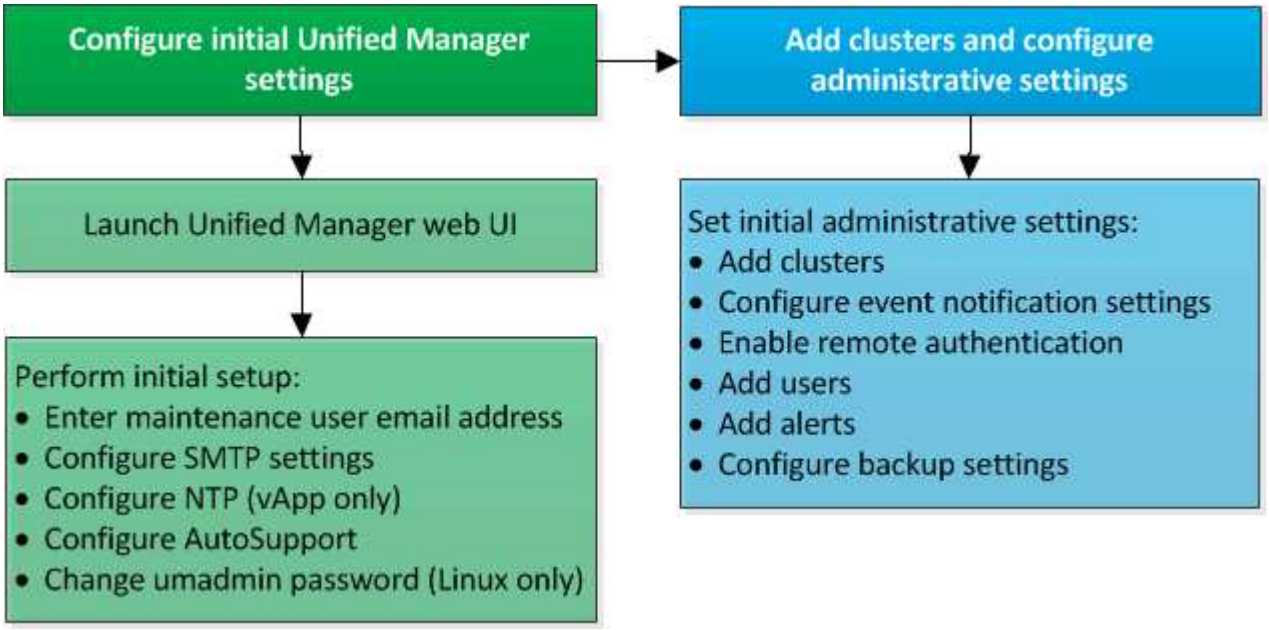
Konfigurieren Von Unified Manager

Nach der Installation von Unified Manager müssen Sie die Ersteinrichtung (auch als Assistent für die erste Erfahrung bezeichnet) abschließen, um auf die Web-Benutzeroberfläche zuzugreifen. Anschließend können Sie weitere Konfigurationsaufgaben ausführen, wie beispielsweise das Hinzufügen von Clustern, die Konfiguration der Remote-Authentifizierung, das Hinzufügen von Benutzern und das Hinzufügen von Warnmeldungen.

Einige der in diesem Handbuch beschriebenen Verfahren sind erforderlich, um die Ersteinrichtung der Unified Manager-Instanz durchzuführen. Andere Verfahren empfehlen Konfigurationseinstellungen, die für die Einrichtung in der neuen Instanz hilfreich sind oder die gut zu wissen sind, bevor Sie mit dem regelmäßigen Monitoring Ihrer ONTAP Systeme beginnen.

Überblick über die Konfigurationssequenz

Der Konfigurations-Workflow beschreibt die Aufgaben, die Sie ausführen müssen, bevor Sie Unified Manager verwenden können.



Zugriff auf die Web-Benutzeroberfläche von Unified Manager

Nach der Installation von Unified Manager können Sie auf die Web-Benutzeroberfläche zugreifen, um Unified Manager einzurichten, damit Sie mit der Überwachung Ihrer ONTAP-Systeme beginnen können.

Bevor Sie beginnen

- Wenn Sie zum ersten Mal auf die Web-UI zugreifen, müssen Sie sich als Wartungbenutzer (oder umadmin-Benutzer für Linux-Installationen) einloggen.
- Wenn Sie Benutzern den Zugriff auf Unified Manager mit dem Kurznamen erlauben möchten, anstatt den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse zu verwenden, muss die Netzwerkkonfiguration diesen Kurznamen auf einen gültigen FQDN auflösen.
- Wenn der Server ein selbstsigniertes digitales Zertifikat verwendet, zeigt der Browser möglicherweise eine Warnung an, dass das Zertifikat nicht vertrauenswürdig ist. Sie können entweder das Risiko bestätigen, dass der Zugriff fortgesetzt wird, oder ein Zertifikat einer Zertifizierungsstelle (CA) installieren, das digitale Zertifikat für die Serverauthentifizierung unterzeichnet hat.

Schritte

1. Starten Sie die Web-UI von Unified Manager über Ihren Browser, indem Sie die am Ende der Installation angezeigte URL verwenden. Die URL ist die IP-Adresse oder der vollqualifizierte Domain-Name (FQDN) des Unified Manager-Servers.

   Der Link hat das folgende Format: https://`URL`.

2. Melden Sie sich mit den Anmeldedaten der Wartungsbenutzer bei der Web-Benutzeroberfläche von Unified Manager an.

Die Ersteinrichtung der Unified Manager-Weboberfläche durchführen

Um Unified Manager zu verwenden, müssen Sie zunächst die anfänglichen Setup-Optionen konfigurieren, einschließlich des NTP-Servers, der Wartungs-Benutzer-E-Mail-Adresse und des SMTP-Server-Host-Namens und -Optionen.

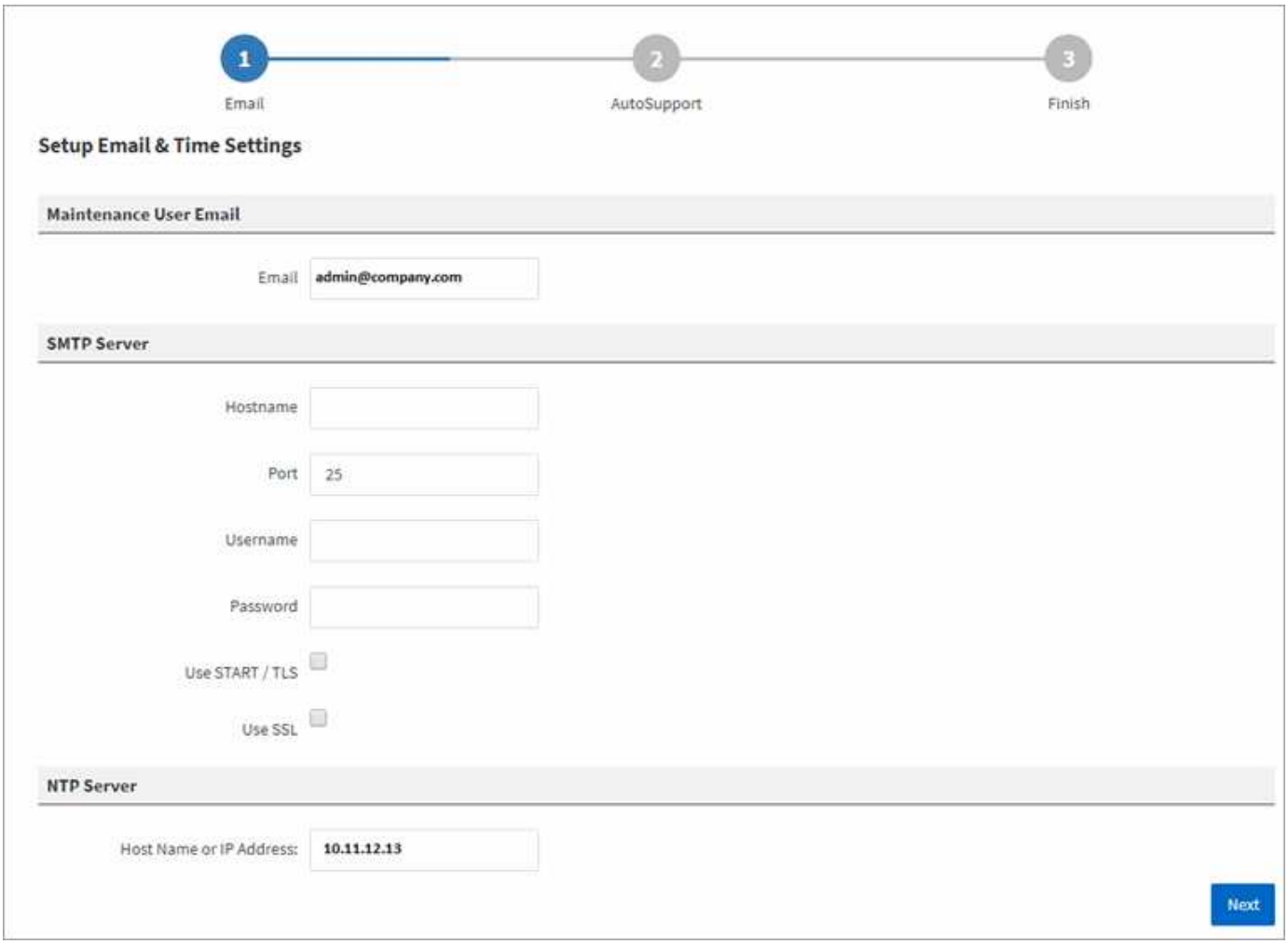
Bevor Sie beginnen

Sie müssen die folgenden Vorgänge durchgeführt haben:

- Die Web-UI von Unified Manager wurde über die nach der Installation bereitgestellte URL gestartet
- Sie sind mit dem während der Installation erstellten Wartungs-Benutzernamen und -Passwort (umadmin-Benutzer für Linux-Installationen) angemeldet

Über diese Aufgabe

Die Seite „Initial Setup“ von OnCommand Unified Manager wird nur angezeigt, wenn Sie das erste Mal auf die Web-Benutzeroberfläche zugreifen. Die folgende Seite ist von einer Installation auf VMware.



Wenn Sie später eine dieser Optionen ändern möchten, können Sie die Verwaltungsoptionen verwenden, auf die Sie zugreifen können, indem Sie auf die Schaltfläche * klicken* Aus der Symbolleiste von Unified Manager.

Schritte

1. Geben Sie im Fenster **OnCommand Unified Manager Initial Setup** die E-Mail-Adresse des Wartungsbenutzers, den SMTP-Serverhostnamen und weitere SMTP-Optionen sowie den NTP-Server (nur VMware-Installationen) ein. Klicken Sie anschließend auf **Weiter**.
2. Klicken Sie auf der Seite **AutoSupport** auf **zustimmen und fortfahren**, um AutoSupport zu aktivieren.

   Wenn Sie einen Proxy für den Zugriff auf das Internet festlegen müssen, um AutoSupport-Inhalte an den Support zu senden, oder wenn Sie AutoSupport deaktivieren möchten, verwenden Sie die Verwaltungsoptionen.

3. Auf Red hat- und CentOS-Systemen können Sie das umadmin-Benutzerpasswort von der standardmäßigen Zeichenfolge „`admin`“ in eine personalisierte Zeichenfolge ändern.

Ergebnisse

Das anfängliche Setup-Fenster wird geschlossen, und die Unified Manager Web-Benutzeroberfläche wird angezeigt. Die Seite Configuration/Cluster Data Sources wird angezeigt, sodass Sie Cluster zu Ihrem System hinzufügen können.

Hinzufügen von Clustern

Sie können OnCommand Unified Manager um ein Cluster erweitern, sodass Sie das Cluster überwachen können. Dazu gehört beispielsweise die Möglichkeit, Cluster-Informationen wie Systemzustand, Kapazität, Performance und Konfiguration des Clusters abzurufen, damit Sie etwaige auftretende Probleme finden und beheben können.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die folgenden Informationen haben:
  - Host-Name oder Cluster-Management-IP-Adresse

    Der Hostname ist der FQDN oder der Kurzname, den Unified Manager zur Verbindung mit dem Cluster verwendet. Der Host-Name muss bis zur Cluster-Management-IP-Adresse aufgelöst werden.

    Die Cluster-Management-IP-Adresse muss die Cluster-Management-LIF der administrativen Storage Virtual Machine (SVM) sein. Wenn Sie eine Node-Management-LIF verwenden, schlägt der Vorgang fehl.
  - Benutzername und Passwort für den Data ONTAP-Administrator

    Für dieses Konto muss die Rolle *admin* mit dem Anwendungszugriff auf *ontapi*, *ssh* und *http* eingestellt sein.
  - Typ des Protokolls (HTTP oder HTTPS), der auf dem Cluster konfiguriert werden kann und die Portnummer, die zum Herstellen einer Verbindung zum Cluster verwendet wird

    Sie können Cluster hinzufügen, die sich hinter einer NAT/Firewall befinden, indem Sie die Unified Manager NAT IP-Adresse verwenden. Alle angeschlossenen Workflow-Automatisierungs- oder SnapProtect-Systeme müssen sich auch hinter der NAT/Firewall befinden, und SnapProtect-API-Aufrufe müssen die NAT-IP-Adresse verwenden, um den Cluster zu identifizieren.
- Der FQDN des Unified Managers muss in der Lage sein, das ONTAP-System zu pingen.

  Sie können dies mit dem folgenden ONTAP-Befehl überprüfen: `ping -node node_name -destination Unified_Manager_FQDN`.
- Auf dem Unified Manager-Server muss ausreichend Speicherplatz vorhanden sein. Sie können dem Server kein Cluster hinzufügen, wenn mehr als 90 % des Speicherplatzes im Datenbankverzeichnis bereits belegt sind.

Über diese Aufgabe

Für eine MetroCluster Konfiguration müssen Sie sowohl die lokalen als auch die Remote-Cluster hinzufügen, und die Cluster müssen korrekt konfiguriert sein.

Sie können ein einzelnes Cluster durch zwei Instanzen von Unified Manager überwachen, vorausgesetzt, Sie haben eine zweite Cluster-Management-LIF im Cluster konfiguriert, sodass jede Instanz von Unified Manager über eine andere LIF verbunden ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Cluster-Datenquellen**.
2. Klicken Sie auf der Seite **Konfiguration/Cluster-Datenquellen** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Cluster hinzufügen** die erforderlichen Werte an, z. B. Hostname oder IP-Adresse des Clusters, Benutzername, Passwort, Protokoll für die Kommunikation und Portnummer.

   Standardmäßig sind das HTTPS-Protokoll und Port 443 ausgewählt.

   Sie können die Cluster-Management-IP-Adresse von IPv6 zu IPv4 oder von IPv4 zu IPv6 ändern. Die neue IP-Adresse wird im Cluster-Raster und die Seite der Cluster-Konfiguration nach Abschluss des nächsten Überwachungszyklus angezeigt.

4. Klicken Sie Auf **Absenden**.
5. Wenn HTTPS ausgewählt ist, führen Sie die folgenden Schritte aus:

   a. Klicken Sie im Dialogfeld **Autorisieren Host** auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.

   b. Klicken Sie Auf **Ja**.

      Unified Manager überprüft das Zertifikat nur, wenn das Cluster zunächst hinzugefügt wird. Unified Manager überprüft nicht das Zertifikat für jeden API-Aufruf an ONTAP.

   Wenn das Zertifikat abgelaufen ist, können Sie kein neues Cluster hinzufügen. Sie müssen zuerst das SSL-Zertifikat erneuern und dann den Cluster hinzufügen.

Ergebnisse

Nachdem alle Objekte für ein neues Cluster erkannt wurden (ca. 15 Minuten), erfasst Unified Manager die historischen Performance-Daten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktionalität zur Datenerfassung erfasst. Diese Funktion bietet Ihnen sofort nach dem Hinzufügen mehr als zwei Wochen Performance-Informationen für einen Cluster. Nach Abschluss des Datenerfassungszyklus werden Cluster-Performance-Daten in Echtzeit standardmäßig alle fünf Minuten erfasst.

Da die Sammlung von 15 Tagen Leistungsdaten CPU-intensiv ist, empfiehlt es sich, das Hinzufügen neuer Cluster zu staffeln, so dass Datenkontinuitätssammlung nicht auf zu vielen Clustern zur gleichen Zeit laufen. Wenn Sie Unified Manager während des Datenerfassungszeitraums neu starten, wird die Sammlung angehalten, und es werden für den fehlenden Zeitraum Lücken in den Leistungsdiagrammen angezeigt.

Wenn Sie eine Fehlermeldung erhalten, dass Sie das Cluster nicht hinzufügen können, prüfen Sie, ob die folgenden Probleme vorhanden sind:

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

Konfigurieren von Unified Manager zum Senden von Warnmeldungen

Sie können Unified Manager so konfigurieren, dass Sie Benachrichtigungen über Ereignisse in Ihrer Umgebung senden. Bevor Benachrichtigungen gesendet werden können, müssen Sie mehrere andere Unified Manager-Optionen konfigurieren.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Nach der Bereitstellung von Unified Manager und dem Abschluss der Erstkonfiguration sollten Sie Ihre Umgebung in Betracht ziehen, um Warnmeldungen auszulösen und auf der Grundlage des Eingangs von Ereignissen Benachrichtigungs-E-Mails oder SNMP-Traps zu generieren.

Schritte

1. Konfigurieren Sie die Einstellungen für Ereignisbenachrichtigungen

   Wenn Sie Benachrichtigungen senden möchten, wenn bestimmte Ereignisse in Ihrer Umgebung auftreten, müssen Sie einen SMTP-Server konfigurieren und eine E-Mail-Adresse angeben, von der die Benachrichtigung gesendet wird. Wenn Sie SNMP-Traps verwenden möchten, können Sie diese Option auswählen und die erforderlichen Informationen angeben.

2. Aktivieren Sie die Remote-Authentifizierung

   Wenn Remote-LDAP- oder Active Directory-Benutzer auf die Unified Manager-Instanz zugreifen und Warnmeldungen erhalten möchten, müssen Sie die Remote-Authentifizierung aktivieren.

3. Authentifizierungsserver hinzufügen

   Sie können Authentifizierungsserver hinzufügen, sodass Remote-Benutzer innerhalb des Authentifizierungsservers auf Unified Manager zugreifen können.

4. Benutzer hinzufügen

   Sie können mehrere verschiedene Typen von lokalen oder Remote-Benutzern hinzufügen und bestimmte Rollen zuweisen. Wenn Sie eine Warnmeldung erstellen, weisen Sie einen Benutzer zu, der die Benachrichtigungen erhält.

5. Warnmeldungen hinzufügen

   Nachdem Sie die E-Mail-Adresse zum Senden von Benachrichtigungen hinzugefügt haben, Benutzer hinzugefügt, um die Benachrichtigungen zu empfangen, Netzwerkeinstellungen konfiguriert und SMTP- und SNMP-Optionen konfiguriert, die für Ihre Umgebung erforderlich sind, können Sie Benachrichtigungen zuweisen.

Konfigurieren von Einstellungen für Ereignisbenachrichtigungen

Sie können Unified Manager so konfigurieren, dass Benachrichtigungen gesendet werden, wenn ein Ereignis generiert wird oder ein Ereignis einem Benutzer zugewiesen ist. Sie können den SMTP-Server konfigurieren, der zum Senden der Warnmeldung

verwendet wird, und Sie können verschiedene Benachrichtigungsmechanismen festlegen – beispielsweise können Alarmbenachrichtigungen als E-Mails oder SNMP-Traps gesendet werden.

Bevor Sie beginnen

Sie müssen die folgenden Informationen haben:

- E-Mail-Adresse, von der die Benachrichtigung gesendet wird

  Die E-Mail-Adresse wird im Feld „`von`“ in gesendeten Warnmeldungen angezeigt. Falls die E-Mail aus irgendeinem Grund nicht zugestellt werden kann, wird diese E-Mail-Adresse auch als Empfänger für nicht lieferbare E-Mails verwendet.

- Hostname des SMTP-Servers sowie Benutzername und Kennwort für den Zugriff auf den Server
- SNMP-Version, Trap-Ziel-Host-IP-Adresse, Outbound-Trap-Port und die Community zum Konfigurieren des SNMP-Trap

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Setup-Menü auf **Benachrichtigungen**.
2. Konfigurieren Sie auf der Seite **Setup/Benachrichtigungen** die entsprechenden Einstellungen und klicken Sie auf **Speichern**.

   Hinweise:

   - Wenn die von-Adresse mit der Adresse „`OnCommand@localhost.com`“ ausgefüllt ist, sollten Sie sie in eine echte, funktionierende E-Mail-Adresse ändern, um sicherzustellen, dass alle E-Mail-Benachrichtigungen erfolgreich versendet werden.
   - Wenn der Hostname des SMTP-Servers nicht aufgelöst werden kann, können Sie anstelle des Host-Namens die IP-Adresse (IPv4 oder IPv6) des SMTP-Servers angeben.

Aktivieren der Remote-Authentifizierung

Sie können die Remote-Authentifizierung aktivieren, damit der Unified Manager-Server mit Ihren Authentifizierungsservern kommunizieren kann. Die Benutzer des Authentifizierungsservers können auf die grafische Schnittstelle von Unified Manager zugreifen, um Storage-Objekte und Daten zu managen.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Der Unified Manager-Server muss direkt mit dem Authentifizierungsserver verbunden sein. Sie müssen alle lokalen LDAP-Clients wie SSSD (System Security Services Daemon) oder NSLCD (Name Service LDAP Caching Daemon) deaktivieren.

Über diese Aufgabe

Sie können die Remote-Authentifizierung entweder über Open LDAP oder Active Directory aktivieren. Wenn die Remote-Authentifizierung deaktiviert ist, können Remote-Benutzer nicht auf Unified Manager zugreifen.

Die Remote-Authentifizierung wird über LDAP und LDAPS (Secure LDAP) unterstützt. Unified Manager verwendet 389 als Standardport für nicht sichere Kommunikation und 636 als Standardport für sichere Kommunikation.

Das Zertifikat, das zur Authentifizierung von Benutzern verwendet wird, muss dem X.509-Format entsprechen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** die Option **Remote-Authentifizierung aktivieren** aus.
3. Wählen Sie im Feld **Authentifizierungsdienst** den Diensttyp aus und konfigurieren Sie den Authentifizierungsdienst.

Für Authentifizierungstyp…	Geben Sie die folgenden Informationen ein…
Active Directory	• Administratorname des Authentifizierungsservers in einem der folgenden Formate: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (Mit der entsprechenden LDAP-Schreibweise) • Administratorpasswort • Basisname (unter Verwendung der entsprechenden LDAP-Notation)
Öffnen Sie LDAP	• Distinguished Name binden (in der entsprechenden LDAP-Notation) • Kennwort binden • Basisname mit Distinguished Name

Wenn die Authentifizierung eines Active Directory-Benutzers sehr viel Zeit oder Zeit in Anspruch nimmt, benötigt der Authentifizierungsserver wahrscheinlich eine lange Zeit, um darauf zu reagieren. Wenn Sie die Unterstützung für verschachtelte Gruppen in Unified Manager deaktivieren, wird die Authentifizierungszeit möglicherweise verkürzt.

Wenn Sie die Option Sichere Verbindung verwenden für den Authentifizierungsserver auswählen, kommuniziert Unified Manager mit dem Authentifizierungsserver über das SSL-Protokoll (Secure Sockets Layer).

4. Fügen Sie Authentifizierungsserver hinzu, und testen Sie die Authentifizierung.

5. Klicken Sie auf **Speichern und Schließen**.

Deaktivieren verschachtelter Gruppen von der Remote-Authentifizierung

Wenn die Remote-Authentifizierung aktiviert ist, können Sie die verschachtelte Gruppenauthentifizierung deaktivieren, sodass sich nur einzelne Benutzer und nicht Gruppenmitglieder im Remote-Zugriff auf Unified Manager authentifizieren können. Sie können verschachtelte Gruppen deaktivieren, wenn Sie die Reaktionszeit der Active Directory-Authentifizierung verbessern möchten.

Bevor Sie beginnen

- Sie müssen die OnCommand-Administratorrolle besitzen.
- Das Deaktivieren verschachtelter Gruppen ist nur bei Verwendung von Active Directory anwendbar.

Über diese Aufgabe

Wenn Sie die Unterstützung für verschachtelte Gruppen in Unified Manager deaktivieren, wird die Authentifizierungszeit möglicherweise verkürzt. Wenn die Unterstützung verschachtelter Gruppen deaktiviert ist und eine Remote-Gruppe zu Unified Manager hinzugefügt wird, müssen einzelne Benutzer Mitglieder der Remote-Gruppe sein, um sich bei Unified Manager zu authentifizieren.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Aktivieren Sie auf der Seite **Setup/Authentifizierung** das Kontrollkästchen **Nested Group Lookup deaktivieren**.
3. Klicken Sie Auf **Speichern**.

Hinzufügen von Authentifizierungsservern

Sie können Authentifizierungsserver hinzufügen und die Remote-Authentifizierung auf dem Verwaltungsserver aktivieren, sodass Remote-Benutzer innerhalb des Authentifizierungsservers auf Unified Manager zugreifen können.

Bevor Sie beginnen

- Folgende Informationen müssen zur Verfügung stehen:
  - Hostname oder IP-Adresse des Authentifizierungsservers
  - Portnummer des Authentifizierungsservers
- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst so konfiguriert haben, dass der Verwaltungsserver Remote-Benutzer oder -Gruppen im Authentifizierungsserver authentifizieren kann.
- Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Wenn der neue Authentifizierungsserver Teil eines Hochverfügbarkeitspaars (HA-Paar) ist (unter Verwendung derselben Datenbank), können Sie auch den Authentifizierungsserver des Partners hinzufügen. Dadurch kann

der Management-Server mit dem Partner kommunizieren, wenn einer der Authentifizierungsserver nicht erreichbar ist.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Klicken Sie auf der Seite **Setup/Authentifizierung** auf **Management Server** > **Authentifizierung**.
3. Aktivieren oder Deaktivieren der Option * Sichere Verbindungsauthentifizierung verwenden*:

Ihr Ziel ist	Dann tun Sie das…
Aktivieren Sie sie	a. Aktivieren Sie im Kontrollkästchen Remoteauthentifizierung aktivieren die Option **Sichere Verbindung verwenden**. b. Klicken Sie im Bereich Authentication Servers auf **Add**. c. Geben Sie im Dialogfeld Authentifizierungsserver hinzufügen den Authentifizierungsnamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein. d. Klicken Sie im Dialogfeld Host autorisieren auf Zertifikat anzeigen. e. Überprüfen Sie im Dialogfeld Zertifikat anzeigen die Zertifikatinformationen und klicken Sie dann auf **Schließen**. f. Klicken Sie im Dialogfeld Host autorisieren auf **Ja**. Wenn Sie die Option **Sichere Verbindungsauthentifizierung verwenden** aktivieren, kommuniziert Unified Manager mit dem Authentifizierungsserver und zeigt das Zertifikat an. Unified Manager verwendet 636 als Standardport für sichere Kommunikation und Portnummer 389 für nicht sichere Kommunikation.

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren	a. Deaktivieren Sie im Kontrollkästchen Remoteauthentifizierung aktivieren die Option **Sichere Verbindung verwenden**. b. Klicken Sie im Bereich Authentication Servers auf **Add**. c. Geben Sie im Dialogfeld Authentifizierungsserver hinzufügen entweder den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) des Servers und die Portdetails an. d. Klicken Sie Auf **Hinzufügen**.

Der hinzugefügte Authentifizierungsserver wird im Bereich Server angezeigt.

4. Führen Sie eine Testauthentifizierung durch, um zu bestätigen, dass Sie Benutzer im hinzugefügten Authentifizierungsserver authentifizieren können.

Die Konfiguration der Authentifizierungsserver wird getestet

Sie können die Konfiguration Ihrer Authentifizierungsserver überprüfen, um sicherzustellen, dass der Verwaltungsserver mit diesen Servern kommunizieren kann. Sie können die Konfiguration validieren, indem Sie von Ihren Authentifizierungsservern nach einem Remote-Benutzer oder einer Remotegruppe suchen und diese unter Verwendung der konfigurierten Einstellungen authentifizieren.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst so konfiguriert haben, dass der Unified Manager-Server den Remote-Benutzer oder die Remote-Gruppe authentifizieren kann.
- Sie müssen Ihre Authentifizierungsserver hinzugefügt haben, damit der Verwaltungsserver von diesen Servern nach dem Remote-Benutzer oder der Remote-Gruppe suchen und diese authentifizieren kann.
- Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Wenn der Authentifizierungsservice auf Active Directory festgelegt ist und Sie die Authentifizierung von Remote-Benutzern validieren, die zur primären Gruppe des Authentifizierungsservers gehören, werden in den Authentifizierungsergebnissen keine Informationen zur primären Gruppe angezeigt.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Klicken Sie auf der Seite **Setup/Authentifizierung** auf **Testauthentifizierung**.
3. Geben Sie im Dialogfeld **Testbenutzer** den Benutzernamen und das Kennwort des Remote-Benutzers oder den Benutzernamen der Remote-Gruppe an und klicken Sie dann auf **Test**.

Wenn Sie eine Remote-Gruppe authentifizieren, müssen Sie das Kennwort nicht eingeben.

Benutzer hinzufügen

Sie können lokale Benutzer oder Datenbankbenutzer über die Seite Verwaltung/Benutzer hinzufügen. Sie können auch Remote-Benutzer oder -Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Sie können diesen Benutzern Rollen zuweisen. Anhand der Berechtigungen der Rollen können Benutzer Storage-Objekte und -Daten mit Unified Manager managen oder die Daten in einer Datenbank anzeigen.

Bevor Sie beginnen

- Sie müssen die OnCommand-Administratorrolle besitzen.
- Um einen Remote-Benutzer oder eine Remotegruppe hinzuzufügen, müssen Sie die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsserver konfiguriert haben.
- Wenn Sie die SAML-Authentifizierung so konfigurieren möchten, dass ein Identitäts-Provider (IdP) Benutzer authentifiziert, die auf die grafische Schnittstelle zugreifen, stellen Sie sicher, dass diese Benutzer als „`remote`“-Benutzer definiert sind.

  Der Zugriff auf die Benutzeroberfläche ist Benutzern vom Typ „`local`“ oder „`maintBuße`“ nicht erlaubt, wenn die SAML-Authentifizierung aktiviert ist.

Über diese Aufgabe

Wenn Sie eine Gruppe aus Windows Active Directory hinzufügen, können sich alle direkten Mitglieder und geschachtelten Untergruppen bei Unified Manager authentifizieren, es sei denn, geschachtelte Untergruppen sind deaktiviert. Wenn Sie eine Gruppe von OpenLDAP oder anderen Authentifizierungsdiensten hinzufügen, können sich nur die direkten Mitglieder dieser Gruppe bei Unified Manager authentifizieren.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.
2. Klicken Sie auf der Seite **Verwaltung/Benutzer** auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld **Benutzer hinzufügen** den Benutzertyp aus, den Sie hinzufügen möchten, und geben Sie die erforderlichen Informationen ein.

   Wenn Sie die erforderlichen Benutzerinformationen eingeben, müssen Sie eine E-Mail-Adresse angeben, die für diesen Benutzer eindeutig ist. Sie müssen vermeiden, E-Mail-Adressen anzugeben, die von mehreren Benutzern gemeinsam verwendet werden.

4. Klicken Sie Auf **Hinzufügen**.

Hinzufügen von Meldungen

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

Bevor Sie beginnen

- Sie müssen Benachrichtigungseinstellungen wie die Benutzer-E-Mail-Adresse, SMTP-Server und SNMP-Trap-Host konfiguriert haben, damit der Unified Manager-Server diese Einstellungen verwenden kann, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Meldung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie ein Skript basierend auf dem Ereignis ausführen möchten, müssen Sie das Skript mithilfe der Seite Management/Scripts zu Unified Manager hinzugefügt haben.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können eine Warnmeldung direkt auf der Seite Ereignisdetails erstellen, nachdem Sie ein Ereignis empfangen haben. Zusätzlich können Sie eine Warnung auf der Seite Konfiguration/Warnmeldungen erstellen, wie hier beschrieben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Alerting**.
2. Klicken Sie auf der Seite **Konfiguration/Alarmfunktionen** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
4. Klicken Sie auf **Ressourcen**, und wählen Sie die Ressourcen aus, die in die Warnung aufgenommen oder von ihr ausgeschlossen werden sollen.

   Sie können einen Filter festlegen, indem Sie im Feld **Name enthält** eine Textzeichenfolge angeben, um eine Gruppe von Ressourcen auszuwählen. Die Liste der verfügbaren Ressourcen zeigt auf der Grundlage der angegebenen Textzeichenfolge nur die Ressourcen an, die der Filterregel entsprechen. Die von Ihnen angegebene Textzeichenfolge ist die Groß-/Kleinschreibung.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschl- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschließregel, und die Warnung wird nicht für Ereignisse generiert, die sich auf die ausgeschlossene Ressource beziehen.

5. Klicken Sie auf **Events** und wählen Sie die Ereignisse basierend auf dem Ereignisnamen oder dem Schweregrad aus, für den Sie eine Warnung auslösen möchten.

   Um mehrere Ereignisse auszuwählen, drücken Sie die Strg-Taste, während Sie Ihre Auswahl treffen.

6. Klicken Sie auf **Actions**, und wählen Sie die Benutzer aus, die Sie benachrichtigen möchten, wählen Sie die Benachrichtigungshäufigkeit aus, wählen Sie aus, ob ein SNMP-Trap an den Trap-Empfänger gesendet wird, und weisen Sie ein Skript zu, das ausgeführt werden soll, wenn eine Warnung erzeugt wird.

   Wenn Sie die für den Benutzer angegebene E-Mail-Adresse ändern und die Warnmeldung zur Bearbeitung erneut öffnen, erscheint das Feld Name leer, da die geänderte E-Mail-Adresse dem zuvor ausgewählten Benutzer nicht mehr zugeordnet ist. Wenn Sie die E-Mail-Adresse des ausgewählten Benutzers auf der Seite Verwaltung/Benutzer geändert haben, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

Sie können auch Benutzer über SNMP-Traps benachrichtigen.

7. Klicken Sie Auf **Speichern**.

Beispiel für das Hinzufügen einer Meldung

Dieses Beispiel zeigt, wie eine Warnung erstellt wird, die die folgenden Anforderungen erfüllt:

- Alarmname: HealthTest
- Ressourcen: Enthält alle Volumes, deren Name „`abc`“ enthält und schließt alle Volumes aus, deren Name „`xyz`“ enthält
- Ereignisse: Umfasst alle kritischen Systemzustandsereignisse
- Aktionen: Enthält “sample@domain.com”, ein Skript “Test”, und der Benutzer muss alle 15 Minuten benachrichtigt werden

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

1. Klicken Sie auf **Name** und geben Sie ein `HealthTest` Im Feld **Alarmname**.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
   a. Eingabe `abc` Im Feld **Name enthält** werden die Volumes angezeigt, deren Name „`abc`“ enthält.
   b. Wählen Sie im Bereich Verfügbare Ressourcen **<<All Volumes whose name contains 'abc'>>** aus, und verschieben Sie sie in den Bereich Ausgewählte Ressourcen.
   c. Klicken Sie auf **Ausschließe**, und geben Sie ein `xyz` Klicken Sie im Feld **Name enthält** auf **Hinzufügen**.
3. Klicken Sie auf **Events** und wählen Sie im Feld Ereignis Severity * die Option **kritisch** aus.
4. Wählen Sie im Bereich passende Ereignisse die Option * Alle kritischen Ereignisse* aus, und verschieben Sie sie in den Bereich Ausgewählte Ereignisse.
5. Klicken Sie auf **Aktionen** und geben Sie ein `sample@domain.com` Im Feld „Diese Benutzer benachrichtigen“.
6. Wählen Sie **alle 15 Minuten**, um den Benutzer alle 15 Minuten zu benachrichtigen.

   Sie können eine Warnung konfigurieren, um wiederholt Benachrichtigungen an die Empfänger für eine bestimmte Zeit zu senden. Legen Sie fest, zu welchem Zeitpunkt die Ereignisbenachrichtigung für die Warnmeldung aktiv ist.

7. Wählen Sie im Menü Skript zum Ausführen auswählen die Option **Test** Skript .
8. Klicken Sie Auf **Speichern**.

EMS-Ereignisse, die automatisch dem Unified Manager hinzugefügt werden

Bei der Verwendung von Unified Manager 9.4 oder höher werden die folgenden ONTAP EMS-Ereignisse automatisch dem Unified Manager hinzugefügt. Diese Ereignisse werden generiert, wenn sie auf jedem Cluster ausgelöst werden, das Unified Manager überwacht.

Die folgenden EMS-Ereignisse stehen zur Verfügung, wenn Cluster mit ONTAP 9.5 oder höher überwacht werden:

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad der ONTAP
Objektspeicherzugriff für Aggregatverschiebung verweigert	arl.netra.ca.check.failed	Aggregat	Fehler
Objektspeicherzugriff während eines Storage Failover für Aggregatverschiebung verweigert	gb.netra.ca.check.failed	Aggregat	Fehler
FabricPool Speicherplatz fast voll	Fabricpool.Fast.full	Cluster	Fehler
Beginn des NVMe-of-Grace-Zeitraums	nvmf.graceperiod.start	Cluster	Warnung
NVMe-of-Grace-Zeitraum aktiv	nvmf.graceperiod.active	Cluster	Warnung
NVMe-of-Grace-Zeitraum abgelaufen	nvmf.graceperiod.expired	Cluster	Warnung
LUN wurde zerstört	lun.destroy	LUN	Informationsdaten
Cloud AWS MetaDataConnFail	Cloud.aws.metadataConnFail	Knoten	Fehler
Cloud AWS IAMCredsExpired – Cloud	Cloud.aws.iamCredsExpired	Knoten	Fehler
Cloud AWS IAMCredsungültig	Cloud.aws.iamCredsungültig	Knoten	Fehler
Cloud AWS IAMCredsNotFound	Cloud.aws.iamCredsNotFound	Knoten	Fehler
Cloud AWS IAMCredsNotinitialisiert	Cloud.aws.iamNotinitialisiert	Knoten	Informationsdaten
Cloud AWS IAMRoleInvalid	Cloud.AWS.iamRoleIngültig	Knoten	Fehler
Cloud AWS IAMRoleNotFound	Cloud.aws.iamRoleNotFound	Knoten	Fehler

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad der ONTAP
Objstore Host Unlösbar	Objstore.Host.unlösbar	Knoten	Fehler
Objstore InterClusterLifDown	objstore.interclusterlifDown	Knoten	Fehler
Signatur des Objektspeichers mit Nichtübereinschrift anfordern	osc.signatureMismatch	Knoten	Fehler
Einer der NFSv4-Pools ist erschöpft	Nblade.nfsV4PoolAust	Knoten	Kritisch
QoS Monitor Memory-Besteuerung	qos.Monitor.Memory.maxed	Knoten	Fehler
QoS Monitor Memory nicht gespeichert	qos.Monitor.Memory.abgenutzt	Knoten	Informationsdaten
NVMeNS zerstören	NVMeNS.destroy	Namespace	Informationsdaten
NVMeNS Online	NVMeNS.offline	Namespace	Informationsdaten
NVMeNS Offline	NVMeNS.online	Namespace	Informationsdaten
NVMe Out of Space	NVMeNS.out.of.space	Namespace	Warnung
Synchrone Replizierung Aus Sync Heraus	sms.Status.out.of.Sync	SnapMirror Beziehung	Warnung
Synchrone Replizierung Wiederhergestellt	sms.status.in.sync	SnapMirror Beziehung	Informationsdaten
Fehler Bei Der Automatischen Synchronisierung Der Replikation	sms.Resync.Versuch.failed	SnapMirror Beziehung	Fehler
Viele CIFS-Verbindungen	Nblade.cifsManyAuths	SVM	Fehler
Max. CIFS-Verbindung überschritten	Nblade.cifsMaxOpenSameFile	SVM	Fehler

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad der ONTAP
Max. Anzahl der CIFS-Verbindung pro Benutzer überschritten	Nblade.cifsMaxSessPerUsrConn	SVM	Fehler
CIFS NetBIOS-Namenskonflikt	Nblade.cifsNbNameConflict	SVM	Fehler
Versucht, eine nicht existierende CIFS-Freigabe zu verbinden	Nblade.cifsNoPrivShare	SVM	Kritisch
Fehler beim CIFS Shadow Copy-Vorgang	cifs.shadowcopy.Failure	SVM	Fehler
Vom AV-Server gefundener Virus	Nblade.vscanVirusDetected	SVM	Fehler
Keine AV-Server-Verbindung für Virus Scan	Nblade.vscanNoScannerKonn	SVM	Kritisch
Kein AV-Server registriert	Nblade.vscanNoRegdScanner	SVM	Fehler
Keine reaktionsfähige AV-Server-Verbindung	Nblade.vscanConnInaktiv	SVM	Informationsdaten
AV-Server ist zu beschäftigt, um neue Scananforderung zu akzeptieren	Nblade.vscanConnBackPressure	SVM	Fehler
Nicht autorisierter Benutzer versucht, AV-Server zu verwenden	Nblade.vscanBadUserPrivAccess	SVM	Fehler
FlexGroup-Komponenten haben Platzprobleme	Flexgroup.debestandals.have.space.Issues	Datenmenge	Fehler
FlexGroup-Komponenten-Space-Status alles OK	Flexgroup.Komponenten.space.Status.all.ok	Datenmenge	Informationsdaten
FlexGroup-Komponenten haben Inodes-Probleme	flexgroup.constituents.have.inodes.issues	Datenmenge	Fehler

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad der ONTAP
FlexGroup-Komponenten inodes Status Alle OK	flexgroup.constituents.inodes.status.all.ok	Datenmenge	Informationsdaten
Logischer Volume-Speicherplatz Fast Voll	Monitor.vol.nearFull	Datenmenge	Warnung
Logischer Speicherplatz Des Volume Voll	Monitor.vol.voll	Datenmenge	Fehler
Logischer Speicherplatz Des Volume Ist Normal	Monitor.vol.one.ok	Datenmenge	Informationsdaten
Fehler bei der automatischen WAFL-Volume-Größe	wafl.vol.autoSize.fail	Datenmenge	Fehler
Die automatische WAFL-Volume-Größe ist abgeschlossen	wafl.vol.autoSize.done	Datenmenge	Informationsdaten

Abonnieren von ONTAP EMS-Veranstaltungen

Sie können EMS-Ereignisse (Event Management System) abonnieren, die von Systemen generiert werden, die mit ONTAP Software installiert sind. Eine Untermenge von EMS-Ereignissen wird automatisch an Unified Manager gemeldet. Weitere EMS-Ereignisse werden jedoch nur gemeldet, wenn Sie sich für diese Ereignisse angemeldet haben.

Bevor Sie beginnen

Abonnieren Sie keine EMS-Ereignisse, die bereits Unified Manager hinzugefügt wurden, da dies zu Verwirrung führen kann, wenn Sie zwei Ereignisse für dasselbe Problem erhalten.

Über diese Aufgabe

Sie können eine beliebige Anzahl von EMS-Veranstaltungen abonnieren. Alle Ereignisse, die Sie abonnieren, werden validiert. Nur die validierten Ereignisse werden auf die in Unified Manager überwachten Cluster angewendet. Der *ONTAP 9 EMS Ereigniskatalog* bietet detaillierte Informationen zu allen EMS-Nachrichten für die angegebene Version der ONTAP 9-Software. Suchen Sie auf der Seite ONTAP 9 Produktdokumentation die entsprechende Version des *EMS-Ereigniskatalogs*, um eine Liste der entsprechenden Veranstaltungen zu finden.

"ONTAP 9 Produktbibliothek"

Sie können Benachrichtigungen für die von Ihnen abonnierenden ONTAP EMS-Ereignisse konfigurieren und benutzerdefinierte Skripts für die Ausführung dieser Ereignisse erstellen.

Wenn Sie die ONTAP EMS-Ereignisse, die Sie abonniert haben, kann es möglicherweise ein Problem mit der DNS-Konfiguration des Clusters geben, was verhindert, dass das Cluster den Unified Manager-Server erreicht. Um dieses Problem zu beheben, muss der Cluster-Administrator die DNS-Konfiguration des Clusters korrigieren und dann Unified Manager neu starten. Dadurch werden die ausstehenden EMS-Ereignisse an den Unified Manager-Server gespült.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Ereignisse verwalten**.
2. Klicken Sie auf der Seite **Konfiguration/Ereignisse verwalten** auf die Schaltfläche **EMS-Ereignisse abonnieren**.
3. Geben Sie im Dialogfeld * EMS-Ereignisse abonnieren* den Namen des ONTAP EMS-Events ein, zu dem Sie abonnieren möchten.

   Um die Namen der EMS-Ereignisse anzuzeigen, die Sie in der ONTAP Cluster Shell abonnieren können, können Sie die verwenden `event route show` Befehl (vor ONTAP 9) oder der `event catalog show` Befehl (ONTAP 9 oder höher).

   "So konfigurieren Sie ONTAP EMS-Ereignisabonnements in OnCommand Unified Manager / Active IQ Unified Manager"

4. Klicken Sie Auf **Hinzufügen**.

   Das EMS-Ereignis wird der Liste der abonnierten EMS-Ereignisse hinzugefügt, aber in der Spalte „Cluster anwendbar“ wird für das hinzugefügte EMS-Ereignis der Status als „`Unbekannt`“ angezeigt.

5. Klicken Sie auf **Speichern und Schließen**, um das EMS-Ereignisabonnement mit dem Cluster zu registrieren.
6. Klicken Sie erneut auf **EMS-Events abonnieren**.

   Der Status „`ja`“ wird in der Spalte „gilt für Cluster“ für das EMS-Ereignis, das Sie hinzugefügt haben, angezeigt.

   Wenn der Status nicht „`ja`“ lautet, überprüfen Sie die Schreibweise des EMS-Ereignisnamens von ONTAP. Wenn der Name falsch eingegeben wird, müssen Sie das falsche Ereignis entfernen und das Ereignis erneut hinzufügen.

Nachdem Sie fertig sind

Wenn das ONTAP EMS-Ereignis auftritt, wird das Ereignis auf der Seite „Ereignisse“ angezeigt. Sie können das Ereignis auswählen, um Details zum EMS-Ereignis auf der Seite Ereignisdetails anzuzeigen. Sie können auch das Ergebnis des Ereignisses verwalten oder Alarme für das Ereignis erstellen.

Verwalten von SAML-Authentifizierungseinstellungen

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

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

Anforderungen an Identitätsanbieter

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

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

Unterstützte Verschlüsselungsstandards

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

Validierte Identitätsanbieter

- Shibboleth
- Active Directory Federation Services (ADFS)

ADFS-Konfigurationsanforderungen

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

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

- Sie müssen die Authentifizierungsmethode auf „`Forms Authentication`“ festlegen, oder Benutzer erhalten möglicherweise einen Fehler beim Abmelden von Unified Manager, wenn Sie Internet Explorer verwenden. Führen Sie hierzu folgende Schritte aus:
  a. Öffnen Sie die ADFS-Verwaltungskonsole.
  b. Klicken Sie in der linken Strukturansicht auf den Ordner Authentication Policies.
  c. Klicken Sie unter Aktionen auf der rechten Seite auf Globale primäre Authentifizierungsrichtlinie bearbeiten.
  d. Setzen Sie die Intranet-Authentifizierungsmethode auf „`Forms Authentication`“ anstatt auf die Standardauthentifizierung „`Windows Authentication`“.
- In einigen Fällen wird die Anmeldung über das IdP abgelehnt, wenn das Unified Manager-

Sicherheitszertifikat CA-signiert ist. Es gibt zwei Problemumgehungen zur Lösung dieses Problems:

- Befolgen Sie die Anweisungen im Link, um die Widerrufs-Prüfung auf dem ADFS-Server für verkettete CA-Zertifikat zugeordnete abhängige Partei zu deaktivieren:

  http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

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

Sonstige Konfigurationsanforderungen

- Die Unified Manager-Taktskew ist auf 5 Minuten eingestellt, sodass der Zeitunterschied zwischen dem IdP-Server und dem Unified Manager-Server nicht mehr als 5 Minuten betragen kann oder die Authentifizierung fehlschlägt.
- Wenn Benutzer versuchen, mit Internet Explorer auf Unified Manager zuzugreifen, wird möglicherweise die Meldung angezeigt **die Webseite kann die Seite nicht anzeigen**. Stellen Sie in diesem Fall sicher, dass diese Benutzer die Option „`Sso freundliche HTTP-Fehlermeldungen`“ in **Tools** > **Internetoptionen** > **Erweitert** deaktivieren.

Aktivieren der SAML-Authentifizierung

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML Authentication** aus.
3. Aktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.

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

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

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

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

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

6. Klicken Sie Auf **Speichern**.

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

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

Ergebnisse

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

Nachdem Sie fertig sind

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

> Wenn Sie ADFS als Identitäts-Provider verwenden, wird die Unified Manager-GUI nicht das ADFS-Timeout-Timeout erfüllt und funktioniert weiter, bis das Timeout der Unified Manager-Sitzung erreicht ist. Wenn Unified Manager auf Windows, Red hat oder CentOS bereitgestellt wird, kann das Timeout der GUI-Sitzung mit dem folgenden Unified Manager CLI-Befehl geändert werden: `um option set absolute.session.timeout=00:15:00`Mit diesem Befehl wird das Zeitlimit für die Unified Manager GUI-Sitzung auf 15 Minuten festgelegt.

Konfigurieren von Backup-Einstellungen für Datenbanken

Sie können die Backup-Einstellungen für die Unified Manager Datenbank so konfigurieren, dass der Datenbank-Backup-Pfad, die Aufbewahrungsanzahl und der Backup-Zeitplan festgelegt werden. Sie können tägliche oder wöchentliche geplante Backups aktivieren. Standardmäßig sind geplante Backups deaktiviert.

Bevor Sie beginnen

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

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

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

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Datenbank-Backup**.
2. Klicken Sie auf der Seite **Management/Datenbank-Backup** auf **Aktionen** > **Einstellungen für die Datenbanksicherung**.
3. Konfigurieren Sie die entsprechenden Werte für einen Backup-Pfad und die Anzahl der Aufbewahrung.

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

4. Wählen Sie im Abschnitt **Terminhäufigkeit** das Kontrollkästchen **Aktivieren** aus, und geben Sie dann einen täglichen oder wöchentlichen Zeitplan an.
   - * Daily*

     Wenn Sie diese Option auswählen, müssen Sie eine Zeit im 24-Stunden-Format eingeben, um das Backup zu erstellen. Wenn Sie beispielsweise 18:30 angeben, wird täglich um 6:30 Uhr ein Backup erstellt.

   - **Wöchentlich**

     Wenn Sie diese Option auswählen, müssen Sie die Uhrzeit und den Tag für die Erstellung des Backups angeben. Wenn Sie beispielsweise den Tag als Montag und die Zeit als 16:30 angeben, wird jeden Montag um 4:30 Uhr ein wöchentliches Backup erstellt.

5. Klicken Sie auf **Speichern und Schließen**.

Ändern des lokalen Benutzerpassworts

Sie können Ihr lokales Benutzeranmeldeswort ändern, um potenzielle Sicherheitsrisiken zu vermeiden.

Bevor Sie beginnen

Sie müssen als lokaler Benutzer angemeldet sein.

Über diese Aufgabe

Die Passwörter für den Wartungsbenutzer und für Remote-Benutzer können mit diesen Schritten nicht geändert werden. Wenden Sie sich an Ihren Passwortadministrator, um ein Kennwort für Remote-Benutzer zu ändern. Informationen zum Ändern des Wartungs-Benutzerpassworts finden Sie unter "Verwenden der Wartungskonsole".

Schritte

1. Melden Sie sich bei Unified Manager an.
2. Klicken Sie in der oberen Menüleiste auf das Benutzersymbol und dann auf **Passwort ändern**.

   Die Option **Passwort ändern** wird nicht angezeigt, wenn Sie ein Remote-Benutzer sind.

3. Geben Sie im Dialogfeld **Passwort ändern** das aktuelle Passwort und das neue Passwort ein.
4. Klicken Sie Auf **Speichern**.

Nachdem Sie fertig sind

Wenn Unified Manager in einer Hochverfügbarkeitskonfiguration konfiguriert ist, müssen Sie das Passwort auf dem zweiten Node des Setup ändern. Beide Instanzen müssen dasselbe Passwort haben.

Ändern des Unified Manager-Host-Namens

Irgendwann möchten Sie möglicherweise den Host-Namen des Systems ändern, auf dem Unified Manager installiert ist. Beispielsweise möchten Sie den Host umbenennen, um Ihre Unified Manager-Server nach Typ, Arbeitsgruppe oder überwachten Cluster-Gruppen einfacher zu identifizieren.

Je nachdem, ob Unified Manager auf einem VMware ESXi Server, auf einem Red hat oder CentOS Linux Server oder auf einem Microsoft Windows Server ausgeführt wird, sind die zum Ändern des Host-Namens erforderlichen Schritte unterschiedlich.

Ändern des Host-Namens der virtuellen Unified Manager-Appliance

Dem Netzwerk-Host wird ein Name zugewiesen, wenn die virtuelle Unified Manager-Appliance zuerst bereitgestellt wird. Sie können den Host-Namen nach der Bereitstellung ändern. Wenn Sie den Hostnamen ändern, müssen Sie auch das HTTPS-Zertifikat neu generieren.

Bevor Sie beginnen

Sie müssen bei Unified Manager als Wartungbenutzer angemeldet sein oder Ihnen die Rolle „OnCommand Administrator“ zugewiesen haben, um diese Aufgaben ausführen zu können.

Über diese Aufgabe

Sie können den Host-Namen (oder die Host-IP-Adresse) verwenden, um auf die Unified Manager Web-UI zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, hätten Sie einen Namen für den Netzwerk-Host zugewiesen. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollte der Host-Name aus dem DNS übernommen werden. Wenn DHCP oder DNS nicht richtig konfiguriert ist, wird der Hostname „`OnCommand`“ automatisch zugewiesen und dem Sicherheitszertifikat zugeordnet.

Unabhängig davon, wie der Hostname zugewiesen wurde, wenn Sie den Host-Namen ändern und beabsichtigen, den neuen Hostnamen zum Zugriff auf die Unified Manager Web-UI zu verwenden, müssen Sie ein neues Sicherheitszertifikat generieren.

Wenn Sie über die IP-Adresse des Servers und nicht über den Hostnamen auf die Web-Benutzeroberfläche zugreifen, müssen Sie kein neues Zertifikat generieren, wenn Sie den Hostnamen ändern. Es empfiehlt sich jedoch, das Zertifikat so zu aktualisieren, dass der Hostname im Zertifikat dem tatsächlichen Hostnamen entspricht.

Wenn Sie den Host-Namen in Unified Manager ändern, müssen Sie den Hostnamen in OnCommand Workflow Automation (WFA) manuell aktualisieren. Der Host-Name wird in WFA nicht automatisch aktualisiert.

Das neue Zertifikat wird erst wirksam, wenn die virtuelle Unified Manager-Maschine neu gestartet wird.

Schritte

1. Generieren eines HTTPS-Sicherheitszertifikats

   Wenn Sie den neuen Hostnamen zum Zugriff auf die Web-UI von Unified Manager verwenden möchten, müssen Sie das HTTPS-Zertifikat neu generieren, um es mit dem neuen Hostnamen zu verknüpfen.

2. Starten Sie die Virtual Machine von Unified Manager neu

   Nachdem Sie das HTTPS-Zertifikat erneut generiert haben, müssen Sie die virtuelle Unified Manager-Maschine neu starten.

Erstellen eines HTTPS-Sicherheitszertifikats

Sie können aus mehreren Gründen ein neues HTTPS-Sicherheitszertifikat generieren, z. B. wenn Sie mit einer anderen Zertifizierungsstelle signieren möchten oder wenn das aktuelle Sicherheitszertifikat abgelaufen ist. Das neue Zertifikat ersetzt das vorhandene Zertifikat.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Wenn Sie keinen Zugriff auf die Web-UI von Unified Manager haben, können Sie mithilfe der Wartungskonsole das HTTPS-Zertifikat mit den gleichen Werten neu generieren.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Setup** auf **HTTPS-Zertifikat**.

2. Klicken Sie auf **HTTPS-Zertifikat erneut erstellen**.

   Das Dialogfeld „HTTPS-Zertifikat neu erstellen“ wird angezeigt.

3. Wählen Sie je nach Erstellung des Zertifikats eine der folgenden Optionen aus:

Ihr Ziel ist	Tun Sie das…
Generieren Sie das Zertifikat mit den aktuellen Werten neu	Klicken Sie auf die Option **regenerieren mit aktuellen Zertifikatattributen**.
Generieren Sie das Zertifikat mithilfe anderer Werte	`Click the *Update the Current Certificate Attributes* option. Die Felder allgemeiner Name und Alternative Namen verwenden die Werte aus dem vorhandenen Zertifikat, wenn Sie keine neuen Werte eingeben. Die anderen Felder benötigen keine Werte, aber Sie können Werte eingeben, z. B. für Stadt, Bundesland und Land, wenn diese Werte in das Zertifikat eingetragen werden sollen.`  Sie können das Kontrollkästchen „`lokale Identifizierungsdaten ausschließen (z. B. localhost)`“ aktivieren, wenn Sie die lokalen Identifizierungsdaten aus dem Feld Alternative Namen im Zertifikat entfernen möchten. Wenn dieses Kontrollkästchen aktiviert ist, werden nur die Daten verwendet, die Sie in das Feld Alternative Namen eingeben. Wenn das Zertifikat leer gelassen wird, hat das resultierende Zertifikat überhaupt kein Feld alternativer Namen. +

4. Klicken Sie auf **Ja**, um das Zertifikat erneut zu generieren.
5. Starten Sie den Unified Manager-Server neu, damit das neue Zertifikat wirksam wird.

Nachdem Sie fertig sind

Überprüfen Sie die neuen Zertifikatinformationen, indem Sie das HTTPS-Zertifikat anzeigen.

Starten Sie die Virtual Machine von Unified Manager neu

Sie können die virtuelle Maschine von der Wartungskonsole von Unified Manager aus neu starten. Sie müssen neu starten, nachdem Sie ein neues Sicherheitszertifikat erstellt haben oder wenn ein Problem mit der virtuellen Maschine auftritt.

Bevor Sie beginnen

Die virtuelle Appliance wird eingeschaltet.

Sie sind als Maintenance-Benutzer bei der Wartungskonsole angemeldet.

Über diese Aufgabe

Sie können die virtuelle Maschine von vSphere auch mit der Option **Neustart Gast** neu starten. Weitere Informationen finden Sie in der VMware Dokumentation.

Schritte

1. Öffnen Sie die Wartungskonsole.
2. Wählen Sie **Systemkonfiguration** > **Virtuelle Maschine Neu Starten**.

Ändern des Unified Manager Host-Namens auf Linux-Systemen

Irgendwann möchten Sie den Host-Namen von Red hat Enterprise Linux oder CentOS Rechner ändern, auf dem Unified Manager installiert ist. Sie möchten beispielsweise den Host umbenennen, um Ihre Unified Manager-Server nach Typ, Arbeitsgruppe oder überwachten Cluster-Gruppen einfacher zu identifizieren, wenn Sie Ihre Linux-Maschinen auflisten.

Bevor Sie beginnen

Sie müssen über Root-Benutzerzugriff auf das Linux-System verfügen, auf dem Unified Manager installiert ist.

Über diese Aufgabe

Sie können den Host-Namen (oder die Host-IP-Adresse) verwenden, um auf die Unified Manager Web-UI zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, hätten Sie einen Namen für den Netzwerk-Host zugewiesen. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollte der Hostname vom DNS-Server übernommen werden.

Unabhängig davon, wie der Hostname zugewiesen wurde, müssen Sie ein neues Sicherheitszertifikat erstellen, wenn Sie den Hostnamen ändern und den neuen Hostnamen für den Zugriff auf die Unified Manager Web-UI verwenden möchten.

Wenn Sie über die IP-Adresse des Servers und nicht über den Hostnamen auf die Web-Benutzeroberfläche zugreifen, müssen Sie kein neues Zertifikat generieren, wenn Sie den Hostnamen ändern. Es empfiehlt sich jedoch, das Zertifikat zu aktualisieren, sodass der Hostname im Zertifikat dem tatsächlichen Hostnamen entspricht. Das neue Zertifikat wird erst wirksam, wenn der Linux-Rechner neu gestartet wird.

Wenn Sie den Host-Namen in Unified Manager ändern, müssen Sie den Hostnamen in OnCommand Workflow Automation (WFA) manuell aktualisieren. Der Host-Name wird in WFA nicht automatisch aktualisiert.

Schritte

1. Melden Sie sich als Root-Benutzer beim Unified Manager-System an, das Sie ändern möchten.
2. Beenden Sie die Unified Manager Software und die zugehörige MySQL Software, indem Sie die folgenden Befehle in der angezeigten Reihenfolge eingeben:
3. Ändern Sie den Host-Namen mit Linux `hostnamectl` Befehl: `hostnamectl set-hostname new_FQDN`

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Generieren Sie das HTTPS-Zertifikat für den Server erneut:`/opt/netapp/essentials/bin/cert.sh create`
5. Netzwerkdienst neu starten: `service network restart`
6. Überprüfen Sie nach dem Neustart des Dienstes, ob der neue Hostname selbst pingen kann: `ping new_hostname`

   ```
   ping nuhost
   ```

   Dieser Befehl sollte dieselbe IP-Adresse zurückgeben, die zuvor für den ursprünglichen Hostnamen festgelegt wurde.

7. Nachdem Sie die Änderung Ihres Host-Namens abgeschlossen und überprüft haben, starten Sie Unified Manager neu, indem Sie in der angezeigten Reihenfolge die folgenden Befehle eingeben:

Online-Hilfe

Einführung in OnCommand Unified Manager

OnCommand Unified Manager ermöglicht das Monitoring und Management des Systemzustands sowie der Performance Ihrer ONTAP Storage-Systeme über eine einheitliche Benutzeroberfläche.

Unified Manager bietet folgende Funktionen:

- Bestandsaufnahme, Monitoring und Benachrichtigungen für Systeme, die mit der ONTAP Software installiert sind
- Dashboards zur Anzeige von Kapazität, Verfügbarkeit, Schutz und Performance-Zustand der Umgebung
- Erweiterte Alarmfunktionen, Ereignisse und Schwellenwertsinfrastruktur.
- Zeigt detaillierte Diagramme an, die Workload-Aktivitäten im Zeitverlauf darstellen, einschließlich IOPS (Vorgänge), MB/s (Durchsatz), Latenz (Reaktionszeit), Auslastung, Performance-Kapazität und Cache-Verhältnis.
- Identifiziert Workloads, die zu viel Cluster-Komponenten nutzen, und Workloads, deren Performance durch den gesteigerten Durchsatz beeinträchtigt wird
- Enthält vorgeschlagene Korrekturmaßnahmen, die zur Behebung bestimmter Vorfälle und Ereignisse durchgeführt werden können.
- Integration in OnCommand Workflow Automation zur Ausführung automatisierter Workflows

Einführung in das Monitoring des Systemzustands von OnCommand Unified Manager

Mit Unified Manager können Sie eine große Anzahl von Systemen mit ONTAP Software über eine zentrale Benutzeroberfläche überwachen. Die Unified Manager Serverinfrastruktur bietet Skalierbarkeit, Unterstützbarkeit sowie verbesserte Monitoring- und Benachrichtigungsfunktionen.

Zu den Schlüsselfunktionen von Unified Manager gehören Monitoring, Warnmeldungen, Management der Verfügbarkeit und Kapazität von Clustern, Management von Sicherungsfunktionen, Performance-Überwachung, Konfiguration und Management von Infinite Volumes, Annotationen von Storage-Objekten, Bündelung von Diagnosedaten und Senden an den technischen Support.

Mit Unified Manager können Sie die Cluster überwachen. Wenn im Cluster Probleme auftreten, benachrichtigt Sie Unified Manager über Ereignisse, die Einzelheiten zu solchen Problemen betreffen. Bei einigen Ereignissen erhalten Sie zudem eine Abhilfemaßung, die Sie zur Behebung der Probleme ergreifen können. Sie können Benachrichtigungen für Ereignisse so konfigurieren, dass bei Auftreten von Problemen Sie über E-Mail und SNMP-Traps benachrichtigt werden.

Mit Unified Manager können Sie Storage-Objekte in Ihrer Umgebung managen, indem Sie sie mit Annotationen verknüpfen. Sie können benutzerdefinierte Anmerkungen erstellen und Cluster, Storage Virtual Machines (SVMs) und Volumes dynamisch mit den Annotationen über Regeln verknüpfen.

Zudem können Sie die Storage-Anforderungen Ihrer Cluster-Objekte anhand der Informationen in den Kapazitäts- und Integritätsdiagrammen für das jeweilige Cluster-Objekt planen.

Unified Manager Funktionen für das Monitoring des Systemzustands

Unified Manager basiert auf einer Serverinfrastruktur, die Skalierbarkeit, Unterstützbarkeit sowie verbesserte Monitoring- und Benachrichtigungsfunktionen bietet. Unified Manager unterstützt das Monitoring von Systemen mit ONTAP Software.

Unified Manager umfasst die folgenden Funktionen:

- Bestandsaufnahme, Monitoring und Benachrichtigungen für Systeme, die mit der ONTAP Software installiert sind:
  - Physische Objekte: Nodes, Festplatten, Festplatten-Shelfs, SFO-Paare, Ports, Und Flash Cache
  - Logische Objekte: Cluster, Storage Virtual Machines (SVMs), Aggregate, Volumes, LUNs, Namespaces Qtrees, LIFs, Snapshot Kopien, Verbindungspfade, NFS-Exporte, CIFS-Freigaben, Benutzer- und Gruppenkontingente und Initiatorgruppen
  - Protokolle: CIFS, NFS, FC, iSCSI, NVMe, Und FCoE
  - Storage-Effizienz: SSD-Aggregate, Flash Pool-Aggregate, FabricPool-Aggregate, Deduplizierung und Komprimierung
  - Sicherung: SnapMirror Beziehungen (synchron und asynchron) sowie SnapVault Beziehungen
- Anzeigen des Cluster-Erkennungs- und Überwachungsstatus
- MetroCluster Konfiguration: Anzeigen und Überwachen der Konfiguration, MetroCluster Switches und Bridges, Probleme und des Konnektivitätsstatus der Cluster-Komponenten
- Erweiterte Alarmfunktionen, Ereignisse und Schwellenwertsinfrastruktur
- LDAP, LDAPS, SAML-Authentifizierung und Unterstützung lokaler Benutzer
- RBAC (für vordefinierte Rollen)
- AutoSupport und Support-Bundle
- Erweitertes Dashboard zur Anzeige des Kapazitäts-, Verfügbarkeits-, Sicherungs- und Performance-Zustands der Umgebung
- Interoperabilität bei Volume-Verschiebung, Verlauf der Volume-Verschiebung und Änderungsverlauf für Verbindungspfade
- Bereich „Auswirkungen“, in dem die Ressourcen angezeigt werden, die für Ereignisse wie fehlerhafte Festplatten, heruntergestuften MetroCluster Aggregatspiegelung und MetroCluster-Ersatzfestplatten, die bei Ereignissen noch nicht vorhanden sind, betroffen sind
- Möglicher Effektbereich, der die Wirkung der MetroCluster-Ereignisse anzeigt
- Bereich „Empfohlene Korrekturmaßnahmen“, in dem die Aktionen angezeigt werden, die zur Behebung von Ereignissen durchgeführt werden können, z. B. fehlerhafte Festplatten, eingeschränkte MetroCluster Aggregatspiegelung und nicht mehr vorhandene MetroCluster-Ersatzfestplatten
- Ressourcen, die möglicherweise betroffen sein könnten, zeigen die Ressourcen an, die für Ereignisse wie das Offline-Ereignis von Volume, das Ereignis Volume Restricted und den risikobehaftete Volume-Speicherplatz auf einem Volume mit Thin Provisioning verfügbar sein könnten
- Unterstützung für SVMs mit:
  - FlexVol Volumes
  - FlexGroup Volumes
  - Unbegrenzte Volumes

- Unterstützung für das Monitoring von Root-Volumes der Nodes
- Verbessertes Monitoring von Snapshot Kopien, einschließlich Computing von zurückforderbarem Speicherplatz und Löschen von Snapshot Kopien
- Anmerkungen für Speicherobjekte
- Berichte für die Erstellung und das Management von Storage-Objektinformationen wie physische und logische Kapazität, Auslastung, Platzeinsparungen und zugehörige Ereignisse
- Integration in OnCommand Workflow Automation zur Ausführung von Workflows

  Der Storage Automation Store enthält von NetApp zertifizierte automatisierte Workflow-Pakete für die Verwendung mit OnCommand Workflow Automation (WFA). Sie können die Pakete herunterladen und anschließend in WFA importieren, um sie auszuführen. Die automatisierten Workflows sind im folgenden verfügbar "Storage Automation Store"

Einführung in das Performance-Monitoring von OnCommand Unified Manager

OnCommand Unified Manager bietet Funktionen für das Performance-Monitoring und Ursachenanalyse für Systeme, auf denen NetApp ONTAP Software ausgeführt wird.

Unified Manager hilft Ihnen, Workloads zu identifizieren, die die Cluster-Komponenten überbeanspruchen, und die Performance anderer Workloads auf dem Cluster zu senken. Durch das Definieren von Richtlinien für Performance-Schwellenwerte können Sie auch Maximalwerte für bestimmte Performance-Zähler angeben, sodass Ereignisse bei Überschreitung des Schwellenwerts generiert werden. Unified Manager benachrichtigt Sie über diese Performance-Ereignisse, sodass Korrekturmaßnahmen ergriffen und die Performance wieder auf normalen Niveau des Betriebs wiederhergestellt werden kann. Sie können Ereignisse in der Benutzeroberfläche von Unified Manager anzeigen und analysieren.

Unified Manager überwacht die Performance zweier Workload-Typen:

- Benutzerdefinierte Workloads

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

- Systemdefinierte Workloads

  Diese Workloads bestehen aus interner Systemaktivität.

Funktionen für das Performance-Monitoring in Unified Manager

Unified Manager sammelt und analysiert Performance-Statistiken von Systemen, auf denen ONTAP Software ausgeführt wird. Es nutzt dynamische Performance-Schwellenwerte und benutzerdefinierte Performance-Schwellenwerte, um eine Vielzahl von Performance-Zähler über viele Cluster-Komponenten zu überwachen.

Eine hohe Reaktionszeit (Latenz) gibt an, dass das Storage-Objekt, beispielsweise ein Volume, langsamer als normal läuft. Dieses Problem weist außerdem darauf hin, dass die Performance für Client-Applikationen, die das Volume nutzen, gesunken ist. Unified Manager ermittelt die Storage-Komponente, in der das Performance-Problem liegt, und enthält eine Liste mit Vorschlägen, die Sie zur Behebung des Performance-Problems ergreifen können.

Unified Manager umfasst die folgenden Funktionen:

- Überwachung und Analyse der Workload-Performance-Statistiken eines Systems mit ONTAP Software
- Tracking von Performance-Zählern für Cluster, Nodes, Aggregate, Ports, SVMs Volumes, LUNs, NVMe-Namespaces und LIFs.
- Zeigt detaillierte Diagramme an, die Workload-Aktivitäten im Zeitverlauf darstellen, einschließlich IOPS (Vorgänge), MB/s (Durchsatz), Latenz (Reaktionszeit), Auslastung, Performance-Kapazität und Cache-Verhältnis.
- Ermöglicht die Erstellung benutzerdefinierter Performance-Schwellenwertrichtlinien, die Ereignisse auslösen und E-Mail-Alarme senden, wenn die Schwellenwerte nicht überschritten werden.
- Hier werden systemdefinierte Schwellenwerte und dynamische Performance-Schwellenwerte verwendet, die Informationen zu Ihrer Workload-Aktivität enthalten, um Performance-Probleme zu identifizieren und zu benachrichtigen.
- Ermittelt eindeutig die Clusterkomponente, die mit einem Konflikt in Konflikt steht.
- Identifiziert Workloads, die zu viel Cluster-Komponenten nutzen, und Workloads, deren Performance durch den gesteigerten Durchsatz beeinträchtigt wird

Was macht der Unified Manager Server

Die Unified Manager Server-Infrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Applikationsserver. Die Lösung bietet Infrastrukturservices wie beispielsweise Discovery, Monitoring, rollenbasierte Zugriffssteuerung (RBAC), Audits und Protokollierungsfunktionen.

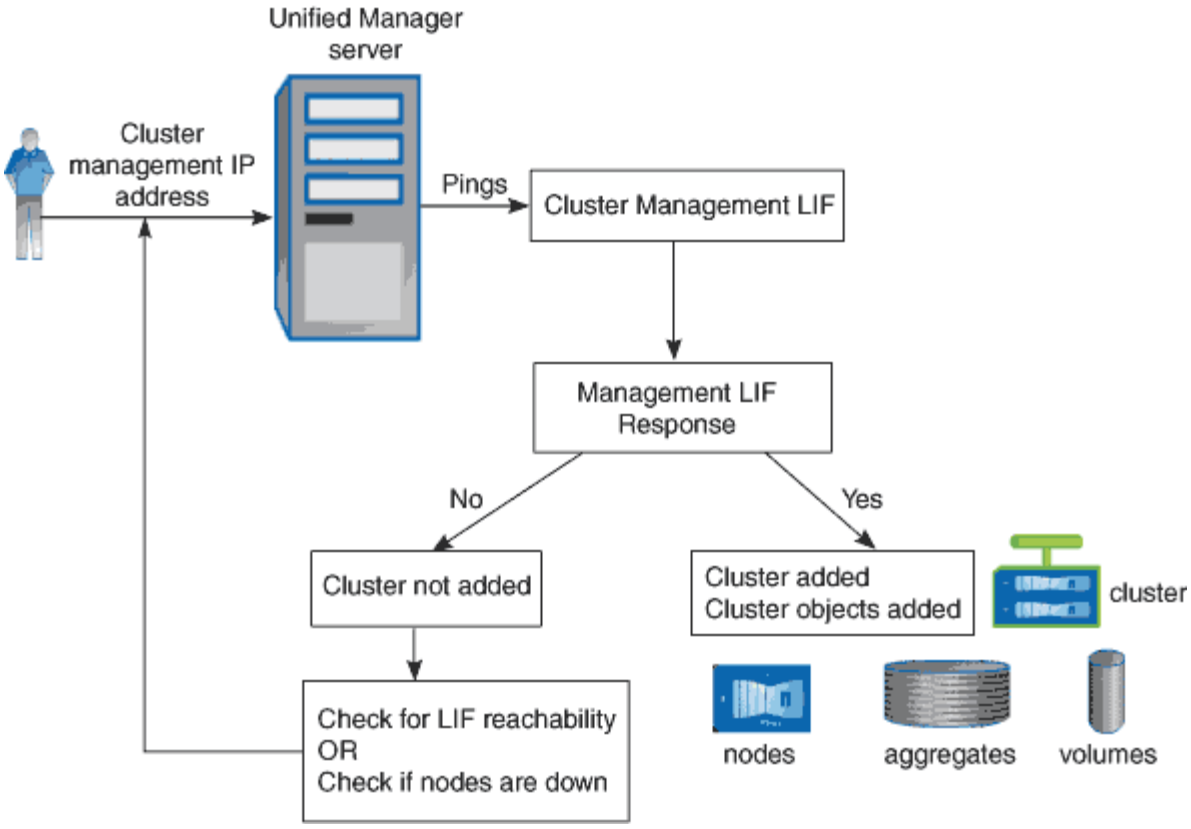
Unified Manager sammelt Cluster-Informationen, speichert die Daten in der Datenbank und analysiert die Daten, um zu prüfen, ob es Cluster-Probleme gibt.

Funktionsweise des Erkennungsvorgangs

Nachdem Sie den Cluster Unified Manager hinzugefügt haben, erkennt der Server die Cluster-Objekte und fügt sie seiner Datenbank hinzu. Wenn Sie verstehen, wie der Erkennungsvorgang funktioniert, können Sie die Cluster und ihre Objekte im Unternehmen managen.

Das Standard-Monitoring-Intervall beträgt 15 Minuten: Wenn Sie zum Unified Manager Server einen Cluster hinzugefügt haben, dauert es 15 Minuten, bis die Cluster-Details in der Benutzeroberfläche von Unified Manager angezeigt werden.

Das folgende Image veranschaulicht den Erkennungsvorgang in OnCommand Unified Manager:



Aktivitäten zur Cluster-Konfiguration und zur Datenerfassung für die Performance

Das Erfassungsintervall für *Cluster-Konfigurationsdaten* beträgt 15 Minuten. Beispielsweise dauert es nach dem Hinzufügen eines Clusters 15 Minuten, bis die Cluster-Details in der UI von Unified Manager angezeigt werden. Dieses Intervall gilt, wenn Sie die Änderungen auch auf einem Cluster vornehmen.

Wenn Sie beispielsweise einer SVM in einem Cluster zwei neue Volumes hinzufügen, werden diese neuen Objekte in der UI nach dem nächsten Abfrageintervall bis zu 15 Minuten angezeigt.

Unified Manager sammelt alle fünf Minuten aktuelle Performance-Statistiken_ von allen überwachten Clustern. Diese Daten werden analysiert, um Performance-Ereignisse und potenzielle Probleme zu identifizieren. Es speichert 30 Tage Verlaufsdaten zu fünf Minuten und 390 Tage historischer Performance-Daten von einer Stunde. So können Sie sehr granulare Performance-Details für den aktuellen Monat und allgemeine Performance-Trends für bis zu ein Jahr anzeigen.

Die Erfassungsumfragen werden um einige Minuten verschoben, sodass Daten aus jedem Cluster nicht gleichzeitig gesendet werden, was die Performance beeinträchtigen kann.

In der folgenden Tabelle werden die Erfassungsaktivitäten beschrieben, die Unified Manager durchführt:

Aktivität	Zeitintervall	Beschreibung
Performance-Statistikabfrage	Alle 5 Minuten	Erfassung von Performance-Daten in Echtzeit von jedem Cluster

Aktivität	Zeitintervall	Beschreibung
Statistische Analyse	Alle 5 Minuten	Nach jeder Statistikabfrage vergleicht Unified Manager die erfassten Daten mit benutzerdefinierten, systemdefinierten und dynamischen Schwellenwerten. Wenn gegen Performance-Schwellenwerte Grenzwerte verstoßen wurde, generiert Unified Manager Ereignisse und sendet E-Mails an die angegebenen Benutzer, sofern hierfür konfiguriert.
Konfigurationsabfrage	Alle 15 Minuten	Erfasst detaillierte Inventarinformationen aus jedem Cluster, um alle Storage-Objekte (Nodes, SVMs, Volumes usw.) zu identifizieren
Zusammenfassung	Jede Stunde	Fasst die letzten 12 fünf-Minuten-Performance-Datensammlungen in einem Durchschnittswert von Stunden zusammen. Die Durchschnittswerte pro Stunde werden in einigen UI-Seiten verwendet und 390 Tage lang aufbewahrt.
Prognoseanalyse und Datenbeschneidung	Jeden Tag nach Mitternacht	Analysiert Cluster-Daten, um dynamische Schwellenwerte für Volume-Latenz und IOPS für die nächsten 24 Stunden festzulegen. Löscht alle fünf-Minuten-Performancedaten, die älter als 30 Tage sind, aus der Datenbank.
Datenbeschnitt	Jeden Tag nach 2 Uhr	Löscht aus der Datenbank alle Ereignisse und dynamischen Schwellenwerte, die älter als 390 Tage sind.
Datenbeschnitt	Jeden Tag nach 3:30 Uhr	Löscht aus der Datenbank alle Leistungsdaten von einer Stunde, die älter als 390 Tage sind.

Was ist ein Data-Continuity-Erfassungszyklus

Durch einen Datenkontinuitätszyklus werden Performancedaten außerhalb des Echtzeit-Zyklus der Cluster-Performance-Erfassung abgerufen, der standardmäßig alle fünf Minuten ausgeführt wird. Datenkontinuitätssammlungen ermöglichen es Unified Manager, Lücken statistischer Daten zu schließen, die auftreten, wenn sie keine Echtzeitdaten erfassen konnten.

Die Datenkontinuitätssammlung wird nur auf Clustern unterstützt, die mit der Software ONTAP Version 8.3.1 oder höher installiert sind.

Unified Manager führt Datenkontinuität-Abfragen der historischen Performance-Daten durch, wenn die folgenden Ereignisse auftreten:

- Dem Unified Manager wird zunächst ein Cluster hinzugefügt.

  Unified Manager sammelt historische Performance-Daten für die letzten 15 Tage. So können Sie einige Stunden nach dem Hinzufügen von Performance-Informationen von zwei Wochen für ein Cluster anzeigen.

  Darüber hinaus werden systemdefinierte Schwellenwertereignisse für den vorherigen Zeitraum gemeldet, sofern vorhanden.

  ⓘ 15 Tage der historischen Volumen-Statistiken werden derzeit nicht gesammelt.

- Der aktuelle Erfassungszyklus für Performance-Daten ist nicht pünktlich abgeschlossen.

  Wenn die Echtzeit-Performance-Umfrage über den fünf-Minuten-Erfassungszeitraum hinausgeht, wird ein Datenkontinuitätssammlungszyklus eingeleitet, um die fehlenden Informationen zu erfassen. Ohne die Datenkontinuitätssammlung wird der nächste Erfassungszeitraum übersprungen.

- Unified Manager war für einen bestimmten Zeitraum nicht zugänglich und dann wieder online, wie in den folgenden Situationen:
  - Es wurde neu gestartet.
  - Sie wurde während eines Software-Upgrades oder beim Erstellen einer Sicherungsdatei heruntergefahren.
  - Ein Netzwerkausfall ist behoben.
- Ein Cluster war für einen Zeitraum nicht zugänglich und dann wieder online, wie in den folgenden Situationen:
  - Ein Netzwerkausfall ist behoben.
  - Eine langsame Wide Area Network-Verbindung verzögerte die normale Erfassung von Performancedaten.

Ein Datenerfassungszyklus kann maximal 24 Stunden historische Daten erfassen. Wenn Unified Manager länger als 24 Stunden ausfällt, wird auf den UI-Seiten eine Lücke in den Performance-Daten angezeigt.

Ein Datenerfassungszyklus und ein Datenerfassungszyklus in Echtzeit können nicht gleichzeitig ausgeführt werden. Der Datenerfassungszyklus muss vor Beginn der Performance-Datenerfassung in Echtzeit abgeschlossen sein. Wenn die Daten-Continuity-Sammlung länger als eine Stunde historische Daten erfasst werden muss, befindet sich oben im Performance Dashboard eine Bannermeldung für den Cluster.

Was bedeutet der Zeitstempel bei erfassten Daten und Ereignissen

Der Zeitstempel, der in den erfassten Systemzustand und Performance-Daten angezeigt wird oder der als Erkennungszeit für ein Ereignis angezeigt wird, basiert auf der ONTAP Cluster-Zeit, die an die im Webbrowser eingestellte Zeitzone angepasst wurde.

Es wird dringend empfohlen, einen NTP-Server (Network Time Protocol) zu verwenden, um die Zeit auf Unified Manager-Servern, ONTAP-Clustern und Webbrowsern zu synchronisieren.

Wenn Zeitstempel, die für ein bestimmtes Cluster nicht korrekt angezeigt werden, möchten Sie möglicherweise überprüfen, ob die Cluster-Zeit ordnungsgemäß festgelegt wurde.

Allgemeines zur Benutzeroberfläche

Die Benutzeroberfläche von Unified Manager besteht hauptsächlich aus einem Dashboard, das einen Überblick über die überwachten Objekte bietet. Über die Benutzeroberfläche können auch alle Cluster-Objekte angezeigt werden.

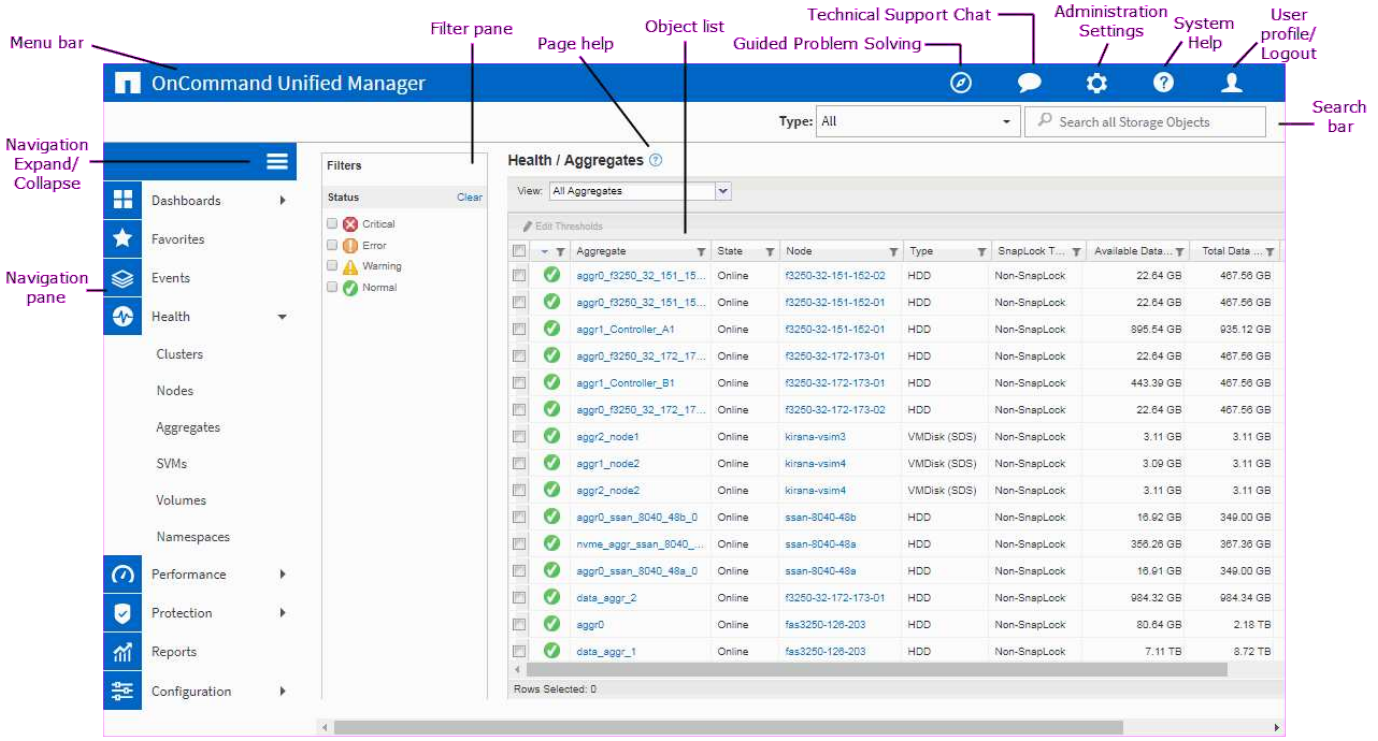
Sie können eine bevorzugte Ansicht auswählen und ggf. die Aktionsschaltflächen verwenden. Ihre Bildschirmkonfiguration wird in einem Arbeitsbereich gespeichert, sodass alle Funktionen verfügbar sind, die Sie benötigen, wenn Sie Unified Manager starten. Wenn Sie jedoch von einer Ansicht zur anderen navigieren und dann zurück navigieren, ist die Ansicht möglicherweise nicht identisch.

Typische Fensterlayouts

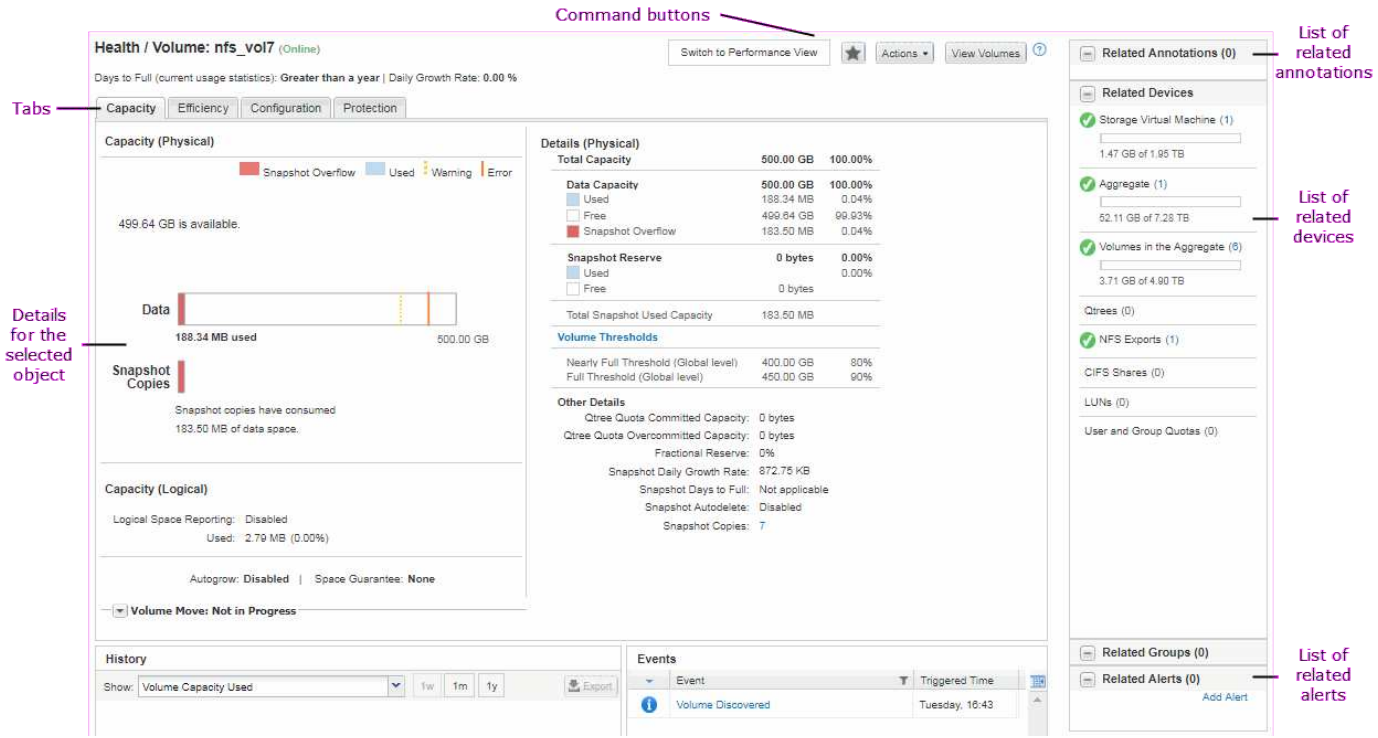
Wenn Sie die typischen Fenster-Layouts kennen, können Sie OnCommand Unified Manager effektiv nutzen. Die meisten Unified Manager-Fenster ähneln einem von zwei allgemeinen Layouts: Objektliste oder Details. Die empfohlene Bildschirmeinstellung beträgt mindestens 1280 x 1024 Pixel.

Nicht jedes Fenster enthält jedes Element in den folgenden Diagrammen.

Layout des Fensters Objektliste



Layout des Fensters „Objektdetails“



Anpassung des Fensterlayouts

OnCommand Unified Manager ermöglicht Ihnen das Anpassen des Layouts für Informationen auf den Storage-Objektseiten. 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) Erscheint für diese Spalte.

- **Filterung**

  Sie können Filter anwenden, um die Anzeige der Informationen auf den Speicherobjektseiten anzupassen, sodass nur Einträge angezeigt werden, die den angegebenen Bedingungen entsprechen. Sie können Filter entweder im Fensterbereich Filter oder in den Spalten anwenden.

  Im Bereich Filter können Sie anhand der ausgewählten Optionen einige Spalten filtern. Auf der Seite „Systemzustand/Volumen-Inventar“ können Sie beispielsweise im Fensterbereich „Filter“ nur die Spalten „Status“ und „Status“ filtern. Um alle Volumes anzuzeigen, die offline sind, können Sie die entsprechende Filteroption unter Status auswählen.

  Alternativ können Sie Filter für Spalten mithilfe des Filtersymbols (festlegen). Sie können dann den Platzhalter-Zeichenfilter (?) verwenden. Oder Platzhalter-String-Filter (*), um Ihre Suche einzugrenzen. Beispielsweise können Sie auf der Seite „Systemzustand/Volumes-Inventar“ unter Verwendung des Stringfilters in der Spalte „Volume“ nach einem Volume von vol234 suchen. Sie können eingeben `*vol`, Und alle Volumen mit Namen mit “vol” sind aufgelistet. Sie können eingeben `vol?` Um die Liste aller Volumes mit dem Namen anzuzeigen, der „`vol`“ enthält, gefolgt von einem weiteren Zeichen, z. B. vol1 oder vol2. Sie können eingeben `vol` Liste aller Volumes mit Namen anzeigen, die mit „`vol`“ beginnen

  Kapazitätsbezogene Spalten in jeder Liste zeigen immer Kapazitätsdaten in entsprechenden Einheiten an, abgerundet auf zwei Dezimalstellen. Dies gilt auch beim Filtern von Kapazitätspalten. Beispiel: Wenn Sie den Filter in der Spalte „Gesamtkapazität Daten“ auf der Seite „Inventar/Aggregate“ verwenden, um Daten größer als 20.45 GB zu filtern, wird die tatsächliche Kapazität von 20.454 GB als 20.45 GB angezeigt. Ebenso wird bei Filtern von Daten unter 20.45 GB die tatsächliche Kapazität von 20.449 GB als 20.45 GB angezeigt.

  Wenn Sie den Filter in der Spalte Available Data % auf der Seite „Health/Aggregates Inventory“ verwenden, um Daten von mehr als 20.45 % zu filtern, wird die tatsächliche Kapazität von 20.454 % als 20.45 % angezeigt. Gleiches gilt, wenn Sie Daten weniger als 20.45% filtern, wird die tatsächliche Kapazität von 20.449% als 20.45% angezeigt. Für Spalten, die Kapazitätsdaten in Prozent anzeigen, können Sie Werte bis zu vier Dezimalstellen anzeigen, indem Sie den Mauszeiger über den Wert bewegen, der in der Spalte angezeigt wird.

- **Ausblenden oder Neuanzeigen der Spalten**

  Sie können auf das Spaltenanzeigesymbol klicken ( ) Um auszuwählen, welche Spalten angezeigt werden sollen.

- **Daten exportieren**

  Sie können auf das Exportsymbol klicken ( ) Zum Exportieren von Daten in kommagetrennte Werte (`.csv`) Datei und verwenden Sie die exportierten Daten, um Berichte zu erstellen.

Verwenden der Unified Manager-Hilfe

Die Hilfe enthält Informationen zu allen in OnCommand Unified Manager enthaltenen Funktionen. Über das Inhaltsverzeichnis, den Index oder das Suchtool finden Sie

Informationen zu den Funktionen und deren Verwendung.

Über diese Aufgabe

Die Hilfe ist über die einzelnen Registerkarten und über die Menüleiste der Benutzeroberfläche von Unified Manager verfügbar.

Das Suchtool in der Hilfe funktioniert nicht für Teilwörter.

Wahlmöglichkeiten

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

  Weitere Informationen finden Sie, indem Sie einen beliebigen Teil des Inhaltsverzeichnisses im Navigationsbereich erweitern.

- Um den Inhalt der Hilfe zu durchsuchen, klicken Sie im Navigationsbereich auf die Registerkarte **Suchen**, geben Sie das Wort oder die Wortreihe ein, die Sie finden möchten, und klicken Sie auf **Go!**
- Um Hilfethemen zu drucken, klicken Sie auf das Druckersymbol.

Lesezeichen für Ihre bevorzugten Hilfethemen

Auf der Registerkarte „Hilfe-Favoriten“ können Sie häufig verwendete Hilfethemen als Lesezeichen hinzufügen. Hilfe-Lesezeichen ermöglichen den schnellen Zugriff auf Ihre bevorzugten Themen.

Schritte

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

Exportieren von Daten in CSV-Dateien zur Berichterstellung

Sie können Daten in kommagetrennte Werte exportieren (`.csv`) Datei, und verwenden Sie die exportierten Daten, um Berichte zu erstellen. Wenn z. B. 10 kritische Ereignisse nicht behoben wurden, können Sie die Daten von der Seite „Ereignisinventar“ exportieren, um einen Bericht zu erstellen, und anschließend entsprechende Maßnahmen ergreifen.

Bevor Sie beginnen

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

Über diese Aufgabe

Sie können Daten in ein exportieren `.csv` Datei auf den Seiten mit den Gesundheits- und Leistungsbeständen und auf der Seite mit dem Ereignisbestand.

Die Exportfunktion wird für die Komponenten eines Infinite Volume nicht unterstützt – Details der Komponenten

können nicht in ein exportiert werden `.csv` Datei:

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Exportieren…	Tun Sie das…
Veranstaltungsdetails	Klicken Sie Auf **Events**.
Details zum Storage-Objektbestand	Klicken Sie im linken Navigationsmenü auf **Health** oder **Performance** und wählen Sie dann ein Speicherobjekt aus.
Details zur Storage-Kapazität und zum Sicherungsverlauf	Klicken Sie auf **Gesundheit** > **Aggregate** oder **Gesundheit** > **Volumes** und wählen Sie dann ein einzelnes Aggregat oder Volume aus.
Qtree oder NFS exportiert Informationen für eine SVM	Klicken Sie auf **Health** > **SVMs**, wählen Sie eine einzelne SVM aus und wählen Sie dann die Registerkarte **Qtrees** oder **NFS Exports** aus.
Storage Objekt: Top 10 Performance-Details	Klicken Sie auf **Performance** > **Cluster**, wählen Sie dann einen Cluster aus und wählen Sie die Registerkarte **Top Performers** aus. Wählen Sie dann ein Storage-Objekt und einen Performance-Zähler aus.

2. Klicken Sie auf die Schaltfläche **Exportieren**.
3. Klicken Sie auf **in CSV exportieren**, um die Exportanforderung zu bestätigen.

   Über die Registerkarte „Top Performers“ und auf der Detailseite zu SVMs können Sie auswählen, einen Bericht mit den Statistiken für den einzelnen Cluster, den Sie anzeigen, oder für alle Cluster im Datacenter herunterzuladen.

   Die Datei wird heruntergeladen.

4. Öffnen Sie das `.csv` Datei in der entsprechenden Anwendung.

Suche nach Speicherobjekten

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

Bevor Sie beginnen

- Sie müssen eine der folgenden Rollen haben, um diese Aufgabe auszuführen: Operator, OnCommand

Administrator oder Storage Administrator.

- Eine gültige Suche muss mindestens drei Zeichen enthalten.

Über diese Aufgabe

Bei Verwendung des Dropdown-Menüwerts Typ „`All`“ zeigt die globale Suche die Gesamtzahl der Ergebnisse aller Objektkategorien an; für jede Objektkategorie sind maximal 25 Suchergebnisse verfügbar. Sie können einen bestimmten Objekttyp aus dem Dropdown-Menü Typ auswählen, um die Suche innerhalb eines bestimmten Objekttyps zu verfeinern. In diesem Fall ist die zurückgegebene Liste nicht auf die Top 25-Objekte beschränkt.

Die folgenden Objekttypen können gesucht werden:

- Cluster
- Knoten
- SVMs
- Aggregate
- Volumes
- Qtrees
- CIFS-Freigaben
- Benutzer- oder Gruppenkontingente
- LUNs
- NVMe Namespaces
- Initiatorgruppen
- Initiatoren

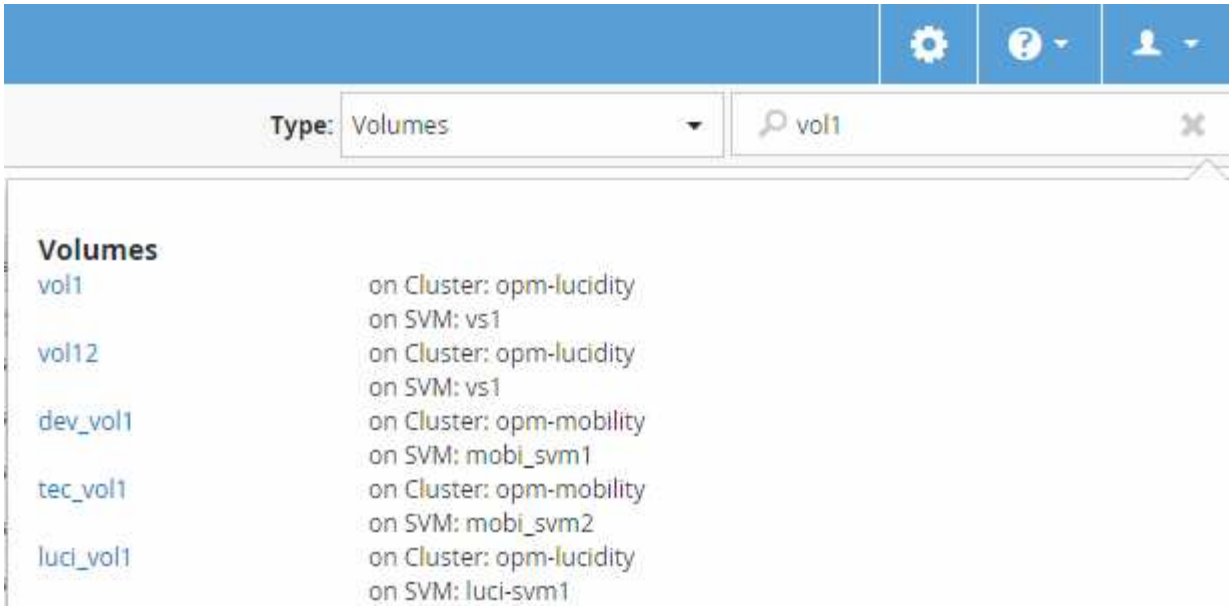
Sie können auf ein beliebiges Objekt in den Suchergebnissen klicken, um zur Seite Gesundheitsdetails für das Objekt zu navigieren. Wenn für ein Objekt keine direkte Integritätsseite vorhanden ist, wird die Seite Systemzustand des übergeordneten Objekts angezeigt. Beispiel: Bei der Suche nach einer bestimmten LUN wird die Seite „SVM Details“ angezeigt, auf der sich die LUN befindet.

In der globalen Suchleiste sind die Ports nicht durchsuchbar.

Schritte

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

   In diesem Beispiel wurde im Dropdown-Feld **Typ** 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.



Filtern des Seiteninhalts zur Leistungsbestandsbestandsliste

Sie können Leistungsbestandsdaten in Unified Manager filtern, um Daten anhand bestimmter Kriterien schnell zu finden. Mithilfe der Filterung können Sie den Inhalt der Seiten von Unified Manager einschränken, um nur die für Sie jeweils interessierten Ergebnisse anzuzeigen. Dies bietet eine sehr effiziente Methode, nur die Leistungsdaten anzuzeigen, an denen Sie interessiert sind.

Über diese Aufgabe

Verwenden Sie **Filterung**, um die Rasteransicht entsprechend Ihren Einstellungen anzupassen. Die verfügbaren Filteroptionen basieren auf dem Objekttyp, der im Raster angezeigt wird. Wenn aktuell Filter angewendet werden, wird links neben dem Filtersteuerelement ein Sternchen (*) angezeigt.

Es werden vier Filterparameter unterstützt.

Parameter	Validierung
Zeichenfolge (Text)	Die Operatoren sind **enthält** und **beginnt mit**.
Nummer	Die Betreiber sind **größer als** und **kleiner als**.
Ressource	Die Operatoren sind **Name enthält** und **Name beginnt mit**.
Status	Die Betreiber sind **ist** und **ist nicht**.

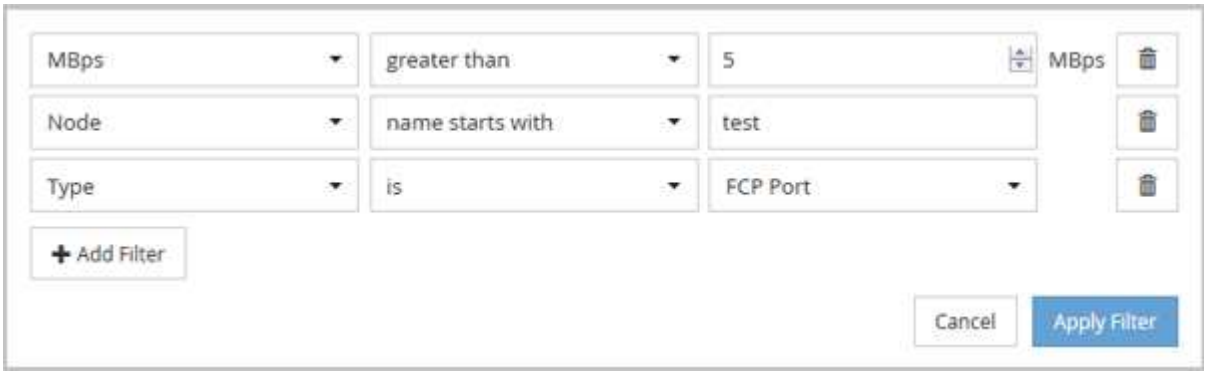
Für jeden Filter sind alle drei Felder erforderlich; die verfügbaren Filter spiegeln die filterbaren Spalten auf der aktuellen Seite wider. Es können maximal vier Filter angewendet werden. Gefilterte Ergebnisse basieren auf kombinierten Filterparametern. Gefilterte Ergebnisse gelten für alle Seiten in Ihrer gefilterten Suche und nicht nur für die aktuell angezeigte Seite.

Sie können Filter über das Filterfenster hinzufügen.

1. Klicken Sie oben auf der Seite auf **Filtern**. Das Filterbedienfeld wird angezeigt.
2. Klicken Sie im Filterfenster auf die linke Dropdown-Liste und wählen Sie einen Objektnamen aus, z. B. *Cluster* oder einen Performance-Zähler.
3. Klicken Sie auf die Dropdown-Liste Mitte, und wählen Sie den booleschen Operator **Name enthält** oder **Name beginnt mit** aus, wenn die erste Auswahl ein Objektname war. Wenn es sich bei der ersten Auswahl um einen Leistungszähler handelte, wählen Sie **größer als** oder **kleiner als** aus. Wenn die erste Auswahl **Status** war, wählen Sie **ist** oder **ist nicht**.
4. Wenn für Ihre Suchkriterien ein numerischer Wert erforderlich ist, werden die nach-oben- und nach-unten-Pfeiltasten im Feld rechts angezeigt. Sie können auf die nach-oben- und nach-unten-Pfeiltasten klicken, um den gewünschten numerischen Wert anzuzeigen.
5. Geben Sie bei Bedarf Ihre nicht-numerischen Suchkriterien in das Textfeld rechts ein.
6. Um Filter hinzuzufügen, klicken Sie auf **Filter hinzufügen**. Es wird ein zusätzliches Filterfeld angezeigt. Führen Sie diesen Filter mithilfe des in den vorherigen Schritten beschriebenen Verfahrens aus. Beachten Sie, dass beim Hinzufügen Ihres vierten Filters die Schaltfläche **Filter hinzufügen** nicht mehr angezeigt wird.
7. Klicken Sie Auf **Filter Anwenden**. Die Filteroptionen werden auf das Raster angewendet, und ein Sternchen (*) wird in der Filterschaltfläche angezeigt.
8. Verwenden Sie den Filterbereich, um einzelne Filter zu entfernen, indem Sie auf das Papierkorb-Symbol rechts neben dem zu entfernenden Filter klicken.
9. Um alle Filter zu entfernen, klicken Sie unten im Filterfenster auf **Zurücksetzen**.

Beispiel für die Filterung

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



Nachdem Sie auf **Filter anwenden** geklickt haben, wird das Filterfenster geschlossen und wendet Ihre Filter an.

Zugriff auf OnCommand System Manager über die Unified Manager Schnittstelle

Wenn für die Fehlerbehebung Konfigurationsänderungen an einem Cluster erforderlich sind, können Sie die grafische Schnittstelle von System Manager anstelle der ONTAP Befehlszeilenschnittstelle verwenden. System Manager ist als Webservice in ONTAP enthalten, ist standardmäßig aktiviert und kann über einen Browser aufgerufen werden.

Bevor Sie beginnen

Sie müssen ein mit dem konfiguriertes Cluster-Benutzerkonto besitzen `admin` Rolle und der `http`, `ontapi`, und `console` Applikationstypen

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboards** > **Clusteransicht**.
2. Wählen Sie auf der Seite **Dashboards/Clusteransicht** den Cluster aus, den Sie verwalten möchten.

   Ein Überblick über den Monitoring-Status, die Kapazität und die Performance des Clusters wird angezeigt.

3. Klicken Sie auf das Symbol **System Manager**.

   Wenn das Cluster ein selbstsigniertes digitales Zertifikat verwendet, wird im Browser möglicherweise eine Warnung angezeigt, dass das Zertifikat nicht vertrauenswürdig ist. Sie können entweder das Risiko bestätigen, den Zugriff fortzusetzen, oder ein von der Zertifizierungsstelle signiertes digitales Zertifikat auf dem Cluster zur Server-Authentifizierung installieren.

4. Melden Sie sich mit den Anmeldedaten des Cluster-Administrators bei System Manager an.

   Wenn die Anmeldung bei der System Manager-Benutzeroberfläche mit SAML-Authentifizierung geschützt ist, geben Sie Ihre Anmeldedaten anstelle der System Manager-Anmeldeseite auf der Anmeldeseite des Identitäts-Providers (IdP) ein.

Monitoring des Clusterzustands und der Performance über die Dashboards

Die Dashboards bieten kumulative Details über den Systemzustand. Mit den Dashboards können Sie die Verfügbarkeit, Kapazität, Performance und den Sicherungsstatus der gemanagten Cluster insgesamt beurteilen und schnell sämtliche eventuell auftretenden Probleme bemerken, lokalisieren, diagnostizieren oder zuweisen.

Drei Dashboards bieten einen einzigartigen Blick auf Zustand und Performance Ihrer Cluster:

- Die Seite Dashboards/Überblick enthält Informationen über Zustand und Performance Ihrer Speicherobjekte.
- Die Seite Dashboards/Leistung bietet einen allgemeinen Leistungsstatus aller zu überwachenden Cluster.
- Die Seite Dashboards/Cluster-Ansicht enthält Informationen zu einzelnen Clustern.

Allgemeines zum Dashboard mit der Gesundheitsübersicht

Das Unified Manager Health Overview Dashboard bietet zusammenfassende Informationen über den Zustand Ihres Storage und Ihrer virtualisierten Umgebung. Die Seite Dashboards/Überblick enthält Systemzustandsinformationen über Storage-Objekte, die in vier Systemkategorien unterteilt sind: Verfügbarkeit, Kapazität, Performance und Sicherung der Storage-Objekte.

Das folgende Bild zeigt die Fensterbereiche, die auf der Seite Dashboards/Übersicht angezeigt werden:

Gesundheitsüberblick

Zeigt als Diagramm Informationen zum Systemzustand Ihrer Storage-Objekte wie Cluster, Aggregate, Storage Virtual Machines (SVMs) und den Zustand der Sicherungsbeziehungen an. Auf der Seite Dashboards/Übersicht werden Ereignisse angezeigt, die für die folgenden Kategorien generiert wurden:

Wenn Sie auf die Zahl über einer der gelben oder roten Balkendiagramme klicken, wird die Seite „Ereignisinventar“ angezeigt, auf der nur diese Ereignisse enthalten sind. Durch Klicken auf die Zahl unterhalb einer der Diagramme wird die Seite „Objektbestand“ mit nur diesen Objekten angezeigt.

- **Verfügbarkeit**

  Zeigt Informationen zur Verfügbarkeit von Clustern, SVMs und Aggregaten an, die von Unified Manager überwacht werden Basierend auf den generierten verfügbarkeitsbezogenen Ereignissen werden die Storage-Objekte als stabil, risikobehaftete oder Zwischenfälle kategorisiert.

- * Kapazität*

  Zeigt Informationen zur Kapazität der SVMs und Aggregate an, die von Unified Manager überwacht werden. Auf der Grundlage der generierten kapazitätsbezogenen Ereignisse werden die Storage-Objekte als gesund, risikobehaftete oder mit Zwischenfällen kategorisiert.

- **Leistung**

  Zeigt Informationen zur Performance von Clustern, SVMs und Volumes an, die von Unified Manager überwacht werden Die Storage-Objekte werden basierend auf den erzeugten Performance-bezogenen Zwischenfällen als ordnungsgemäß, risikobehaftete oder mit Incidents kategorisiert.

- **Schutz**

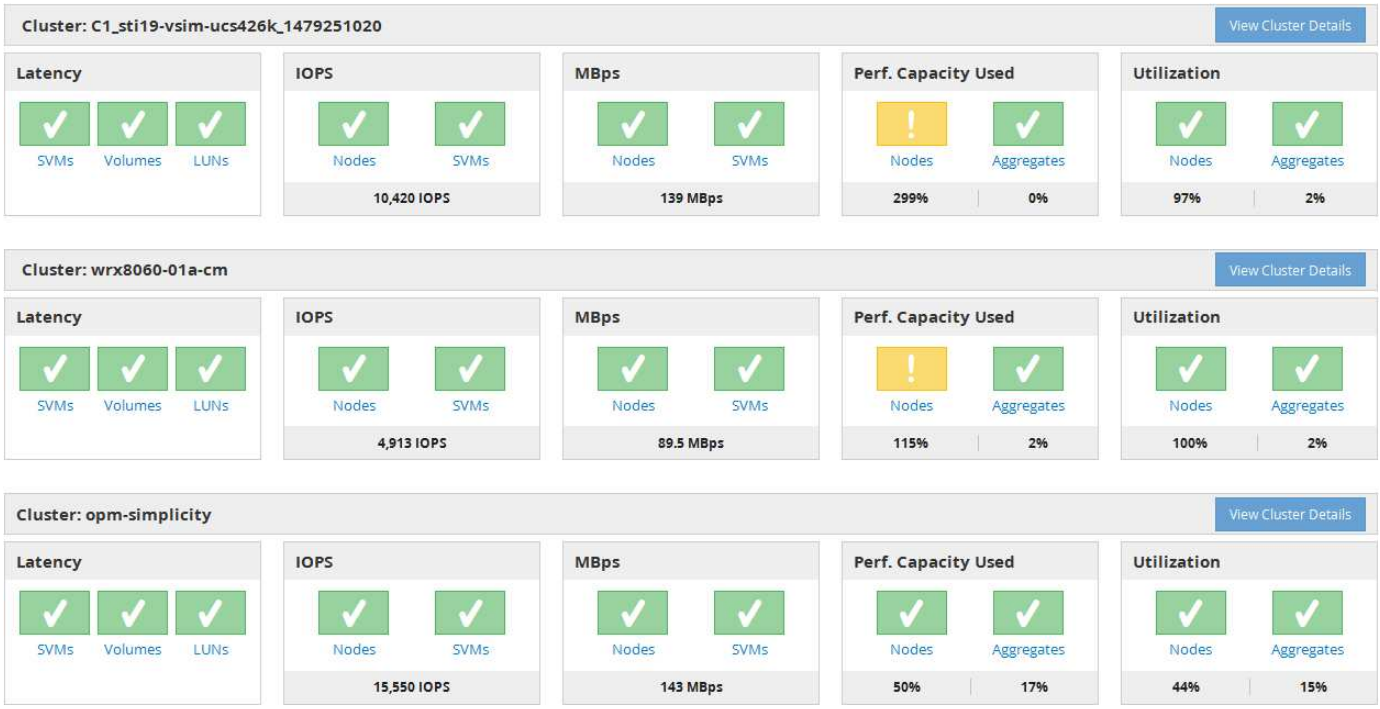
  Zeigt Informationen zu Sicherungsbeziehungen an, die von Unified Manager überwacht werden. Basierend

auf den durch den Schutz bedingten Ereignissen, die erzeugt werden, werden die Schutzbeziehungen als gesund, Warnung oder Fehler kategorisiert.

Allgemeines zum Performance-Dashboard

Das Unified Manager Performance Dashboard bietet einen allgemeinen Überblick über den Performance-Status aller Cluster, die in Ihrer Umgebung überwacht werden. Cluster, die Performance-Probleme haben, werden oben auf der Seite nach Schweregrad geordnet. Die Informationen auf dem Dashboard werden automatisch zu jedem fünf-Minuten-Zeitraum der Performance-Erfassung aktualisiert.

Das folgende Bild zeigt ein Beispiel eines Unified Manager Performance-Dashboards für die Überwachung von zwei Clustern:



Die Statussymbole, die die Storage-Objekte darstellen, können den folgenden Status aufweisen und vom höchsten Schweregrad bis den niedrigsten Schweregrad sortiert sein:

- Kritisch (): Ein oder mehrere neue kritische Performanceereignisse wurden für das Objekt gemeldet.
- Warnung (): Für das Objekt wurden mindestens ein neues Warnungsleistungsereignis gemeldet.
- Normal (): Für das Objekt wurden keine neuen Performanceereignisse gemeldet.

Die Farbe gibt an, ob neue Ereignisse für das Objekt vorhanden sind. Ereignisse, die nicht mehr aktiv sind, die als veraltete Ereignisse bezeichnet werden, haben keinen Einfluss auf die Farbe des Symbols.

Cluster-Performance-Zähler

Für jedes Cluster werden die folgenden Performance-Kategorien angezeigt:

- Latenz

Zeigt, wie schnell das Cluster auf Client-Applikationsanforderungen reagiert, in Millisekunden pro Vorgang.

- IOPS

  Zeigt die Betriebsgeschwindigkeit des Clusters unter der Anzahl der ein-/Ausgabevorgänge pro Sekunde an.

- MB/Sek.

  Zeigt an, wie viele Daten in das und aus dem Cluster in Megabyte pro Sekunde übertragen werden.

- Verwendete Performance-Kapazität

  Zeigt, ob Nodes oder Aggregate die verfügbare Performance-Kapazität überbeanspruchen.

- Auslastung

  Zeigt, ob die Ressourcen auf beliebigen Nodes oder Aggregaten überlastet sind.

Um die Performance Ihres Clusters und Ihrer Storage-Objekte zu analysieren, können Sie eine der folgenden Aktionen durchführen:

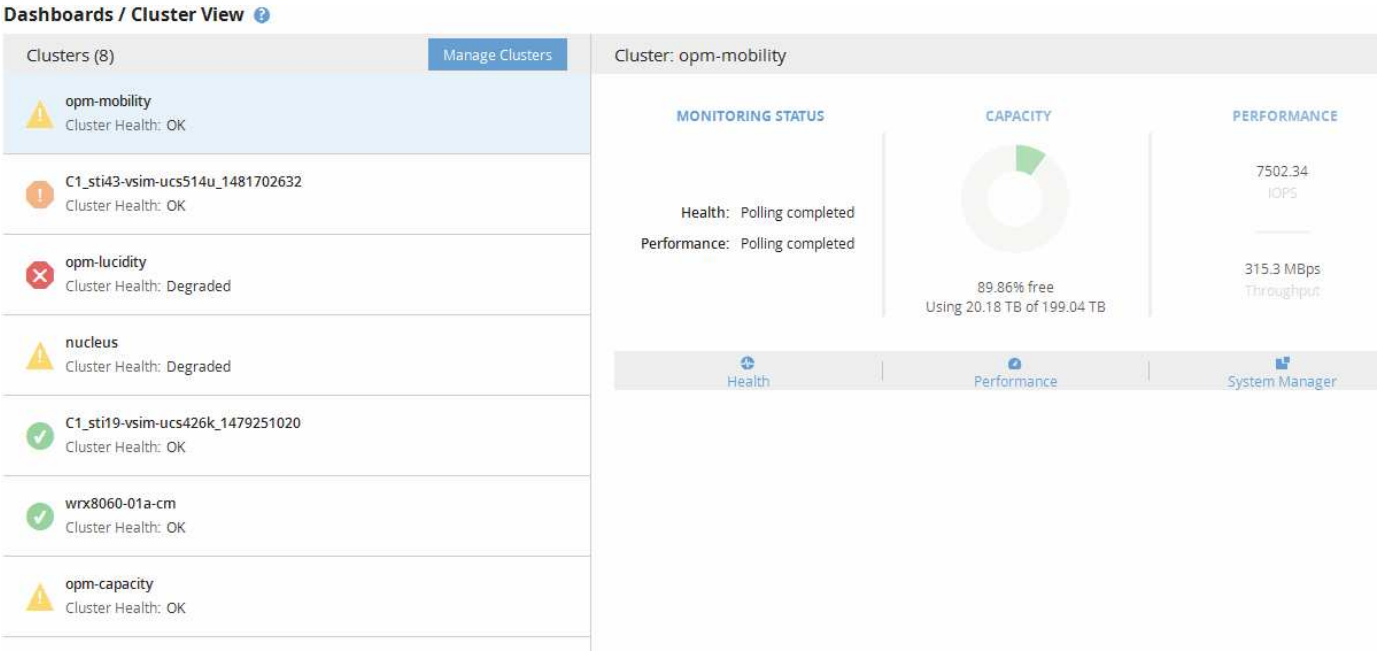
- Sie können auf **Cluster-Details anzeigen** klicken, um die Cluster-Startseite anzuzeigen. Dort werden detaillierte Performance- und Ereignisinformationen für die ausgewählten Cluster- und Speicherobjekte angezeigt.
- Sie können auf eines der roten oder gelben Statussymbole eines Objekts klicken, um die Inventarseite für dieses Objekt anzuzeigen. Dort können Sie Details zum Speicherobjekt anzeigen.

  Beispielsweise wird durch Klicken auf ein Volume-Symbol die Seite „Performance/Volume-Inventar“ mit einer Liste aller Volumes im ausgewählten Cluster angezeigt, die nach der schlechtesten Performance bis zur besten Performance sortiert ist.

Allgemeines zum Dashboard der Cluster-Ansicht

Das Unified ManagerCluster View Overview Dashboard liefert allgemeine Informationen über den Zustand der zu verwaltenden Cluster. Das Dashboard der Clusteransicht besteht aus zwei Hauptbereichen: Verwalteten Clustern (links) und Clusterdetails (rechts).

Das folgende Bild zeigt ein Beispiel eines Unified ManagerCluster View Dashboards für die Überwachung von acht Clustern:



Das Statussymbol neben den einzelnen Cluster-Namen kann in den folgenden Status enthalten sein:

- Kritisch ( ): Ein oder mehrere aktive kritische Ereignisse wurden für den Cluster gemeldet.
- Fehler ( ): Ein oder mehrere aktive Fehlerereignisse wurden für den Cluster gemeldet.
- Warnung ( ): Ein oder mehrere aktive Warnereignisse wurden für den Cluster gemeldet.
- Normal ( ): Für den Cluster wurden keine aktiven Ereignisse gemeldet.

Die Farbe gibt an, ob aktive (neue oder bestätigte) Ereignisse für das Objekt vorhanden sind. Ereignisse, die nicht mehr aktiv sind, die als veraltete Ereignisse bezeichnet werden, haben keinen Einfluss auf die Farbe des Symbols.

Um zusätzliche Informationen über ein Cluster anzuzeigen, können Sie eine der folgenden Aktionen durchführen:

- Sie können auf einen Cluster-Namen klicken, um Überblicksinformationen zu Monitoring-Status, Kapazitätsstatus und Performance-Status des Clusters anzuzeigen.
- Sie können auf **Cluster verwalten** klicken, um die Seite Configuration/Cluster Data Sources anzuzeigen, auf der Sie detaillierte Statusinformationen für alle Cluster anzeigen können, die von dieser Instanz von Unified Manager verwaltet werden.

Beschreibung der Dashboard-Fenster

Über die Dashboard-Seiten können Sie einen schnellen Überblick über die überwachten Objekte erhalten.

Dashboards/Übersichtsseite

Die Seite Dashboards/Überblick wird als Diagramm den Zustand von Storage-Objekten wie Clustern, Aggregaten und Storage Virtual Machines (SVMs) angezeigt. Basierend auf den generierten Ereignissen für Verfügbarkeit, Kapazität, Performance und Sicherung werden diese Storage-Objekte als ordnungsgemäß, risikolos oder als „stabil“, „Warnung“

oder „Fehler“ für schutzbezogene Ereignisse kategorisiert.

Der Balken für den Cluster ist nicht erreichbar

Wenn ein Cluster nicht erreichbar ist, zeigt Unified Manager die Details in einer Leiste oben auf jeder Seite an. Wenn alle Cluster erreichbar sind, ist dieses Fenster ausgeblendet.

Sie können die im Fenster angezeigten Informationen durch Drücken von F5 aktualisieren. Durch diese Aktion wird sichergestellt, dass im Teilfenster die neuesten Informationen über Cluster angezeigt werden, die derzeit nicht erreichbar sind. Wenn beispielsweise ein Cluster mit einem nicht zugänglichen Cluster entfernt wird oder wenn der Status eines Ereignisses veraltet ist, werden Informationen über das Ereignis entfernt, wenn Sie das Teilfenster aktualisieren.

Sie können detaillierte Informationen über ein Cluster anzeigen, das nicht erreichbar ist, indem Sie auf die Schaltfläche **Details** klicken. Durch diese Aktion wird die Seite „Ereignisinventar“ geöffnet. Nach dem Schließen der Leiste wird diese nur noch angezeigt, wenn Sie sich wieder bei Unified Manager anmelden.

Übersichtsbereich

- **Verfügbarkeitsfenster**

  Zeigt Informationen zur Verfügbarkeit von Clustern, Aggregaten und SVMs an, die von Unified Manager überwacht werden Die Speicherobjekte werden als gesund, gefährdet oder Vorfälle eingestuft. So wird beispielsweise der Status eines Clusters ohne freie Festplatten als gefährdet angezeigt.

  In diesem Fenster wird auch die Anzahl der Speicherobjekte in den einzelnen Kategorien angezeigt. Wenn Sie auf einen der Gesamtwerte des Objekts klicken, gelangen Sie zur Seite für dieses Objekt. Beispielsweise wird Sie durch Klicken auf die Registerkarte „Cluster total“ auf die Seite „Systemzustand/Cluster Inventar“ angezeigt. Wenn Sie oben in einer Spalte auf die Zahlen klicken, gelangen Sie zur Seite „Ereignisinventar“.

- **Kapazitätsbereich**

  Zeigt Informationen zur Kapazität von Aggregaten und SVMs an, die von Unified Manager überwacht werden. Die Speicherobjekte werden als gesund, gefährdet oder Vorfälle eingestuft. So wird beispielsweise der Status eines Aggregats angezeigt, dessen genutzte Kapazität den vollen Schwellenwert erreicht hat.

  In diesem Fenster wird auch die Anzahl der Speicherobjekte in den einzelnen Kategorien angezeigt.

- **Performance-Fenster**

  Zeigt Informationen zur Performance von Clustern, SVMs und Volumes an, die von Unified Manager überwacht werden Die Storage-Objekte werden basierend auf den erzeugten Performance-bezogenen Zwischenfällen als ordnungsgemäß, risikobehaftete oder mit Incidents kategorisiert. Beispielsweise wird der Status eines Volumes angezeigt, dessen I/O-Reaktionszeit auf seinen Workload den maximalen Schwellenwert erreicht hat, als Vorfälle auftreten.

  In diesem Teilfenster werden außerdem die Gesamtzahl der Cluster, SVMs und Volumes angezeigt, die von Unified Manager überwacht werden. Wenn Sie auf einen der Gesamtwerte des Objekts klicken, gelangen Sie zur Seite für dieses Objekt. Beispielsweise führt Sie ein Klicken auf die Cluster-Gesamtansicht zur Seite „Performance/Cluster Inventory“.

- **Schutzbereich**

  Zeigt Informationen zu Sicherungsbeziehungen an, die von Unified Manager überwacht werden. Die

Schutzbeziehungen werden als „gesund“, „Warnung“ oder „Fehler“ kategorisiert. Beispielsweise wird eine Beziehung mit einer Verzögerungsdauer angezeigt, die den lag-Warnschwellenwert überschreitet, als Warnung.

In diesem Teilfenster wird außerdem die Gesamtzahl der Storage-Objekte in den einzelnen Sicherungskategorien angezeigt. Wenn Sie auf die Links für die Kategorien „Lag Status“, „Asynchronous Vault“, „Asynchronous Mirror“ oder „Synchronous“ klicken, gelangen Sie zu einer gefilterten Liste dieser Objekte auf der Seite „Protection/Volume Relationships“.

Dashboards/Seite zur Performance

Mithilfe des Unified Manager Performance Dashboard können Sie den allgemeinen Performance-Status aller zu überwachenden Cluster anzeigen. Auf der Seite Dashboards/Performance wird auch eine Bannermeldung angezeigt, wenn Unified Manager nicht mit einem Cluster kommunizieren kann, das überwacht wird.

Überblick

Die Cluster werden nach dem Schweregrad mithilfe der folgenden Kriterien geordnet:

1. Wenn ein Cluster nicht erreichbar ist.
2. Wenn ein Cluster mindestens ein aktives, kritisches Performance-Ereignis aufweist (rotes Objektsymbol)
3. Wenn ein Cluster über ein oder mehrere aktive Warn-Performance-Ereignisse verfügt (gelbes Objektsymbol).
4. Wenn Cluster keine aktiven Performance-Ereignisse aufweisen (grünes Objektsymbol): Die Cluster sind nach den höchsten IOPS sortiert.

Kritische Ereignisse werden generiert, wenn ein kritisches Limit in einer benutzerdefinierten Performance-Schwellenwertrichtlinie überschritten wird. Warnereignisse werden gesendet, wenn ein Warnlimit in einer benutzerdefinierten Performance-Schwellenwertrichtlinie überschritten wird oder eine systemdefinierte Schwellenwertrichtlinie oder ein dynamischer Schwellenwert überschritten wird.

Die Sortierreihenfolge wird durch die Gesamtzahl der aktiven (neuen oder bestätigten) Ereignisse bestimmt, nicht durch die Anzahl der Objekte, die Ereignisse aufweisen. Wenn beispielsweise Cluster A sieben kritische Ereignisse bei der Volume-Latenz hat, Und Cluster B weist zwei kritische Ereignisse bei Volume-Latenz und zwei kritische Node-IOPS-Ereignisse (insgesamt vier kritische Ereignisse) auf. Cluster A (mit einem roten Objektsymbol) erscheint oben in der Liste, obwohl Cluster B über zwei rote Objektsymbole verfügt.

Für jedes Cluster werden die folgenden häufig überwachten Ereignistypen angezeigt:

- Latenzereignisse für Storage Virtual Machines (SVMs), Volumes und LUNs
- IOPS-Ereignisse für Nodes und SVMs
- MB/s-Ereignisse für Nodes und SVMs
- Verwendete Performance-Kapazität Ereignisse für Nodes und Aggregate
- Auslastungsereignisse für Nodes und Aggregate

Unified Manager kann Performance-Ereignisse für andere Storage-Objekte und Zähler empfangen, z. B. MB/s-Ereignisse für Aggregate und IOPS-Ereignisse für Volumes. Wenn ein Cluster diese Ereignistypen aufweist, zeigt das Symbol neben dem Cluster-Namen ein Warnungs- (gelbes) oder kritisches (rotes) Ereignis an.

Dieses Symbol kann bedeuten, dass Ereignisse vorhanden sind, wenn keine der fünf Zählerfeldanzeichen gelb oder rot sind, da diese Ereignistypen nicht in die vorhandenen Kategorien des Zählerfelds passen.

Sie können auf das Objektsymbol klicken, um die Seite „Performance Inventory“ für das Objekt anzuzeigen. Dort können Sie alle Objekte des entsprechenden Typs in diesem Cluster anzeigen. Wenn Sie beispielsweise auf ein Volume-Symbol klicken, wird die Seite „Performance/Volume Inventory“ angezeigt. Hier werden eine Liste aller Volumes im ausgewählten Cluster angezeigt, die nach der schlechtesten bis optimalen Performance sortiert sind.

Performance-Zähler

Für jedes Cluster sind fünf Performance-Zähler vorhanden, die jeweils in einem separaten Panel angezeigt werden. Diese Informationen werden nach jeder fünfminütigen Erfassungszeit automatisch aktualisiert:

Zähler	Beschreibung
Latenz	Zeigt an, wie schnell das Cluster auf Client-Applikationsanforderungen reagiert, in Millisekunden pro Vorgang (ms/op).der Symbolbereich gibt an, ob SVMs, Volumes oder LUNs aktive Ereignisse aufweisen, basierend auf dem Latenzwert, der eine Schwellenwerteinstellung überschreitet.
IOPS	Zeigt die Betriebsgeschwindigkeit des Storage-Systems unter der Anzahl der ein-/Ausgabe-Vorgänge pro Sekunde (IOPS). • Der Symbolbereich gibt an, ob Nodes oder SVMs über aktive Ereignisse verfügen, basierend auf der Anzahl der IOPS, die einen Schwellenwert überschreitet. • Im unteren Bereich werden die gesamten Cluster IOPS der letzten fünf Minuten angezeigt.
MB/Sek.	Zeigt, wie viele Daten in Megabyte pro Sekunde (MB/s) in das und aus dem Cluster übertragen werden. • Der Symbolbereich gibt an, ob Nodes oder SVMs basierend auf dem MB/s-Wert, der eine Schwellenwerteinstellung überschreitet, aktive Ereignisse aufweisen. • Im unteren Bereich wird der gesamte Cluster-Durchsatz der letzten fünf-Minuten-Sammlung angezeigt.

Zähler	Beschreibung
Verwendete Performance-Kapazität	Zeigt, ob Nodes oder Aggregate die verfügbare Performance-Kapazität überbeanspruchen. • Der Symbolbereich gibt an, ob auf Basis des für die Performance verwendeten Werts, der eine Schwellenwerteinstellung überschreitet, Nodes oder Aggregate aktive Ereignisse aufweisen. • Im unteren Bereich werden die am stärksten ausgelasteten Nodes und das am stärksten ausgelasteten Aggregat die höchste Performance-Kapazität angezeigt. Daten zur Performance-Kapazität sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.
Auslastung	Zeigt, ob die Ressourcen auf beliebigen Nodes oder Aggregaten überlastet sind. • Der Symbolbereich gibt an, ob Nodes oder Aggregate basierend auf dem Nutzungswert, der eine Schwellenwerteinstellung überschreitet, aktive Ereignisse aufweisen. • Im unteren Bereich wird der höchste Auslastungswert des am stärksten ausgelasteten Nodes und des am stärksten ausgelasteten Aggregats angezeigt.

Ellipsen (…) Im Kopfbereich wird angegeben, dass Leistungsdaten gerade erfasst werden.

Sie können auf **Cluster-Details** klicken, um einen Cluster mit Performance-Ereignissen anzuzeigen, auf der die Startseite des Performance Cluster angezeigt wird. Dort können Sie detaillierte Performance-Informationen über das Cluster und andere Storage-Objekte anzeigen.

Cluster-Statusmeldungen

Wenn ein von Unified Manager gemanagter Cluster nicht mehr verfügbar ist, wird über den Performance-Zählern ein Statusmeldungs-Banner angezeigt. Eine **Details**-Schaltfläche wird rechts neben dem Statusmeldenbanner angezeigt, wenn das Cluster nicht erreichbar ist. Durch Klicken auf die Schaltfläche **Details** in der Statusmeldung können Sie zur Seite Cluster Data Sources navigieren, die vollständige Informationen zum Problem enthält. Auf der Seite „Cluster-Datenquellen“ finden Sie die Daten, die erforderlich sind, um Probleme zu beheben, aufgrund denen der Cluster nicht mehr verfügbar ist.

Dashboards/Cluster-Ansicht

Auf der Seite Dashboards/Clusteransicht werden Überblicksinformationen zu den zu verwaltenden Clustern angezeigt.

Durch Klicken auf **Cluster verwalten** gelangen Sie zur Seite Configuration/Cluster Data Sources.

Durch Klicken auf ein Cluster werden Überblicksinformationen zu dem Monitoring-Status, dem Kapazitätsstatus und dem Performance-Status des Clusters angezeigt.

Das Dashboard der Clusteransicht besteht aus zwei Hauptbereichen: Verwalteten Clustern (links) und Clusterdetails (rechts).

Abschnitt „verwaltete Cluster“

Listet alle Cluster auf, die von Unified Manager überwacht werden. Für jedes Cluster in der Liste werden folgende Details angegeben:

- Cluster-Status-Symbol: Der Status kann kritisch sein ( ), Fehler ( ), Warnung (Oder normal ( ).
- IP-Adresse oder Hostname: Stellt den Hostnamen des Clusters und die IP-Adresse oder FQDN bereit.
- Cluster-Systemzustand: Bietet Informationen über den Systemzustand des Clusters, die von Unified Manager überwacht werden.

  Der Systemzustand kann einen der folgenden Werte aufweisen: OK, OK mit unterdrückt, beeinträchtigt und die Komponenten sind nicht erreichbar.

Abschnitt „Cluster-Details“

Bietet Informationen zum Monitoring-Status, zur Kapazität und zur Performance des ausgewählten Clusters.

- Überwachungsstatus: Zeigt den kontinuierlichen Status von Zustand und Performance-Überwachung an.

  Der Überwachungsstatus kann die folgenden Werte aufweisen: Ermittlung, Abmeldung abgeschlossen, Abfrage fehlgeschlagen oder nicht verfügbar. Der Überwachungsstatus zeigt eine Fehlermeldung an, wenn der entsprechende Überwachungsauftrag (Zustand oder Leistung) ausfällt.

- Kapazität: Zeigt die gesamte, genutzte und freie Speicherkapazität des ausgewählten Clusters an.
- Performance: Zeigt die durchschnittliche Betriebsgeschwindigkeit des Clusters in Anzahl der IOPS (Eingabe-/Ausgabevorgänge pro Sekunde) und den durchschnittlichen Durchsatz des ausgewählten Clusters in MB/s (Megabyte pro Sekunde) an.

Im Abschnitt „Details“ finden Sie außerdem Links zu den einzelnen Cluster-Detailseiten der OnCommand Unified Manager Applikationen:

- Der Link Systemzustand navigiert zur Seite mit den Angaben zum Systemzustand/Cluster des ausgewählten Clusters.
- Der Link Performance navigiert zur Seite Performance/Cluster-Details des ausgewählten Clusters.
- Der Link System Manager navigiert zur Anmeldeseite für OnCommand System Manager, sodass Sie Cluster-Einstellungen verwalten können.

Verwalten von Speicherobjekten mit der Option Favoriten

Über die Option Favoriten können Sie ausgewählte Speicherobjekte in Unified Manager anzeigen und verwalten, indem Sie sie als Favoriten markieren. So können Sie den Status Ihrer bevorzugten Storage-Objekte schnell einsehen und Probleme beheben, bevor sie kritisch werden.

Aufgaben, die Sie im Dashboard „Favoriten“ ausführen können

- Zeigen Sie die Liste der als Favorit markierten Speicherobjekte an.
- Fügen Sie der Favoritenliste Speicherobjekte hinzu.
- Entfernen Sie Speicherobjekte aus der Favoritenliste.

Anzeigen der Favoritenliste

Sie können die Kapazitäts-, Performance- und Sicherungsdetails ausgewählter Speicherobjekte in der Liste Favoriten anzeigen. Die Details von maximal 20 Speicherobjekten werden in der Favoritenliste angezeigt.

Hinzufügen von Speicherobjekten zur Favoritenliste

Sie können der Liste „Favoriten“ Storage-Objekte hinzufügen und diese Objekte dann für Zustand, Kapazität und Performance überwachen. Sie können Cluster, Volumes und Aggregate nur als Favorit markieren.

Entfernen von Speicherobjekten aus der Favoritenliste

Sie können Speicherobjekte aus der Favoritenliste entfernen, wenn sie nicht mehr als Favorit markiert werden müssen.

Hinzufügen zu und Entfernen von Speicherobjekten aus der Liste Favoriten

Sie können einer Favoritenliste Storage-Objekte hinzufügen, damit Sie diese Objekte im Hinblick auf Zustand, Kapazität und Performance überwachen können. Sie können den Objektstatus in der Favoritenliste verwenden, um Probleme zu ermitteln und zu beheben, bevor sie kritisch werden. Die Favoritenliste enthält außerdem den aktuellsten Überwachungsstatus eines Speicherobjekts. Sie können Speicherobjekte aus der Favoritenliste entfernen, wenn sie nicht mehr als Favorit markiert werden müssen.

Über diese Aufgabe

In der Favoritenliste können bis zu 20 Cluster, Nodes, Aggregate oder Volumes hinzugefügt werden. Wenn Sie der Liste „Favoriten“ einen Node hinzufügen, wird dieser als Cluster angezeigt.

Schritte

1. Rufen Sie die Seite **Details** des Speicherobjekts auf, das Sie als Favorit markieren möchten.
2. Klicken Sie auf das Sternsymbol ( ) Zum Hinzufügen des Speicherobjekts zur Favoritenliste.

Hinzufügen eines Aggregats zur Favoritenliste

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **Aggregate**.
2. Klicken Sie auf der Seite „Inventar/Aggregate“ auf das Aggregat, das Sie der Liste „Favoriten“ hinzufügen möchten.
3. Klicken Sie auf der Seite „Systemzustand/Aggregat-Details“ auf das STAR-Symbol ( ).

Nachdem Sie fertig sind

Um ein Speicherobjekt aus der Liste Favoriten zu entfernen, wechseln Sie zur Listenseite Favoriten, klicken Sie auf das Sternsymbol ( ) Auf der Objektkarte, die Sie entfernen möchten, und wählen Sie dann die Option **aus Favoriten entfernen**.

Cluster-Favorite-Karte

Mit der Cluster Favorite Card können Sie die Kapazitäts-, Konfigurations- und Performance-Details der einzelnen Cluster anzeigen, die Sie als Favoriten markiert haben.

Cluster-Attribute

Auf der Cluster Favorite Card werden die folgenden Attribute der einzelnen Cluster angezeigt:

- **Cluster-Integritätsstatus**

  Ein Symbol, das den Systemzustand des Clusters angibt. Mögliche Werte sind Normal, Warnung, Fehler und kritisch.

- **Clustername**

  Der Name des Clusters.

- * Kapazität*

  Freier Speicherplatz im Cluster.

- **Konfiguration**

  Konfigurationsdetails des Clusters.

  - **IP-Adresse**

    IP-Adresse oder Host-Name der logischen Cluster-Management-Schnittstelle (LIF), die zum Hinzufügen des Clusters verwendet wurde.

  - **Anzahl der Knoten**

    Anzahl Nodes im Cluster.

- **Leistung**

  Performance-Details des Clusters.

  - **IOPS**

    Durchschnittliche Anzahl von I/O-Vorgängen pro Sekunde in den letzten 72 Stunden.

  - **Durchsatz**

    Durchschnittsdurchsatz der letzten 72 Stunden, in Mbps .

Aggregieren der Lieblingskarte

Die bevorzugte Karte für Aggregate ermöglicht Ihnen, die Kapazitäts- und Performance-Details der Aggregate anzuzeigen, die Sie als Favoriten markiert haben.

Aggregatattribute

Auf der Favoriten-Karte für das Aggregat werden die folgenden Aggregatattribute angezeigt:

- * Integritätsstatus aggregieren*

  Ein Symbol, das den Zustand des Aggregats angibt. Mögliche Werte sind Normal, Warnung, Fehler und kritisch.

- **Aggregatname**

  Der Name des Aggregats.

  Positionieren Sie den Cursor über den Aggregatnamen, um den Namen des Clusters anzuzeigen, zu dem das Aggregat gehört.

- * Kapazität*

  Prozentsatz des verfügbaren freien Speicherplatzes im Aggregat und die geschätzte Anzahl an Tagen, bis das Aggregat voll ist.

  Zu beachten ist, dass FabricPool diese Informationen nur die Kapazität auf der lokalen Performance-Tier widerspiegeln. Klicken Sie auf die Kachel „Kapazität“, um detaillierte Informationen auf der Detailseite „Systemzustand/Aggregat“ anzuzeigen.

- **Leistung**

  Performance-Details des Aggregats.

  - **IOPS**

    Durchschnittliche Anzahl von I/O-Vorgängen pro Sekunde in den letzten 72 Stunden.

  - **Durchsatz**

    Durchschnittsdurchsatz der letzten 72 Stunden, in Mbps .

  - **Latenz**

    Die durchschnittliche Reaktionszeit eines Vorgangs wurde in Millisekunden benötigt.

Bevorzugte Karte für Volume

Mit der Favoritkarte Volume können Sie die Kapazitäts-, Sicherungs- und Performancedetails der Volumes anzeigen, die Sie als Favoriten markiert haben.

Volume-Attribute

Die Lieblingskarte für das Volume zeigt die folgenden Volume-Attribute an:

- **Volume-Integritätsstatus**

  Ein Symbol, das den Integritätsstatus des Volumes anzeigt. Mögliche Werte sind Normal, Warnung, Fehler und kritisch.

- **Volumenname**

  Name des Volumes.

- * Kapazität*

  Prozentsatz des verfügbaren freien Speicherplatzes auf dem Volume und die geschätzte Anzahl von Tagen bis zum Abschluss des Volume.

- **Schutz**

  Schutzrolle, die für das Volume festgelegt ist. Die möglichen Werte sind ungeschützt, nicht zutreffend, geschützt und Ziel.

- **Leistung**

  Performance-Statistiken für das Volume.

  - **IOPS**

    Durchschnittliche Anzahl von I/O-Vorgängen pro Sekunde in den letzten 72 Stunden.

  - **Durchsatz**

    Durchschnittlicher Durchsatz der letzten 72 Stunden, in MB/s.

  - **Latenz**

    Die durchschnittliche Reaktionszeit eines Vorgangs wurde in Millisekunden benötigt.

Verwalten von Ereignissen

Ereignisse unterstützen Sie bei der Erkennung von Problemen in den überwachten Clustern.

Was für einen Systemzustand gibt es

Systemzustandsereignisse sind Benachrichtigungen, die automatisch generiert werden, wenn eine vordefinierte Bedingung eintritt oder wenn ein Objekt einen Systemzustandsschwellenwert überschreitet. Mithilfe dieser Ereignisse können Sie Maßnahmen ergreifen, um Probleme zu vermeiden, die zu schlechter Performance und Nichtverfügbarkeit des Systems führen können. Ereignisse umfassen einen Impact-Bereich, einen Schweregrad und einen Impact-Level.

Systemzustandsereignisse werden nach Art der Beeinträchtigungen kategorisiert, z. B. Verfügbarkeit, Kapazität, Konfiguration oder Schutz. Ereignisse werden zudem einem Schweregrad und einem Impact-Level zugewiesen, mit dem Sie feststellen können, ob eine sofortige Aktion erforderlich ist.

Sie können Meldungen so konfigurieren, dass Benachrichtigungen automatisch gesendet werden, wenn bestimmte Ereignisse oder Ereignisse eines bestimmten Schweregrads auftreten.

Veraltete, behobene und informative Ereignisse werden automatisch protokolliert und standardmäßig 180 Tage lang aufbewahrt.

Es ist wichtig, dass Sie umgehend Korrekturmaßnahmen bei Ereignissen mit einem Schweregrad „Fehler“ oder „kritisch“ vornehmen.

Was sind Performance-Ereignisse

Performance-Ereignisse sind Störungen im Zusammenhang mit der Workload-Performance auf einem Cluster. Die Sie bei der Ermittlung von Workloads mit langsamen Reaktionszeiten unterstützen. Zusammen mit gleichzeitig aufgetretenen Gesundheitsereignissen können Sie die Probleme bestimmen, die die langsamen Reaktionszeiten verursacht oder dazu beigetragen haben.

Wenn Unified Manager mehrere Vorkommen derselben Clusterkomponente erkennt, werden alle Vorkommen als einzelnes Ereignis und nicht als separate Ereignisse behandelt.

Was passiert, wenn ein Ereignis empfangen wird

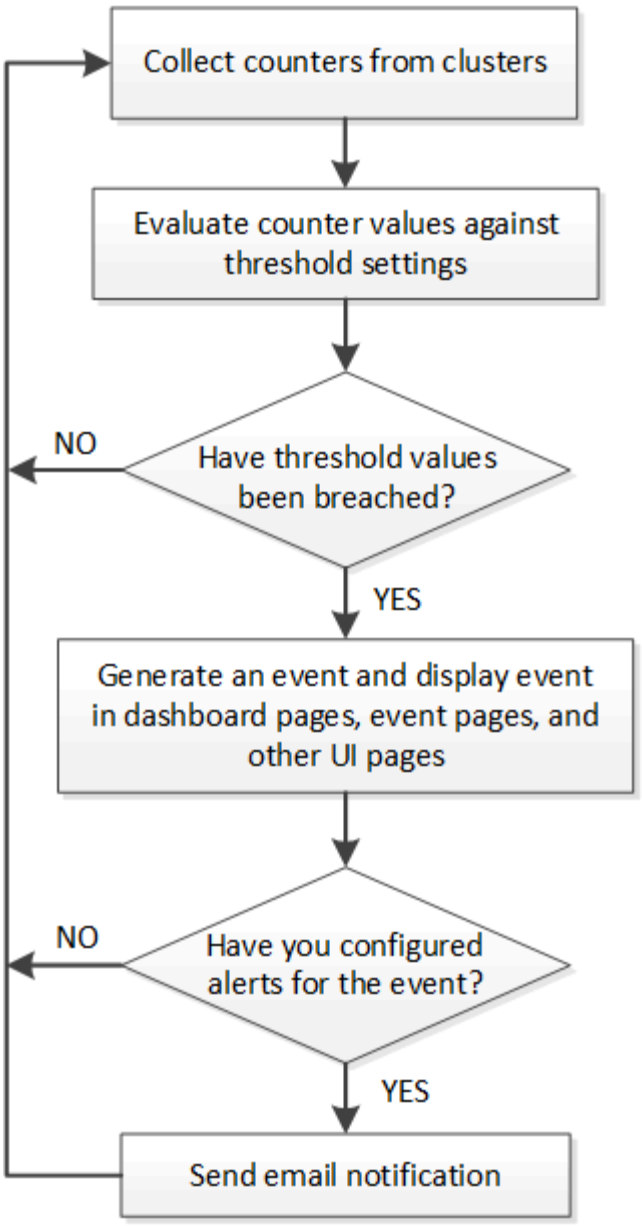
Wenn Unified Manager ein Ereignis empfängt, wird es auf der Seite Dashboards/Übersicht, auf den Registerkarten Zusammenfassung und Explorer der Seite Leistung/Cluster, auf der Seite Ereignisinventar und auf der objektspezifischen Bestandsseite (z. B. auf der Seite „Systemzustand/Volumes-Bestandsaufnahme“) angezeigt.

Wenn Unified Manager mehrere kontinuierliche Vorkommnisse derselben Clusterkomponente erkennt, werden alle Vorkommnisse als einzelnes Ereignis behandelt und nicht als separate Ereignisse. Die Dauer des Ereignisses wird erhöht, um anzugeben, dass das Ereignis noch aktiv ist.

Je nachdem, wie Sie Einstellungen auf der Seite Konfiguration/Warnmeldungen konfigurieren, können Sie andere Benutzer über diese Ereignisse benachrichtigen. Die Meldung bewirkt, dass folgende Aktionen ausgelöst werden:

- Eine E-Mail über das Ereignis kann an alle Unified Manager Administrator-Benutzer gesendet werden.
- Das Ereignis kann an weitere E-Mail-Empfänger gesendet werden.
- Ein SNMP-Trap kann an den Trap-Empfänger gesendet werden.
- Ein benutzerdefiniertes Skript kann ausgeführt werden, um eine Aktion auszuführen.

Dieser Workflow wird im folgenden Diagramm dargestellt.



Von Unified Manager erkannte Konfigurationsänderungen

Unified Manager überwacht Ihre Cluster auf Konfigurationsänderungen. So können Sie feststellen, ob eine Änderung zu einem Performance-Ereignis geführt oder beigetragen hat. Auf den Seiten des Performance Explorer wird ein Symbol für das Änderungsereignis (angezeigt) Zur Angabe des Datums und der Uhrzeit, zu der die Änderung erkannt wurde.

Sie können die Performance-Diagramme auf den Seiten des Performance Explorers und auf der Seite Performance/Volume Details überprüfen, um festzustellen, ob sich das Änderungsereignis auf die Performance des ausgewählten Cluster-Objekts auswirkt. Wenn die Änderung zu oder um die gleiche Zeit wie ein Performance-Ereignis erkannt wurde, hat die Änderung möglicherweise zum Problem beigetragen, was dazu führte, dass die Ereigniswarnung ausgelöst wurde.

Unified Manager erkennt die folgenden Änderungsereignisse, die als Informationsereignisse kategorisiert sind:

- Ein Volume wird zwischen Aggregaten verschoben.

  Unified Manager erkennt, wenn eine Verschiebung gerade ausgeführt, abgeschlossen oder fehlgeschlagen ist. Wenn Unified Manager während einer Volume-Verschiebung ausfällt, erkennt er bei der Sicherung die Volume-Verschiebung und zeigt ein Änderungsereignis für ihn an.

- Der Durchsatz (MB/s oder IOPS) wird von einer QoS-Richtliniengruppe begrenzt, die eine oder mehrere überwachte Workload-Änderungen enthält.

  Das Ändern eines Richtliniengruppenlimits kann zu intermittierenden Latenzspitzen (Antwortzeit) führen, die auch Ereignisse für die Richtliniengruppe auslösen können. Die Latenz kehrt nach und nach wieder in den normalen Zustand zurück und alle durch diese Spitzen verursachten Ereignisse werden obsolet.

- Ein Node in einem HA-Paar übernimmt den Storage seines Partner-Nodes oder gibt ihn zurück.

  Unified Manager erkennt, wann der Takeover-, Teil- oder Giveback-Vorgang abgeschlossen wurde. Wenn der Takeover durch einen Panik- Knoten verursacht wird, erkennt Unified Manager das Ereignis nicht.

- Ein Upgrade oder Zurücksetzen von ONTAP wurde erfolgreich abgeschlossen.

  Die vorherige und die neue Version werden angezeigt.

Konfigurieren von Einstellungen für die Ereignisaufbewahrung

Sie können die Anzahl der Tage angeben, die ein Ereignis im Unified Manager-Server beibehalten wird, bevor es automatisch gelöscht wird. Es werden nur Ereignisse gelöscht, die aufgelöst, veraltet oder vom Typ Informationen sind. Sie können auch die Häufigkeit festlegen, mit der diese Ereignisse gelöscht werden, oder Sie können die Ereignisse auch manuell löschen.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ verfügen, um die Ereigniseinstellungen zu ändern.

Über diese Aufgabe

Die Aufbewahrung von Ereignissen über 180 Tage wirkt sich auf die Serverleistung aus und wird nicht empfohlen. Die untere Grenze für die Ereignisaufbewahrungsdauer beträgt 7 Tage; es gibt keine Obergrenze.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Ereignisse verwalten**.
2. Klicken Sie auf der Seite **Konfiguration/Ereignisse verwalten** auf die Schaltfläche **Ereignisaufbewahrungseinstellungen**.
3. Konfigurieren Sie die entsprechenden Einstellungen im Dialogfeld **Ereignisaufbewahrungseinstellungen**.
4. Klicken Sie auf **Speichern und Schließen**.

Konfigurieren von Einstellungen für Ereignisbenachrichtigungen

Sie können Unified Manager so konfigurieren, dass Benachrichtigungen gesendet werden, wenn ein Ereignis generiert wird oder ein Ereignis einem Benutzer zugewiesen

ist. Sie können den SMTP-Server konfigurieren, der zum Senden der Warnmeldung verwendet wird, und Sie können verschiedene Benachrichtigungsmechanismen festlegen – beispielsweise können Alarmbenachrichtigungen als E-Mails oder SNMP-Traps gesendet werden.

Bevor Sie beginnen

Sie müssen die folgenden Informationen haben:

- E-Mail-Adresse, von der die Benachrichtigung gesendet wird

  Die E-Mail-Adresse wird im Feld „`von`“ in gesendeten Warnmeldungen angezeigt. Falls die E-Mail aus irgendeinem Grund nicht zugestellt werden kann, wird diese E-Mail-Adresse auch als Empfänger für nicht lieferbare E-Mails verwendet.

- Hostname des SMTP-Servers sowie Benutzername und Kennwort für den Zugriff auf den Server
- SNMP-Version, Trap-Ziel-Host-IP-Adresse, Outbound-Trap-Port und die Community zum Konfigurieren des SNMP-Trap

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Setup-Menü auf **Benachrichtigungen**.
2. Konfigurieren Sie auf der Seite **Setup/Benachrichtigungen** die entsprechenden Einstellungen und klicken Sie auf **Speichern**.

   Hinweise:

   - Wenn die von-Adresse mit der Adresse „`OnCommand@localhost.com`“ ausgefüllt ist, sollten Sie sie in eine echte, funktionierende E-Mail-Adresse ändern, um sicherzustellen, dass alle E-Mail-Benachrichtigungen erfolgreich versendet werden.
   - Wenn der Hostname des SMTP-Servers nicht aufgelöst werden kann, können Sie anstelle des Host-Namens die IP-Adresse (IPv4 oder IPv6) des SMTP-Servers angeben.

Die Ereignisse des Event Management-Systems sind

Das Event Management System (EMS) sammelt Ereignisdaten aus verschiedenen Teilen des ONTAP Kernels und bietet Mechanismen zur Ereignisweiterleitung. Diese ONTAP Ereignisse können im Unified Manager als EMS-Ereignisse gemeldet werden. Die zentralisierte Überwachung und Verwaltung erleichtert die Konfiguration kritischer EMS-Ereignisse und Alarmbenachrichtigungen auf der Grundlage dieser EMS-Ereignisse.

Die Unified Manager-Adresse wird dem Cluster als Benachrichtigungsziel hinzugefügt, wenn Sie das Cluster Unified Manager hinzufügen. Ein EMS-Ereignis wird gemeldet, sobald das Ereignis im Cluster auftritt.

Für den Empfang von EMS-Ereignissen in Unified Manager gibt es zwei Methoden:

- Eine bestimmte Anzahl wichtiger EMS-Ereignisse wird automatisch gemeldet.

- Sie können sich für den Erhalt einzelner EMS-Events anmelden.

Die EMS-Ereignisse, die durch Unified Manager generiert werden, werden abhängig von der Methode, in der das Ereignis generiert wurde, unterschiedlich berichtet:

Funktionalität	Automatische EMS-Nachrichten	Abonnierte EMS-Nachrichten
Verfügbare EMS-Events	Teilmenge der EMS-Ereignisse	Alle EMS-Ereignisse
EMS-Nachrichtenname bei Auslösung	Unified Manager Ereignisname (aus EMS-Ereignisname konvertiert)	Nicht spezifisch im Format „`Error EMS received`“. Die detaillierte Meldung liefert das Punktnotationsformat des tatsächlichen EMS-Ereignisses
Empfangene Nachrichten	Sobald das Cluster erkannt wurde	Nach dem Hinzufügen jedes erforderlichen EMS-Ereignisses zu Unified Manager und nach dem nächsten 15-minütigen Abfragzyklus
Ereignislebenszyklus	Wie andere Unified Manager Ereignisse: Neuer, bestätigter, gelöster und überholter Status	Das EMS-Ereignis wird nach der Aktualisierung des Clusters nach 15 Minuten nach dem Erstellen des Ereignisses veraltet
Erfasst Ereignisse während Unified Manager-Downtime	Ja, wenn das System gestartet wird, kommuniziert es mit jedem Cluster, um fehlende Ereignisse zu erfassen	Nein
Veranstaltungsdetails	Vorgeschlagene Korrekturmaßnahmen werden direkt aus ONTAP importiert, um konsistente Lösungen zu bieten	Korrekturmaßnahmen sind auf der Seite Ereignisdetails nicht verfügbar

Bei einigen der neuen automatischen EMS-Ereignisse handelt es sich um Informationsereignisse, die darauf hinweisen, dass ein vorheriges Ereignis behoben wurde. So zeigt das Informationsereignis „`FlexGroup Komponenten Raumstatus alles OK`“ an, dass das Fehler „`FlexGroup-Komponenten haben Platzprobleme`“ behoben wurde. Informationsereignisse können nicht mit demselben Ereignislebenszyklus verwaltet werden wie andere Arten von Schweregrad. Das Ereignis wird jedoch automatisch veraltet, wenn das gleiche Volume ein weiteres Fehlerereignis „`SPace Problems`“ erhält.

EMS-Ereignisse, die automatisch dem Unified Manager hinzugefügt werden

Bei der Verwendung von Unified Manager 9.4 oder höher werden die folgenden ONTAP EMS-Ereignisse automatisch dem Unified Manager hinzugefügt. Diese Ereignisse werden generiert, wenn sie auf jedem Cluster ausgelöst werden, das Unified Manager überwacht.

Die folgenden EMS-Ereignisse stehen zur Verfügung, wenn Cluster mit ONTAP 9.5 oder höher überwacht werden:

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad der ONTAP
Objektspeicherzugriff für Aggregatverschiebung verweigert	arl.netra.ca.check.failed	Aggregat	Fehler
Objektspeicherzugriff während eines Storage Failover für Aggregatverschiebung verweigert	gb.netra.ca.check.failed	Aggregat	Fehler
FabricPool Speicherplatz fast voll	Fabricpool.Fast.full	Cluster	Fehler
Beginn des NVMe-of-Grace-Zeitraums	nvmf.graceperiod.start	Cluster	Warnung
NVMe-of-Grace-Zeitraum aktiv	nvmf.graceperiod.active	Cluster	Warnung
NVMe-of-Grace-Zeitraum abgelaufen	nvmf.graceperiod.expired	Cluster	Warnung
LUN wurde zerstört	lun.destroy	LUN	Informationsdaten
Cloud AWS MetaDataConnFail	Cloud.aws.metadataConnFail	Knoten	Fehler
Cloud AWS IAMCredsExpired – Cloud	Cloud.aws.iamCredsExpired	Knoten	Fehler
Cloud AWS IAMCredsungültig	Cloud.aws.iamCredsungültig	Knoten	Fehler
Cloud AWS IAMCredsNotFound	Cloud.aws.iamCredsNotFound	Knoten	Fehler
Cloud AWS IAMCredsNotinitialisiert	Cloud.aws.iamNotinitialisiert	Knoten	Informationsdaten
Cloud AWS IAMRoleInvalid	Cloud.AWS.iamRoleIngültig	Knoten	Fehler

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad der ONTAP
Cloud AWS IAMRoleNotFound	Cloud.aws.iamRoleNotFound	Knoten	Fehler
Objstore Host Unlösbar	Objstore.Host.unlösbar	Knoten	Fehler
Objstore InterClusterLifDown	objstore.interclusterlifDown	Knoten	Fehler
Signatur des Objektspeichers mit Nichtübereinschrift anfordern	osc.signatureMismatch	Knoten	Fehler
Einer der NFSv4-Pools ist erschöpft	Nblade.nfsV4PoolAust	Knoten	Kritisch
QoS Monitor Memory-Besteuerung	qos.Monitor.Memory.maxed	Knoten	Fehler
QoS Monitor Memory nicht gespeichert	qos.Monitor.Memory.abgenutzt	Knoten	Informationsdaten
NVMeNS zerstören	NVMeNS.destroy	Namespace	Informationsdaten
NVMeNS Online	NVMeNS.offline	Namespace	Informationsdaten
NVMeNS Offline	NVMeNS.online	Namespace	Informationsdaten
NVMe Out of Space	NVMeNS.out.of.space	Namespace	Warnung
Synchrone Replizierung Aus Sync Heraus	sms.Status.out.of.Sync	SnapMirror Beziehung	Warnung
Synchrone Replizierung Wiederhergestellt	sms.status.in.sync	SnapMirror Beziehung	Informationsdaten
Fehler Bei Der Automatischen Synchronisierung Der Replikation	sms.Resync.Versuch.failed	SnapMirror Beziehung	Fehler
Viele CIFS-Verbindungen	Nblade.cifsManyAuths	SVM	Fehler

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad der ONTAP
Max. CIFS-Verbindung überschritten	Nblade.cifsMaxOpenSameFile	SVM	Fehler
Max. Anzahl der CIFS-Verbindung pro Benutzer überschritten	Nblade.cifsMaxSessPerUsrConn	SVM	Fehler
CIFS NetBIOS-Namenskonflikt	Nblade.cifsNbNameConflict	SVM	Fehler
Versucht, eine nicht existierende CIFS-Freigabe zu verbinden	Nblade.cifsNoPrivShare	SVM	Kritisch
Fehler beim CIFS Shadow Copy-Vorgang	cifs.shadowcopy.Failure	SVM	Fehler
Vom AV-Server gefundener Virus	Nblade.vscanVirusDetected	SVM	Fehler
Keine AV-Server-Verbindung für Virus Scan	Nblade.vscanNoScannerConn	SVM	Kritisch
Kein AV-Server registriert	Nblade.vscanNoRegdScanner	SVM	Fehler
Keine reaktionsfähige AV-Server-Verbindung	Nblade.vscanConnInaktiv	SVM	Informationsdaten
AV-Server ist zu beschäftigt, um neue Scananforderung zu akzeptieren	Nblade.vscanConnBackPressure	SVM	Fehler
Nicht autorisierter Benutzer versucht, AV-Server zu verwenden	Nblade.vscanBadUserPrivAccess	SVM	Fehler
FlexGroup-Komponenten haben Platzprobleme	Flexgroup.debestandals.have.space.Issues	Datenmenge	Fehler
FlexGroup-Komponenten-Space-Status alles OK	Flexgroup.Komponenten.space.Status.all.ok	Datenmenge	Informationsdaten

Name des Unified Manager Events	EMS-Ereignisname	Betroffene Ressource	Schweregrad der ONTAP
FlexGroup-Komponenten haben Inodes-Probleme	flexgroup.constituents.have.inodes.issues	Datenmenge	Fehler
FlexGroup-Komponenten inodes Status Alle OK	flexgroup.constituents.inodes.status.all.ok	Datenmenge	Informationsdaten
Logischer Volume-Speicherplatz Fast Voll	Monitor.vol.nearFull	Datenmenge	Warnung
Logischer Speicherplatz Des Volume Voll	Monitor.vol.voll	Datenmenge	Fehler
Logischer Speicherplatz Des Volume Ist Normal	Monitor.vol.one.ok	Datenmenge	Informationsdaten
Fehler bei der automatischen WAFL-Volume-Größe	wafl.vol.autoSize.fail	Datenmenge	Fehler
Die automatische WAFL-Volume-Größe ist abgeschlossen	wafl.vol.autoSize.done	Datenmenge	Informationsdaten

Abonnieren von ONTAP EMS-Veranstaltungen

Sie können EMS-Ereignisse (Event Management System) abonnieren, die von Systemen generiert werden, die mit ONTAP Software installiert sind. Eine Untermenge von EMS-Ereignissen wird automatisch an Unified Manager gemeldet. Weitere EMS-Ereignisse werden jedoch nur gemeldet, wenn Sie sich für diese Ereignisse angemeldet haben.

Bevor Sie beginnen

Abonnieren Sie keine EMS-Ereignisse, die bereits Unified Manager hinzugefügt wurden, da dies zu Verwirrung führen kann, wenn Sie zwei Ereignisse für dasselbe Problem erhalten.

Über diese Aufgabe

Sie können eine beliebige Anzahl von EMS-Veranstaltungen abonnieren. Alle Ereignisse, die Sie abonnieren, werden validiert. Nur die validierten Ereignisse werden auf die in Unified Manager überwachten Cluster angewendet. Der *ONTAP 9 EMS Ereigniskatalog* bietet detaillierte Informationen zu allen EMS-Nachrichten für die angegebene Version der ONTAP 9-Software. Suchen Sie auf der Seite ONTAP 9 Produktdokumentation die entsprechende Version des *EMS-Ereigniskatalogs*, um eine Liste der entsprechenden Veranstaltungen zu finden.

"ONTAP 9 Produktbibliothek"

Sie können Benachrichtigungen für die von Ihnen abonnierenden ONTAP EMS-Ereignisse konfigurieren und

benutzerdefinierte Skripts für die Ausführung dieser Ereignisse erstellen.

> Wenn Sie die ONTAP EMS-Ereignisse, die Sie abonniert haben, kann es möglicherweise ein Problem mit der DNS-Konfiguration des Clusters geben, was verhindert, dass das Cluster den Unified Manager-Server erreicht. Um dieses Problem zu beheben, muss der Cluster-Administrator die DNS-Konfiguration des Clusters korrigieren und dann Unified Manager neu starten. Dadurch werden die ausstehenden EMS-Ereignisse an den Unified Manager-Server gespült.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Ereignisse verwalten**.
2. Klicken Sie auf der Seite **Konfiguration/Ereignisse verwalten** auf die Schaltfläche **EMS-Ereignisse abonnieren**.
3. Geben Sie im Dialogfeld * EMS-Ereignisse abonnieren* den Namen des ONTAP EMS-Events ein, zu dem Sie abonnieren möchten.

   Um die Namen der EMS-Ereignisse anzuzeigen, die Sie in der ONTAP Cluster Shell abonnieren können, können Sie die verwenden `event route show` Befehl (vor ONTAP 9) oder der `event catalog show` Befehl (ONTAP 9 oder höher). Eine ausführliche Anleitung zur Identifizierung einzelner EMS-Ereignisse ist in der Knowledgebase Antwort 1072320 verfügbar.

   "So konfigurieren und erhalten Sie Benachrichtigungen von ONTAP EMS-Ereignisabonnement in Active IQ Unified Manager"

4. Klicken Sie Auf **Hinzufügen**.

   Das EMS-Ereignis wird der Liste der abonnierten EMS-Ereignisse hinzugefügt, aber in der Spalte „Cluster anwendbar“ wird für das hinzugefügte EMS-Ereignis der Status als „`Unbekannt`“ angezeigt.

5. Klicken Sie auf **Speichern und Schließen**, um das EMS-Ereignisabonnement mit dem Cluster zu registrieren.
6. Klicken Sie erneut auf **EMS-Events abonnieren**.

   Der Status „`ja`“ wird in der Spalte „gilt für Cluster“ für das EMS-Ereignis, das Sie hinzugefügt haben, angezeigt.

   Wenn der Status nicht „`ja`“ lautet, überprüfen Sie die Schreibweise des EMS-Ereignisnamens von ONTAP. Wenn der Name falsch eingegeben wird, müssen Sie das falsche Ereignis entfernen und das Ereignis erneut hinzufügen.

Nachdem Sie fertig sind

Wenn das ONTAP EMS-Ereignis auftritt, wird das Ereignis auf der Seite „Ereignisse“ angezeigt. Sie können das Ereignis auswählen, um Details zum EMS-Ereignis auf der Seite Ereignisdetails anzuzeigen. Sie können auch das Ergebnis des Ereignisses verwalten oder Alarme für das Ereignis erstellen.

Anzeigen von Ereignisdetails

Sie können die Details zu einem Ereignis anzeigen, das von Unified Manager ausgelöst wird, um Korrekturmaßnahmen zu ergreifen. Wenn beispielsweise ein

Systemzustandsereignis-Volume Offline vorhanden ist, können Sie auf dieses Ereignis klicken, um die Details anzuzeigen und Korrekturmaßnahmen durchzuführen.

Bevor Sie beginnen

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

Über diese Aufgabe

Die Ereignisdetails enthalten Informationen wie die Quelle des Ereignisses, die Ursache des Ereignisses und alle Notizen, die mit dem Ereignis zusammenhängen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Events**.
2. Klicken Sie auf der Seite **Events** Inventar auf den Ereignisnamen, dessen Details Sie anzeigen möchten.

   Die Ereignisdetails werden auf der Seite Ereignisdetails angezeigt.

Anzeigen nicht zugewiesener Ereignisse

Sie können nicht zugewiesene Ereignisse anzeigen und anschließend jedem Benutzer zuweisen, der diese auflösen kann.

Bevor Sie beginnen

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

Schritte

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

   Standardmäßig werden neue und bestätigte Ereignisse auf der Seite „Ereignisinventar“ angezeigt.

2. Wählen Sie im Fensterbereich **Filter** die Option **nicht zugewiesen** Filter im Bereich **zugewiesen zu** aus.

Bestätigen und Beheben von Ereignissen

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

Bevor Sie beginnen

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

Über diese Aufgabe

Sie können mehrere Ereignisse gleichzeitig bestätigen und beheben.

Sie können keine Informationsereignisse bestätigen.

Schritte

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

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

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

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

Zuweisen von Ereignissen zu bestimmten Benutzern

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

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Events**.
2. Wählen Sie auf der Seite **Ereignisse** Inventar ein oder mehrere Ereignisse aus, die Sie zuweisen

möchten.

3. Ordnen Sie das Ereignis zu, indem Sie eine der folgenden Optionen auswählen:

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

Hinzufügen und Überprüfen von Notizen zu einem Ereignis

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

Bevor Sie beginnen

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

Schritte

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

Deaktivieren oder Aktivieren von Ereignissen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Wenn Sie ein Ereignis für ein Objekt deaktivieren (z. B. das `vol offline` Ereignis), und später aktivieren Sie das Ereignis, generiert Unified Manager keine neuen Ereignisse für Objekte, die offline geschaltet wurden, wenn das Ereignis im Status „deaktiviert“ war. Unified Manager generiert ein neues Ereignis nur, wenn nach der Aktivierung des Ereignisses eine Änderung im Objektstatus erfolgt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Ereignisse verwalten**.
2. Deaktivieren oder aktivieren Sie auf der Seite **Konfiguration/Ereignisse verwalten** Ereignisse, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren von Ereignissen	a. Klicken Sie Auf **Deaktivieren**. b. Wählen Sie im Dialogfeld Ereignisse deaktivieren den Schweregrad des Ereignisses aus. c. Wählen Sie in der Spalte „übereinstimmende Ereignisse“ die Ereignisse aus, die aufgrund des Schweregrads des Ereignisses deaktiviert werden sollen, und klicken Sie dann auf den Pfeil nach rechts, um diese Ereignisse in die Spalte „Ereignisse deaktivieren“ zu verschieben. d. Klicken Sie auf **Speichern und Schließen**. e. Überprüfen Sie, ob die deaktivierten Ereignisse in der Listenansicht der Seite Konfiguration/Ereignisse verwalten angezeigt werden.

Ihr Ziel ist	Dann tun Sie das…
Aktivieren von Ereignissen	a. Aktivieren Sie das Kontrollkästchen für das Ereignis oder die Ereignisse, die Sie aktivieren möchten. b. Klicken Sie Auf **Aktivieren**.

Was für ein Unified Manager-Wartungsfenster ist

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

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

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

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

Planen eines Wartungsfensters zum Deaktivieren der Cluster-Ereignisbenachrichtigungen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

Schritte

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

Das Kalenderfenster wird angezeigt.

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

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

Ergebnisse

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

Ändern oder Abbrechen eines geplanten Wartungsfensters

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

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

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

Anzeigen von Ereignissen, die während eines Wartungsfensters aufgetreten sind

Bei Bedarf können Sie die Ereignisse anzeigen, die während eines Unified Manager-Wartungsfensters für alle Storage-Objekte generiert wurden. Die meisten Ereignisse werden nach Abschluss des Wartungsfensters im Status „veraltet“ angezeigt und alle Systemressourcen werden gesichert und ausgeführt.

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

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

   Standardmäßig werden alle aktiven (Neu- und bestätigten) Ereignisse auf der Seite Ereignisbestand angezeigt.

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

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

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

Verwalten von Ressourcenereignissen des Host-Systems

Unified Manager umfasst einen Service zur Überwachung von Ressourcenproblemen auf dem Host-System, auf dem Unified Manager installiert ist. Probleme wie der fehlende Speicherplatz oder der fehlende Arbeitsspeicher auf dem Hostsystem können Ereignisse der Managementstation auslösen, die als Banner-Meldungen oben in der Benutzeroberfläche angezeigt werden.

Über diese Aufgabe

Ereignisse der Managementstation zeigen ein Problem mit dem Hostsystem an, auf dem Unified Manager installiert ist. Beispiele für Probleme mit Management Station sind Festplattenspeicherplatz, der auf dem Host-System niedrig ist, Unified Manager fehlt einen regelmäßigen Datenerfassungszyklus, und Nichtabschluss oder späterer Abschluss der Statistikanalyse, da die nächste Erfassungsabfrage gestartet wurde.

Im Gegensatz zu allen anderen Unified Manager-Ereignismeldungen werden diese speziellen Warnmeldungen der Management Station sowie kritische Ereignisse in Bannermeldungen angezeigt.

Schritte

1. So zeigen Sie Ereignisinformationen der Management Station an:

Ihr Ziel ist	Tun Sie das…
Zeigen Sie Details der Veranstaltung an	Klicken Sie auf das Veranstaltungsbanner, um die Seite Veranstaltungsdetails mit Lösungsvorschlägen für das Problem anzuzeigen.
Alle Veranstaltungen der Management Station anzeigen	a. Klicken Sie im linken Navigationsbereich auf **Events**. b. Klicken Sie im Fensterbereich Filter auf der Seite Ereignisinventar in der Liste Ausgangstyp auf das Feld für Management Station.

Allgemeines zu Ereignissen

Wenn Sie die Konzepte zu Ereignissen verstehen, können Sie Ihre Cluster und Cluster-Objekte effizient managen und Warnmeldungen entsprechend definieren.

Definition des Ereignisstatus

Der Status eines Ereignisses hilft Ihnen, zu identifizieren, ob eine geeignete Korrekturmaßnahme ergriffen werden muss. Ein Ereignis kann neu, bestätigt, aufgelöst oder veraltet sein. Beachten Sie, dass sowohl neue als auch bestätigte Ereignisse als aktive Ereignisse betrachtet werden.

Die Ereigniszustände sind wie folgt:

- * Neu*

  Der Status eines neuen Ereignisses.

- * Bestätigt*

  Der Status eines Ereignisses, wenn Sie es bestätigt haben.

- * Gelöst*

  Der Status eines Ereignisses, wenn es als gelöst markiert ist.

- **Veraltet**

  Der Status eines Ereignisses, wenn es automatisch korrigiert wird oder wenn die Ursache des Ereignisses nicht mehr gültig ist.

  Sie können ein überholetes Ereignis nicht bestätigen oder beheben.

Beispiel für unterschiedliche Zustände eines Ereignisses

Die folgenden Beispiele veranschaulichen manuelle und automatische Änderungen des Ereignisstatus.

Wenn das Ereignis Cluster nicht erreichbar ist ausgelöst wird, ist der Ereignisstatus Neu. Wenn Sie das Ereignis bestätigen, ändert sich der Ereignisstatus in quittiert. Wenn Sie eine entsprechende Korrekturmaßnahme ergriffen haben, müssen Sie das Ereignis als gelöst markieren. Anschließend wird der Ereignisstatus in „gelöst“ geändert.

Wenn das Ereignis „Cluster nicht erreichbar“ aufgrund eines Stromausfalls generiert wird, funktioniert das Cluster nach Wiederherstellung der Stromversorgung ohne ein Eingreifen des Administrators. Daher ist das Ereignis „Cluster nicht erreichbar“ nicht mehr gültig, und im nächsten Überwachungszyklus wird der Ereignisstatus auf „veraltet“ geändert.

Unified Manager sendet eine Warnmeldung, wenn sich ein Ereignis im Status „veraltet“ oder „gelöst“ befindet. Die E-Mail-Betreffzeile und der E-Mail-Inhalt einer Meldung enthalten Informationen zum Ereignisstatus. Ein SNMP-Trap enthält auch Informationen zum Ereignisstatus.

Beschreibung der Ereignistypen

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

- * Kritisch*

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

  Performance-kritische Ereignisse werden nur von benutzerdefinierten Schwellenwerten gesendet.

- **Fehler**

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

- **Warnung**

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

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

- **Information**

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

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

Beschreibung der Level der Ereignisauswirkungen

Jedes Ereignis ist mit einer Folgenabstufe (Vorfall, Risiko oder Ereignis) verbunden, um Ihnen bei der Priorisierung von Ereignissen zu helfen, für die sofortige Korrekturmaßnahmen erforderlich sind.

- **Vorfall**

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

- **Risiko**

  Ein Risiko ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster nicht mehr Daten für den Client bereitstellt, und nicht mehr genügend Speicherplatz zum Speichern von Daten vorhanden ist. Ereignisse mit Risikoeinwirkung können zu Serviceunterbrechungen führen. Möglicherweise ist eine Korrekturmaßnahme erforderlich.

- **Veranstaltung**

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

Beschreibung der Bereiche für Ereignisauswirkungen

Die Ereignisse werden in fünf Bereiche mit Auswirkungen (Verfügbarkeit, Kapazität, Konfiguration, Leistung und Schutz) unterteilt, damit Sie sich auf die Arten von Ereignissen konzentrieren können, für die Sie verantwortlich sind.

- **Verfügbarkeit**

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

- * Kapazität*

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

- **Konfiguration**

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

- **Leistung**

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

- **Schutz**

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

Wie der Objektstatus berechnet wird

Der Objektstatus wird durch das schwerste Ereignis bestimmt, das derzeit einen neuen oder bestätigten Status aufweist. Wenn z. B. der Objektstatus „Fehler“ lautet, weist eines der Ereignisse des Objekts den Schweregrad „Fehler“ auf. Wenn Korrekturmaßnahmen ergriffen wurden, wird der Ereignisstatus auf „gelöst“ verschoben.

Quellen von Leistungsereignissen

Performance-Ereignisse sind Probleme im Zusammenhang mit der Workload-Performance auf einem Cluster. Sie helfen dabei, Storage-Objekte mit langen Reaktionszeiten zu identifizieren, die auch als hohe Latenz bezeichnet werden. Zusammen mit anderen gleichzeitig aufgetretenen Gesundheitsereignissen können Sie die Probleme bestimmen, die die langsamen Reaktionszeiten verursacht oder dazu beigetragen haben.

Unified Manager erhält Leistungsereignisse aus den folgenden Quellen:

- **Benutzerdefinierte Richtlinienereignisse für Leistungsschwellenwerte**

  Leistungsprobleme basierend auf festgelegten benutzerdefinierten Schwellenwerten. Sie konfigurieren Richtlinien für Performance-Schwellenwerte für Storage-Objekte, wie z. B. Aggregate und Volumes, so dass Ereignisse generiert werden, wenn ein Schwellenwert für einen Performance-Zähler überschritten wurde.

  Sie müssen eine Performance-Schwellenwertrichtlinie definieren und sie einem Storage-Objekt zuweisen, um diese Ereignisse zu empfangen.

- **Systemdefinierte Leistungsschwellenwerte-Policy-Ereignisse**

  Performance-Probleme basierend auf Schwellenwerten, die systemdefiniert sind. Diese Schwellenwertrichtlinien sind in der Installation von Unified Manager enthalten, um allgemeine Performance-Probleme zu beheben.

  Diese Schwellenwertrichtlinien sind standardmäßig aktiviert und Sie können Ereignisse kurz nach dem Hinzufügen eines Clusters sehen.

- **Dynamische Leistungsschwellenwerte**

  Performance-Probleme, die auf Fehler oder Fehler in EINER IT-Infrastruktur zurückzuführen sind oder durch eine zu hohe Auslastung der Cluster-Ressourcen führen. Die Ursache dieser Ereignisse kann ein einfaches Problem sein, das sich über einen bestimmten Zeitraum selbst korrigiert oder durch eine Reparatur- oder Konfigurationsänderung behoben werden kann. Ein dynamisches Schwellenwertereignis gibt an, dass Volume-Workloads in einem ONTAP System aufgrund anderer Workloads mit hohen

Anforderungen an gemeinsam genutzte Cluster-Komponenten nur langsam sind.

Diese Schwellenwerte sind standardmäßig aktiviert, und bei Ihnen kann es Ereignisse nach drei Tagen nach dem Erfassen von Daten aus einem neuen Cluster geben.

Details des dynamischen Performance-Ereignidiagramms

Bei dynamischen Performance-Ereignissen werden auf der Seite „Ereignisdetails“ im Abschnitt „Systemdiagnose“ die wichtigsten Workloads mit der höchsten Latenz oder der höchsten Auslastung der Clusterkomponente angezeigt, die nicht besonders geeignet ist. Die Performance-Statistiken basieren auf dem Zeitpunkt, zu dem das Performance-Ereignis bis zum letzten Mal erkannt wurde, als das Ereignis analysiert wurde. In den Diagrammen werden außerdem Verlaufsstatistiken zur Performance für die Cluster-Komponente angezeigt, die mit Konflikten in Konflikt sind.

Beispielsweise können Sie Workloads mit hoher Auslastung einer Komponente identifizieren, um zu ermitteln, welcher Workload in eine Komponente verschoben werden soll, die weniger genutzt wird. Durch ein Verschieben des Workloads würde der Arbeitsaufwand für die aktuelle Komponente verringert, sodass möglicherweise die Komponente nicht mehr unter Konflikten steht. In diesem Abschnitt wird der Zeit- und Datumsbereich angezeigt, in dem ein Ereignis erkannt und zuletzt analysiert wurde. Bei aktiven Ereignissen (neu oder bestätigt) wird die zuletzt analysierte Zeit weiterhin aktualisiert.

Die Latenz- und Aktivitätsdiagramme zeigen die Namen der wichtigsten Workloads an, wenn Sie den Mauszeiger über das Diagramm bewegen. Wenn Sie rechts im Diagramm auf das Menü „Workload Type“ klicken, können Sie die Workloads anhand ihrer Rolle beim Ereignis, einschließlich *Haie*, *bullies* oder *Opfern*, sortieren und Details zu ihrer Latenz und ihrer Verwendung für die Clusterkomponente anzeigen, deren Konflikte vorliegen. Sie können den tatsächlichen Wert mit dem erwarteten Wert vergleichen, um festzustellen, wann der Workload den erwarteten Latenzbereich oder die Auslastung betrug. Siehe Workloads werden von Unified Manager überwacht.

Wenn Sie bei der Latenzspitze nach Abweichungen sortieren, werden systemdefinierte Workloads nicht in der Tabelle angezeigt, da sich die Latenz nur auf benutzerdefinierte Workloads bezieht. Workloads mit sehr niedrigen Latenzwerten werden in der Tabelle nicht angezeigt.

Weitere Informationen über die dynamischen Leistungsschwellenwerte finden Sie unter Welche Ereignisse sind. Informationen zum Sortieren der Workloads in Unified Manager und zum ermitteln der Sortierreihenfolge finden Sie unter Wie Unified Manager die Auswirkungen auf die Performance eines Ereignisses ermittelt.

Die Daten in den Diagrammen zeigen 24 Stunden Performance-Statistiken vor dem letzten Mal, wenn das Ereignis analysiert wurde. Die tatsächlichen Werte und die erwarteten Werte für jeden Workload basieren auf der Zeit, an der der Workload am Ereignis beteiligt war. Beispielsweise kann ein Workload in ein Ereignis einbezogen werden, nachdem das Ereignis erkannt wurde. Die Performance-Statistiken entsprechen daher zum Zeitpunkt der Ereigniserkennung möglicherweise nicht den Werten. Standardmäßig werden die Workloads nach oberster (höchster) Abweichung der Latenz sortiert.

Da Unified Manager maximal 30 Tage historische Performance- und Ereignisdaten von 5 Minuten speichert, werden keine Leistungsdaten angezeigt, wenn das Ereignis mehr als 30 Tage alt ist.

- * Spalte Workload Sortieren*

- **Latenzdiagramm**

  Zeigt die Auswirkungen des Ereignisses auf die Latenz des Workloads während der letzten Analyse an.

- **Spalte Komponentenverwendung**

  Zeigt Details zur Workload-Nutzung der Clusterkomponente an, die mit einem Konflikt zu Konflikten führen ist. In den Diagrammen ist die tatsächliche Verwendung eine blaue Linie. Ein roter Balken markiert die Ereignisdauer von der Erkennungszeit bis zur letzten analysierten Zeit. Weitere Informationen finden Sie unter Workload-Performance-Messungen.

  Da für die Netzwerkkomponente Statistiken zur Netzwerk-Performance aus dem Cluster stammen, wird diese Spalte nicht angezeigt.

- **Komponentenverwendung**

  Zeigt den Auslastungsverlauf in Prozent für die Netzwerkverarbeitung, Datenverarbeitung und Aggregatkomponenten oder den Verlauf des Vorgangs in Prozent für die Komponente der QoS-Richtliniengruppe an. Das Diagramm wird nicht für die Netzwerk- oder Verbindungskomponenten angezeigt. Sie können mit der Statistik zu einem bestimmten Zeitpunkt die Nutzungsstatistiken anzeigen.

- **Total Write Mbps Historie**

  Nur für die Komponente MetroCluster Ressourcen wird der gesamte Schreibdurchsatz in Megabyte pro Sekunde (MB/s) für alle Volume Workloads angezeigt, die in einer MetroCluster-Konfiguration dem Partner-Cluster gespiegelt werden.

- **Veranstaltungsverlauf**

  Zeigt in den rot schattierten Zeilen die historischen Ereignisse für die zu versagende Komponente an. Bei veralteten Ereignissen zeigt das Diagramm Ereignisse an, die vor dem Erkennen des ausgewählten Ereignisses aufgetreten sind und nach dessen Behebung behoben wurden.

Typen systemdefinierter Performance-Schwellenwerte

Unified Manager bietet einige standardmäßige Schwellenwertrichtlinien, die die Cluster-Performance überwachen und Ereignisse automatisch generieren. Diese Richtlinien sind standardmäßig aktiviert und erzeugen Warn- oder Informationsereignisse, wenn die überwachten Performance-Schwellenwerte nicht eingehalten werden.

Systemdefinierte Performance-Schwellenwerte sind auf Cloud Volumes ONTAP-, ONTAP Edge- oder ONTAP Select-Systemen nicht aktiviert.

Wenn Sie von einer systemdefinierten Performance-Schwellenwertrichtlinie unnötige Ereignisse erhalten, können Sie einzelne Richtlinien auf der Seite „Konfiguration/Ereignisse verwalten“ deaktivieren.

Richtlinien für Node-Schwellwerte

Die systemdefinierten Richtlinien für Node-Performance-Schwellenwerte werden standardmäßig jedem Node in den von Unified Manager überwachten Clustern zugewiesen:

- **Node-Ressourcen werden überausgelastet**

  Identifiziert Situationen, in denen ein einzelner Node über dem Grenzen seiner betrieblichen Effizienz arbeitet und so Workload-Latenzen potenziell beeinträchtigen kann. Dies ist ein Warnereignis.

  Bei Nodes, die mit ONTAP 8.3.x und früherer Software installiert sind, sucht dieser Vorgang nach Nodes, die mehr als 30 Minuten lang mehr als 85 % ihrer CPU- und RAM-Ressourcen (Auslastung der Nodes) nutzen.

  Bei Knoten, die mit der Software ONTAP 9.0 und höher installiert werden, sucht dieser Vorgang nach Nodes, die mehr als 30 Minuten lang mehr als 100 % ihrer Performance-Kapazität nutzen.

- **Node HA-Paar überausgelastet**

  Bestimmt, in welchen Fällen die Nodes in einem HA-Paar über den Grenzen der betrieblichen Effizienz des HA-Paars arbeiten. Dies ist ein Informationsereignis.

  Bei Nodes, die mit ONTAP 8.3.x und früherer Software installiert sind, wird dies durch einen Blick auf die CPU- und RAM-Nutzung für die beiden Nodes im HA-Paar erreicht. Wenn die kombinierte Node-Auslastung der beiden Nodes über 140 % für mehr als eine Stunde beträgt, wirkt sich ein Controller-Failover auf die Workload-Latenzen aus.

  Bei Nodes, die mit der Software ONTAP 9.0 und höher installiert sind, werden dabei die verwendeten Performance-Kapazität für die beiden Nodes im HA-Paar untersucht. Wenn die kombinierte Performance-Kapazität der beiden Nodes über 200 % für mehr als eine Stunde beträgt, wirkt sich ein Controller-Failover auf die Workload-Latenzen aus.

- **Node-Disk-Fragmentierung**

  Die Situation erkennt, dass eine Festplatte oder eine Festplatte in einem Aggregat fragmentiert ist, was die Services eines wichtigen Systems verlangsamt und die Workload-Latenzen auf einem Node potenziell beeinträchtigt.

  Hier werden bestimmte Lese- und Schreibverhältnisse über alle Aggregate auf einem Node hinweg betrachtet. Diese Richtlinie kann auch während der Resynchronisierung der SyncMirror ausgelöst werden oder wenn Fehler während des Scrub-Betriebs der Festplatte gefunden werden. Dies ist ein Warnereignis.

  > Die Richtlinie „`Node Disk Fragmentierung`“ analysiert rein HDD-basierte Aggregate; Flash Pool, SSD und FabricPool Aggregate werden nicht analysiert.

Aggregieren von Schwellenwertrichtlinien

Die vom System definierte Richtlinie für aggregierte Performance-Grenzwerte wird standardmäßig jedem Aggregat in den Clustern zugewiesen, das von Unified Manager überwacht wird.

- **Aggregat Festplatten überausgelastet**

  Die Situation erkennt, in denen ein Aggregat über den Grenzen seiner betrieblichen Effizienz arbeitet und so die Workload-Latenzen potenziell beeinträchtigt werden. Es identifiziert diese Situationen durch die Suche nach Aggregaten, bei denen die Festplatten im Aggregat mehr als 95% für mehr als 30 Minuten ausgelastet sind. Diese Multicondition-Richtlinie führt dann die folgende Analyse durch, um die Ursache des Problems zu ermitteln:

  - Wird eine Festplatte im Aggregat derzeit im Hintergrund gewartet?

Zu den Hintergrund-Wartungsaktivitäten, für die eine Festplatte möglicherweise benötigt wird, zählen die Festplattenrekonstruktion, der Festplattenscrub, die SyncMirror-Neusynchronisierung und das Reparität.

- Gibt es einen Kommunikationsengpass für den Fibre Channel Interconnect im Platten-Shelf?
- Gibt es zu wenig freien Platz im Aggregat? Ein Warnereignis wird für diese Richtlinie nur dann ausgegeben, wenn eine (oder mehrere) der drei untergeordneten Richtlinien ebenfalls als verletzt betrachtet wird. Ein Performance-Ereignis wird nicht ausgelöst, wenn nur die Festplatten im Aggregat mehr als 95 % ausgelastet sind.

Die Richtlinie „`Aggregate Disks Over-used`“ analysiert rein HDD-basierte Aggregate und Flash Pool (Hybrid) Aggregate, SSD- und FabricPool-Aggregate werden nicht analysiert.

QoS-Schwellenwertrichtlinien

Die systemdefinierten QoS-Performance-Schwellenwertrichtlinien werden jedem Workload mit einer konfigurierten ONTAP QoS-Richtlinie für einen maximalen Durchsatz (IOPS, IOPS/TB oder MB/s) zugewiesen. Unified Manager löst ein Ereignis aus, wenn der Workload-Durchsatzwert 15 % geringer ist als der konfigurierte QoS-Wert.

- **QoS max IOPS oder MB/s Schwellenwert**

  Identifiziert Volumes und LUNs, die ihre maximalen IOPS-Werte durch QoS oder Durchsatzwerte von MB/s überschritten haben und die eine Workload-Latenz beeinträchtigen. Dies ist ein Warnereignis.

  Wird einem einzelnen Workload einer Richtliniengruppe zugewiesen, so wird dies durch Workloads gesucht, die während jedes Erfassungszeitraums für die vorherige Stunde den in der zugewiesenen QoS-Richtliniengruppe definierten Maximaldurchsatz überschritten haben.

  Wenn mehrere Workloads eine einzelne QoS-Richtlinie gemeinsam nutzen, werden dazu die IOPS oder MB/s aller Workloads in der Richtlinie hinzugefügt und die Gesamtsumme im Vergleich zum Schwellenwert überprüft.

- **QoS Peak IOPS/TB oder IOPS/TB mit Block Size Schwellenwert**

  Identifiziert Volumes, die die adaptive QoS-Grenze für IOPS/TB-Durchsatz überschritten haben (oder IOPS/TB mit Blockgrößen-Limit) und die sich auf die Workload-Latenz auswirken. Dies ist ein Warnereignis.

  Dazu wird der in der adaptiven QoS-Richtlinie definierte IOPS-Spitzenwert pro TB in einen QoS-Maximalwert für IOPS basierend auf der Größe jedes Volumes konvertiert. Anschließend werden Volumes untersucht, die während jedes Performance-Erfassungszeitraums für die vorherige Stunde die maximalen IOPS-Werte für QoS überschritten haben.

  Diese Richtlinie wird nur auf Volumes angewendet, wenn das Cluster mit ONTAP 9.3 und höher installiert ist.

  Wurde in der anpassungsfähigen QoS-Richtlinie das Element „`Blockgröße`“ definiert, wird dieser Schwellenwert basierend auf der Größe jedes Volumes in einen QoS-Maximalwert umgewandelt. Dann sucht es nach Volumes, die die maximalen MB/s der QoS in jedem Performance-Erfassungszeitraum für die vorherige Stunde überschritten haben.

Diese Richtlinie wird nur auf Volumes angewendet, wenn das Cluster mit ONTAP 9.5 und höher installiert ist.

Liste von Ereignissen und Schweregraden

Sie können die Liste der Ereignisse verwenden, um mit Ereigniskategorien, Ereignisnamen und Schweregrad jedes Ereignisses, das Sie möglicherweise in Unified Manager sehen, vertraut zu werden. Die Ereignisse werden in alphabetischer Reihenfolge nach Objektkategorie aufgeführt.

Aggregieren von Ereignissen

Aggregierte Ereignisse liefern Ihnen Informationen zum Status von Aggregaten, sodass Sie bei potenziellen Problemen überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ein Sternchen (*) identifiziert EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Aggregate Offline(ocumEvtAggregateOffline)	Vorfall	Aggregat	Kritisch
Aggregat ist fehlgeschlagen (ocumEvtAggregateStateFailed)	Vorfall	Aggregat	Kritisch
Aggregat eingeschränkt(ocumEvtAggregateStateRestricted)	Dar	Aggregat	Warnung
Aggregat-Rekonstruktion (ocumEvtAggregateRaidStateRekonstruktion)	Dar	Aggregat	Warnung
Aggregat herabgestuft (ocumEvtAggregateRaidStateDegradiert)	Dar	Aggregat	Warnung
Cloud Tier teilweise erreichbar (ocumEventCloudTierPartiallyAbnehmbar)	Dar	Aggregat	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Cloud Tier nicht erreichbar (ocumEventCloudTiernicht erreichbar)	Dar	Aggregat	Fehler
MetroCluster Aggregat links hinter(ocumEvtMetroClusterAggregateLeftBehind)	Dar	Aggregat	Fehler
MetroCluster Aggregatspiegelung mit herabgestufter(occumEvtMetroClusterAggregateMirrorDegradiert)	Dar	Aggregat	Fehler
Objektspeicherzugriff für Aggregatverschiebung * verweigert	Dar	Aggregat	Fehler
Objektspeicherzugriff während eines Storage Failover * für Aggregatverschiebung verweigert	Dar	Aggregat	Fehler

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Aggregat-Platz fast voll (ocumEvtAggregateNearFull)	Dar	Aggregat	Warnung
Aggregierter Platz voll (okumEvtAggregateFull)	Dar	Aggregat	Fehler
Aggregieren Sie Tage bis voll (ocumEvtAggregateTagenUntilFullSoon)	Dar	Aggregat	Fehler
Aggregat überengagiert (ocumEvtAggregateOverwockt)	Dar	Aggregat	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Aggregat fast überengagiert (ocumEvtAggregateAlmostOverengagiert)	Dar	Aggregat	Warnung
Aggregat-Snapshot-Reserve voll (ocumEvtaggregateSnapReserveFull)	Dar	Aggregat	Warnung
Aggregierte Wachstumsrate anormal (ocumEvtAggregateGrowthRateAbnormal)	Dar	Aggregat	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Aggregat entdeckt (nicht zutreffend)	Ereignis	Aggregat	Informationsdaten
Aggregat umbenannt(nicht zutreffend)	Ereignis	Aggregat	Informationsdaten
Aggregat gelöscht (nicht zutreffend)	Ereignis	Knoten	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreitster kritischer IOPS-Schwellenwert (okumAggregateIopsVorfall)	Vorfall	Aggregat	Kritisch
Unterschreitster Schwellenwert für die Aggregat-IOPS-Warnung (ocumAggregateIopsWarnung)	Dar	Aggregat	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreitster kritischer Schwellenwert für Aggregatabbps (okumAggregateMbpsVorfall)	Vorfall	Aggregat	Kritisch
Warnung: Aggregatabbps, nicht verletzt (ocumAggregateMbpsWarnung)	Dar	Aggregat	Warnung
Unterschreiten der kritischen Latenzzeit für das Aggregat (ocumAggregateLatencyVorfall)	Vorfall	Aggregat	Kritisch
Warnung: Aggregatlatenz - nicht erreichenem Schwellenwert (okumAggregateLatencyWarnung)	Dar	Aggregat	Warnung
Aggregierte Performance Verwendete Kapazität – kritischer Schwellenwert überschritten (OktumAggregatePerfkapazitätVerwendungVorfall)	Vorfall	Aggregat	Kritisch
Aggregierte Performance Verwendete Kapazität – Warnung: Nicht genutzter Schwellenwert (ocumAggregatePerfkapazitätVerwendWarnung)	Dar	Aggregat	Warnung
Unterschreiten der Aggregatauslastung zum kritischen Schwellenwert (okumAggregateUtilizationVorfall)	Vorfall	Aggregat	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Warnung vor nicht durchbrochenem Aggregat-Auslastungsschwellenwert (ocumAggregateUtilizationWarnung)	Dar	Aggregat	Warnung
Überlasteter Schwellenwert für Aggregat-Festplatten (ocumAggregateFestplattenOverUtilizedWarnung)	Dar	Aggregat	Warnung
Nicht durchbrochenes dynamisches Aggregat-Schwellenwert (okumAggregateDynamicEventWarnung)	Dar	Aggregat	Warnung

Cluster-Ereignisse

Cluster-Ereignisse bieten Informationen zum Status von Clustern. So können Sie das Cluster auf potenzielle Probleme überwachen. Die Ereignisse sind nach dem Impact-Bereich gruppiert und umfassen den Event-Namen, den Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ein Sternchen (*) identifiziert EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Cluster fehlt es an Spare Disks (ocumEvtDiscsNoSpares)	Dar	Cluster	Warnung
Cluster nicht erreichbar (ocumEvtClusternicht erreichbar)	Dar	Cluster	Fehler
Cluster-Überwachung fehlgeschlagen (ocumEvtClusterMonitoringFailed)	Dar	Cluster	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Kapazitätsbeschränkungen für Cluster-FabricPool-Lizenz, überschritten (OktEvtexterne KapazitätenTierSpaceFull)	Dar	Cluster	Warnung
NVMe-of Grace-Zeitraum gestartet *(nvmfGracePeriodStart)	Dar	Cluster	Warnung
NVMe-of Grace Period aktiv *(nvmfGracePeriodActive)	Dar	Cluster	Warnung
NVMe-of Grace-Zeitraum abgelaufen *(nvmfGracePeriodExpired)	Dar	Cluster	Warnung
Objekt-Wartungsfenster gestartet (ObjektPflege-Fenster gestartet)	Ereignis	Cluster	Kritisch
Objekt-Wartungsfenster beendet(ObjectWartungs-Fenster beendet)	Ereignis	Cluster	Informationsdaten
MetroCluster Ersatzfestplatten übrig (ocumEvtSpareDiskLeftBehind)	Dar	Cluster	Fehler
MetroCluster Automatische ungeplante Umschaltung deaktiviert (ocumEvtMccAutomaticUnplanedSwitchOverdisabled)	Dar	Cluster	Warnung

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Cluster-Cloud-Tier-Planung (ClusterCloudTierPlanningWarnung)	Dar	Cluster	Warnung
FabricPool Space fast voll *	Dar	Cluster	Fehler

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Node hinzugefügt (nicht zutreffend)	Ereignis	Cluster	Informationsdaten
Node entfernt(nicht zutreffend)	Ereignis	Cluster	Informationsdaten
Cluster entfernt (nicht zutreffend)	Ereignis	Cluster	Informationsdaten
Cluster-Add fehlgeschlagen (nicht zutreffend)	Ereignis	Cluster	Fehler
Cluster-Name geändert(nicht zutreffend)	Ereignis	Cluster	Informationsdaten
Notfallhilfe erhalten (nicht zutreffend)	Ereignis	Cluster	Kritisch
Erhalten von wichtigen EMS (nicht zutreffend)	Ereignis	Cluster	Kritisch
Alarm EMS empfangen (nicht zutreffend)	Ereignis	Cluster	Fehler
Fehler EMS empfangen (nicht zutreffend)	Ereignis	Cluster	Warnung
Warnung EMS empfangen (nicht zutreffend)	Ereignis	Cluster	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Debug EMS empfangen (nicht zutreffend)	Ereignis	Cluster	Warnung
Hinweis erhalten EMS (nicht zutreffend)	Ereignis	Cluster	Warnung
Information EMS empfangen (nicht zutreffend)	Ereignis	Cluster	Warnung

ONTAP EMS-Ereignisse sind in drei Schweregrade für Ereignisse von Unified Manager unterteilt.

Schweregrad für Unified Manager Ereignisse	Schweregrad des ONTAP EMS-Ereignisses-Ereignisses
Kritisch	Notfall Kritisch
Fehler	Alarm
Warnung	Fehler Warnung Debuggen Hinweis Informativ

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreitster Cluster-IOPS-Schwellenwert (OktumClusterIopsVorfall)	Vorfall	Cluster	Kritisch
Unterschreitster Cluster IOPS-Warnungsschwellenwert (ocumClusterIopsWarnung)	Dar	Cluster	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreitster Cluster/MB/s-Schwellenwert (ocumClusterMbpsVorfall)	Vorfall	Cluster	Kritisch
Unterschreitster Warnungsschwellenwert für Cluster-Mbps (ocumClusterMbpsWarnung)	Dar	Cluster	Warnung
Nicht verbundenes dynamischer Schwellenwert (ocumClusterDynamicEventWarnung)	Dar	Cluster	Warnung

Festplatten-Ereignisse

Festplatten-Events liefern Ihnen Informationen zum Status von Festplatten, sodass Sie Monitoring-Funktionen auf potenzielle Probleme ausführen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Flash-Festplatten – Spare Blocks fast verbraucht (ocumEvtClusterFlashDiskFewerSpaeBlockError)	Dar	Cluster	Fehler
Flash-Festplatten – keine Spare-Blöcke (ocumEvtClusterFlashDiskNoSpareBlockkritisch)	Vorfall	Cluster	Kritisch
Einige nicht zugewiesene Festplatten (ocumEvtClusterUnzuweisedDisksSome)	Dar	Cluster	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Einige ausgefallene Festplatten (ocumEvtDisksSomeFailed)	Vorfall	Cluster	Kritisch

Gehäuse-Ereignisse

Gehäuse-Events liefern Ihnen Informationen zum Status der Festplatten-Shelf-Gehäuse im Datacenter, sodass Sie mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Platten-Shelf-Lüfter fehlgeschlagen(ocumEvtShelfFanFailed)	Vorfall	Storage Shelf	Kritisch
Fehler bei der Festplatten-Shelf-Stromversorgung(ocumEvtShelfPowerSupplyFailed)	Vorfall	Storage Shelf	Kritisch
Platten-Shelf Multipath nicht konfiguriert (ocumDiskShelfConnectivityNotInMultiPath) Dieses Ereignis gilt nicht für: • Cluster, die sich in einer MetroCluster-Konfiguration befinden • Die folgenden Plattformen: FAS2554, FAS2552, FAS2520 und FAS2240	Dar	Knoten	Warnung
Festplatten-Shelf-Pfad-Ausfall(ocumDiskShelfConnectivitätPathFailure)	Dar	Storage Shelf	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Festplatten-Shelf erkannt (nicht zutreffend)	Ereignis	Knoten	Informationsdaten
Entfernte Festplatten-Shelfs (nicht zutreffend)	Ereignis	Knoten	Informationsdaten

Fan-Events

Lüfterereignisse versorgen Sie mit Informationen zu den Statusventilatoren auf Nodes in Ihrem Datacenter, sodass Sie mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Ein oder mehrere ausgefallene Lüfter(ocumEvtFansOneOrMoreFailed)	Vorfall	Knoten	Kritisch

Flash-Kartenereignisse

Flash-Karten-Events informieren Sie über den Status der auf Nodes in Ihrem Datacenter installierten Flash-Karten und überwachen mögliche Probleme. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Flash-Karten offline(ocumEvtFlashCardOffline)	Vorfall	Knoten	Kritisch

Inodes-Events

Inode-Ereignisse liefern Informationen, wenn die Inode voll oder fast voll ist, sodass Sie auf potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp

und den Schweregrad.

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Inodes fast voll (ocumEvtInodesAlmostFull)	Dar	Datenmenge	Warnung
Inodes Full (ocumEvtInodesFull)	Dar	Datenmenge	Fehler

Ereignisse der logischen Schnittstelle (LIF)

LIF-Ereignisse liefern Informationen zum Status Ihrer LIFs, sodass Sie Monitoring auf potenzielle Probleme durchführen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LIF-Status aus(ocumEvtLifStatusDown)	Dar	Schnittstelle	Fehler
LIF Failover nicht möglich (ocumEvtLifFailOverPossible)	Dar	Schnittstelle	Warnung
LIF nicht am Home Port(ocumEvtLifNotAtHomePort)	Dar	Schnittstelle	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LIF-Route nicht konfiguriert (nicht zutreffend)	Ereignis	Schnittstelle	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Netzwerk-LIF MBit/s kritischer Schwellenwert überschritten (ocumNetworkLifMbpsVorfall)	Vorfall	Schnittstelle	Kritisch
Netzwerk-LIF Mbps Warnung: Überschreitung des Schwellenwerts (ocumNetworkLifMbpsWarnung)	Dar	Schnittstelle	Warnung
Überschreitung kritischer Schwellenwert für FCP-LIF/MB/s (ocumFcpLifMbpsVorfall)	Vorfall	Schnittstelle	Kritisch
FCP LIF MB/s Warnung: Nicht behebter Schwellenwert (ocumFcpLifMbpsWarnung)	Dar	Schnittstelle	Warnung
NVMf FCP LIF MBit/s Critical Threshold Überlaufen (ocumNvmfFcLifMbpsVorfall)	Vorfall	Schnittstelle	Kritisch
NVMf FCP LIF MBit/s Warnung Überschreiten (ocumNvmfFcLifMbpsWarnung)	Dar	Schnittstelle	Warnung

LUN-Ereignisse

LUN-Ereignisse liefern Ihnen Informationen zum Status Ihrer LUNs, sodass Sie ein Monitoring auf potenzielle Probleme durchführen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ein Sternchen (*) identifiziert EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN Offline(ocumEvtLunOffline)	Vorfall	LUN	Kritisch
LUN wurde zerstört *	Ereignis	LUN	Informationsdaten
Einzel aktiv Pfad für den Zugriff auf LUN(occumEvtLunSingle ActivePath)	Dar	LUN	Warnung
Keine aktiven Pfade zum Zugriff auf die LUN (occumEvtLunNoteAbable)	Vorfall	LUN	Kritisch
Keine optimierten Pfade zum Zugriff auf LUN(ocumEvtLunOptimizedPathInaktiv)	Dar	LUN	Warnung
Keine Pfade zum LUN vom HA Partner(ocumEvtLunHaPathInaktiv)	Dar	LUN	Warnung

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unzureichender Speicherplatz für LUN Snapshot Kopie (ocumEvtLunSnapshotmöglich)	Dar	Datenmenge	Warnung

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreiten kritischer Schwellenwert für LUN-IOPS (OktumLunIopsVorfall)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreitr. LUN IOPS-Warnungsschwellenwert (ocumLunIopsWarnung)	Dar	LUN	Warnung
Unterschreiten kritischen Schwellenwert für LUN/MB/s (ocumLunMbpsVorfall)	Vorfall	LUN	Kritisch
LUN Mbps: Überschreitung des Warnungsschwellenwerts (ocumLunMbpsWarnung)	Dar	LUN	Warnung
LUN-Latenz ms/op Critical Threshold undurchbrochen (ocumLunenzIncident)	Vorfall	LUN	Kritisch
LUN-Latenz ms/op Warnschwellenwert nicht eingehalten (ocumLunLatenzWarnung)	Dar	LUN	Warnung
LUN-Latenz und IOPS – kritischer Schwellenwert – nicht erreicht (ocumLunLatenzenIopsVorfall)	Vorfall	LUN	Kritisch
LUN-Latenz und IOPS - Überschreitung des Warnungsschwellenwerts (ocumLunLatenzIopsWarnung)	Dar	LUN	Warnung
LUN-Latenz und MB/s kritischer Schwellenwert überschritten (ocumLunenzLatency MbpsVorfall)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN-Latenz und MB/s-Warnung nicht erreichender Schwellenwert (ocumLunenzMbpsWarnung)	Dar	LUN	Warnung
LUN-Latenz und aggregierte Performance Verwendete Kapazität – kritischer Schwellenwert nicht erreicht (ocumLunenzyAggregatePerfkapazitätUsedVorfall)	Vorfall	LUN	Kritisch
LUN-Latenz und aggregierte Performance Verwendete Kapazität – Warnung nicht erreichter Schwellenwert (ocumLunenzAggregatePerfkapazitätUsedWarnung)	Dar	LUN	Warnung
LUN-Latenz und aggregierte Auslastung kritischer Schwellenwert überschritten (ocumLunenzAggregateUtilizationVorfall)	Vorfall	LUN	Kritisch
LUN-Latenz und Aggregat-Auslastung Warnschwellenwert nicht erreicht (ocumLunenzAggregateUtilizationWarnung)	Dar	LUN	Warnung
LUN-Latenz und Node-Performance: Verwendete Kapazität – kritischer Schwellenwert nicht erreicht (ocumLunenzyNodePerfdataPerformance UsedIncident)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN-Latenz und Node-Performance: Verwendete Kapazität – Warnung: Nicht erreichter Schwellenwert (ocumLunenzyNodePerfkapazitätUsedWarnung)	Dar	LUN	Warnung
LUN-Latenz und Node-Performance: Verwendete Kapazität – Übernahme kritischer Schwellenwert verletzt (ocumLunLatencyAggregatePerfkapazitätUseTakeoverIncident)	Vorfall	LUN	Kritisch
LUN-Latenz und Node-Performance: Verwendete Kapazität – Übernahmewarnschwellenwert verletzt (ocumLunLatenAggregatePerfkapazitätUseTakeoverWarning)	Dar	LUN	Warnung
LUN-Latenz und Node-Auslastung – kritischer Schwellenwert – nicht erreicht (ocumLunLatenzenNodeUtilizationVorfall)	Vorfall	LUN	Kritisch
LUN-Latenz und Node-Auslastung Warnung nicht erreichender Schwellenwert (ocumLunenzNodeUtilizationWarnung)	Dar	LUN	Warnung
QoS LUN Max. IOPS Warnschwellenwert nicht erreicht (ocumQosLunMaxIopsWarnung)	Dar	LUN	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
QoS LUN Max. Mbit/s Warnschwellenwert überschritten (ocumQosLunMaxMbpsWarnung)	Dar	LUN	Warnung

Management Station-Events

Management Station-Ereignisse geben Ihnen Informationen über den Status des Servers, auf dem Unified Manager installiert ist, sodass Sie auf mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unified Manager Server Disk Space Fast Full (ocumEvtUnifiedManagerDiskSpaceNearlyFull)	Dar	Management Station	Warnung
Voller Speicherplatz auf dem Unified Manager-Server (ocumEvtUnifiedManagerDiskSpaceFull)	Vorfall	Management Station	Kritisch
Unified Manager Server, auf dem der Speicher gering ist (ocumEvtUnifiedManagerMemoryLow)	Dar	Management Station	Warnung
Unified Manager Server fast nicht genügend Arbeitsspeicher (ocumEvtUnifiedManagerMemoryAlmostOut)	Vorfall	Management Station	Kritisch

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Performance Data Analysis is hited(ocumEvtUnifiedManagerDataMissingAnalyze)	Dar	Management Station	Warnung
Performance Data Collection ist betroffen(OktEvtUnifiedManagerDataMissingCollection)	Vorfall	Management Station	Kritisch

Die beiden letzten Performance-Ereignisse waren nur für Unified Manager 7.2 verfügbar. Wenn eines dieser Ereignisse im Status „Neu“ vorhanden ist und Sie dann auf eine neuere Version der Unified Manager-Software aktualisieren, werden die Ereignisse nicht automatisch gelöscht. Sie müssen die Ereignisse manuell in den Status „aufgelöst“ verschieben.

Veranstaltungen auf der MetroCluster Bridge

MetroCluster Bridge Events informieren Sie über den Status der Brücken, sodass Sie auf mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Brücke nicht erreichbar(OktEvtBridgeheUnerreichbar)	Vorfall	MetroCluster-Brücke	Kritisch
Brückentemperatur anormal (occumEvtBridgeTemperatureAbnormal)	Vorfall	MetroCluster-Brücke	Kritisch

Veranstaltungen für MetroCluster-Konnektivität

Konnektivitätsereignisse bieten Ihnen Informationen über die Konnektivität zwischen den Komponenten eines Clusters und zwischen den Clustern in einer MetroCluster Konfiguration, sodass Sie Monitoring auf potenzielle Probleme durchführen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Alle Inter-Switch Links Down(ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Vorfall	MetroCluster-Inter-Switch-Verbindung	Kritisch
Alle Links zwischen MetroCluster Partnern ausgefallen(occumEvtMetroClusterAllLinksBetweenPartnerDown)	Vorfall	MetroCluster Beziehung	Kritisch
FC-SAS Bridge zu Storage Stack Link Down (ocumEvtBridgeSasPortDown)	Vorfall	MetroCluster Bridge-Stack-Verbindung	Kritisch
MetroCluster Konfiguration umgeschaltet ((ocumEvtMetroClusterDRStatusImpacted)	Dar	MetroCluster Beziehung	Warnung
MetroCluster Konfiguration teilweise umgeschaltet(ocumEvtMetroClusterDRStatusPartially ImpACTED)	Dar	MetroCluster Beziehung	Fehler
Betroffene MetroCluster Disaster Recovery-Funktion (ocumEvtMetroClusterDRStatusImpacted)	Dar	MetroCluster Beziehung	Kritisch
MetroCluster Partner nicht über Peering-Netzwerk erreichbar(ocumEvtMetroClusterPartnerNotErreichbarkeit oberhalb von Netzwerk)	Vorfall	MetroCluster Beziehung	Kritisch
Knoten zu FC Switch Alle FC-VI Interconnect Links Down (ocumEvtMccNodeSwitchFcviLinksDown)	Vorfall	MetroCluster-Node-Switch-Verbindung	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Knoten zu FC Switch ein oder mehrere FC-Initiator Links nach unten(ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Dar	MetroCluster-Node-Switch-Verbindung	Warnung
Knoten zu FC Switch Alle FC-Initiator Links nach unten (ocumEvtMccNodeSwitchFcLinksDown)	Vorfall	MetroCluster-Node-Switch-Verbindung	Kritisch
Switch to FC-SAS Bridge FC Link Down (ocumEvtMccSwitchBridgeFcLinksDown)	Vorfall	Verbindung mit der MetroCluster-Switch-Bridge	Kritisch
Inter Node All FC VI Interconnect Links Down (ocumEvtMccInterNodeLinksDown)	Vorfall	Verbindung zwischen Knoten	Kritisch
Inter Node One oder More FC VI Interconnect Links Down (ocumEvtMccInterNodeLinksOneOrMoreDown)	Dar	Verbindung zwischen Knoten	Warnung
Knoten zu Brücke Link nach unten (ocumEvtMccNodeBridgeLinksDown)	Vorfall	Node-Bridge-Verbindung	Kritisch
Node zu Storage Stack All SAS Links Down (ocumEvtMccNodeStackLinksDown)	Vorfall	Node-Stack-Verbindung	Kritisch
Knoten zu Storage-Stack eine oder mehrere SAS-Links nach unten (occumEvtMccNodeStackLinksOneOrMoreDown)	Dar	Node-Stack-Verbindung	Warnung

Ereignisse auf dem MetroCluster-Switch

MetroCluster Switch-Ereignisse liefern Ihnen Informationen zum Status der MetroCluster Switches, damit Sie ein Monitoring auf potenzielle Probleme ermöglichen. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Schalttemperatur anormal (OktEvtSwitchTemperaturAbnormal)	Vorfall	MetroCluster-Switch	Kritisch
Switch nicht erreichbar (ocumEvtSwitchnicht erreichbar)	Vorfall	MetroCluster-Switch	Kritisch
Switch-Lüfter fehlgeschlagen (ocumEvtSwitchFansOneOrMoreFailed)	Vorfall	MetroCluster-Switch	Kritisch
Switch-Netzteile fehlgeschlagen (ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Vorfall	MetroCluster-Switch	Kritisch
Schalter Temperatursensoren fehlgeschlagen (OcumEvtSwitchTemperatursensordefekt) Dieses Ereignis gilt nur für Cisco Switches.	Vorfall	MetroCluster-Switch	Kritisch

NVMe Namespace-Ereignisse

NVMe Namespace Ereignisse liefern Ihnen Informationen zum Status Ihrer Namespaces, damit Sie ein Monitoring auf potenzielle Probleme ermöglichen. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Ein Sternchen (*) identifiziert EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
NVMe Offline *(nvmeNamespaceStatus Offline)	Ereignis	Namespace	Informationsdaten
NVMe Online * (nvmeNamespaceStatus Online)	Ereignis	Namespace	Informationsdaten
NVMe außerhalb des Speicherplatzes * (nvmeNamespaceSpace OutOfSpace)	Dar	Namespace	Warnung
NVMeNS Destroy * (nvmeNamespaceDestroy)	Ereignis	Namespace	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreiten des kritischen Schwellenwerts für NVMe-Namespace-IOPS (ocumNvmeNamespaceIopsVorfall)	Vorfall	Namespace	Kritisch
NVMe Namespace IOPS – Warnung nicht behebter Schwellenwert (ocumNvmeNamespaceIopsWarnung)	Dar	Namespace	Warnung
Unterschreitster kritischer Schwellenwert für NVMe-Namespace/MB/s (ocumNvmeNamespaceMbpsVorfall)	Vorfall	Namespace	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
NVMe Namespace MB/s – Warnung: Nicht überschritten (ocumNvmeNamespaceMbpsWarnung)	Dar	Namespace	Warnung
NVMe Namespace-Latenz ms/op Critical Threshold Undurchbrochen (ocumNvmeNamespeaceLatenturVorfall)	Vorfall	Namespace	Kritisch
NVMe Namespace-Latenz ms/op Warnschwellenwert nicht eingehalten (ocumNvmeNamespaceLatency – Warnung)	Dar	Namespace	Warnung
NVMe Namespace-Latenz und IOPS-kritischer Schwellenwert – nicht erreicht (ocumNvmeNamespaceLatenzenIopsVorfall)	Vorfall	Namespace	Kritisch
NVMe Namespace-Latenz und IOPS Warnschwellenwert nicht erreicht (ocumNvmeNamespaceLatentenzIopsWarnung)	Dar	Namespace	Warnung
NVMe Namespace-Latenz und Mbps Critical Threshold Rectorals (occumNvmeNamespeaceLatentenzMbpsVorfall)	Vorfall	Namespace	Kritisch
NVMe Namespace-Latenz und MB/s Warnschwellenwert nicht verwendet (ocumNvmeNamespaceLatentenzMbpsWarnung)	Dar	Namespace	Warnung

Node-Ereignisse

Node-Ereignisse bieten Ihnen Informationen zum Node-Status, sodass Sie Ihr System auf potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Ein Sternchen (*) identifiziert EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Node-Root-Volume-Speicherplatz fast voll (ocumEvtClusterNodeRootVolumeSpaceNearline)	Dar	Knoten	Warnung
Cloud AWS MetaDataConnFail * (ocumCloudAwsMetadataConnFail)	Dar	Knoten	Fehler
Cloud AWS IAMCredsExpired * (ocumCloudAwsIamCredsExpired)	Dar	Knoten	Fehler
Cloud AWS IAMCredsIngültig * (ocumCloudAwsIamCredsungültig)	Dar	Knoten	Fehler
Cloud AWS IAMCredsNotFound * (ocumCloudAwsIamCredsNotFound)	Dar	Knoten	Fehler
Cloud AWS IAMCredsNotinitialisiert * (ocumCloudAwsIamCredsNotinitialisiert)	Ereignis	Knoten	Informationsdaten
Cloud AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	Dar	Knoten	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Cloud AWS IAMRoleNotFound * (ocumCloudAwsIamRole NotFound)	Dar	Knoten	Fehler
Objstore Host unlösbar *(ocumObjstoreHostUnlösbar)	Dar	Knoten	Fehler
Objstore InterClusterLifDown *(ocumObjstoreInterClusterLifDown)	Dar	Knoten	Fehler
Signatur des Objektspeichers * anfordern	Dar	Knoten	Fehler
Einer der NFSv4 Pools ist erschöpft *	Vorfall	Knoten	Kritisch

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
QoS Monitor Memory maxed * (ocumQosMonitorMemory)	Dar	Knoten	Fehler
QoS Monitor Memory abited *(ocumQosMonitorMemoryAbed)	Ereignis	Knoten	Informationsdaten

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Knoten umbenannt(nicht zutreffend)	Ereignis	Knoten	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Nicht behebgter Node-IOPS-Schwellenwert (OktumNodeIopsVorfall)	Vorfall	Knoten	Kritisch
Nicht beIOPS-Warnungsschwellenwert (OktumNodeIopsWarnung)	Dar	Knoten	Warnung
Unterschreiten kritischen Schwellenwert für Node/MBit/s (ocumNodeMbpsVorfall)	Vorfall	Knoten	Kritisch
Node Mbps: Überschreitung des Warnungsschwellenwerts (OccumNodeMbpsWarnung)	Dar	Knoten	Warnung
Node-Latenz ms/op Critical Threshold undurchbrochen (OktumNodeLatenzIncident)	Vorfall	Knoten	Kritisch
Node-Latenz ms/op Warnschwellenwert nicht überschritten (OktumNodeLatenWarnung)	Dar	Knoten	Warnung
Node-Performance: Verwendete Kapazität – kritischer Schwellenwert überschritten (OktumNodePerftätVerwendungVorfall)	Vorfall	Knoten	Kritisch
Node-Performance: Verwendete Kapazität – Warnung: Nicht überschritten (OktumNodePerftätNutzungWarnung)	Dar	Knoten	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Verwendete Node-Kapazität – Überschreiten kritischer Schwellenwert (OktumNodePerformance-NutzungÜbernahmeVorfall)	Vorfall	Knoten	Kritisch
Verwendete Node-Kapazität – Überschreitung der Warnschwelle (überschritten mit OktumNodePerformance-FunktionNutzungÜbernahmeWarnung)	Dar	Knoten	Warnung
Unterschreitem kritischen Schwellenwert für die Node-Auslastung (OkumNodeUtilizationVorfall)	Vorfall	Knoten	Kritisch
Unterschreitr. Schwellenwert für Node-Auslastung (OkumNodeUtilizationWarnung)	Dar	Knoten	Warnung
Überlasteter Schwellenwert für Node-HA-Paar (OktumNodeHaPairOverUtilizedInformation)	Ereignis	Knoten	Informationsdaten
Unterschreitender Schwellenwert für die Node-Festplattenfragmentierung (ocumNodeDiskFragmentationWarnung)	Dar	Knoten	Warnung
Nicht genutzte Node-Schwelle überschritten (OktumNodeOverUtilizedWarnung)	Dar	Knoten	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Nicht behebener dynamischer Knotenschwellenwert (ocumNodeDynamicEventWarnung)	Dar	Knoten	Warnung

Ereignisse der NVRAM-Batterie

NVRAM-Batterieereignisse geben Ihnen Informationen zum Status Ihrer Akkus, sodass Sie auf mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
NVRAM-Batterie schwach(OktEvtNvraBatterienNiedrig)	Dar	Knoten	Warnung
Entladene NVRAM-Batterie (OktEvtNvramBatteryEntladung)	Dar	Knoten	Fehler
NVRAM-Batterie übermäßig geladen (OktEvtNvramBatteryÜberCharged)	Vorfall	Knoten	Kritisch

Port-Ereignisse

Port-Ereignisse bieten Ihnen den Status zu Cluster-Ports, sodass Sie Änderungen oder Probleme am Port überwachen können, z. B. ob der Port ausgefallen ist.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Port Status Down (ocumEvtPortStatusDown)	Vorfall	Knoten	Kritisch

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreitster Schwellenwert für Netzwerkport Mbps (ocumNetworkPortMbpsVorfall)	Vorfall	Port	Kritisch
Mbps-Warnung für Netzwerkanschluss, Überschreitung des Schwellenwerts (ocumNetworkPortMbpsWarnung)	Dar	Port	Warnung
Überschreitung kritischer Schwellenwert für FCP-Port/MB/s (ocumFcpPortMbpsVorfall)	Vorfall	Port	Kritisch
Warnung: Nicht verwendetes Warnschwellenwert für FCP-Port-Mbit/s (ocumFcpPortMbpsWarnung)	Dar	Port	Warnung
Auslastung des Netzwerkports – kritischer Schwellenwert – unterlaufen (NetzwerkPortUtilizationVorfall)	Vorfall	Port	Kritisch
Warnung über Netzwerk-Port-Auslastung, nicht überschritten (OktumNetzwerkPortUtilizationWarnung)	Dar	Port	Warnung
Unterschreitender Schwellenwert für die FCP-Port-Auslastung (ocumFcpPortUtilizationVorfall)	Vorfall	Port	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Warnung: Nicht gestauter Schwellenwert für die FCP-Port-Auslastung (ocumFcpPortUtilizationWarnung)	Dar	Port	Warnung

Netzteile

Netzteile liefern Ihnen Informationen über den Status Ihrer Hardware, sodass Sie Monitoring auf potenzielle Probleme ermöglichen. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Ein oder mehrere ausgefallene Netzteile (ocumEvtPowerSupplyOneOrMoreFailed)	Vorfall	Knoten	Kritisch

Schutzereignisse

Schutzereignisse geben an, ob ein Job ausgefallen ist oder abgebrochen wurde, damit Sie eine Überwachung auf Probleme durchführen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Schutzjob fehlgeschlagen (ocumEvtProtectionJobTaskFailed)	Vorfall	Volume oder Storage-Service	Kritisch
Schutzauftrag abgebrochen(OktaVerkündungSchutzJobAbgebrochen)	Dar	Volume oder Storage-Service	Warnung

Qtree Ereignisse

Qtree Events liefern Ihnen Informationen zur qtree Kapazität sowie Datei- und Festplattengrenzwerte, damit Sie potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Qtree Space nahezu vollständig (ocumEvtQtreeSpaceNearFull)	Dar	Qtree	Warnung
Qtree Space Full(ocumEvtQtreeSpaceFull)	Dar	Qtree	Fehler
Qtree Space normal(ocumEvtQtreeSpaceThresholdOk)	Ereignis	Qtree	Informationsdaten
Harte Grenze für qtree Dateien erreicht(ocumEvtQtreeDateienHardLimitReached)	Vorfall	Qtree	Kritisch
Qtree-Dateien Grenzverletzungen weichen(occumEvtQtreeDateienSoftLimitBreached)	Dar	Qtree	Warnung
Qtree Space Hard Limit erreicht(ocumEvtQtreeSpaceHardLimitReached)	Vorfall	Qtree	Kritisch
Qtree Space Soft Limit Procted (ocumEvtQtreeSpaceSoftLimitBreached)	Dar	Qtree	Warnung

Ereignisse des Service-Prozessors

Bei Service-Prozessor-Ereignissen erhalten Sie Informationen über den Status Ihres Prozessors. Diese Informationen können Sie auf potenzielle Probleme überwachen. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Service Processor nicht konfiguriert (ocumEvtServiceProcessorNotConfigured)	Dar	Knoten	Warnung
Service Processor Offline(ocumEvtServiceProcessorOffline)	Dar	Knoten	Fehler

SnapMirror Beziehungsereignisse

Informationen zum Status Ihrer SnapMirror Beziehungen erhalten Sie bei SnapMirror Beziehungsereignissen, sodass Sie mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Aufprallbereich: Schutz

Ein Sternchen (*) identifiziert EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Spiegelreplikation ungesund(occumEvtSnapmirrorRelationshipUnHealthy)	Dar	SnapMirror Beziehung	Warnung
Spiegelreplikation - broken-off(ocumEvtSnapmirrorRelationshipStateBrokenoff)	Dar	SnapMirror Beziehung	Fehler
Spiegelreplikation wird initialisiert fehlgeschlagen(OktEvtSnapmirrorRelationshipInitialisierenFailed)	Dar	SnapMirror Beziehung	Fehler
Aktualisierung der Spiegelreplikation fehlgeschlagen(ocumEvtSnapmirrorRelationshipUpdateFailed)	Dar	SnapMirror Beziehung	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Spiegelreplikation – Fehler (occumEvtSnapMirrorRelationshipLagerFehler)	Dar	SnapMirror Beziehung	Fehler
Spiegelreplikation Verzögerung Warnung(occumEvtSnapMirrorRelationshipLagerWarnung)	Dar	SnapMirror Beziehung	Warnung
Resync der Spiegelreplikation fehlgeschlagen(OccumEvtSnapmirrorRelationshipResyncFailed)	Dar	SnapMirror Beziehung	Fehler
Mirror Replication DeletedocumEvtSnapmirrorRelationship Deleted	Dar	SnapMirror Beziehung	Warnung
Synchrone Replizierung Aus Sync *	Dar	SnapMirror Beziehung	Warnung
Synchrone Replizierung Wiederhergestellt *	Ereignis	SnapMirror Beziehung	Informationsdaten
Fehler Beim Automatischen Neusynchronisierung Der Synchronen Replikation *	Dar	SnapMirror Beziehung	Fehler

Snapshot Ereignisse

Snapshot Ereignisse liefern Informationen zum Status von Snapshots, mit denen Sie die Snapshots auf potenzielle Probleme überwachen können. Die Ereignisse sind nach dem Impact-Bereich gruppiert und umfassen den Event-Namen, den Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Snapshot Auto-delete deaktiviert (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Automatische Löschung von Snapshot aktiviert (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Snapshot Auto-delete-Konfiguration geändert(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten

SnapVault Beziehungsereignisse

SnapVault Beziehungsveranstaltungen enthalten Informationen zum Status Ihrer SnapVault Beziehungen, sodass Sie mögliche Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Asynchronous Vault ungesund(OcumEvtSnapVaultRelationshipUnHealthy)	Dar	SnapMirror Beziehung	Warnung
Asynchronous Vault broken-off (ocumEvtSnapVaultRelationshipStateBrokenoff)	Dar	SnapMirror Beziehung	Fehler
Asynchrone Vault-Initialisierung fehlgeschlagen (OktEvtSnapVaultRelationshierInitialisierenFailed)	Dar	SnapMirror Beziehung	Fehler
Asynchrones Vault Update fehlgeschlagen (OktEvtSnapVaultRelationshipUpdateFailed)	Dar	SnapMirror Beziehung	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Asynchroner Vault lag Fehler (ocumEvtSnapVaultRelationshipLagerFehler)	Dar	SnapMirror Beziehung	Fehler
Asynchronous Vault lag Warnung (ocumEvtSnapVaultRelationshipLagerWarnung)	Dar	SnapMirror Beziehung	Warnung
Resync für asynchronen Tresor fehlgeschlagen (ocumEvtsnapvaultRelationshipResyncFailed)	Dar	SnapMirror Beziehung	Fehler

Ereignisse auf Storage-Failover-Einstellungen

Ereignisse im Rahmen der Storage-Failover-Einstellungen (SFO) informieren Sie darüber, ob Ihr Storage-Failover deaktiviert oder nicht konfiguriert ist, damit Sie das System auf potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Storage Failover Interconnect eine oder mehrere Links nach unten (OktEvtSfoVerbindungsOneOrMehrLinksDown)	Dar	Knoten	Warnung
Storage Failover deaktiviert(ocumEvtSfoSettingsdeaktiviert)	Dar	Knoten	Fehler
Storage-Failover nicht konfiguriert(ocumEvtSfoSettingsNotConfigured)	Dar	Knoten	Fehler
Storage-Failover-Status – Übernahme (OktEvtSfoStateTakeover)	Dar	Knoten	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Storage Failover State - Partial GiveBack(ocumEvtSfoStatePartialGiveBack)	Dar	Knoten	Fehler
Storage Failover Node Status Down (ocumEvtSfoNodeStatusDown)	Dar	Knoten	Fehler
Storage-Failover-Übernahme nicht möglich (OktEvtSfoÜbernahmemöglich)	Dar	Knoten	Fehler

Ereignisse auf Storage-Services

Bei Storage-Services-Ereignissen erhalten Sie Informationen über die Erstellung und das Abonnement von Storage-Services, sodass Sie potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Storage-Service erstellt(nicht zutreffend)	Ereignis	Storage-Service	Informationsdaten
Storage Service abonniert (nicht zutreffend)	Ereignis	Storage-Service	Informationsdaten
Storage Service nicht abonniert (nicht zutreffend)	Ereignis	Storage-Service	Informationsdaten

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unerwartetes Löschen von Managed SnapMirror RelationshipokumEvtStorageServiceUnsupportedRelationshipDeltion	Dar	Storage-Service	Warnung
Unerwartetes Löschen von Storage Service Member Volume(occumEvtStorageServiceUnexpectedVolumeDeltion)	Vorfall	Storage-Service	Kritisch

Storage-Shelf-Ereignisse

Storage Shelf-Ereignisse geben an, ob Ihr Storage Shelf anormal ist, sodass Sie nach potenziellen Problemen überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Anormaler Spannungsbereich (ocumEvtShelfVoltageAbnormal)	Dar	Storage Shelf	Warnung
Anormaler Strombereich (ocumEvtShelfAktuellesAbnormal)	Dar	Storage Shelf	Warnung
Anormale Temperatur(OkumEvtShelfTemperatureAbnormal)	Dar	Storage Shelf	Warnung

SVM-Ereignisse

SVM-Ereignisse liefern Ihnen Informationen zum Status Ihrer SVMs. So können Sie das System auf potenzielle Probleme überwachen. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Verfügbarkeit

Ein Sternchen (*) identifiziert EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
SVM CIFS Service-Down(ocumEvtVserverCifsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM CIFS-Service nicht konfiguriert (nicht zutreffend)	Ereignis	SVM	Informationsdaten
Versucht, eine nicht existierende CIFS-Freigabe * zu verbinden	Vorfall	SVM	Kritisch
CIFS NetBIOS Namenskonflikt *	Dar	SVM	Fehler
Fehler beim CIFS Shadow Copy-Vorgang *	Dar	SVM	Fehler
Viele CIFS-Verbindungen *	Dar	SVM	Fehler
Die max. CIFS-Verbindung wurde überschritten *	Dar	SVM	Fehler
Max. Anzahl der CIFS-Verbindung pro Benutzer überschritten *	Dar	SVM	Fehler
SVM FC/FCoE Service-Down (ocumEvtVserverFcServiceStatusDown)	Vorfall	SVM	Kritisch
SVM iSCSI Service-Down(ocumEvtVserverIscsiServiceStatusDown)	Vorfall	SVM	Kritisch
SVM NFS-Service-Down (ocumEvtVserverNfsServiceStatusDown)	Vorfall	SVM	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
SVM FC/FCoE-Service nicht konfiguriert (nicht zutreffend)	Ereignis	SVM	Informationsdaten
SVM iSCSI-Service nicht konfiguriert (nicht zutreffend)	Ereignis	SVM	Informationsdaten
SVM NFS-Service nicht konfiguriert (nicht zutreffend)	Ereignis	SVM	Informationsdaten
SVM angehalten(ocumEvtVserverDown)	Dar	SVM	Warnung
AV-Server zu beschäftigt, um neue Scananforderung zu akzeptieren *	Dar	SVM	Fehler
Keine AV-Server-Verbindung für Virus Scan *	Vorfall	SVM	Kritisch
Kein AV-Server registriert *	Dar	SVM	Fehler
Keine Responsive AV-Serververbindung *	Ereignis	SVM	Informationsdaten
Nicht autorisierter Benutzer versucht AV-Server *	Dar	SVM	Fehler
Virus von AV Server gefunden *	Dar	SVM	Fehler
SVM mit Infinite Volume Storage nicht verfügbar (ocumEvtVserverStorageUnverfügbar)	Vorfall	SVMs mit Infinite Volume	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
SVM mit Infinite Volume Storage teilweise verfügbar(ocumEvtVserverStoragePartiallyverfügbar)	Dar	SVMs mit Infinite Volume	Fehler
SVM mit Infinite Volume Namespace Mirror Komponenten mit Verfügbarkeitsproblemen (occumEvtVserverNsMirrorVerfügbarkeitHavingIssues)	Dar	SVMs mit Infinite Volume	Warnung

Impact Area: Kapazität

Die folgenden Kapazitätsereignisse gelten nur für SVMs mit Infinite Volume.

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
SVM mit Infinite Volume Space Full (ocumEvtVserverFull)	Dar	SVM	Fehler
SVM mit Infinite Volume nahezu voll (ocumEvtVserverNearsFull)	Dar	SVM	Warnung
SVM mit Infinite Volume Snapshot Nutzungslimit überschritten (ocumEvtVserverSnapshotUsageExceped)	Dar	SVM	Warnung
SVM mit Infinite Volume Namespace voll (ocumEvtVserverNamespaceFull)	Dar	SVM	Fehler
SVM mit Infinite Volume Namespace fast voll (ocumEvtVserverNamespaceNearyFull)	Dar	SVM	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
SVM erkannt (nicht zutreffend)	Ereignis	SVM	Informationsdaten
SVM gelöscht (nicht zutreffend)	Ereignis	Cluster	Informationsdaten
SVM umbenannt (nicht zutreffend)	Ereignis	SVM	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreitkter SVM-IOPS-Schwellenwert (OktumSvmIopsVorfall)	Vorfall	SVM	Kritisch
Unterschreiten SVM-IOPS-Warnungsschwellenwert (ocumSvmIopsWarnung)	Dar	SVM	Warnung
Unterschreitkter SVM/s-Schwellenwert (ocumSvmMbpsVorfall)	Vorfall	SVM	Kritisch
Unterschreitenter SVM/s-Warnungsschwellenwert (ocumSvmMbpsWarnung)	Dar	SVM	Warnung
Unterschreiten kritischen Schwellenwert für SVM-Latenz (ocumSvmLatencyVorfall)	Vorfall	SVM	Kritisch
Unterschreitung – SVM-Latenzschwellenwert (ocumSvmLatencyWarnung)	Dar	SVM	Warnung

Ereignisse der SVM Storage-Klasse

SVM Storage-Klassenveranstaltungen versorgen Sie mit Informationen zum Status Ihrer Storage-Klassen. So können Sie auf mögliche Probleme überwachen. SVM-Storage-

Klassen sind nur in SVMs mit Infinite Volume vorhanden. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Die folgenden SVM Storage-Ereignisse gelten nur für SVMs mit Infinite Volume.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
SVM Storage Class nicht verfügbar(ocumEvtVserverStorageClassNoverfügbar)	Vorfall	Storage-Klasse	Kritisch
SVM Storage Class teilweise verfügbar(ocumEvtVserverStorageClassPartiallyverfügbar)	Dar	Storage-Klasse	Fehler

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
SVM Storage Class Space nahezu voll(ocumEvtVserverStorageClassNearFull)	Dar	Storage-Klasse	Warnung
SVM Storage Class Space Full(ocumEvtVserverStorageClassFull)	Dar	Storage-Klasse	Fehler
Snapshot-Nutzungsgrenze für SVM Storage-Klasse überschritten (ocumEvtVserverStorageClassSnapshotUsageExceped)	Dar	Storage-Klasse	Warnung

Ereignisse für Benutzer- und Gruppenkontingente

Benutzer- und Gruppenkontingente liefern Ihnen Informationen über die Kapazität des Benutzer- und Benutzergruppenkontingens sowie über die Datei- und Festplattenlimits, damit Sie potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area

gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
User- oder Group Quota Disk Space Soft Limit Proceed (ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Dar	Benutzer- oder Gruppenkontingente	Warnung
Hard Limit für User- oder Group Quota Disk Space (ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingente	Kritisch
Anzahl der Benutzer- oder Gruppenkontingente-Dateien weiche Grenze überschritten (ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Dar	Benutzer- oder Gruppenkontingente	Warnung
Benutzer- oder Gruppenkontingente Dateianzahl harte Grenze erreicht(ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingente	Kritisch

Volume-Ereignisse

Volume-Ereignisse liefern Informationen zum Status von Volumes, mit denen Sie auf potenzielle Probleme überwachen können. Die Ereignisse sind nach dem Impact-Bereich gruppiert und umfassen den Event-Namen, den Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Ein Sternchen (*) identifiziert EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volumenbeschränkungen (occumEvtVolumeRestricted)	Dar	Datenmenge	Warnung
Volume Offline(ocumEvtVolumeOffline)	Vorfall	Datenmenge	Kritisch
Datenträger teilweise verfügbar(occumEvtVolumePartiallyverfügbar)	Dar	Datenmenge	Fehler
Volumen abgehängt (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume angehängt(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume neu eingebunden (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume Junction Path Inaktiv (ocumEvtVolumeJunctionPathInaktiv)	Dar	Datenmenge	Warnung
Automatische Volumengröße aktiviert (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Automatische Volume-Größe deaktiviert (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Automatische Volumengröße maximale Kapazität geändert(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Größe der automatischen Volume-Größe geändert (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume-Speicherplatz mit Thin Provisioning (ozumThinProvisionVolumeSpaceAtFestplatten)	Dar	Datenmenge	Warnung
Voll Volume-Speicherplatz(occumEvtVolumeFull)	Dar	Datenmenge	Fehler
Volume fast voll (ocumEvtVolumeNearline)	Dar	Datenmenge	Warnung
Logischer Speicherplatz des Volume voll * (VolumeLogicalSpaceFull)	Dar	Datenmenge	Fehler
Logischer Speicherplatz des Volume fast voll * (VolumeLogicalSpaceNearlyFull)	Dar	Datenmenge	Warnung
Logischer Speicherplatz des Volume normal *(VolumeLogicalSpaceAllOK)	Ereignis	Datenmenge	Informationsdaten
Volume Snapshot Reserve voll(ocumEvtSnapshotvoll)	Dar	Datenmenge	Warnung
Zu viele Snapshot-Kopien (ocumEvtSnapshotTooManche)	Dar	Datenmenge	Fehler
Volume Qtree Kontingent überengagiert (occumEvtVolumeQtreeQuotaÜberengagiert)	Dar	Datenmenge	Fehler
Volume Qtree Kontingent fast überengagiert (ocumEvtVolumeQtreeQuotaAlmostÜberengagiert)	Dar	Datenmenge	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volumenwachstumsrate anormal (ocumEvtVolumeGrowth RowthRateAbnormal)	Dar	Datenmenge	Warnung
Volume-Tage bis voll (ocumEvtVolumeTagesUntilFullSoon)	Dar	Datenmenge	Fehler
Volume Space Guarantee deaktiviert(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume-Space-Garantie Aktiviert (Nicht Zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume-Space-Garantie geändert(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume Snapshot Reserve – Tage bis voll (ocumEvtVolumeSnapshotReserviertDaysUntilFullSoon)	Dar	Datenmenge	Fehler
FlexGroup-Komponenten haben Raumprobleme *(FlexGroupInhaltHaveSpaceIssues)	Dar	Datenmenge	Fehler
FlexGroup-Komponenten Raumstatus alles OK *(flexGruppeKonstitelenSpaceStatusAllOK)	Ereignis	Datenmenge	Informationsdaten
FlexGroup-Bestandteile haben Inodes-Probleme *(flexGroupKonstitutionen HaveInodesIssues)	Dar	Datenmenge	Fehler
FlexGroup-Komponenten inodes Status alles OK *(flexGroupConstitutionen InodesStatusAllOK)	Ereignis	Datenmenge	Informationsdaten

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Fehler bei der automatischen WAFL-Volume-Größe *	Dar	Datenmenge	Fehler
Automatische WAFL-Volume-Größe abgeschlossen *	Ereignis	Datenmenge	Informationsdaten

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volumen umbenannt(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Ermittelte Volumes (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume gelöscht (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
QoS Volume Max. IOPS Warnschwellenwert nicht erreicht (ocumQosVolumeMaxIopsWarnung)	Dar	Datenmenge	Warnung
QoS Volume Max Mbps Warnungsschwellenwert überschritten (ocumQosVolumeMaxMbpsWarnung)	Dar	Datenmenge	Warnung
QoS Volume Max. IOPS/TB Warnschwellenwert nicht erreicht (ocumQosVolumeMaxIopsPerTbWarnung)	Dar	Datenmenge	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreiten des kritischen Schwellenwerts für Volume-IOPS (OktumVolumeIopsVorfall)	Vorfall	Datenmenge	Kritisch
Unterschreitr. Volume IOPS-Warnungsschwellenwert (ocumVolumeIopsWarnung)	Dar	Datenmenge	Warnung
Unterschreiten kritischen Schwellenwert für Volume-MB/s (ocumVolumeMbpsVorfall)	Vorfall	Datenmenge	Kritisch
Volume Mbps Warnungsschwellenwert überschritten (ocumVolumeMbpsWarnung)	Dar	Datenmenge	Warnung
Volume-Latenz ms/op kritischer Schwellenwert – nicht überschritten (OktumVolumeLatenVorfall)	Vorfall	Datenmenge	Kritisch
Volume-Latenz ms/op Warnungsschwellenwert nicht überschritten (ocumVolumeLatencyWarnung)	Dar	Datenmenge	Warnung
Volume Cache Miss-Verhältnis – kritischer Schwellenwert überschritten (ocumVolumeCacheMissRatioVorfall)	Vorfall	Datenmenge	Kritisch
Volume Cache Miss Ratio Warnung nicht überschritten (ocumVolumeCacheMissRatioWarnung)	Dar	Datenmenge	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume-Latenz und IOPS – kritischer Schwellenwert – nicht erreicht (ocumVolumeLatencyIops Vorfall)	Vorfall	Datenmenge	Kritisch
Nicht erreichender Volume-Latenz und IOPS -Warnungsschwellenwert (ocumVolumeLatencyIops Warnung)	Dar	Datenmenge	Warnung
Nicht erreichender Volume-Latenz und MB/s-kritischer Schwellenwert (ocumVolumeLatencyMbpsVorfall)	Vorfall	Datenmenge	Kritisch
Nicht erreichender Volume-Latenz und MB/s-Warnungsschwellenwert (ocumVolumeLatencyMbpsWarnung)	Dar	Datenmenge	Warnung
Volume-Latenz und aggregierte Performance Verwendete Kapazität – kritischer Schwellenwert nicht erreicht (ocumVolumeLatencyAggregatePerfkapazitätUsedVorfall)	Vorfall	Datenmenge	Kritisch
Volume-Latenz und aggregierte Performance Verwendete Kapazität – Warnung: Nicht erreichter Schwellenwert (ocumVolumeLatencyAggregatePerfkapazitätUsed Warnung)	Dar	Datenmenge	Warnung
Volume-Latenz und aggregierte Auslastung kritischer Schwellenwert überschritten (ocumVolumeLatenAggregateUtilizationVorfall)	Vorfall	Datenmenge	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume-Latenz und Aggregatauslastung Warnschwellenwert nicht erreicht (ocumVolumeLatenAggregateUtilizationWarnung)	Dar	Datenmenge	Warnung
Volume-Latenz und Node-Performance: Verwendete Kapazität – kritischer Schwellenwert nicht erreicht (ocumVolumeLatencyNodePerfkapazitätBenutzerfall)	Vorfall	Datenmenge	Kritisch
Volume-Latenz und Node-Performance: Verwendete Kapazität – Warnung: Nicht erreichter Schwellenwert (ocumVolumeLatencyNodePerformance-FunktionenWarnung)	Dar	Datenmenge	Warnung
Volume-Latenz und Node-Performance: Verwendete Kapazität – Übernahme kritischer Schwellenwert verletzt (ocumVolumeLatencyAggregatePerfkapazitätUseTakeoverVorfall)	Vorfall	Datenmenge	Kritisch
Volume-Latenz und Node-Performance: Verwendete Kapazität – Überschreitung der Schwellenberührte Überschreitung (VolumeLatencyAggregatePerfkapazitätUseTakeoverWarning)	Dar	Datenmenge	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume-Latenz und Node-Auslastung – kritischer Schwellenwert – nicht erreicht (ocumVolumeLatencyNotilationVorfall)	Vorfall	Datenmenge	Kritisch
Nicht erreichender Schwellenwert für Volume-Latenz und Node-Auslastung (ocumVolumeLatencyNodeUtilizationWarnung)	Dar	Datenmenge	Warnung

Statusereignisse für Volume-Verschiebung

Status-Events zur Volume-Verschiebung informieren Sie über den Status Ihrer Volume-Verschiebung, sodass Sie Ihr System auf potenzielle Probleme überwachen können. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Status der Volume-Verschiebung: In Bearbeitung (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Status der Volume-Verschiebung – fehlgeschlagen (OktEvtVolumeMoveFailed)	Dar	Datenmenge	Fehler
Status der Volume-Verschiebung: Abgeschlossen (nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten
Volume-Verschiebung - zurückgeschobener Umstieg (OktEvtVolumeMoveCustoverDeferred)	Dar	Datenmenge	Warnung

Beschreibung der Ereignisfenster und Dialogfelder

Ereignisse informieren Sie über Probleme in Ihrer Umgebung. Sie können die Seite „Ereignisinventar“ und die Seite „Ereignisdetails“ verwenden, um alle Ereignisse zu überwachen. Über das Dialogfeld „Benachrichtigungseinstellungen“ können Sie Benachrichtigungen konfigurieren. Über die Seite „Ereignisse konfigurieren/managen“ können Ereignisse deaktiviert oder aktiviert werden.

Dialogfeld „Einstellungen für die Ereignisaufbewahrung“

Sie können die Ereigniseinstellungen so konfigurieren, dass Ereignisse (Informationen, aufgelöst oder veraltet) nach einer bestimmten Zeit und zu einer bestimmten Frequenz automatisch gelöscht werden. Sie können diese Ereignisse auch manuell löschen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Ereigniseinstellungen

Sie können die folgenden Optionen konfigurieren:

- **Löschen von Informationen, gelösten und veralteten Ereignissen, die älter sind als**

  Hiermit können Sie den Aufbewahrungszeitraum festlegen, nach dem Ereignisse, die als Information, Lösung oder veraltet markiert sind, vom Verwaltungsserver entfernt werden.

  Der Standardwert ist 180 Tage. Die Aufbewahrung der Ereignisse über mehr als 180 Tage wirkt sich auf die Leistung aus und wird nicht empfohlen. Die untere Grenze für die Ereignisaufbewahrungsdauer beträgt 7 Tage, obwohl es keine Obergrenze gibt.

- **Zeitplan Löschen**

  Hiermit können Sie festlegen, wie oft alle Ereignisse, die als Information, Lösung oder veraltet markiert sind und deren Altersgrenze überschritten wurde, automatisch vom Verwaltungsserver gelöscht werden. Die möglichen Werte sind „Daily“, „Weekly“ oder „Monthly“.

  Der Standardwert ist Daily.

- **Jetzt Löschen**

  Ermöglicht Ihnen das manuelle Löschen aller Informationen, gelösten und veralteten Ereignisse, die den angegebenen Aufbewahrungszeitraum überschritten haben.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die Setup-Optionen speichern oder abbrechen:

- **Speichern und Schließen**

  Speichert die Konfigurationseinstellungen für die ausgewählte Option und schließt das Dialogfeld.

- **Abbrechen**

  Bricht die letzten Änderungen ab und schließt das Dialogfeld.

Setup-/Benachrichtigungsseite

Sie können den Unified Manager-Server so konfigurieren, dass Benachrichtigungen gesendet werden, wenn ein Ereignis generiert wird oder wenn es einem Benutzer zugewiesen ist. Sie können auch die Benachrichtigungsmechanismen konfigurieren. Benachrichtigungen können beispielsweise als E-Mails oder SNMP-Traps gesendet werden.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

E-Mail

In diesem Bereich können Sie die folgenden E-Mail-Einstellungen für die Benachrichtigung von Warnmeldungen konfigurieren:

- * Von Adresse*

  Gibt die E-Mail-Adresse an, von der die Benachrichtigung gesendet wird. Dieser Wert wird auch als „von“-Adresse für einen Bericht verwendet, wenn er freigegeben wird. Wenn die von-Adresse mit der Adresse „`OnCommand@localhost.com`“ ausgefüllt ist, sollten Sie sie in eine echte, funktionierende E-Mail-Adresse ändern, um sicherzustellen, dass alle E-Mail-Benachrichtigungen erfolgreich versendet werden.

SMTP-Server

In diesem Bereich können Sie die folgenden SMTP-Servereinstellungen konfigurieren:

- **Hostname oder IP-Adresse**

  Gibt den Hostnamen Ihres SMTP-Hostservers an, der dazu verwendet wird, die Benachrichtigung an die angegebenen Empfänger zu senden.

- **Benutzername**

  Gibt den SMTP-Benutzernamen an. SMTP-Benutzername ist nur erforderlich, wenn der SMTPAUTH auf dem SMTP-Server aktiviert ist.

- **Passwort**

  Gibt das SMTP-Passwort an. SMTP-Benutzername ist nur erforderlich, wenn der SMTPAUTH auf dem SMTP-Server aktiviert ist.

- **Port**

  Gibt den Port an, der vom SMTP-Hostserver zum Senden von Warnmeldungen verwendet wird.

  Der Standardwert ist 25.

- **Verwenden Sie STARTTLS**

  Durch Aktivieren dieses Kontrollkästchens wird eine sichere Kommunikation zwischen dem SMTP-Server und dem Verwaltungsserver mithilfe der TLS/SSL-Protokolle (auch als Start_tls und StartTLS bezeichnet) ermöglicht.

- * Verwenden Sie SSL*

Durch Aktivieren dieses Kontrollkästchens wird eine sichere Kommunikation zwischen dem SMTP-Server und dem Verwaltungsserver mithilfe des SSL-Protokolls ermöglicht.

SNMP

In diesem Bereich können Sie die folgenden SNMP-Trap-Einstellungen konfigurieren:

- **Version**

  Gibt die SNMP-Version an, die Sie je nach Art der erforderlichen Sicherheit verwenden möchten. Die Optionen umfassen Version 1, Version 3, Version 3 mit Authentifizierung und Version 3 mit Authentifizierung und Verschlüsselung. Der Standardwert ist Version 1.

- **Trap Destination Host**

  Gibt den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) an, die die vom Verwaltungsserver gesendeten SNMP-Traps empfängt.

- * Ausgebundener Trap Port*

  Gibt den Port an, über den der SNMP-Server die Traps empfängt, die vom Verwaltungsserver gesendet werden.

  Der Standardwert ist 162.

- **Gemeinschaft**

  Die Community-Zeichenfolge für den Zugriff auf den Host.

- **Motor-ID**

  Gibt die eindeutige Kennung des SNMP-Agenten an und wird automatisch vom Verwaltungsserver generiert. Die Engine-ID ist verfügbar mit SNMP Version 3, SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung.

- **Benutzername**

  Gibt den SNMP-Benutzernamen an. Benutzername ist verfügbar mit SNMP Version 3, SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung.

- **Authentifizierungsprotokoll**

  Gibt das Protokoll an, das zur Authentifizierung eines Benutzers verwendet wird. Die Protokolloptionen umfassen MD5 und SHA. MD5 ist der Standardwert. Das Authentifizierungsprotokoll ist verfügbar mit SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung.

- **Authentifizierungskennwort**

  Gibt das Passwort an, das bei der Authentifizierung eines Benutzers verwendet wird. Authentifizierungspasswort ist verfügbar mit SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung.

- **Datenschutzprotokoll**

  Gibt das Datenschutzprotokoll an, das zur Verschlüsselung von SNMP-Nachrichten verwendet wird. Die

Protokolloptionen umfassen AES 128 und DES. Der Standardwert ist AES 128. Das Datenschutzprotokoll ist mit SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Datenschutzkennwort**

  Gibt das Passwort an, wenn das Datenschutzprotokoll verwendet wird. Das Passwort für den Datenschutz ist mit SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

Seite „Ereignisinventar“

Auf der Seite „Ereignisinventar“ können Sie eine Liste der aktuellen Ereignisse und ihrer Eigenschaften anzeigen. Sie können Aufgaben wie Quittieren, Auflösen und Zuweisen von Ereignissen durchführen. Sie können auch eine Warnung zu bestimmten Ereignissen hinzufügen.

Standardmäßig werden die Informationen auf dieser Seite alle 5 Minuten automatisch aktualisiert, um sicherzustellen, dass die aktuellen neuen Ereignisse angezeigt werden.

Komponenten filtern

Hier können Sie die in der Ereignisliste angezeigten Informationen anpassen. Sie können die Liste der Ereignisse, die mit den folgenden Komponenten angezeigt werden, verfeinern:

- Menü Ansicht zur Auswahl aus einer vordefinierten Liste von Filterauswahlen.

  Dazu gehören beispielsweise alle aktiven (neuen und bestätigten) Ereignisse, aktive Performanceereignisse, mir zugewiesene Ereignisse (der angemeldete Benutzer) und alle während aller Wartungsfenster generierten Ereignisse.

- Suchbereich zum Verfeinern der Liste der Ereignisse durch Eingabe vollständiger oder teilweiser Begriffe.
- Die Filterschaltfläche öffnet den Fensterbereich Filter, sodass Sie aus jedem verfügbaren Feld und Feldattribut auswählen können, um die Ereignisliste zu verfeinern.
- Zeitauswahl zur Verfeinerung der Ereignisliste um den Zeitpunkt, an dem das Ereignis ausgelöst wurde.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Zuweisen Zu**

  Hiermit können Sie den Benutzer auswählen, dem das Ereignis zugeordnet ist. Wenn Sie einem Benutzer ein Ereignis zuweisen, werden der Benutzername und die Uhrzeit, zu der Sie das Ereignis zugewiesen haben, in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt.

  - Ich

    Weist das Ereignis dem derzeit angemeldeten Benutzer zu.

  - Einem anderen Benutzer

    Zeigt das Dialogfeld „Eigentümer zuweisen“ an, in dem Sie das Ereignis anderen Benutzern zuweisen oder neu zuweisen können. Sie können auch die Zuweisung von Ereignissen aufheben, indem Sie das Feld Eigentumsrechte leer lassen.

- * Quittieren*

  Bestätigt die ausgewählten Ereignisse.

  Wenn Sie ein Ereignis bestätigen, werden Ihr Benutzername und die Uhrzeit, zu der Sie das Ereignis bestätigt haben, in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt. Wenn Sie ein Ereignis bestätigen, sind Sie für die Verwaltung dieses Ereignisses verantwortlich.

  Sie können keine Informationsereignisse bestätigen.

- **Als Gelöst Markieren**

  Ermöglicht Ihnen die Änderung des Ereignisstatus in „gelöst“.

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

- **Alarm Hinzufügen**

  Zeigt das Dialogfeld Alarm hinzufügen an, in dem Sie Warnmeldungen für die ausgewählten Ereignisse hinzufügen können.

- **Export**

  Ermöglicht das Exportieren von Details aller Ereignisse in kommagetrennte Werte (`.csv`) Datei.

- **Spaltenauswahl**

  Hier können Sie die Spalten auswählen, die auf der Seite angezeigt werden, und die Reihenfolge auswählen, in der sie angezeigt werden.

Ereignisliste

Zeigt Details zu allen Ereignissen an, die nach ausgelöster Zeit geordnet sind.

Standardmäßig werden neue und bestätigte Ereignisse für die letzten sieben Tage des Schweregrads kritisch, Fehler und Warnung angezeigt.

- **Auslösezeit**

  Die Zeit, zu der das Ereignis generiert wurde.

- **Severity**

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

- **Bundesland**

  Der Ereignisstatus: Neu, bestätigt, aufgelöst oder veraltet.

- **Impact Level**

  Die Ereigniseinwirkung: Vorfall, Risiko oder Ereignis.

- **Aufprallbereich**

  Die Auswirkung auf das Ereignis: Verfügbarkeit, Kapazität, Performance, Schutz oder Konfiguration.

- **Name**

  Der Ereignisname.

  Sie können den Ereignisnamen auswählen, um die Seite Ereignisdetails anzuzeigen.

- **Quelle**

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

  Wenn eine Richtlinienverletzung bei Shared QoS auftritt, wird in diesem Feld nur das Workload-Objekt angezeigt, das die meisten IOPS oder MB/s verbraucht. Weitere Workloads, die diese Richtlinie verwenden, werden auf der Seite Ereignisdetails angezeigt.

  Sie können den Quellnamen auswählen, um die Seite für den Systemzustand oder die Performance-Details für das Objekt anzuzeigen.

- **Quelltyp**

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

- * Zugewiesen Zu*

  Der Name des Benutzers, dem das Ereignis zugeordnet ist.

- **Hinweise**

  Die Anzahl der Notizen, die für ein Ereignis hinzugefügt werden.

- **Tage Herausragend**

  Die Anzahl der Tage seit der ersten Erzeugung des Ereignisses.

- **Zugewiesene Zeit**

  Die Zeit, die seit der Zuweisung des Ereignisses an einen Benutzer verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, zu dem das Ereignis einem Benutzer zugewiesen wurde.

- * Bestätigt Durch*

  Der Name des Benutzers, der das Ereignis bestätigt hat. Das Feld ist leer, wenn das Ereignis nicht bestätigt wird.

- * Quittierte Zeit*

  Die Zeit, die seit dem Ereignis vergangen ist, wurde bestätigt. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, zu dem das Ereignis bestätigt wurde.

- * Gelöst Von*

  Der Name des Benutzers, der das Ereignis aufgelöst hat. Das Feld ist leer, wenn das Ereignis nicht

aufgelöst wird.

- * Zeit Gelöst*

  Die Zeit, die seit der Behebung des Ereignisses abgelaufen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, zu dem das Ereignis aufgelöst wurde.

- **Veraltete Zeit**

  Die Zeit, in der der Zustand des Ereignisses obsolet wurde.

Seite mit den Veranstaltungsdetails

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

- **Name Des Events**

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

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

- **Veranstaltungsbeschreibung**

  Eine kurze Beschreibung der Veranstaltung.

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

- **Komponente in Konflikt**

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

  Die folgenden Komponenten können angezeigt werden:

  - **Netzwerk**

    Zeigt die Wartezeit von I/O-Anfragen durch iSCSI-Protokolle oder Fibre Channel-Protokollen (FC) des Clusters an. Die Wartezeit liegt darin, auf die Transaktionen „iSCSI Ready to Transfer“ (R2T) oder „FCP Transfer Ready“ (XFER_RDY) zu warten, bis der Cluster auf eine I/O-Anforderung antworten kann. Wenn die Netzwerkkomponente unter einem Konflikt steht, bedeutet dies, dass hohe Wartezeiten auf der Protokollebene des Blocks die Latenz eines oder mehrerer Workloads beeinflussen.

  - * Netzwerkverarbeitung*

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

Auslastung des Node zur Netzwerkverarbeitung die Latenz eines oder mehrerer Workloads beeinträchtigt.

- **QoS-Richtlinie**

  Steht für die Storage-Richtliniengruppe für Quality of Service (QoS), der Mitglied des Workloads ist Wenn die Richtliniengruppe Konflikte hat, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch das festgelegte Durchsatzlimit gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- * Cluster Interconnect*

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

- **Datenverarbeitung**

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

- **MetroCluster Ressourcen**

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

- **Aggregate oder SSD Aggregate Ops**

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

- **Cloud-Latenz**

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

- **Sync SnapMirror**

  Repräsentiert die Software-Komponente in dem Cluster, die mit der Replizierung von Benutzerdaten vom primären Volume auf das sekundäre Volume in einer SnapMirror Synchronous-Beziehung beteiligt ist Wenn die synchrone SnapMirror Komponente Konflikte verursacht, bedeutet dies, dass die

Aktivitäten des synchronen Betriebs von SnapMirror sich auf die Latenz eines oder mehrerer Workloads auswirken.

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

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Notizen-Symbol**

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

Aktionen Menü

- **Mir zuweisen**

  Weist Ihnen das Ereignis zu.

- **Anderen zuweisen**

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

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

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

- * Quittieren*

  Bestätigt die ausgewählten Ereignisse, damit Sie keine Wiederholungsbenachrichtigungen erhalten.

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

- **Als Gelöst Markieren**

  Ermöglicht Ihnen die Änderung des Ereignisstatus in „gelöst“.

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

- **Alarm Hinzufügen**

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

Das wird im Abschnitt „Ereignisinformationen“ angezeigt

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

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

- **Ereignis Trigger Zeit**

  Die Zeit, zu der das Ereignis generiert wurde.

- **Bundesland**

  Der Ereignisstatus: Neu, bestätigt, aufgelöst oder veraltet.

- **Veraltete Ursache**

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

- **Veranstaltungsdauer**

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

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

- **Zuletzt Gesehen**

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

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

- **Severity**

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

- **Impact Level**

  Die Ereigniseinwirkung: Vorfall, Risiko oder Ereignis.

- **Aufprallbereich**

  Die Auswirkung auf das Ereignis: Verfügbarkeit, Kapazität, Performance, Schutz oder Konfiguration.

- **Quelle**

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

  Wenn sich die Details zu einem Ereignis für eine Shared QoS-Richtlinie anzeigen lassen, werden in

diesem Feld bis zu drei Workload-Objekte aufgeführt, die die meisten IOPS oder MB/s verbrauchen.

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

- **Quellanmerkungen**

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

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

- **Quellgruppen**

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

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

- **Quelltyp**

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

- * Auf Cluster*

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

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

- **Betroffene Objekte Zählen**

  Die Anzahl der vom Ereignis betroffenen Objekte.

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

  Dieses Feld wird nur für Performanceereignisse angezeigt.

- * Betroffene Volumen*

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

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

- * Ausgelöste Richtlinie*

  Der Name der Schwellenwertrichtlinie, die das Ereignis ausgegeben hat.

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

  Dieses Feld wird nur für Performanceereignisse angezeigt.

- * Bestätigt durch*

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

- * Gelöst von*

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

- * Zugewiesen zu*

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

- **Warnmeldungseinstellungen**

  Die folgenden Informationen über Meldungen werden angezeigt:

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

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

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

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

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

    Sie können die Seite Konfiguration/Warnmeldungen öffnen, indem Sie auf den Link klicken, um weitere Details zu diesen Warnmeldungen anzuzeigen.

  Deaktivierte Warnmeldungen werden nicht angezeigt.

- **Letzte Benachrichtigung Gesendet**

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

- **Gesendet Über**

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

- **Vorherige Skriptausführung**

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

Anzeigen des Abschnitts Systemdiagnose

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

Dieser Bereich wird nur für bestimmte Ereignisse angezeigt.

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

Für dynamische Performance-Ereignisse werden die folgenden Diagramme angezeigt:

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

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

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

Der Abschnitt „Empfohlene Maßnahmen“ wird angezeigt

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

Dieser Bereich wird nur für bestimmte Ereignistypen angezeigt.

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

In diesem Hilfethema werden auch einige Links angezeigt.

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

Seite „Ereignisse konfigurieren/managen“

Auf der Seite „Ereignisse konfigurieren/managen“ wird die Liste der deaktivierten Ereignisse angezeigt, und es werden Informationen wie der zugehörige Objekttyp und der Schweregrad des Ereignisses angezeigt. Sie können auch Aufgaben wie Deaktivieren oder Aktivieren von Ereignissen global ausführen.

Sie können diese Seite nur aufrufen, wenn Sie die Rolle „OnCommand-Administrator“ oder „Storage-Administrator“ besitzen.

Befehlsschaltflächen

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

- **Deaktivieren**

Öffnet das Dialogfeld Ereignisse deaktivieren, mit dem Sie Ereignisse deaktivieren können.

- **Aktivieren**

  Aktiviert ausgewählte Ereignisse, die Sie zuvor deaktiviert hatten.

- **EMS Events abonnieren**

  Öffnet das Dialogfeld „EMS-Ereignisse abonnieren“, in dem Sie spezielle EMS-Ereignisse (Event Management System) aus den von Ihnen überwachten Clustern abonnieren können. Das EMS sammelt Informationen über Ereignisse, die auf dem Cluster auftreten. Wenn eine Benachrichtigung für ein abonniertes EMS-Ereignis erhalten wird, wird ein Unified Manager-Ereignis mit dem entsprechenden Schweregrad generiert.

- **Einstellungen Für Die Ereignisaufbewahrung**

  Öffnet das Dialogfeld „Ereignisaufbewahrungseinstellungen“, in dem Sie den Aufbewahrungszeitraum festlegen können, nach dem die Informationen, aufgelösten und veralteten Ereignisse vom Verwaltungsserver entfernt werden. Der Standardwert für die Aufbewahrung ist 180 Tage.

Listenansicht

In der Listenansicht werden Informationen zu deaktivierten Ereignissen (im Tabellenformat) angezeigt. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen.

- **Veranstaltung**

  Zeigt den Namen des Ereignisses an, das deaktiviert ist.

- **Severity**

  Zeigt den Schweregrad des Ereignisses an. Der Schweregrad kann kritisch, Fehler, Warnung oder Informationen sein.

- **Quelltyp**

  Zeigt den Quelltyp an, für den das Ereignis generiert wird.

Dialogfeld „Ereignisse deaktivieren“

Im Dialogfeld Ereignisse deaktivieren wird die Liste der Ereignistypen angezeigt, für die Sie Ereignisse deaktivieren können. Sie können Ereignisse für einen Ereignistyp auf der Grundlage eines bestimmten Schweregrads oder für eine Reihe von Ereignissen deaktivieren.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Bereich Ereigniseigenschaften

Im Bereich Ereigniseigenschaften werden die folgenden Ereigniseigenschaften angegeben:

- **Ereignis Severity**

  Ermöglicht die Auswahl von Ereignissen auf der Grundlage des Schweregrads, der kritisch sein kann,

Fehler, Warnung oder Informationen.

- **Ereignisname Enthält**

  Ermöglicht es Ihnen, Ereignisse zu filtern, deren Name die angegebenen Zeichen enthält.

- **Passende Ereignisse**

  Zeigt die Liste der Ereignisse an, die dem Schweregrad des Ereignisses und dem angegebenen Textstring entsprechen.

- **Ereignisse deaktivieren**

  Zeigt die Liste der Ereignisse an, die Sie zur Deaktivierung ausgewählt haben.

  Der Schweregrad des Ereignisses wird auch zusammen mit dem Event-Namen angezeigt.

Befehlsschaltflächen

Mit den Schaltflächen des Befehls können Sie die folgenden Aufgaben für die ausgewählten Ereignisse ausführen:

- * Speichern und schließen*

  Deaktiviert den Ereignistyp und schließt das Dialogfeld.

- **Abbrechen**

  Die Änderungen werden diskCards und das Dialogfeld geschlossen.

Verwalten von Meldungen

Sie können Benachrichtigungen so konfigurieren, dass Benachrichtigungen automatisch gesendet werden, wenn bestimmte Ereignisse oder Ereignisse bestimmter Schweregrade auftreten. Sie können auch eine Warnung einem Skript zuordnen, das ausgeführt wird, wenn eine Warnung ausgelöst wird.

Um welche Warnmeldungen geht es

Während Ereignisse kontinuierlich auftreten, generiert der Unified Manager eine Meldung nur, wenn ein Ereignis die angegebenen Filterkriterien erfüllt. Sie können die Ereignisse auswählen, für die Warnmeldungen generiert werden sollen. Beispielsweise wenn ein Speicherplatzschwellenwert überschritten wird oder ein Objekt in den Offline-Modus wechselt. Sie können auch eine Warnung einem Skript zuordnen, das ausgeführt wird, wenn eine Warnung ausgelöst wird.

Filterkriterien umfassen Objektklasse, Namen oder Ereignisschweregrad.

Welche Informationen sind in einer Alarm-E-Mail enthalten

Die Warnmeldungen von Unified Manager liefern die Art des Ereignisses, den

Schweregrad des Ereignisses, den Namen der Richtlinie, die gegen das Ereignis verstoßen wurde, und eine Beschreibung des Ereignisses. Die E-Mail-Nachricht enthält auch einen Hyperlink für jedes Ereignis, mit dem Sie die Detailseite für das Ereignis in der Benutzeroberfläche anzeigen können.

Alle Benutzer, die sich für den Erhalt von Benachrichtigungen angemeldet haben, erhalten Warnmeldungen per E-Mail.

Wenn sich ein Performance-Zähler oder Kapazitätswert während einer Inkassofrist groß ändert, kann es dazu führen, dass sowohl ein kritisches als auch ein Warnereignis gleichzeitig für dieselbe Schwellenwertrichtlinie ausgelöst werden. In diesem Fall erhalten Sie möglicherweise eine E-Mail für das Warnereignis und eine für das kritische Ereignis. Dies liegt daran, dass Sie mit Unified Manager separat Warnmeldungen für Warnung und kritische Schwellenwertverletzungen erhalten.

Nach dem Upgrade auf Unified Manager 7.2 oder höher funktionieren Links zu Ereignissen und Warnmeldungen von E-Mails, die von älteren Versionen von Unified Manager gesendet wurden, aufgrund einer Änderung des Ereignisses und der Alarm-URLs nicht mehr.

Nachstehend finden Sie eine Beispiel-E-Mail für eine Warnmeldung:

From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from OnCommand Unified Manager: Thin-Provisioned Volume Space At Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1

Hinzufügen von Meldungen

Sie können Benachrichtigungen konfigurieren, um Sie über die Erzeugung eines bestimmten Ereignisses zu benachrichtigen. Sie können Meldungen für eine einzelne

Ressource, für eine Gruppe von Ressourcen oder für Ereignisse mit einem bestimmten Schweregrad konfigurieren. Sie können die Häufigkeit angeben, mit der Sie benachrichtigt werden möchten, und ein Skript der Warnmeldung zuordnen.

Bevor Sie beginnen

- Sie müssen Benachrichtigungseinstellungen wie die Benutzer-E-Mail-Adresse, SMTP-Server und SNMP-Trap-Host konfiguriert haben, damit der Unified Manager-Server diese Einstellungen verwenden kann, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Meldung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie ein Skript basierend auf dem Ereignis ausführen möchten, müssen Sie das Skript mithilfe der Seite Management/Scripts zu Unified Manager hinzugefügt haben.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können eine Warnmeldung direkt auf der Seite Ereignisdetails erstellen, nachdem Sie ein Ereignis empfangen haben. Zusätzlich können Sie eine Warnung auf der Seite Konfiguration/Warnmeldungen erstellen, wie hier beschrieben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Alerting**.
2. Klicken Sie auf der Seite **Konfiguration/Alarmfunktionen** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
4. Klicken Sie auf **Ressourcen**, und wählen Sie die Ressourcen aus, die in die Warnung aufgenommen oder von ihr ausgeschlossen werden sollen.

   Sie können einen Filter festlegen, indem Sie im Feld **Name enthält** eine Textzeichenfolge angeben, um eine Gruppe von Ressourcen auszuwählen. Die Liste der verfügbaren Ressourcen zeigt auf der Grundlage der angegebenen Textzeichenfolge nur die Ressourcen an, die der Filterregel entsprechen. Die von Ihnen angegebene Textzeichenfolge ist die Groß-/Kleinschreibung.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschl- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschließregel, und die Warnung wird nicht für Ereignisse generiert, die sich auf die ausgeschlossene Ressource beziehen.

5. Klicken Sie auf **Events** und wählen Sie die Ereignisse basierend auf dem Ereignisnamen oder dem Schweregrad aus, für den Sie eine Warnung auslösen möchten.

   Um mehrere Ereignisse auszuwählen, drücken Sie die Strg-Taste, während Sie Ihre Auswahl treffen.

6. Klicken Sie auf **Actions**, und wählen Sie die Benutzer aus, die Sie benachrichtigen möchten, wählen Sie die Benachrichtigungshäufigkeit aus, wählen Sie aus, ob ein SNMP-Trap an den Trap-Empfänger gesendet wird, und weisen Sie ein Skript zu, das ausgeführt werden soll, wenn eine Warnung erzeugt wird.

Wenn Sie die für den Benutzer angegebene E-Mail-Adresse ändern und die Warnmeldung zur Bearbeitung erneut öffnen, erscheint das Feld Name leer, da die geänderte E-Mail-Adresse dem zuvor ausgewählten Benutzer nicht mehr zugeordnet ist. Wenn Sie die E-Mail-Adresse des ausgewählten Benutzers auf der Seite Verwaltung/Benutzer geändert haben, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

Sie können auch Benutzer über SNMP-Traps benachrichtigen.

7. Klicken Sie Auf **Speichern**.

Beispiel für das Hinzufügen einer Meldung

Dieses Beispiel zeigt, wie eine Warnung erstellt wird, die die folgenden Anforderungen erfüllt:

- Alarmname: HealthTest
- Ressourcen: Enthält alle Volumes, deren Name „`abc`“ enthält und schließt alle Volumes aus, deren Name „`xyz`“ enthält
- Ereignisse: Umfasst alle kritischen Systemzustandsereignisse
- Aktionen: Enthält “sample@domain.com”, ein Skript “Test”, und der Benutzer muss alle 15 Minuten benachrichtigt werden

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

1. Klicken Sie auf **Name** und geben Sie ein `HealthTest` Im Feld **Alarmname**.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
   a. Eingabe `abc` Im Feld **Name enthält** werden die Volumes angezeigt, deren Name „`abc`“ enthält.
   b. Wählen Sie im Bereich Verfügbare Ressourcen **<<All Volumes whose name contains 'abc'>>** aus, und verschieben Sie sie in den Bereich Ausgewählte Ressourcen.
   c. Klicken Sie auf **Ausschließe**, und geben Sie ein `xyz` Klicken Sie im Feld **Name enthält** auf **Hinzufügen**.
3. Klicken Sie auf **Events** und wählen Sie im Feld Ereignis Severity * die Option **kritisch** aus.
4. Wählen Sie im Bereich passende Ereignisse die Option * Alle kritischen Ereignisse* aus, und verschieben Sie sie in den Bereich Ausgewählte Ereignisse.
5. Klicken Sie auf **Aktionen** und geben Sie ein `sample@domain.com` Im Feld „Diese Benutzer benachrichtigen“.
6. Wählen Sie **alle 15 Minuten**, um den Benutzer alle 15 Minuten zu benachrichtigen.

   Sie können eine Warnung konfigurieren, um wiederholt Benachrichtigungen an die Empfänger für eine bestimmte Zeit zu senden. Legen Sie fest, zu welchem Zeitpunkt die Ereignisbenachrichtigung für die Warnmeldung aktiv ist.

7. Wählen Sie im Menü Skript zum Ausführen auswählen die Option **Test** Skript .
8. Klicken Sie Auf **Speichern**.

Richtlinien zum Hinzufügen von Warnmeldungen

Auf Basis von Ressourcen wie Cluster, Node, Aggregat oder Volume lassen sich Warnmeldungen oder Ereignisse mit einem bestimmten Schweregrad hinzufügen. Als Best Practice können Sie eine Meldung für alle Ihre kritischen Objekte hinzufügen, nachdem Sie den Cluster hinzugefügt haben, zu dem das Objekt gehört.

Sie können die folgenden Richtlinien und Überlegungen nutzen, um Warnmeldungen für eine effiziente Verwaltung Ihrer Systeme zu erstellen:

- Alarmbeschreibung

  Sie sollten eine Beschreibung für die Warnung angeben, damit Sie Ihre Warnmeldungen effektiv verfolgen können.

- Ressourcen

  Sie sollten entscheiden, welche physische oder logische Ressource eine Warnmeldung benötigt. Bei Bedarf können Sie Ressourcen ein- und ausschließen. Wenn Sie beispielsweise Ihre Aggregate durch eine Warnmeldung genau überwachen möchten, müssen Sie die erforderlichen Aggregate aus der Liste der Ressourcen auswählen.

- Schweregrad des Ereignisses

  Sie sollten entscheiden, ob ein Ereignis eines bestimmten Schweregrades (kritisch, Fehler, Warnung) die Warnmeldung auslösen soll und, falls ja, welchen Schweregrad.

- Ereignis-Name

  Wenn Sie eine Meldung basierend auf dem generierten Ereignistyp hinzufügen, sollten Sie entscheiden, für welche Ereignisse eine Meldung erforderlich ist

- Aktionen

  Sie müssen Benutzernamen und E-Mail-Adressen der Benutzer angeben, die die Benachrichtigung erhalten. Sie können auch einen SNMP-Trap als Benachrichtigungsmodus angeben. Sie können Ihre Skripte einer Warnung zuordnen, damit sie bei der Erzeugung einer Warnmeldung ausgeführt werden.

- Benachrichtigungshäufigkeit

  Sie können eine Warnung konfigurieren, um wiederholt Benachrichtigungen an die Empfänger für eine bestimmte Zeit zu senden. Legen Sie fest, zu welchem Zeitpunkt die Ereignisbenachrichtigung für die Warnmeldung aktiv ist. Wenn Sie möchten, dass die Ereignisbenachrichtigung wiederholt wird, bis das Ereignis bestätigt ist, sollten Sie festlegen, wie oft die Benachrichtigung wiederholt werden soll.

- Skript Ausführen

  Sie können Ihr Skript mit einer Warnung verknüpfen. Ihr Skript wird ausgeführt, wenn die Warnung erzeugt wird.

Hinzufügen von Meldungen für Performance-Ereignisse

Sie können Benachrichtigungen für einzelne Performance-Ereignisse wie alle anderen Ereignisse, die Unified Manager empfangen hat, konfigurieren. Außerdem können Sie

eine einzelne Benachrichtigung erstellen, wenn alle Performance-Ereignisse gleich behandelt werden sollen und E-Mails an dieselbe Person gesendet werden sollen, wenn kritische bzw. Warnereignisse ausgelöst werden.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Das folgende Beispiel zeigt, wie ein Ereignis für alle Ereignisse bezüglich kritischer Latenz, IOPS und MB/s erstellt wird. Sie können diese Methode verwenden, um Ereignisse aus allen Leistungszählern und für alle Warnungsereignisse auszuwählen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Alerting**.
2. Klicken Sie auf der Seite **Konfiguration/Alarmfunktionen** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
4. Wählen Sie auf der Seite **Ressourcen** keine Ressourcen aus.

   Da keine Ressourcen ausgewählt werden, wird die Warnmeldung auf alle Cluster, Aggregate, Volumes usw. angewendet, für die diese Ereignisse empfangen werden.

5. Klicken Sie auf **Events** und führen Sie die folgenden Aktionen aus:
   a. Wählen Sie in der Liste Ereignis Severity die Option **kritisch** aus.
   b. Geben Sie im Feld Ereignisname enthält ein `latency` Und klicken Sie dann auf den Pfeil, um alle übereinstimmenden Ereignisse auszuwählen.
   c. Geben Sie im Feld Ereignisname enthält ein `iops` Und klicken Sie dann auf den Pfeil, um alle übereinstimmenden Ereignisse auszuwählen.
   d. Geben Sie im Feld Ereignisname enthält ein `mbps` Und klicken Sie dann auf den Pfeil, um alle übereinstimmenden Ereignisse auszuwählen.
6. Klicken Sie auf **Aktionen** und wählen Sie dann den Namen des Benutzers aus, der die Benachrichtigung per E-Mail im Feld * Diese Benutzer benachrichtigen* erhält.
7. Konfigurieren Sie alle anderen Optionen auf dieser Seite für die Ausgabe von SNMP-Taps und die Ausführung eines Skripts.
8. Klicken Sie Auf **Speichern**.

Ausschließen von Ziel-Volumes für Disaster Recovery von Alarmmeldungen

Bei der Konfiguration von Volume-Warnmeldungen können Sie im Dialogfeld Warnung eine Zeichenfolge angeben, die ein Volume oder eine Volume-Gruppe identifiziert. Wenn Sie Disaster Recovery für SVMs konfiguriert haben, jedoch haben die Quell- und Ziel-Volumes denselben Namen, sodass Sie Warnmeldungen für beide Volumes erhalten.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die Alarme für Disaster-Recovery-Ziel-Volumes lassen sich deaktivieren, indem Volumes mit dem Namen der Ziel-SVM ausgeschlossen werden. Das ist möglich, da die Kennung für Volume-Ereignisse sowohl den SVM-Namen als auch den Volume-Namen im Format „`<svm_name>:/<volume_name>`“ enthält.

Das folgende Beispiel zeigt, wie Warnmeldungen für das Volume „`vol1`“ auf der primären SVM „`vs1`“ erstellt werden, schließt jedoch die Warnmeldung aus, die auf einem Volume mit demselben Namen auf SVM generiert wird“`vs1-dr`“.

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

Schritte

1. Klicken Sie auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
2. Klicken Sie auf **Ressourcen** und wählen Sie dann die Registerkarte **include** aus.
   a. Wählen Sie in der Dropdown-Liste **Volumen** aus, und geben Sie dann ein `vol1` Im Feld **Name enthält** werden die Volumes angezeigt, deren Name „`vol1`“ enthält.
   b. Wählen Sie **[All Volumes whose name contains 'vol1']** Aus dem Bereich **Verfügbare Ressourcen**, und verschieben Sie ihn in den Bereich **Ausgewählte Ressourcen**.
3. Wählen Sie die Registerkarte **exclude** aus, wählen Sie **Lautstärke**, geben Sie ein `vs1-dr` Klicken Sie im Feld **Name enthält** auf **Hinzufügen**.

   Ausgeschlossen ist die Warnmeldung aus der Erzeugung für das Volume „`vol1`“ auf SVM“`vs1-dr`“.
4. Klicken Sie auf **Events** und wählen Sie das Ereignis oder die Ereignisse aus, die Sie auf das Volume oder die Volumes anwenden möchten.
5. Klicken Sie auf **Aktionen** und wählen Sie dann den Namen des Benutzers aus, der die Benachrichtigung per E-Mail im Feld * Diese Benutzer benachrichtigen* erhält.
6. Konfigurieren Sie alle anderen Optionen auf dieser Seite, um SNMP-Traps auszugeben und ein Skript auszuführen, und klicken Sie dann auf **Speichern**.

Warnungen werden getestet

Sie können eine Meldung testen, um zu überprüfen, ob Sie sie richtig konfiguriert haben. Wenn ein Ereignis ausgelöst wird, wird eine Warnmeldung generiert und eine Warnmeldung an die konfigurierten Empfänger gesendet. Sie können anhand der Testwarnung überprüfen, ob die Benachrichtigung gesendet wird und ob Ihr Skript ausgeführt wird.

Bevor Sie beginnen

- Sie müssen Benachrichtigungseinstellungen wie die E-Mail-Adresse der Empfänger, SMTP-Server und SNMP-Trap konfiguriert haben.

  Der Unified Manager-Server kann diese Einstellungen verwenden, um Benachrichtigungen an Benutzer zu

senden, wenn ein Ereignis generiert wird.

- Sie müssen ein Skript zugewiesen und das Skript so konfiguriert haben, dass es ausgeführt wird, wenn die Warnung erzeugt wird.
- Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Alerting**.
2. Wählen Sie auf der Seite **Konfiguration/Alerting** die Warnmeldung aus, die Sie testen möchten, und klicken Sie dann auf **Test**.

   Eine Test-Alarm-E-Mail wird an die E-Mail-Adressen gesendet, die Sie beim Erstellen der Warnmeldung angegeben haben.

Anzeigen von Meldungen

Auf der Seite Konfiguration/Warnmeldungen können Sie die Liste der für verschiedene Ereignisse erstellten Warnmeldungen anzeigen. Zudem können Sie Eigenschaften von Warnmeldungen anzeigen, z. B. Alarmbeschreibung, Benachrichtigungsmethode und -Häufigkeit, Ereignisse, die die Warnung auslösen, E-Mail-Empfänger der Warnmeldungen und betroffene Ressourcen wie Cluster, Aggregate und Volumes.

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Alerting**.

   Die Liste der Warnungen wird auf der Seite Konfiguration/Warnmeldungen angezeigt.

Bearbeiten von Warnungen

Sie können Eigenschaften von Warnmeldungen bearbeiten, z. B. die Ressource, mit der die Warnmeldung verknüpft ist, Ereignisse, Empfänger, Benachrichtigungsoptionen, Benachrichtigungshäufigkeit, Und zugehörigen Skripts.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Alerting**.
2. Wählen Sie auf der Seite **Konfiguration/Alerting** den zu bearbeitenden Alarm aus, und klicken Sie auf **Bearbeiten**.
3. Bearbeiten Sie im Dialogfeld **Alarm bearbeiten** den Namen, die Ressourcen, Ereignisse und Aktionen.

Nach Bedarf.

Sie können das Skript, das der Warnung zugeordnet ist, ändern oder entfernen.

4. Klicken Sie Auf **Speichern**.

Löschen von Meldungen

Sie können eine Meldung löschen, wenn sie nicht mehr benötigt wird. Beispielsweise können Sie eine Warnmeldung löschen, die für eine bestimmte Ressource erstellt wurde, wenn diese Ressource nicht mehr von Unified Manager überwacht wird.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Alerting**.
2. Wählen Sie auf der Seite **Konfiguration/Alerting** die zu löschenden Warnmeldungen aus, und klicken Sie auf **Löschen**.
3. Klicken Sie auf **Ja**, um die Löschanforderung zu bestätigen.

Beschreibung der Warnfenster und Dialogfelder

Sie sollten Benachrichtigungen für den Empfang von Benachrichtigungen über Ereignisse konfigurieren, indem Sie das Dialogfeld Alarm hinzufügen verwenden. Sie können die Liste der Warnmeldungen auch auf der Seite Konfiguration/Warnmeldungen anzeigen.

Konfigurations-/Alarmseite

Auf der Seite Konfiguration/Warnmeldungen wird eine Liste von Warnungen angezeigt und Informationen über den Namen von Warnmeldungen, den Status, die Benachrichtigungsmethode und die Benachrichtigungshäufigkeit angezeigt. Sie können auf dieser Seite auch Warnmeldungen hinzufügen, bearbeiten, entfernen, aktivieren oder deaktivieren.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Befehlsschaltflächen

- **Hinzufügen**

  Zeigt das Dialogfeld Alarm hinzufügen an, in dem Sie neue Warnmeldungen hinzufügen können.

- **Bearbeiten**

  Zeigt das Dialogfeld Alarm bearbeiten an, in dem Sie ausgewählte Warnmeldungen bearbeiten können.

- **Löschen**

Löscht die ausgewählten Warnmeldungen.

- **Aktivieren**

  Aktiviert das Senden von Benachrichtigungen durch die ausgewählten Warnungen.

- **Deaktivieren**

  Deaktiviert die ausgewählten Warnungen, wenn Sie vorübergehend das Senden von Benachrichtigungen beenden möchten.

- **Test**

  Testet die ausgewählten Warnungen, um ihre Konfiguration nach dem Hinzufügen oder Bearbeiten zu überprüfen.

Listenansicht

Die Listenansicht zeigt in tabellarischer Form Informationen zu den erstellten Warnmeldungen an. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen. Sie können auch eine Warnung auswählen, um weitere Informationen darüber im Detailbereich anzuzeigen.

- **Status**

  Gibt an, ob eine Meldung aktiviert ist (Oder deaktiviert ( ).

- **Alarm**

  Zeigt den Namen der Warnmeldung an.

- **Beschreibung**

  Zeigt eine Beschreibung für die Warnmeldung an.

- **Benachrichtigungsmethode**

  Zeigt die Benachrichtigungsmethode an, die für die Warnmeldung ausgewählt ist. Sie können Benutzer per E-Mail oder SNMP-Traps benachrichtigen.

- **Benachrichtigungshäufigkeit**

  Gibt die Häufigkeit (in Minuten) an, mit der der Verwaltungsserver weiterhin Benachrichtigungen sendet, bis das Ereignis bestätigt, aufgelöst oder in den veralteten Status verschoben wird.

Detailbereich

Im Detailbereich finden Sie weitere Informationen zur ausgewählten Warnmeldung.

- **Name Des Alarms**

  Zeigt den Namen der Warnmeldung an.

- **Warnhinweis**

  Zeigt eine Beschreibung für die Warnmeldung an.

- **Veranstaltungen**

  Zeigt die Ereignisse an, für die die Meldung ausgelöst werden soll.

- **Ressourcen**

  Zeigt die Ressourcen an, für die die Warnmeldung ausgelöst werden soll.

- **Inklusive**

  Zeigt die Gruppe von Ressourcen an, für die die Warnmeldung ausgelöst werden soll.

- **Ohne**

  Zeigt die Gruppe von Ressourcen an, für die Sie die Warnung nicht auslösen möchten.

- **Benachrichtigungsmethode**

  Zeigt die Benachrichtigungsmethode für die Warnmeldung an.

- **Benachrichtigungshäufigkeit**

  Zeigt die Häufigkeit an, mit der der Verwaltungsserver weiterhin Warnmeldungen sendet, bis das Ereignis bestätigt, aufgelöst oder in den veralteten Status verschoben wird.

- **Skriptname**

  Zeigt den Namen des Skripts an, das der ausgewählten Warnmeldung zugeordnet ist. Dieses Skript wird ausgeführt, wenn eine Warnung erzeugt wird.

- **E-Mail-Empfänger**

  Zeigt die E-Mail-Adressen von Benutzern an, die die Benachrichtigung erhalten.

Dialogfeld „Alarm hinzufügen“

Sie können Benachrichtigungen erstellen, um Sie nach der Generierung eines bestimmten Ereignisses zu benachrichtigen, sodass Sie dieses Problem schnell beheben und die Auswirkungen auf Ihre Umgebung minimieren können. Sie können Meldungen für eine einzelne Ressource oder eine Gruppe von Ressourcen und für Ereignisse mit einem bestimmten Schweregrad erstellen. Sie können auch die Benachrichtigungsmethode und die Häufigkeit der Warnmeldungen festlegen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Name

In diesem Bereich können Sie einen Namen und eine Beschreibung für die Warnung angeben:

- **Name Des Alarms**

  Ermöglicht Ihnen die Angabe eines Warnungsnamens.

- **Warnhinweis**

Ermöglicht Ihnen die Angabe einer Beschreibung für die Warnmeldung.

Ressourcen

In diesem Bereich können Sie eine einzelne Ressource auswählen oder die Ressourcen anhand einer dynamischen Regel gruppieren, für die Sie die Warnung auslösen möchten. Eine_dynamische Regel_ ist der Satz von Ressourcen, der anhand der angegebenen Textzeichenfolge gefiltert wird. Sie können nach Ressourcen suchen, indem Sie einen Ressourcentyp aus der Dropdown-Liste auswählen oder den genauen Ressourcennamen angeben, um eine bestimmte Ressource anzuzeigen.

Wenn Sie eine Warnung von einer der Detailseiten des Speicherobjekts erstellen, wird das Speicherobjekt automatisch in die Warnmeldung aufgenommen.

- **Einschließlich**

  Ermöglicht Ihnen, die Ressourcen einzuschließen, für die Sie Warnmeldungen auslösen möchten. Sie können eine Textzeichenfolge angeben, um Ressourcen zu gruppieren, die mit dem String übereinstimmen, und diese Gruppe auswählen, die in die Warnmeldung aufgenommen werden soll. Beispielsweise können Sie alle Volumes gruppieren, deren Name die Zeichenfolge „`abc`“ enthält.

- **Ausschluss**

  Hiermit können Sie Ressourcen ausschließen, für die keine Warnmeldungen ausgelöst werden sollen. Sie können beispielsweise alle Volumes ausschließen, deren Name den String „`xyz`“ enthält.

  Die Registerkarte Ausschließen wird nur angezeigt, wenn Sie alle Ressourcen eines bestimmten Ressourcentyps auswählen: Z. B. [All Volumes] Oder [All Volumes whose name contains '*xyz*'].

  Wenn eine Ressource sowohl den von Ihnen angegebenen Einschließen- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschlussregel, und die Warnmeldung wird nicht für das Ereignis generiert.

Veranstaltungen

In diesem Bereich können Sie die Ereignisse auswählen, für die Sie die Warnungen erstellen möchten. Sie können Meldungen für Ereignisse auf der Grundlage eines bestimmten Schweregrads oder für eine Reihe von Ereignissen erstellen.

Um mehrere Ereignisse auszuwählen, sollten Sie die Strg-Taste gedrückt halten, während Sie Ihre Auswahl treffen.

- **Ereignis Severity**

  Ermöglicht die Auswahl von Ereignissen auf der Grundlage des Schweregrads, der kritisch sein kann, Fehler oder Warnung.

- **Ereignisname Enthält**

  Ermöglicht Ihnen die Auswahl von Ereignissen, deren Name angegebene Zeichen enthält.

Aktionen

In diesem Bereich können Sie die Benutzer angeben, die Sie benachrichtigen möchten, wenn eine Warnung ausgelöst wird. Sie können auch die Benachrichtigungsmethode und die Benachrichtigungshäufigkeit

angeben.

- **Diese Benutzer benachrichtigen**

  Ermöglicht die Angabe der E-Mail-Adresse oder des Benutzernamens des Benutzers zum Empfangen von Benachrichtigungen.

  Wenn Sie die für den Benutzer angegebene E-Mail-Adresse ändern und die Warnmeldung zur Bearbeitung erneut öffnen, erscheint das Feld Name leer, da die geänderte E-Mail-Adresse dem zuvor ausgewählten Benutzer nicht mehr zugeordnet ist. Wenn Sie die E-Mail-Adresse des ausgewählten Benutzers auf der Seite Verwaltung/Benutzer geändert haben, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

- **Benachrichtigungshäufigkeit**

  Hiermit können Sie festlegen, wie oft der Verwaltungsserver Benachrichtigungen sendet, bis das Ereignis bestätigt, aufgelöst oder in den veralteten Status verschoben wird.

  Sie können die folgenden Benachrichtigungsmethoden wählen:

  - Nur einmal benachrichtigen
  - Benachrichtigung in einer bestimmten Frequenz
  - Benachrichtigung bei einer bestimmten Frequenz innerhalb des angegebenen Zeitbereichs

- **SNMP-Trap ausgeben**

  Durch Auswahl dieses Kontrollkästchens können Sie festlegen, ob SNMP-Traps an den global konfigurierten SNMP-Host gesendet werden sollen.

- **Skript Ausführen**

  Ermöglicht Ihnen das Hinzufügen Ihres benutzerdefinierten Skripts zur Benachrichtigung. Dieses Skript wird ausgeführt, wenn eine Warnung erzeugt wird.

Befehlsschaltflächen

- **Speichern**

  Erstellt eine Meldung und schließt das Dialogfeld.

- **Abbrechen**

  Die Änderungen werden diskCards und das Dialogfeld geschlossen.

Dialogfeld „Warnung bearbeiten“

Sie können Eigenschaften von Warnmeldungen bearbeiten, z. B. die Ressource, mit der die Warnmeldung verknüpft ist, sowie die Optionen für Ereignisse, Skripts und Benachrichtigungen.

Name

In diesem Bereich können Sie den Namen und die Beschreibung der Warnmeldung bearbeiten.

- **Name Des Alarms**

  Ermöglicht Ihnen das Bearbeiten des Warnungsnamens.

- **Warnhinweis**

  Ermöglicht Ihnen die Angabe einer Beschreibung für die Warnmeldung.

- * Warnstatus*

  Ermöglicht Ihnen, die Meldung zu aktivieren oder zu deaktivieren.

Ressourcen

In diesem Bereich können Sie eine einzelne Ressource auswählen oder die Ressourcen anhand einer dynamischen Regel gruppieren, für die Sie die Warnung auslösen möchten. Sie können nach Ressourcen suchen, indem Sie einen Ressourcentyp aus der Dropdown-Liste auswählen oder den genauen Ressourcennamen angeben, um eine bestimmte Ressource anzuzeigen.

- **Einschließlich**

  Ermöglicht Ihnen, die Ressourcen einzuschließen, für die Sie Warnmeldungen auslösen möchten. Sie können eine Textzeichenfolge angeben, um Ressourcen zu gruppieren, die mit dem String übereinstimmen, und diese Gruppe auswählen, die in die Warnmeldung aufgenommen werden soll. Beispielsweise können Sie alle Volumes gruppieren, deren Name die Zeichenfolge „`vol0`“ enthält.

- **Ausschluss**

  Hiermit können Sie Ressourcen ausschließen, für die keine Warnmeldungen ausgelöst werden sollen. Sie können beispielsweise alle Volumes ausschließen, deren Name den String „`xyz`“ enthält.

> Die Registerkarte Exclude wird nur angezeigt, wenn Sie alle Ressourcen eines bestimmten Ressourcentyps auswählen, z. B. [All Volumes] Oder [All Volumes whose name contains '*xyz*'].

Veranstaltungen

In diesem Bereich können Sie die Ereignisse auswählen, für die Sie die Warnungen auslösen möchten. Sie können eine Meldung für Ereignisse auf der Grundlage eines bestimmten Schweregrads oder für eine Reihe von Ereignissen auslösen.

- **Ereignis Severity**

  Ermöglicht die Auswahl von Ereignissen auf der Grundlage des Schweregrads, der kritisch sein kann, Fehler oder Warnung.

- **Ereignisname Enthält**

  Ermöglicht Ihnen die Auswahl von Ereignissen, deren Name die angegebenen Zeichen enthält.

Aktionen

In diesem Bereich können Sie die Benachrichtigungsmethode und die Benachrichtigungshäufigkeit angeben.

- **Diese Benutzer benachrichtigen**

  Ermöglicht Ihnen, die E-Mail-Adresse oder den Benutzernamen zu bearbeiten oder eine neue E-Mail-Adresse oder einen neuen Benutzernamen für den Empfang von Benachrichtigungen anzugeben.

- **Benachrichtigungshäufigkeit**

  Hiermit können Sie die Häufigkeit bearbeiten, mit der der Verwaltungsserver Benachrichtigungen sendet, bis das Ereignis bestätigt, aufgelöst oder in den veralteten Status verschoben wird.

  Sie können die folgenden Benachrichtigungsmethoden wählen:

  - Nur einmal benachrichtigen
  - Benachrichtigung in einer bestimmten Frequenz
  - Benachrichtigung bei einer bestimmten Frequenz innerhalb des angegebenen Zeitbereichs

- **SNMP-Trap ausgeben**

  Hiermit können Sie festlegen, ob SNMP-Traps an den global konfigurierten SNMP-Host gesendet werden sollen.

- **Skript Ausführen**

  Hiermit können Sie ein Skript mit der Warnmeldung verknüpfen. Dieses Skript wird ausgeführt, wenn eine Warnung erzeugt wird.

Befehlsschaltflächen

- **Speichern**

  Speichert die Änderungen und schließt das Dialogfeld.

- **Abbrechen**

  Die Änderungen werden diskCards und das Dialogfeld geschlossen.

Verwalten von Skripten

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

Funktionsweise von Skripten mit Warnmeldungen

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

Wenn eine Warnung für ein Ereignis in Unified Manager generiert wird, wird eine Alarm-E-Mail an die

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

Das Skript verwendet die folgenden Argumente zur Ausführung:

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

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

Beispiel zum Abrufen von Argumenten aus Skripts

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

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

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

Skripte werden hinzugefügt

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

Bevor Sie beginnen

- Sie müssen die Skripte erstellt und gespeichert haben, die Sie dem Unified Manager-Server hinzufügen möchten.
- Die unterstützten Dateiformate für Skripte sind Perl, Shell, PowerShell und `.bat` Dateien:
  - Für Perl-Skripte muss Perl auf dem Unified Manager-Server installiert sein. Wenn Perl nach Unified Manager installiert wurde, müssen Sie den Unified Manager-Server neu starten.
  - Bei PowerShell Skripten muss auf dem Server die entsprechende PowerShell Ausführungsrichtlinie

festgelegt werden, damit die Skripte ausgeführt werden können.

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

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

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Scripts**.
2. Klicken Sie auf der Seite **Management/Scripts** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Skript hinzufügen** auf **Durchsuchen**, um die Skriptdatei auszuwählen.
4. Geben Sie eine Beschreibung für das ausgewählte Skript ein.
5. Klicken Sie Auf **Hinzufügen**.

Skripte werden gelöscht

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

Bevor Sie beginnen

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Scripts**.
2. Wählen Sie auf der Seite **Management/Scripts** das Skript aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang, indem Sie auf **Ja** klicken.

Skriptausführung wird getestet

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

Bevor Sie beginnen

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Scripts**.
2. Fügen Sie auf der Seite * Management/Scripts* Ihr Testskript hinzu.
3. Führen Sie auf der Seite **Konfiguration/Alarmfunktionen** eine der folgenden Aktionen aus:

An…	Tun Sie das…
Fügen Sie eine Meldung hinzu	a. Klicken Sie auf der Seite Konfiguration/Warnmeldungen auf **Hinzufügen**. b. Verknüpfen Sie im Abschnitt Aktionen den Alarm mit Ihrem Testskript.
Bearbeiten Sie eine Meldung	a. Wählen Sie auf der Seite Konfiguration/Alarmfunktionen eine Warnmeldung aus und klicken Sie dann auf **Bearbeiten**. b. Verknüpfen Sie im Abschnitt Aktionen den Alarm mit Ihrem Testskript.

4. Klicken Sie Auf **Speichern**.
5. Wählen Sie auf der Seite **Konfiguration/Alarmfunktionen** die Warnmeldung aus, die Sie hinzugefügt oder geändert haben, und klicken Sie dann auf **Test**.

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

Beschreibung der Skriptfenster und Dialogfelder

Auf der Seite „Management/Scripts“ können Sie Skripte zu Unified Manager hinzufügen.

Seite „Management/Skripts“

Auf der Seite „Management/Scripts“ können Sie benutzerdefinierte Skripts zu Unified Manager hinzufügen. Sie können diese Skripte mit Warnmeldungen verknüpfen, um die automatische Neukonfiguration von Speicherobjekten zu ermöglichen.

Auf der Seite „Management/Scripts“ können Sie Skripte aus Unified Manager hinzufügen oder löschen.

Befehlsschaltflächen

- **Hinzufügen**

  Zeigt das Dialogfeld Skript hinzufügen an, in dem Sie Skripts hinzufügen können.

- **Löschen**

  Löscht das ausgewählte Skript.

Listenansicht

In der Listenansicht werden die Skripte in Tabellenformat angezeigt, die Sie Unified Manager hinzugefügt haben.

- **Name**

  Zeigt den Namen des Skripts an.

- **Beschreibung**

  Zeigt die Beschreibung des Skripts an.

Dialogfeld „Skript hinzufügen“

Im Dialogfeld Skript hinzufügen können Sie Skripts zu Unified Manager hinzufügen. Sie können Benachrichtigungen mit Ihren Skripten konfigurieren, um automatisch Ereignisse zu beheben, die für Speicherobjekte generiert werden.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Wählen Sie Skriptdatei**

  Ermöglicht die Auswahl eines Skripts für die Warnmeldung.

- **Beschreibung**

  Hier können Sie eine Beschreibung für das Skript angeben.

Unterstützte CLI-Befehle von Unified Manager

Als Storage-Administrator führen Sie mit den CLI-Befehlen Abfragen für die Storage-Objekte durch, z. B. für Cluster, Aggregate, Volumes, Qtrees und LUNs. Sie können die CLI-Befehle verwenden, um die interne Datenbank von Unified Manager und die ONTAP-Datenbank abzufragen. Sie können auch CLI-Befehle in Skripten verwenden, die zu Beginn oder am Ende eines Vorgangs ausgeführt oder ausgeführt werden, wenn eine Meldung ausgelöst wird.

Allen Befehlen muss der Befehl vorangestellt sein `um cli login` Und einen gültigen Benutzernamen und ein gültiges Passwort für die Authentifizierung.

CLI-Befehl	Beschreibung	Ausgabe
`um run cmd [ -t <timeout> ] <cluster> <command>`	Die einfachste Methode, einen Befehl auf einem oder mehreren Hosts auszuführen. Hauptsächlich wird verwendet für Alert Scripting um ONTAP zu erhalten oder eine Operation durchzuführen. Das optionale Argument für die Zeitüberschreitung setzt eine maximale Zeitgrenze (in Sekunden), damit der Befehl auf dem Client ausgeführt werden kann. Der Standardwert ist 0 (ewig warten).	Nach Erhalt bei ONTAP.
`um run query <sql command>`	Führt eine SQL-Abfrage aus. Es sind nur Abfragen erlaubt, die aus der Datenbank gelesen werden. Aktualisierungsvorgänge, Einfügevorgänge oder Löschvorgänge werden nicht unterstützt.	Die Ergebnisse werden in tabellarischer Form angezeigt. Wenn ein leerer Satz zurückgegeben wird, oder wenn ein Syntaxfehler oder eine fehlerhafte Anforderung vorliegt, wird die entsprechende Fehlermeldung angezeigt.
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Fügt der Liste der gemanagten Speichersysteme eine Datenquelle hinzu. Eine Datenquelle beschreibt, wie Verbindungen zu Speichersystemen hergestellt werden. Beim Hinzufügen einer Datenquelle müssen die Optionen -U (Benutzername) und -P (Passwort) angegeben werden. Die Option -t (Protocol) gibt das Protokoll an, das zur Kommunikation mit dem Cluster verwendet wird (http oder https). Wenn das Protokoll nicht angegeben wird, werden beide Protokolle versucht, die Option -p (Port) gibt den Port an, der zur Kommunikation mit dem Cluster verwendet wird. Wenn der Port nicht angegeben wird, wird versucht, den Standardwert des entsprechenden Protokolls zu verwenden. Dieser Befehl kann nur vom Storage-Admin ausgeführt werden.	Fordert den Benutzer auf, das Zertifikat anzunehmen, und druckt die entsprechende Meldung.

CLI-Befehl	Beschreibung	Ausgabe
`um datasource list [ <datasource-id>]`	Zeigt die Datenquellen für verwaltete Speichersysteme an.	Zeigt die folgenden Werte im Tabellenformat an: `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message.`
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	Ändert eine oder mehrere Datenquellenoptionen. Kann nur vom Storage-Administrator ausgeführt werden.	Zeigt die entsprechende Meldung an.
`um datasource remove <datasource-id>`	Entfernt die Datenquelle aus Unified Manager.	Zeigt die entsprechende Meldung an.
`um option list [ <option> .. ]`	Listenoptionen.	Zeigt die folgenden Werte im Tabellenformat an: `Name, Value, Default Value, and Requires Restart.`
`um option set <option-name>=<option-value> [ <option-name>=<option-value> ... ]`	Legt eine oder mehrere Optionen fest. Der Befehl kann nur vom Storage-Admin ausgeführt werden.	Zeigt die entsprechende Meldung an.
`um version`	Zeigt die Softwareversion von Unified Manager an.	`Version ("7.0")`
`um lun list [-q] [ -ObjectType <object-id>]`	Führt die LUNs nach dem Filtern auf das angegebene Objekt auf. -q ist für alle Befehle geeignet, keine Kopfzeile anzuzeigen. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, svm: Beispiel: `um lun list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Mit dem Befehl werden alle LUNs im Cluster mit der ID 1 aufgeführt.	Zeigt die folgenden Werte im Tabellenformat an: `ID and LUN path.`

CLI-Befehl	Beschreibung	Ausgabe
`um svm list [-q] [ -ObjectType <object-id>]`	Listet die SVMs nach dem Filtern auf dem angegebenen Objekt auf. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, svm: Beispiel: `um svm list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle SVMs innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an: `Name and Cluster ID`.
`um qtree list [-q] [ -ObjectType <object-id>]`	Führt die qtrees nach dem Filtern auf dem angegebenen Objekt auf. -q ist für alle Befehle geeignet, keine Kopfzeile anzuzeigen. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, svm: Beispiel: `um qtree list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Mit dem Befehl werden alle qtrees im Cluster mit der ID 1 aufgelistet.	Zeigt die folgenden Werte im Tabellenformat an: `Qtree ID and Qtree Name`.
`um disk list [-q] [- ObjectType <object-id>]`	Listet die Festplatten nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster sein. Beispiel: `um disk list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Festplatten im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `ObjectType and object-id`.
`um cluster list [-q] [- ObjectType <object-id>]`	Listet die Cluster nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster, lun, sein Qtree, Volume, Kontingent, svm. Beispiel:`um cluster list -aggr 1` In diesem Beispiel ist "-aggr" der objectType und "1" die objectId. Der Befehl listet das Cluster auf, zu dem das Aggregat mit der ID 1 gehört.	Zeigt die folgenden Werte im Tabellenformat an: `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key`.

CLI-Befehl	Beschreibung	Ausgabe
`um cluster node list [-q] [-ObjectType <object-id>]`	Führt die Cluster-Nodes nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster sein. Beispiel: `um cluster node list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Nodes im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Name and Cluster ID.`
`um volume list [-q] [-ObjectType <object-id>]`	Listet die Volumes nach dem Filtern auf dem angegebenen Objekt auf. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, svm, Aggregat: Beispiel: `um volume list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Volumes im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Volume ID and Volume Name.`
`um quota user list [-q] [-ObjectType <object-id>]`	Listet die Quota-Benutzer nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann qtree, Cluster, Volume, Kontingent und svm sein. Beispiel: `um quota user list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Kontingentbenutzer innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `ID, Name, SID and Email.`
`um aggr list [-q] [-ObjectType <object-id>]`	Führt die Aggregate nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster, Volume sein. Beispiel: `um aggr list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Aggregate innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Aggr ID, and Aggr Name.`

CLI-Befehl	Beschreibung	Ausgabe
`um event ack <event-ids>`	Bestätigt ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event resolve <event-ids>`	Löst ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event assign -u <username> <event-id>`	Weist einem Benutzer ein Ereignis zu.	Zeigt die entsprechende Meldung an.
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Listet die vom System oder Benutzer generierten Ereignisse auf. Filtern von Ereignissen nach Quelle, Status und IDs	Zeigt die folgenden Werte im Tabellenformat an `Source, Source type, Name, Severity, State, User and Timestamp.`
`um cli login -u <username> [-p <password>`	Melden Sie sich bei der CLI an. Die Sitzung läuft nach drei Stunden ab dem Zeitpunkt der Anmeldung ab. Danach muss sich der Benutzer erneut anmelden.	Zeigt die entsprechende Meldung an.
`um cli logout`	Melden Sie sich über die CLI ab.	Zeigt die entsprechende Meldung an.
`um backup restore -f <backup_file_path_and_name>`	Stellt eine Datenbanksicherung mithilfe von .7z-Dateien wieder her.	Zeigt die entsprechende Meldung an.
`um help`	Zeigt alle Unterbefehle der ersten Ebene an.	Zeigt alle Unterbefehle der ersten Ebene an.

Verwalten von Systemzustandsschwellenwerten

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

Welche Schwellenwerte für den Zustand von Storage-Kapazität sind

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

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

Konfigurieren von globalen Schwellenwerteinstellungen für den Systemzustand

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

Über diese Aufgabe

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

Auf der Seite „Schwellenwerte für Konfiguration/Zustand“ können Sie auf globale Schwellenwerteinstellungen zugreifen. Sie können Schwellwerteinstellungen für einzelne Objekte auch auf der Bestandsseite oder auf der Detailseite für das Objekt ändern.

Wahlmöglichkeiten

- Konfigurieren von globalen Integritätsschwellenwerten für das Aggregat

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

- Konfigurieren von globalen Schwellenwerten für den Zustand des Volumes

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

- Konfigurieren von globalen qtree-Zustandsschwellenwerten

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

- Bearbeiten von Verzögerungszustands-Schwellenwerten für nicht verwaltete Schutzbeziehungen

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

Konfigurieren von globalen Integritätsschwellenwerten für das Aggregat

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

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

Systemzustandsschwellenwerte gelten nicht für das Root-Aggregat des Nodes.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Health Schwellenwerte**.
2. Klicken Sie auf der Seite **Configuration/Health Schwellenwerte** auf **Aggregate**.
3. Konfigurieren Sie die entsprechenden Schwellenwerte für Kapazität, Wachstum und Snapshot-Kopien.
4. Klicken Sie Auf **Speichern**.

Konfigurieren von globalen Schwellenwerten für den Zustand des Volumes

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Health Schwellenwerte**.
2. Klicken Sie auf der Seite **Configuration/Health Schwellenwerte** auf **Volumes**.

3. Konfigurieren Sie die entsprechenden Schwellenwerte für Kapazität, Snapshot-Kopien, qtree-Kontingente, Volume-Wachstum und Inodes.
4. Klicken Sie Auf **Speichern**.

Konfigurieren von globalen qtree-Zustandsschwellenwerten

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Health Schwellenwerte**.
2. Klicken Sie auf der Seite **Konfiguration/Gesundheit Schwellenwerte** auf **Qtrees**.
3. Konfigurieren Sie die entsprechenden Kapazitätsschwellenwerte.
4. Klicken Sie Auf **Speichern**.

Bearbeiten von Verzögerungszustands-Schwellenwerten für nicht verwaltete Schutzbeziehungen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Health Schwellenwerte**.
2. Klicken Sie auf der Seite **Konfiguration/Gesundheit Schwellenwerte** auf **Beziehungen**.
3. Erhöhen oder verringern Sie je nach Bedarf den globalen Standard-Warn- oder Fehlerverzögerungsgrad.
4. Klicken Sie Auf **Speichern**.

Bearbeiten einzelner Zustandsschwellenwerte für das Aggregat

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

Schritte

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

Bearbeiten von Schwellenwerten für den Zustand einzelner Volumes

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

Schritte

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

Bearbeiten einzelner qtree-Statusschwellenwerte

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory die SVM aus, auf der sich der qtree befindet.
3. Klicken Sie auf der Seite * Health/Storage Virtual Machine* Details auf die Registerkarte qtrees.
4. Wählen Sie eine oder mehrere qtrees aus und klicken Sie dann auf **Schwellenwerte bearbeiten**.
5. Ändern Sie im Dialogfeld **Qtree Schwellenwerte bearbeiten** die Kapazitätsschwellenwerte für den ausgewählten qtree oder qtrees und klicken Sie auf **Speichern**.

Beschreibung der Seiten für den Systemzustand

Sie können die entsprechende Seite Configuration/Health schwellers verwenden, um globale Statusschwellenwerte für Aggregate und Volumes zu konfigurieren und globale lag-Warn- und Fehlerschwellenwerte für nicht gemanagte Sicherungsbeziehungen zu konfigurieren.

Konfigurations-/Health-Schwellenwerte für Aggregate

Auf der Seite Configuration/Health schwells für Aggregate können Sie globale Statusschwellenwerte für überwachte Aggregate konfigurieren. Wenn Sie die Optionen global konfigurieren, werden die Standardwerte aller Objekte geändert. Wenn jedoch die Standardwerte auf Objektebene geändert wurden, werden die globalen Werte nicht geändert.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Ereignisse werden erzeugt, wenn ein Schwellenwert überschritten wird. Sie können für solche Ereignisse Korrekturmaßnahmen ergreifen.

Die Schwellenwerte sind für das Root-Aggregat des Knotens nicht anwendbar.

Sie können für die folgenden Aggregate einen Zustandsschwellenwert festlegen: Kapazität, Aggregatwachstum und Snapshot Kopien für Aggregate.

Kapazität

Im Kapazitätsbereich können Sie die folgenden Bedingungen für die Aggregat-Kapazität festlegen. Beachten Sie, dass bei Aktivierung von Autogrow auf Volumes im Aggregat die Kapazitätsschwellenwerte für das Aggregat basierend auf der durch Autogrow festgelegten maximalen Volume-Größe gelten, nicht jedoch auf der ursprünglichen Volume-Größe.

- **Raum Fast Voll**

  Gibt den Prozentsatz an, bei dem ein Aggregat als fast voll erachtet wird:

  - Standardwert: 80 Prozent

    Der Wert für diesen Schwellenwert muss niedriger sein als der Wert für den Gesamtschwellenwert für den Verwaltungsserver, um ein Ereignis zu generieren.

  - Generiertes Ereignis: Fast voll aggregieren
  - Ereignis Schweregrad: Warnung
- **Raum Voll**

  Gibt den Prozentsatz an, bei dem ein Aggregat als voll betrachtet wird:

  - Standardwert: 90 Prozent
  - Event generiert: Aggregat voll
  - Ereignis Schweregrad: Fehler
- **Fast Überengagiert**

Gibt den Prozentsatz an, an dem ein Aggregat als fast überengagiert betrachtet wird:

- Standardwert: 95 Prozent

  Der Wert für diesen Schwellenwert muss niedriger sein als der Wert für den zu hohen Gesamtschwellenwert für den Verwaltungsserver, um ein Ereignis zu generieren.

- Event generiert: Fast überengagiert zusammenfassen
- Ereignis Schweregrad: Warnung

- **Überengagiert**

  Gibt den Prozentsatz an, an dem ein Aggregat als überengagiert betrachtet wird:

  - Standardwert: 100 Prozent
  - Event generiert: Zusammenfassung überengagiert
  - Ereignis Schweregrad: Fehler

- **Tage Bis Voll**

  Gibt die Anzahl der verbleibenden Tage an, bevor die volle Kapazität des Aggregats erreicht ist:

  - Standardwert: 7
  - Event generiert: Tage aggregieren bis voll
  - Ereignis Schweregrad: Fehler

Wachstumsbereich

Im Wachstumsbereich können Sie die folgenden Schwellwerte für das Gesamtwachstum festlegen:

- **Wachstumsrate**

  Gibt den Prozentsatz an, bei dem die Wachstumsrate eines Aggregats als normal angesehen wird, bevor das System ein ungewöhnliches Ereignis für die Aggregatwachstumsrate generiert:

  - Standardwert: 1 Prozent
  - Generiertes Ereignis: Aggregierte Wachstumsrate anormal
  - Ereignis Schweregrad: Warnung

- **Empfindlichkeit Der Wachstumsrate**

  Gibt den Faktor an, der auf die Standardabweichung der Wachstumsrate eines Aggregats angewendet wird. Wenn die Wachstumsrate die faktorierte Standardabweichung überschreitet, wird ein ungewöhnliches Ereignis für die aggregierte Wachstumsrate generiert.

  Ein niedrigerer Wert für die Wachstumsrate zeigt an, dass das Aggregat sehr empfindlich auf Veränderungen der Wachstumsrate reagiert. Der Bereich für die Empfindlichkeit der Wachstumsrate liegt zwischen 1 und 5.

  - Standardwert: 2

  > Wenn Sie die Wachstumssensitivität für Aggregate auf der globalen Schwellenebene ändern, wird die Änderung auch auf die Wachstumsratenempfindlichkeit für Volumes auf der globalen Schwellenebene angewendet.

Bereich der Snapshot-Kopien

Im Bereich Snapshot Kopien können Sie die folgenden Schwellwerte der Snapshot Reserve einstellen:

- **Snapshot Reserve Voll**

  Gibt den Prozentsatz an, an dem ein Aggregat den gesamten reservierten Speicherplatz für Snapshot Kopien belegt hat:

  - Standardwert: 90 Prozent
  - Event generiert: Zusammenfassung der Snapshot Reserve voll
  - Ereignis Schweregrad: Warnung

Befehlsschaltflächen

- **Wiederherstellen auf Werkseinstellungen**

  Ermöglicht die Wiederherstellung der Konfigurationseinstellungen auf die werkseitigen Standardwerte.

- **Speichern**

  Speichert die Konfigurationseinstellungen für die ausgewählte Option.

Seite „Konfigurations-/Statusschwellenwerte“ für Volumes

Auf der Seite Configuration/Health schwelles für Volumes können Sie globale Schwellenwerte für den Systemzustand für überwachte Volumes konfigurieren. Sie können Schwellenwerte für einzelne Volumes oder für alle Volumes weltweit festlegen. Wenn Sie die Optionen global konfigurieren, werden die Standardwerte aller Objekte geändert. Wenn jedoch die Standardwerte auf Objektebene geändert wurden, werden die globalen Werte nicht geändert.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Ereignisse werden erzeugt, wenn ein Schwellenwert überschritten wird. Sie können für solche Ereignisse Korrekturmaßnahmen ergreifen.

Für folgende Zwecke können Sie Schwellenwerte festlegen: Kapazität, Volume Snapshot-Kopien, Kontingente, Volume-Wachstum und Inodes.

Kapazität

Im Kapazitätsbereich können Sie die folgenden Schwellwerte für die Volume-Kapazität einstellen. Beachten Sie, dass bei Aktivierung von Autogrow auf einem Volume die Kapazitätsschwellenwerte basierend auf der durch Autogrow festgelegten maximalen Volume-Größe gelten und nicht auf der ursprünglichen Volume-Größe basieren.

- **Raum Fast Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als fast voll betrachtet wird:

  - Standardwert: 80 Prozent

Der Wert für diesen Schwellenwert muss niedriger sein als der Wert für den Schwellenwert „Volume Full“, damit der Verwaltungsserver ein Ereignis generieren kann.

  - Event generiert: Volumen fast voll
  - Ereignis Schweregrad: Warnung

- **Raum Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als voll betrachtet wird:

  - Standardwert: 90 Prozent
  - Event generiert: Volumen voll
  - Ereignis Severity: Fehler

- **Tage Bis Voll**

  Gibt die Anzahl der verbleibenden Tage an, bevor die volle Kapazität des Volume erreicht ist:

  - Standardwert: 7
  - Event generiert: Volume Days bis Full
  - Ereignis Schweregrad: Fehler

Bereich der Snapshot-Kopien

Im Bereich Snapshot Kopien können Sie die folgenden Schwellwerte für die Snapshot Kopien im Volume festlegen:

- **Snapshot Reserve Voll**

  Gibt den Prozentsatz an, an dem der für Snapshot Kopien reservierte Speicherplatz voll berücksichtigt wird:

  - Standardwert: 90 Prozent
  - Event generiert: Volume Snapshot Reserve voll
  - Ereignis Schweregrad: Fehler

- **Tage Bis Voll**

  Gibt die Anzahl der Tage an, die noch verbleiben, bevor der für Snapshot Kopien reservierte Speicherplatz mit der vollen Kapazität erreicht wird:

  - Standardwert: 7
  - Event generiert: Volume Snapshot Reserve Days bis Kapazitätsreserve
  - Ereignis Schweregrad: Fehler

- * Anzahl*

  Gibt die Anzahl der Snapshot Kopien auf einem Volume an, die als zu viele Kopien gelten:

  - Standardwert: 250
  - Generiertes Ereignis: Zu viele Snapshot Kopien
  - Ereignis Schweregrad: Fehler

Qtree-Kontingentbereich

Der Qtree Quota Bereich ermöglicht es Ihnen, die folgenden Volumen Quota Schwellenwerte einzustellen:

- **Fast Überengagiert**

  Gibt den Prozentsatz an, mit dem ein Volume als beinahe durch qtree Kontingente überengagiert werden soll:

  - Standardwert: 95 Prozent
  - Event erzeugt: Volumen Qtree Kontingent fast überengagiert
  - Ereignis Schweregrad: Warnung
- **Überengagiert**

  Gibt den Prozentsatz an, mit dem ein Volume als durch qtree Kontingente überengagiert werden soll:

  - Standardwert: 100 Prozent
  - Event erstellt: Volumen Qtree Kontingent überfordert
  - Ereignis Schweregrad: Fehler

Wachstumsbereich

Im Wachstumsbereich können Sie die folgenden Schwellwerte für das Volumenwachstum festlegen:

- **Wachstumsrate**

  Gibt den Prozentsatz an, bei dem die Wachstumsrate eines Volumes als normal angesehen wird, bevor das System ein ungewöhnliches Ereignis der Volumenwachstumsrate generiert:

  - Standardwert: 1 Prozent
  - Generiertes Ereignis: Volumenwachstumsrate anormal
  - Ereignis Schweregrad: Warnung
- **Empfindlichkeit Der Wachstumsrate**

  Gibt den Faktor an, der auf die Standardabweichung der Wachstumsrate eines Volumens angewendet wird. Wenn die Wachstumsrate die faktorierte Standardabweichung überschreitet, wird ein ungewöhnliches Ereignis der Volumenwachstumsrate generiert.

  Ein niedrigerer Wert für die Empfindlichkeit der Wachstumsrate zeigt an, dass das Volumen sehr empfindlich auf Veränderungen der Wachstumsrate reagiert. Der Bereich für die Empfindlichkeit der Wachstumsrate liegt zwischen 1 und 5.

  - Standardwert: 2

  > Wenn Sie die Wachstumssensitivität für Volumes auf der globalen Schwellenebene ändern, wird die Änderung auch auf die Wachstumsratenempfindlichkeit für Aggregate auf der globalen Schwellenebene angewendet.

Inodes-Bereich

Im Inodes-Bereich können Sie die folgenden Schwellwerte für Inodes festlegen:

- **Fast Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als den Großteil seiner Inodes verbraucht wurde:

  - Standardwert: 80 Prozent
  - Event generiert: Inodes fast voll
  - Ereignis Schweregrad: Warnung

- **Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als „alle Inodes verbraucht“ betrachtet wird:

  - Standardwert: 90 Prozent
  - Event generiert: Inodes voll
  - Ereignis Schweregrad: Fehler

Befehlsschaltflächen

- **Wiederherstellen auf Werkseinstellungen**

  Ermöglicht die Wiederherstellung der Konfigurationseinstellungen auf die werkseitigen Standardwerte.

- **Speichern**

  Speichert die Konfigurationseinstellungen für die ausgewählte Option.

Verzögerungsschwellenwerte für die Seite „nicht verwaltete Beziehungen“

Auf der Seite „lag Schwellenwerte für nicht verwaltete Beziehungen“ können Sie globale Verzögerungs- und Fehlerschwellenwerte für nicht verwaltete Schutzbeziehungen konfigurieren, damit Sie benachrichtigt werden und Maßnahmen ergreifen können, wenn Verzögerungs- oder Schwellenwertfehler auftreten. Änderungen an diesen Einstellungen werden bei der nächsten geplanten Aktualisierung übernommen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Ereignisse werden erzeugt, wenn ein Schwellenwert überschritten wird. Sie können für solche Ereignisse Korrekturmaßnahmen ergreifen. Verzögerungsschwellenwerte für nicht verwaltete Beziehungen sind standardmäßig aktiviert.

Der lag-Schwellenwert gibt einen Prozentsatz an, der die Verzögerungszeit nicht überschreiten darf. Mit einem Beispiel von einer Stunde, wenn der lag-Schwellenwert als 150 % definiert ist, dann erhalten Sie ein Ereignis, wenn die Verzögerungszeit mehr als 1.5 Stunden beträgt.

Verzögerungsschwellenwerte für Bereich „nicht verwaltete Beziehungen“

Im Bereich „lag“ können Sie für die folgenden Bedingungen unverwaltete Beziehungs-lag-Schwellenwerte festlegen:

- **Warnung**

  Gibt den Prozentsatz an, bei dem die Verzögerungsdauer dem lag-Warnungsschwellenwert entspricht oder

überschreitet:

- Standardwert: 150 Prozent
- Ereignisse generiert: SnapMirror Beziehung Verzögerung Warnung oder SnapVault Beziehung Verzögerung Warnung
- Ereignis Schweregrad: Warnung

- **Fehler**

  Gibt den Prozentsatz an, bei dem die Verzögerungsdauer gleich oder größer als der lag-Fehlerschwellenwert ist:

  - Standardwert: 250 Prozent
  - Erzeugte Ereignisse: SnapMirror Beziehung Verzögerung Fehler oder SnapVault Beziehung Verzögerung Fehler
  - Ereignis Schweregrad: Fehler

Befehlsschaltflächen

- **Wiederherstellen auf Werkseinstellungen**

  Ermöglicht die Wiederherstellung der Konfigurationseinstellungen auf die werkseitigen Standardwerte.

- **Speichern**

  Speichert die Konfigurationseinstellungen für die ausgewählte Option.

Seite „Schwellenwerte für Konfiguration/Systemzustand“ für qtrees

Auf der Seite Configuration/Health Schwellen für qtrees können Sie globale Schwellenwerte für den Systemzustand für überwachte qtrees konfigurieren. Ereignisse werden nur dann für einen qtree erzeugt, wenn ein qtree Kontingent oder eine Standard-Quote auf dem qtree festgelegt wurde. Ereignisse werden nicht generiert, wenn der in einem Benutzerkontingent oder Gruppenkontingent definierte Speicherplatz den Schwellenwert überschritten hat.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Ereignisse werden erzeugt, wenn ein Schwellenwert überschritten wird. Sie können für solche Ereignisse Korrekturmaßnahmen ergreifen.

Kapazität

Im Kapazitätsbereich können Sie die folgenden qtree-Kapazitätsschwellenwerte festlegen.

- **Raum Fast Voll**

  Gibt den Prozentsatz an, bei dem ein qtree als nahezu voll erachtet wird:

  - Standardwert: 80 Prozent

    Der Wert für diesen Schwellenwert muss niedriger sein als der Wert für den Qtree Full Schwellenwert.

- Event generiert: Qtree fast voll
- Ereignis Schweregrad: Warnung

- **Raum Voll**

  Gibt den Prozentsatz an, bei dem ein qtree als voll erachtet wird:

  - Standardwert: 90 Prozent
  - Ereignis generiert: Qtree voll
  - Ereignis Schweregrad: Fehler

Befehlsschaltflächen

- **Wiederherstellen auf Werkseinstellungen**

  Ermöglicht die Wiederherstellung der Konfigurationseinstellungen auf die werkseitigen Standardwerte.

- **Speichern**

  Speichert die Konfigurationseinstellungen für die ausgewählte Option.

Dialogfeld „Aggregat-Schwellenwerte bearbeiten“

Sie können Benachrichtigungen konfigurieren, um Benachrichtigungen zu senden, wenn ein Ereignis bezüglich der Kapazität eines Aggregats generiert wird. Korrekturmaßnahmen können vorgenommen werden, um das Ereignis einzuleiten. Beispielsweise können Sie für den Schwellenwert für „Aggregate Full“ eine Meldung konfigurieren, um eine Benachrichtigung zu senden, wenn der Zustand über einen bestimmten Zeitraum beibehalten wird.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Im Dialogfeld „Aggregat-Schwellenwerte bearbeiten“ können Sie Schwellenwerte auf Aggregatebene konfigurieren, die auf ausgewählte Aggregate angewendet werden. Wenn Sie Schwellenwerte auf Aggregatebene konfigurieren, haben diese Vorrang vor den globalen Schwellenwerten. Sie können Schwellwerte für Kapazität, Wachstum und Snapshot Kopien auf Aggregatebene konfigurieren. Wenn diese Einstellungen nicht konfiguriert sind, werden die globalen Schwellenwerte angewendet.

Die Schwellenwerte sind für das Root-Aggregat des Knotens nicht anwendbar.

Kapazität

Im Kapazitätsbereich können Sie die folgenden Bedingungen für die Aggregat-Kapazität festlegen:

- **Raum Fast Voll**

  Gibt den Prozentsatz an, bei dem ein Aggregat als fast voll erachtet wird. Er zeigt auch die Größe des Aggregats an, die dem angegebenen Schwellwert entspricht.

  Sie können auch den Schieberegler verwenden, um den Schwellenwert festzulegen.

- **Raum Voll**

Gibt den Prozentsatz an, bei dem ein Aggregat als voll betrachtet wird. Er zeigt auch die Größe des Aggregats an, die dem angegebenen Schwellwert entspricht.

Sie können auch den Schieberegler verwenden, um den Schwellenwert festzulegen.

- **Fast Überengagiert**

  Gibt den Prozentsatz an, bei dem ein Aggregat als fast zu hoch angesetzt betrachtet wird.

- **Überengagiert**

  Gibt den Prozentsatz an, mit dem ein Aggregat als überengagiert betrachtet wird.

- **Tage Bis Voll**

  Gibt die Anzahl der verbleibenden Tage an, bevor die volle Kapazität des Aggregats erreicht ist.

Wachstumsbereich

Im Wachstumsbereich können Sie die folgenden Schwellwerte für das Gesamtwachstum festlegen:

- **Wachstumsrate**

  Gibt den Prozentsatz an, bei dem die Wachstumsrate eines Aggregats als normal angesehen wird, bevor das System ein ungewöhnliches Ereignis für die aggregierte Wachstumsrate generiert.

- **Empfindlichkeit Der Wachstumsrate**

  Gibt den Faktor an, der auf die Standardabweichung der Wachstumsrate eines Aggregats angewendet wird. Wenn die Wachstumsrate die faktorierte Standardabweichung überschreitet, wird ein ungewöhnliches Ereignis für die aggregierte Wachstumsrate generiert.

  Ein niedrigerer Wert für die Wachstumsrate zeigt an, dass das Aggregat sehr empfindlich auf Veränderungen der Wachstumsrate reagiert.

> Wenn Sie die Wachstumssensitivität für Aggregate auf der globalen Schwellenebene ändern, wird die Änderung auch auf die Wachstumsratenempfindlichkeit für Volumes auf der globalen Schwellenebene angewendet.

Bereich der Snapshot-Kopien

Im Bereich Snapshot Kopien können Sie die folgenden Schwellwerte der Snapshot Reserve einstellen:

- **Snapshot Reserve Voll**

  Gibt den Prozentsatz an, an dem ein Aggregat den gesamten reservierten Speicherplatz für Snapshot Kopien verbraucht hat.

  Sie können auch den Schieberegler verwenden, um den Schwellenwert festzulegen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für ein ausgewähltes Aggregat ausführen:

- **Auf Standard zurücksetzen**

  Ermöglicht es Ihnen, die Schwellenwerte auf Aggregatebene auf die globalen Werte wiederherzustellen.

- **Speichern**

  Speichert alle Schwellwerteinstellungen.

- **Speichern und Schließen**

  Speichert alle Schwellwerteinstellungen und schließt das Dialogfeld.

- **Abbrechen**

  Ignoriert die Änderungen (falls vorhanden) an den Schwellenwerteinstellungen und schließt das Dialogfeld.

Dialogfeld „Volumenschwellenwerte bearbeiten“

Sie können Benachrichtigungen konfigurieren, um Benachrichtigungen zu senden, wenn ein Ereignis bezüglich der Kapazität eines Volume generiert wird, und Sie können Korrekturmaßnahmen für das Ereignis ergreifen. Beispielsweise können Sie für den Schwellenwert „Volume Full“ eine Meldung konfigurieren, um eine Benachrichtigung zu senden, wenn der Zustand über einen bestimmten Zeitraum beibehalten wird.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Im Dialogfeld Volume-Schwellenwerte bearbeiten können Sie Schwellenwerte auf Volume-Ebene konfigurieren, die auf die ausgewählten Volumes angewendet werden. Wenn Schwellenwerte auf Volume-Ebene konfiguriert werden, haben sie Vorrang vor den Schwellenwerten auf Gruppenebene oder den globalen Schwellenwerten.

Sie können Schwellenwerteinstellungen für Kapazität, Snapshot Kopien, qtree-Kontingent, Wachstum und Inodes auf Volume-Ebene konfigurieren. Wenn eine Gruppenaktion des Schwellenwerttyps des Volumes konfiguriert ist, werden die Schwellenwerte der Gruppenaktion für Einstellungen verwendet, die nicht auf der Volume-Ebene konfiguriert sind. Wenn keine Gruppenaktion des Volume-Schwellenwerttyps konfiguriert ist, verwenden Sie im Dialogfeld „Volumenschwellenwerte bearbeiten“ Bereiche, die nicht konfiguriert sind, globale Schwellenwerte.

Kapazität

Im Kapazitätsbereich können Sie die folgenden Schwellwerte für die Volume-Kapazität einstellen:

- **Raum Fast Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als fast voll angesehen wird. Er zeigt auch die Größe des Volumens an, die dem angegebenen Schwellenwert entspricht.

  Sie können auch den Schieberegler verwenden, um den Schwellenwert festzulegen.

- **Raum Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als voll betrachtet wird. Er zeigt auch die Größe des Volumens an, die dem angegebenen Schwellenwert entspricht.

Sie können auch den Schieberegler verwenden, um den Schwellenwert festzulegen.

- **Tage Bis Voll**

  Gibt die Anzahl der verbleibenden Tage an, bevor das Volume die volle Kapazität erreicht hat.

Snapshots

Im Bereich Snapshot Kopien können Sie die folgenden Schwellwerte für die Snapshot Kopien im Volume festlegen.

- **Snapshot Reserve Voll**

  Gibt den Prozentsatz an, mit dem der für Snapshot Kopien reservierte Speicherplatz als voll betrachtet wird.

- **Tage Bis Voll**

  Gibt die Anzahl der Tage an, die noch verbleiben, bevor der für Snapshot Kopien reservierte Speicherplatz mit der vollen Kapazität erreicht wird.

- * Anzahl*

  Gibt die Anzahl der Snapshot Kopien auf einem Volume an, die als zu viele Kopien gelten.

Qtree-Kontingentbereich

Der Qtree Quota Bereich ermöglicht es Ihnen, die folgenden qtree Quota Schwellenwerte für die ausgewählten Volumen festzulegen:

- **Fast Überengagiert**

  Gibt den Prozentsatz an, mit dem ein Volume als beinahe durch qtree Kontingente überengagiert werden soll.

- **Überengagiert**

  Gibt den Prozentsatz an, mit dem ein Volume als durch qtree Kontingente überengagiert werden soll.

Wachstumsbereich

Im Wachstumsbereich können Sie die folgende Schwellwertbedingung für das Volumenwachstum festlegen:

- **Wachstumsrate**

  Gibt den Prozentsatz an, bei dem die Wachstumsrate eines Volumes als normal angesehen wird, bevor das System ein ungewöhnliches Ereignis der Volumenwachstumsrate generiert.

- **Empfindlichkeit Der Wachstumsrate**

  Gibt den Faktor an, der auf die Standardabweichung der Wachstumsrate eines Volumens angewendet wird. Wenn die Wachstumsrate die faktorierte Standardabweichung überschreitet, wird ein ungewöhnliches Ereignis der Volumenwachstumsrate generiert.

  Ein niedrigerer Wert für die Empfindlichkeit der Wachstumsrate zeigt an, dass das Volumen sehr

empfindlich auf Veränderungen der Wachstumsrate reagiert.

Wenn Sie die Wachstumssensitivität für Volumes auf der globalen Schwellenebene ändern, wird die Änderung auch auf die Wachstumsratenempfindlichkeit für Aggregate auf der globalen Schwellenebene angewendet.

Inodes-Bereich

Im Inodes-Bereich können Sie die folgenden Schwellwerte für Inodes festlegen:

- **Fast Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als den Großteil seiner Inodes verbraucht wurde.

  Sie können auch die Schieberegler verwenden, um den Schwellenwert festzulegen.

- **Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als verbraucht wurde, alle Inodes verbraucht zu haben.

  Sie können auch die Schieberegler verwenden, um den Schwellenwert festzulegen.

Befehlsschaltflächen

Über die Schaltflächen können Sie die folgenden Aufgaben für ein ausgewähltes Volume ausführen:

- **Auf Standard zurücksetzen**

  Ermöglicht Ihnen, die Schwellenwerte auf einen der folgenden Werte wiederherzustellen:

  - Gruppenwerte, wenn das Volume zu einer Gruppe gehört und diese Gruppe über einen Aktionstyp Volume-Schwellenwert verfügt.
  - Globale Werte, wenn das Volume nicht zu einer Gruppe gehört oder zu einer Gruppe gehört, die keinen Aktionstyp für den Volumenschwellenwert hat.

- **Speichern**

  Speichert alle Schwellwerteinstellungen.

- **Speichern und Schließen**

  Speichert alle Schwellwerteinstellungen und schließt das Dialogfeld.

- **Abbrechen**

  Ignoriert die Änderungen (falls vorhanden) an den Schwellenwerteinstellungen und schließt das Dialogfeld.

Dialogfeld „Qtree-Schwellenwerte bearbeiten“

Sie können Benachrichtigungen konfigurieren, um Benachrichtigungen zu senden, wenn ein Ereignis bezüglich der Kapazität eines qtree generiert wird. Sie können Korrekturmaßnahmen für das Ereignis ergreifen. Beispielsweise können Sie für den Schwellenwert für qtree „voll“ eine Meldung konfigurieren, um eine Benachrichtigung zu

senden, wenn der Zustand über einen bestimmten Zeitraum beibehalten wird.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Im Dialogfeld Qtree-Schwellenwerte bearbeiten können Sie Schwellenwerte auf qtree-Ebene konfigurieren, die auf die ausgewählten qtrees angewendet werden. Wenn Schwellenwerte auf qtree-Ebene konfiguriert werden, haben sie Vorrang vor den Schwellenwerte auf Gruppenebene oder den globalen Schwellenwerten.

Sie können Schwellwerte für die Kapazität auf qtree-Ebene konfigurieren. Wenn eine Gruppenaktion des qtree Schwellenwerts konfiguriert wird, werden die Gruppenaktion Schwellenwerte für Einstellungen verwendet, die nicht auf qtree-Ebene konfiguriert sind. Wenn keine Gruppenaktion des qtree Schwellenwerts konfiguriert ist, verwenden Sie Bereiche im Dialogfeld Qtree-Schwellenwerte bearbeiten, die nicht konfiguriert sind, globale Schwellenwerte.

Kapazität

Im Kapazitätsbereich können Sie die folgenden qtree-Kapazitätsschwellenwerte festlegen:

- **Raum Fast Voll**

  Gibt den Prozentsatz an, bei dem ein qtree als fast voll erachtet wird. Er zeigt auch die Größe des qtree an, die dem angegebenen Schwellenwert entsprechen.

  Sie können auch den Schieberegler verwenden, um den Schwellenwert festzulegen.

- **Raum Voll**

  Gibt den Prozentsatz an, bei dem ein qtree als voll erachtet wird. Er zeigt auch die Größe des qtree an, die dem angegebenen Schwellenwert entsprechen.

  Sie können auch den Schieberegler verwenden, um den Schwellenwert festzulegen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie für einen ausgewählten qtree die folgenden Aufgaben ausführen:

- **Auf Standard zurücksetzen**

  Ermöglicht Ihnen, die Schwellenwerte auf einen der folgenden Werte wiederherzustellen:

  - Gruppenwerte, wenn der qtree zu einer Gruppe gehört und diese Gruppe über einen qtree Schwellenwert verfügt.
  - Globale Werte, wenn der qtree nicht zu einer Gruppe gehört oder zu einer Gruppe gehört, die keinen qtree Schwellenwert hat

- **Speichern**

  Speichert alle Schwellwerteinstellungen.

- **Speichern und Schließen**

  Speichert alle Schwellwerteinstellungen und schließt das Dialogfeld.

- **Abbrechen**

Ignoriert die Änderungen (falls vorhanden) an den Schwellenwerteinstellungen und schließt das Dialogfeld.

Verwalten von benutzerdefinierten Performance-Schwellenwerten

Mithilfe von Performance-Schwellenwertrichtlinien können Sie den Zeitpunkt bestimmen, an dem Unified Manager ein Ereignis generiert, um Systemadministratoren über Probleme zu informieren, die sich auf die Workload-Performance auswirken könnten. Diese Schwellenwertrichtlinien werden als „*user-defined* Performance Schwellenwerte“ bezeichnet.

Diese Version unterstützt benutzerdefinierte, systemdefinierte und dynamische Performance-Schwellenwerte. Bei dynamischen und systemdefinierten Performance-Schwellenwerten analysiert Unified Manager die Workload-Aktivität, um den entsprechenden Schwellwert zu ermitteln. Mit benutzerdefinierten Schwellenwerten können Sie die oberen Performance-Grenzen für viele Performance-Zähler und für viele Storage-Objekte definieren.

Systemdefinierte Performance-Schwellenwerte und dynamische Performance-Schwellenwerte werden von Unified Manager festgelegt und können nicht konfiguriert werden. Wenn Sie von einer systemdefinierten Performance-Schwellenwertrichtlinie unnötige Ereignisse erhalten, können Sie einzelne Richtlinien auf der Seite „Konfiguration/Ereignisse verwalten“ deaktivieren.

Funktionsweise benutzerdefinierter Richtlinien für Leistungsschwellenwerte

Sie legen für Storage-Objekte Richtlinien für Performance-Schwellenwerte fest (z. B. für Aggregate und Volumes), damit ein Ereignis an den Storage-Administrator gesendet werden kann, um den Administrator zu informieren, dass im Cluster ein Performance-Problem auftritt.

Sie erstellen eine Performance-Schwellenwertrichtlinie für ein Storage-Objekt durch:

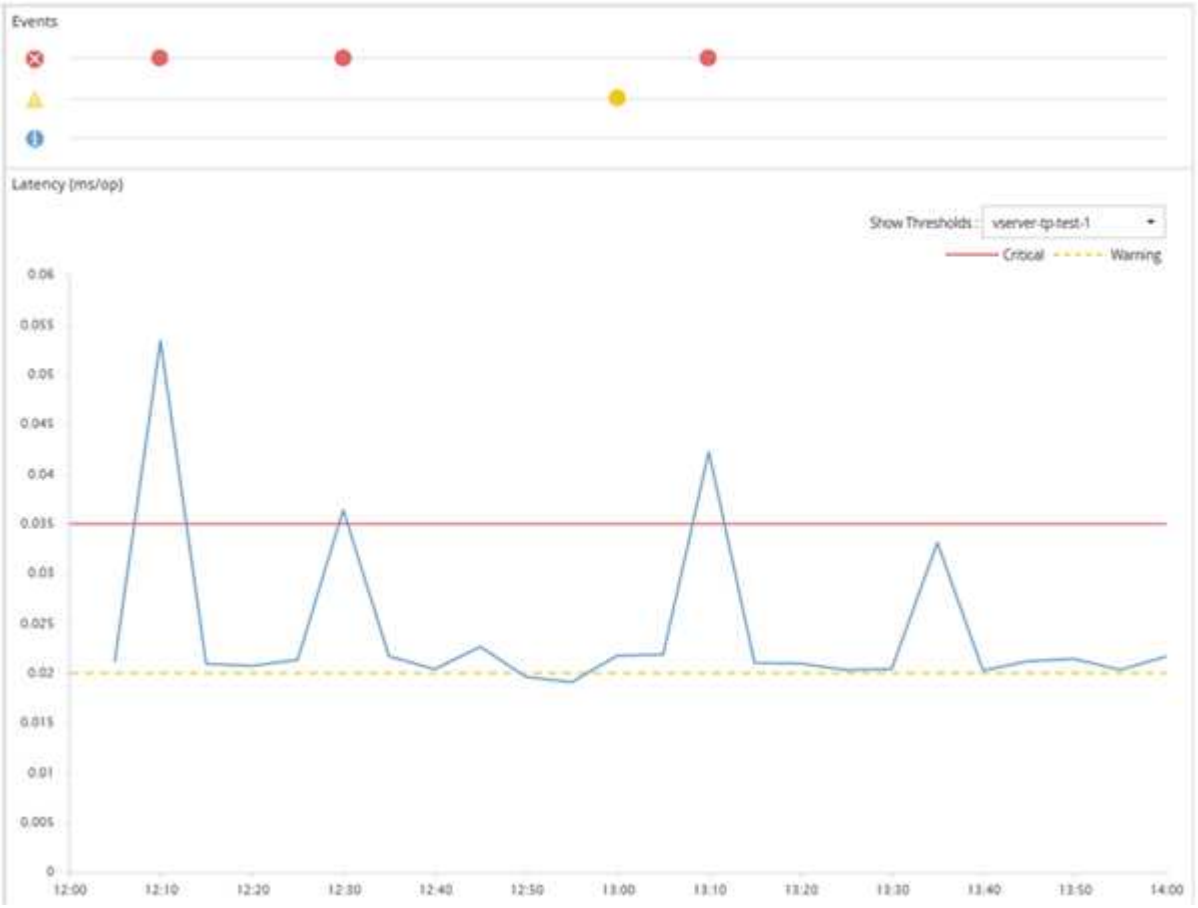
- Auswählen eines Storage-Objekts
- Auswählen eines Performance-Zählers, der diesem Objekt zugeordnet ist
- Festlegen von Werten, die die oberen Grenzwerte des Performance-Zählers definieren, die als Warnung und kritische Situationen gelten
- Geben Sie einen Zeitraum an, der definiert, wie lange der Zähler den oberen Grenzwert überschreiten muss

Beispielsweise können Sie eine Performance-Schwellenwertrichtlinie für ein Volume festlegen, damit Sie bei jedem IOPS für dieses Volume 750 in 10 aufeinanderfolgenden Minuten eine wichtige Ereignisbenachrichtigung erhalten. Diese Schwellenwertrichtlinie kann auch festlegen, dass ein Warnereignis gesendet wird, wenn IOPS mehr als 500 Operationen pro Sekunde für 10 Minuten beträgt.

Der aktuelle Release bietet Schwellenwerte, die Ereignisse senden, wenn ein Zählerwert die Schwellenwerteinstellung überschreitet. Sie können keine Schwellenwerte festlegen, die Ereignisse senden, wenn ein Zählerwert unter eine Schwellenwerteinstellung fällt.

Hier wird ein Beispiel für ein Zählerdiagramm angezeigt, das angibt, dass ein Warnschwellenwert (gelbes

Symbol) um 1:00 verletzt wurde und dass ein kritischer Schwellenwert (rotes Symbol) um 12:10, 12:30 und 1:10 Uhr verletzt wurde:



Für die angegebene Dauer muss eine Schwellenverletzung kontinuierlich auftreten. Wenn der Schwellenwert aus irgendeinem Grund unter die Grenzwerte fällt, wird eine spätere Verletzung als Beginn einer neuen Dauer betrachtet.

Durch einige Cluster-Objekte und Performance-Zähler können Sie eine kombinierte Schwellenwertrichtlinie erstellen, bei der zwei Performance-Zähler ihre Höchstgrenzen überschreiten müssen, bevor ein Ereignis generiert wird. Sie können beispielsweise anhand der folgenden Kriterien eine Schwellenwertrichtlinie erstellen:

Cluster-Objekt	Performance-Zähler	Warnschwellenwert	Kritischer Schwellenwert	Dauer
Datenmenge	Latenz	10 Millisekunden	20 Millisekunden	15 Minuten

Schwellenwertrichtlinien, die zwei Cluster-Objekte verwenden, führen dazu, dass ein Ereignis nur generiert wird, wenn beide Bedingungen nicht erfüllt sind. Beispiel anhand der in der Tabelle definierten Schwellwertrichtlinie:

Wenn Volume-Latenz durchschnittlich ist…	Und Festplatten-Auslastung aggregieren ist…	Dann…
15 Millisekunden	50 % erzielt	Es wird kein Ereignis gemeldet.

15 Millisekunden	75 % erzielt	Ein Warnereignis wird gemeldet.
25 Millisekunden	75 % erzielt	Ein Warnereignis wird gemeldet.
25 Millisekunden	90 % erzielt	Ein kritisches Ereignis wird gemeldet.

Was passiert, wenn eine Performance-Richtlinie nicht eingehalten wird

Wenn ein Zählerwert den definierten Performance-Schwellenwert für die in der Dauer angegebene Zeit überschreitet, wird der Schwellenwert überschritten und ein Ereignis wird gemeldet.

Das Ereignis veranlasst folgende Aktionen:

- Das Ereignis wird auf der Seite Performance Dashboard, der Seite Performance Cluster Summary, der Seite Events und der objektspezifischen Seite Performance Inventory angezeigt.
- (Optional) eine E-Mail-Benachrichtigung über das Ereignis kann an einen oder mehrere E-Mail-Empfänger gesendet werden, und ein SNMP-Trap kann an einen Trap-Empfänger gesendet werden.
- (Optional) Ein Skript kann ausgeführt werden, um Speicherobjekte automatisch zu ändern oder zu aktualisieren.

Die erste Aktion wird immer ausgeführt. Sie konfigurieren, ob die optionalen Aktionen auf der Seite Konfiguration/Warnmeldungen ausgeführt werden. Je nachdem, ob eine Warnung oder eine kritische Grenzwertrichtlinie nicht eingehalten wird, können Sie eindeutige Aktionen definieren.

Nach einer Richtlinienverletzung bei einem Performance-Schwellenwert für ein Storage-Objekt werden für diese Richtlinie keine weiteren Ereignisse generiert, bis der Zählerwert den Schwellenwert überschreitet und zu diesem Zeitpunkt wird die Dauer für dieses Limit zurückgesetzt. Während der Schwellenwert weiterhin überschritten wird, wird die Endzeit des Ereignisses kontinuierlich aktualisiert, sodass dieses Ereignis fortgesetzt wird.

Ein Schwellenwertereignis erfasst oder friert die Informationen in Bezug auf Schweregrad und Richtliniendefinition so ein, dass eindeutige Schwellenwertinformationen mit dem Ereignis angezeigt werden, auch wenn die Schwellenwertrichtlinie zukünftig geändert wird.

Welche Performance-Zähler können mithilfe von Schwellenwerten verfolgt werden

Einige allgemeine Performance-Zähler wie IOPS und MB/s können Schwellenwerte für alle Storage-Objekte festlegen. Es gibt andere Zähler, deren Schwellenwerte nur für bestimmte Speicherobjekte festgelegt werden können.

Verfügbare Performance-Zähler

Storage Objekt	Performance-Zähler	Beschreibung
Cluster	IOPS	Durchschnittliche Anzahl von ein-/Ausgabeoperationen, die das Cluster pro Sekunde verarbeitet.

Storage Objekt	Performance-Zähler	Beschreibung
MB/Sek.	Durchschnittliche Anzahl der Megabyte an Daten, die in diesen und von diesem Cluster pro Sekunde übertragen werden.	Knoten
IOPS	Durchschnittliche Anzahl der ein-/Ausgabevorgänge der Knoten verarbeitet pro Sekunde.	MB/Sek.
Durchschnittliche Anzahl der Megabyte an Daten, die in diesen Node pro Sekunde übertragen werden.	Latenz	Durchschnittliche Anzahl von Millisekunden, in denen der Node auf Applikationsanforderungen reagiert.
Auslastung	Durchschnittlicher Prozentsatz der CPU und des RAM des Node, der verwendet wird.	Verwendete Performance-Kapazität
Durchschnittlicher Prozentsatz der Performance-Kapazität, die vom Node verbraucht wird.	Verwendete Performance-Kapazität – Übernahme	Durchschnittlicher Prozentsatz der Performance-Kapazität, die vom Node verbraucht wird, sowie die Performance-Kapazität des Partner-Nodes.
Aggregat	IOPS	Durchschnittliche Anzahl der ein-/Ausgabevorgänge die aggregierten Prozesse pro Sekunde.
MB/Sek.	Durchschnittliche Anzahl der Megabyte an Daten, die in dieses Aggregat pro Sekunde übertragen werden.	Latenz
Durchschnittliche Anzahl von Millisekunden, die das Aggregat zur Reaktion auf Applikationsanforderungen benötigt.	Auslastung	Durchschnittlicher Prozentsatz der verwendeten Festplatten des Aggregats.
Verwendete Performance-Kapazität	Durchschnittlicher Prozentsatz der Performance-Kapazität, die vom Aggregat verbraucht wird.	Storage Virtual Machine (SVM)
IOPS	Durchschnittliche Anzahl von ein-/Ausgabevorgängen, die die SVM in einer Sekunde verarbeitet	MB/Sek.

Storage Objekt	Performance-Zähler	Beschreibung
Durchschnittliche Anzahl der in und von dieser SVM pro Sekunde übertragenen Megabyte.	Latenz	Durchschnittliche Anzahl von Millisekunden, die SVM zur Beantwortung von Applikationsanforderungen benötigt.
Datenmenge	IOPS	Durchschnittliche Anzahl der ein-/Ausgabevorgänge die Volume-Prozesse pro Sekunde.
MB/Sek.	Durchschnittliche Anzahl der Megabyte an Daten, die in dieses Volume pro Sekunde übertragen werden.	Latenz
Durchschnittliche Anzahl von Millisekunden, die das Volume zur Beantwortung von Applikationsanforderungen benötigt.	Cache-fehlsverhältnis	Durchschnittlicher Prozentsatz von Leseanforderungen von Client-Applikationen, die vom Volume zurückgegeben werden, anstatt vom Cache zurückgegeben zu werden.
LUN	IOPS	Durchschnittliche Anzahl der ein-/Ausgabevorgänge, die das LUN pro Sekunde verarbeitet.
MB/Sek.	Durchschnittliche Anzahl der Megabyte an Daten, die in diese LUN pro Sekunde übertragen werden.	Latenz
Durchschnittliche Anzahl von Millisekunden, die die LUN benötigt, um auf Applikationsanforderungen zu reagieren.	Namespace	IOPS
Durchschnittliche Anzahl der ein-/Ausgabevorgänge, die der Namespace pro Sekunde verarbeitet.	MB/Sek.	Durchschnittliche Anzahl der Megabyte an Daten, die in diesen Namespace pro Sekunde übertragen werden.
Latenz	Durchschnittliche Anzahl von Millisekunden, in denen der Namespace auf Applikationsanforderungen reagiert.	Port

Storage Objekt	Performance-Zähler	Beschreibung
Bandbreitenauslastung	Durchschnittlicher Prozentsatz der verfügbaren Bandbreite des Ports, die verwendet wird.	MB/Sek.
Durchschnittliche Anzahl der Megabyte an Daten, die in diesen Port pro Sekunde übertragen werden.	Logische Schnittstelle (LIF)	MB/Sek.

Daten zur Performance-Kapazität sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.

Welche Objekte und Zähler können in Schwellwertrichtlinien für Kombinationen verwendet werden

Nur einige Leistungsindikatoren können in Kombinationsrichtlinien kombiniert werden. Wenn primäre und sekundäre Performance-Zähler angegeben werden, müssen beide Performance-Zähler ihre Höchstgrenzen überschreiten, bevor ein Ereignis generiert wird.

Primäres Speicherobjekt und Zähler	Sekundäres Storage Objekt und Zähler
Volume-Latenz	Volume IOPS
Volumen-Mbps	Aggregatauslastung
Verwendete Aggregat-Performance-Kapazität	Node-Auslastung
Verwendete Node-Performance-Kapazität	Verwendete Node-Performance-Kapazität – Übernahme
LUN-Latenz	LUN IOPS
LUN MBit/Sek.	Aggregatauslastung
Verwendete Aggregat-Performance-Kapazität	Node-Auslastung
Verwendete Node-Performance-Kapazität	Verwendete Node-Performance-Kapazität – Übernahme

Wenn eine Richtlinie für eine Volume-Kombination auf ein FlexGroup Volume anstatt auf ein FlexVol Volume angewendet wird, können nur die Attribute „`Volume IOPS`“ und „`Volume Mbps`“ als sekundärer Zähler ausgewählt werden. Wenn die Schwellenwertrichtlinie eines der Node- oder Aggregatattribute enthält, wird die Richtlinie nicht auf das FlexGroup Volume angewendet. Die hier vorliegende Fehlermeldung wird veröffentlicht. Der Grund dafür ist, dass FlexGroup Volumes auf mehr als einem Node oder Aggregat vorhanden sein können.

Benutzerdefinierte Richtlinien für Leistungsschwellenwerte werden erstellt

Sie erstellen Performance-Schwellenwertrichtlinien für Storage-Objekte, damit Benachrichtigungen gesendet werden, wenn ein Performance-Zähler einen bestimmten Wert überschreitet. Die Ereignisbenachrichtigung identifiziert, dass ein Performance-Problem auf dem Cluster auftritt.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Sie erstellen Richtlinien für Leistungsschwellenwerte, indem Sie die Schwellenwerte auf der Seite Schwellenwertrichtlinie erstellen eingeben. Sie können neue Richtlinien erstellen, indem Sie alle Richtlinienwerte auf dieser Seite definieren, oder Sie können eine Kopie einer vorhandenen Richtlinie erstellen und die Werte in der Kopie ändern (genannt *Cloning*).

Gültige Schwellenwerte sind 0.001 bis 10,000,000 für Zahlen, 0.001-100 für Prozentsätze und 0.001-200 für Performance-Kapazität verwendet Prozentwerte.

Der aktuelle Release bietet Schwellenwerte, die Ereignisse senden, wenn ein Zählerwert die Schwellenwerteinstellung überschreitet. Sie können keine Schwellenwerte festlegen, die Ereignisse senden, wenn ein Zählerwert unter eine Schwellenwerteinstellung fällt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Konfiguration** > **Leistungsschwellenwerte**.

   Die Seite Konfiguration/Leistungsschwellenwerte wird angezeigt.

2. Je nachdem, ob Sie eine neue Richtlinie erstellen möchten oder eine ähnliche Richtlinie klonen und die geklonte Version ändern möchten, klicken Sie auf die entsprechende Schaltfläche.

An…	Klicken Sie Auf…
Erstellen Sie eine neue Richtlinie	**Erstellen**
Vorhandene Richtlinie klonen	Wählen Sie eine vorhandene Richtlinie aus, und klicken Sie auf **Clone**

   Die Seite Schwellenwertrichtlinie erstellen oder Schwellenwertrichtlinie klonen wird angezeigt.

3. Definieren Sie die Schwellenwertrichtlinie, indem Sie die Performance-Zählerschwellenwerte angeben, die für bestimmte Storage-Objekte festgelegt werden sollen:

   a. Wählen Sie den Speicherobjekttyp aus, und geben Sie einen Namen und eine Beschreibung für die Richtlinie an.

   b. Wählen Sie den zu verfollenden Leistungszähler aus und geben Sie die Grenzwerte an, die Warnungs- und kritische Ereignisse definieren.

      Sie müssen mindestens eine Warnung oder einen kritischen Grenzwert definieren. Sie müssen nicht

beide Arten von Limits definieren.

c. Wählen Sie ggf. einen sekundären Leistungsindikenzähler aus und geben Sie die Grenzwerte für Warnungs- und kritische Ereignisse an.

   Zum Einbeziehen eines sekundären Zählers müssen beide Zähler die Grenzwerte überschreiten, bevor der Schwellenwert überschritten wird und ein Ereignis gemeldet wird. Es können nur bestimmte Objekte und Zähler anhand einer Kombinationsrichtlinie konfiguriert werden.

d. Wählen Sie die Dauer aus, für die die Grenzwerte für ein zu sendes Ereignis überschritten werden müssen.

Beim Klonen einer vorhandenen Richtlinie müssen Sie einen neuen Namen für die Richtlinie eingeben.

4. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

   Sie gelangen wieder zur Seite Konfigurations-/Performance-Schwellenwerte. Eine Erfolgsmeldung oben auf der Seite bestätigt, dass die Schwellenwertrichtlinie erstellt wurde und einen Link zur Inventarseite für diesen Objekttyp enthält, damit Sie die neue Richtlinie sofort auf Speicherobjekte anwenden können.

Nachdem Sie fertig sind

Wenn Sie die neue Schwellenwertrichtlinie zu diesem Zeitpunkt auf Speicherobjekte anwenden möchten, können Sie auf den Link **Gehe zu Object_type now** klicken, um zur Inventarseite zu gelangen.

Zuweisen von Richtlinien zu Performance-Schwellenwerten zu Storage-Objekten

Sie weisen einem Storage-Objekt eine benutzerdefinierte Performance-Schwellenwertrichtlinie zu, damit Unified Manager ein Ereignis meldet, wenn der Wert des Performance-Zählers die Richtlinieneinstellung überschreitet.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Die Richtlinie für Performance-Schwellenwerte oder -Richtlinien, die Sie auf das Objekt anwenden möchten, müssen vorhanden sein.

Über diese Aufgabe

Sie können nur eine Performance-Richtlinie gleichzeitig auf ein Objekt oder eine Gruppe von Objekten anwenden.

Sie können jedem Storage-Objekt maximal drei Schwellenwertrichtlinien zuweisen. Wenn bei der Zuweisung von Richtlinien zu mehreren Objekten bereits die maximale Anzahl an Richtlinien zugewiesen ist, führt Unified Manager die folgenden Aktionen durch:

- Wendet die Richtlinie auf alle ausgewählten Objekte an, die ihr Maximum nicht erreicht haben
- Ignoriert die Objekte, die die maximale Anzahl von Richtlinien erreicht haben
- Zeigt eine Meldung an, dass die Richtlinie nicht allen Objekten zugewiesen wurde

Wenn zudem einige Objekte den in der Schwellenwertrichtlinie verfolgten Zähler nicht unterstützen, wird die Richtlinie nicht auf das Objekt angewendet. Wenn Sie beispielsweise eine Schwellenwertrichtlinie

„`Performance Capacity used`“ erstellen und sie dann einem Node zuweisen, der über keine ONTAP 9.0 oder höher installierte Software verfügt, wird die Richtlinie nicht auf diesen Node angewendet.

Schritte

1. Wählen Sie auf der Seite „Performance Inventory“ eines beliebigen Storage-Objekts das Objekt oder die Objekte aus, denen Sie eine Schwellenwertrichtlinie zuweisen möchten:

So weisen Sie Schwellenwerte zu…	Klicken Sie Auf…
Ein einzelnes Objekt	Das Kontrollkästchen links neben dem Objekt.
Mehrere Objekte	Das Kontrollkästchen links von jedem Objekt.
Alle Objekte auf der Seite	Der ☐▾ Dropdown-Feld, und wählen Sie **Wählen Sie alle Objekte auf dieser Seite** aus.
Alle Objekte desselben Typs	Der ☐▾ Dropdown-Feld, und wählen Sie **Alle Objekte auswählen**.

   Mithilfe der Sortier- und Filterfunktion können Sie die Objektliste auf der Bestandsseite verfeinern, um die Anwendung von Schwellenwertrichtlinien auf viele Objekte zu erleichtern.

2. Treffen Sie Ihre Auswahl und klicken Sie dann auf **Richtlinie für Leistungsschwellenwert zuweisen**.

   Die Seite „Grenzwertrichtlinie zuweisen“ wird angezeigt und zeigt eine Liste von Schwellenwertrichtlinien an, die für diesen spezifischen Typ von Speicherobjekt vorhanden sind.

3. Klicken Sie auf die einzelnen Richtlinien, um die Details zu den Einstellungen für den Leistungsschwellenwert anzuzeigen, um zu überprüfen, ob Sie die richtige Schwellenwertrichtlinie ausgewählt haben.
4. Klicken Sie nach Auswahl der entsprechenden Schwellenwertrichtlinie auf **Richtlinie zuweisen**.

   Eine Erfolgsmeldung oben auf der Seite bestätigt, dass die Schwellenwertrichtlinie dem Objekt oder den Objekten zugewiesen wurde und stellt einen Link zur Seite Alerting bereit, sodass Sie die Warnungseinstellungen für dieses Objekt und die Richtlinie konfigurieren können.

Nachdem Sie fertig sind

Wenn Sie Benachrichtigungen über E-Mail oder als SNMP-Trap senden möchten, um Sie darüber zu informieren, dass ein bestimmtes Leistungsereignis generiert wurde, müssen Sie die Alarmeinstellungen auf der Seite Konfiguration/Alarmauslösung konfigurieren.

Anzeigen von Richtlinien für Performance-Schwellenwerte

Sie können alle derzeit definierten Performance-Schwellenwertrichtlinien auf der Seite Konfiguration/Performance-Schwellenwerte anzeigen.

Über diese Aufgabe

Die Liste der Schwellenwertrichtlinien wird alphabetisch nach Richtlinienname sortiert und umfasst Richtlinien

für alle Arten von Storage-Objekten. Sie können auf eine Spaltenüberschrift klicken, um die Richtlinien nach dieser Spalte zu sortieren. Wenn Sie nach einer bestimmten Richtlinie suchen, können Sie mithilfe der Filter- und Suchmechanismen die Liste der Schwellenwertrichtlinien, die in der Bestandsliste angezeigt werden, verfeinern.

Sie können den Mauszeiger über den Richtliniennamen und den Bedingungsnamen bewegen, um die Konfigurationsdetails der Richtlinie anzuzeigen. Zusätzlich können Sie mithilfe der bereitgestellten Schaltflächen benutzerdefinierte Schwellenwertrichtlinien erstellen, klonen, bearbeiten und löschen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Konfiguration** > **Leistungsschwellenwerte**.

   Die Seite Konfiguration/Leistungsschwellenwerte wird angezeigt.

Bearbeiten benutzerdefinierter Richtlinien für Leistungsschwellenwerte

Sie können die Schwellenwerteinstellungen für vorhandene Performance-Schwellenwertrichtlinien bearbeiten. Dies kann nützlich sein, wenn Sie feststellen, dass Sie zu viele oder zu wenige Warnmeldungen für bestimmte Schwellwerte erhalten.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Sie können den Richtliniennamen oder den Typ des Storage-Objekts, das für vorhandene Schwellenwertrichtlinien überwacht wird, nicht ändern.

Schritte

1. Wählen Sie im linken Navigationsbereich **Konfiguration** > **Leistungsschwellenwerte**.

   Die Seite Konfigurations-/Leistungsschwellenwerte wird angezeigt.

2. Wählen Sie die Schwellenwertrichtlinie aus, die Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

   Die Seite „Schwellenwertrichtlinie bearbeiten“ wird angezeigt.

3. Nehmen Sie Ihre Änderungen an der Schwellenwertrichtlinie vor und klicken Sie auf **Speichern**.

   Sie gelangen wieder zur Seite Konfigurations-/Performance-Schwellenwerte.

Ergebnisse

Nachdem sie gespeichert wurden, werden Änderungen sofort für alle Speicherobjekte aktualisiert, die die Richtlinie verwenden.

Nachdem Sie fertig sind

Je nach Art der Änderungen, die Sie an der Richtlinie vorgenommen haben, sollten Sie möglicherweise die für die Objekte konfigurierten Warnungseinstellungen überprüfen, die die Richtlinie auf der Seite

Konfiguration/Alarmauslösung verwenden.

Entfernen von Richtlinien für Performance-Schwellenwerte aus Storage-Objekten

Sie können eine benutzerdefinierte Performance-Schwellenwertrichtlinie aus einem Storage-Objekt entfernen, wenn Unified Manager den Wert des Performance-Zählers nicht mehr überwachen soll.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Sie können jeweils nur eine Richtlinie aus einem ausgewählten Objekt entfernen.

Sie können eine Schwellenwertrichtlinie aus mehreren Speicherobjekten entfernen, indem Sie mehr als ein Objekt in der Liste auswählen.

Schritte

1. Wählen Sie auf der Seite **Inventory** eines Speicherobjekts ein oder mehrere Objekte aus, auf denen mindestens eine Richtlinie für Leistungsschwellenwerte angewendet wurde.

So löschen Sie Schwellenwerte aus…	Tun Sie das…
Ein einzelnes Objekt	Aktivieren Sie das Kontrollkästchen links neben dem Objekt.
Mehrere Objekte	Aktivieren Sie das Kontrollkästchen links neben jedem Objekt.
Alle Objekte auf der Seite	Klicken Sie Auf Und wählen Sie **Wählen Sie alle Objekte auf dieser Seite** aus.
Alle Objekte desselben Typs	Klicken Sie Auf Und wählen Sie **Alle Objekte auswählen**.

2. Klicken Sie Auf **Richtlinie Für Leistungsschwellenwert Löschen**.

   Auf der Seite Schwellenwertrichtlinie löschen wird eine Liste mit Schwellenwertrichtlinien angezeigt, die den Speicherobjekten derzeit zugewiesen sind.

3. Wählen Sie die Schwellenwertrichtlinie aus, die Sie aus den Objekten entfernen möchten, und klicken Sie auf **Richtlinie löschen**.

   Wenn Sie eine Schwellenwertrichtlinie auswählen, werden die Details der Richtlinie angezeigt, damit Sie bestätigen können, dass Sie die entsprechende Richtlinie ausgewählt haben.

Was passiert, wenn eine Performance-Schwellenwertrichtlinie geändert wird

Wenn Sie den Zählerwert oder die Dauer einer vorhandenen Richtlinie für den Performance-Schwellenwert anpassen, wird die Richtlinienänderung auf alle Storage-Objekte angewendet, die die Richtlinie verwenden. Die neue Einstellung erfolgt sofort und Unified Manager beginnt, die Performance-Zählerwerte mit den neuen Schwellenwerten für alle neu erfassten Performance-Daten zu vergleichen.

Falls für Objekte, die die geänderte Schwellenwertrichtlinie verwenden, aktive Ereignisse vorhanden sind, werden die Ereignisse als veraltet markiert, und die Schwellenwertrichtlinie beginnt, den Zähler als neu definierte Schwellenwertrichtlinie zu überwachen.

Wenn Sie den Zähler anzeigen, auf dem der Schwellenwert in der Detailansicht Zählerdiagramme angewendet wurde, spiegeln die kritischen und Warnschwellenwerte die aktuellen Schwellenwerteinstellungen wider. Die ursprünglichen Schwellwerteinstellungen werden auf dieser Seite nicht angezeigt, auch wenn Sie historische Daten anzeigen, wenn die alte Schwellenwerteinstellung wirksam war.

Da ältere Schwellenwerteinstellungen nicht in der detaillierten Ansicht der Zählerdiagramme angezeigt werden, werden möglicherweise historische Ereignisse unter den aktuellen Schwellenwerten angezeigt.

Was passiert mit Performance-Schwellenwertrichtlinien, wenn ein Objekt verschoben wird

Da Performance-Schwellenwertrichtlinien Storage-Objekten zugewiesen werden. Wenn Sie ein Objekt verschieben, bleiben alle zugewiesenen Schwellenwertrichtlinien nach Abschluss der Verschiebung mit dem Objekt verbunden. Wenn Sie beispielsweise ein Volume oder eine LUN zu einem anderen Aggregat verschieben, sind die Schwellenwertrichtlinien weiterhin für das Volume oder die LUN auf dem neuen Aggregat aktiv.

Wenn für die Schwellenwertrichtlinie eine sekundäre Zählerbedingung (eine Kombinationsrichtlinie) besteht – z. B. wenn einem Aggregat oder einem Node eine zusätzliche Bedingung zugewiesen ist – wird die sekundäre Zählerbedingung auf das neue Aggregat bzw. den Node angewendet, auf das das Volume oder die LUN verschoben wurde.

Falls für Objekte, die die geänderte Schwellenwertrichtlinie verwenden, neue aktive Ereignisse vorhanden sind, werden die Ereignisse als veraltet markiert und die Schwellenwertrichtlinie beginnt, den Zähler als neu definierte Schwellenwertrichtlinie zu überwachen.

Ein Vorgang zum Verschieben eines Volumes führt dazu, dass ONTAP ein Informationseränderungsereignis sendet. Auf der Seite „Performance Explorer“ und auf der Seite „Performance/Volume Details“ wird ein Symbol für das Änderungsereignis angezeigt, um die Uhrzeit anzugeben, zu der der Vorgang abgeschlossen wurde.

Wenn Sie ein Objekt in ein anderes Cluster verschieben, wird die benutzerdefinierte Schwellenwertrichtlinie aus dem Objekt entfernt. Falls erforderlich, müssen Sie dem Objekt nach Abschluss des Verschiebevorgangs eine Schwellenwertrichtlinie zuweisen. Dynamische und systemdefinierte Schwellenwertrichtlinien werden jedoch nach dem Verschieben in ein neues Cluster automatisch auf ein Objekt angewendet.

Schwellenwertrichtlinien-Funktionalität während HA Takeover und Giveback

Wenn ein Takeover- oder Giveback-Vorgang in einer Hochverfügbarkeits-(HA-)Konfiguration durchgeführt werden, behalten Objekte, die von einem Node auf den anderen Node verschoben werden, ihre Schwellenwertrichtlinien auf dieselbe Weise wie bei der manuellen Verschiebung bei. Da Unified Manager alle 15 Minuten nach Änderungen der Cluster-Konfiguration sucht, werden die Auswirkungen der Umschaltung auf den neuen Node erst nach der nächsten Abfrage der Cluster-Konfiguration identifiziert.

Wenn sowohl ein Takeover- als auch ein Giveback-Vorgang innerhalb des Erfassungszeitraums von 15 Minuten Konfigurationsänderungen durchgeführt werden, werden die Performance-Statistiken von einem Node zu einem anderen Node verschoben.

Schwellenwertrichtlinien während der Aggregatverschiebung

Wenn Sie ein Aggregat mithilfe von von von einem Node zu einem anderen Node verschieben `aggregate relocation start` Der Befehl wird sowohl für alle Objekte als auch für kombinierte Schwellwerte beibehalten und der Node-Teil der Schwellenwertrichtlinie wird auf den neuen Node angewendet.

Schwellenwertrichtlinien während der MetroCluster Umschaltung

Objekte, die in einer MetroCluster-Konfiguration von einem Cluster zu einem anderen Cluster verschoben werden, behalten ihre benutzerdefinierten Richtlinieneinstellungen nicht bei. Bei Bedarf können Sie Schwellenwertrichtlinien für die Volumes und LUNs anwenden, die zum Partner-Cluster verschoben wurden. Nachdem ein Objekt zurück in das ursprüngliche Cluster verschoben wurde, wird die benutzerdefinierte Schwellenwertrichtlinie automatisch neu angewendet.

Volume-Verhalten während des Umschalens und Zurück

Beschreibungen der Seiten für Richtlinien zu Leistungsschwellenwerten

Sie verwenden die Seite Configuration/Performance schwellungen, um Richtlinien für Performance-Schwellenwerte zu erstellen, zu bearbeiten, zu klonen, zu löschen und anzuzeigen.

Die folgenden Themen werden angezeigt, wenn Sie auf der entsprechenden Seite auf **Hilfe** klicken.

Seite „Konfigurations-/Performance-Schwellenwerte“ beschrieben

Über die Seite Konfiguration/Performance-Schwellenwerte können Sie alle aktuell definierten Performance-Schwellenwertrichtlinien anzeigen. Diese Seite bietet auch die Funktionen zum Erstellen, Klonen, Bearbeiten und Löschen von Schwellenwertrichtlinien.

Die Liste der Performance-Schwellenwertrichtlinien wird alphabetisch nach Richtliniennamen sortiert. Sie können auf eine Spaltenüberschrift klicken, um die Richtlinien nach dieser Spalte zu sortieren. Wenn Sie nach einer bestimmten Richtlinie suchen, können Sie die Filter- und Suchmechanismen verwenden, um die Liste der Schwellenwertrichtlinien, die in der Bestandsliste angezeigt werden, zu verfeinern.

Filter- und Suchleiste

Mit der Schaltfläche **Filtern** können Sie die Liste der Schwellenwertrichtlinien verfeinern, indem Sie nur die Richtlinien anzeigen, die bestimmten Kriterien entsprechen.

Mit der Schaltfläche **Suchen** können Sie nach bestimmten Richtlinien suchen, indem Sie vollständige oder

partielle Richtliniennamen eingeben, um die Liste der Schwellenwertrichtlinien, die in der Bestandsliste angezeigt werden, zu verfeinern.

Befehlsschaltflächen

- **Erstellen**

  Erstellt eine neue Richtlinie für Leistungsschwellenwerte.

- **Klonen**

  Erstellt auf der Grundlage einer Kopie der ausgewählten Richtlinie eine neue Richtlinie für Leistungsschwellenwerte.

- **Bearbeiten**

  Ändert die von Ihnen ausgewählte Performance-Schwellenwertrichtlinie. Alle Speicherobjekte, die die Richtlinie verwenden, werden aktualisiert und verwenden die überarbeitete Richtlinie.

- **Löschen**

  Löscht die Richtlinie für Leistungsschwellenwerte, die Sie ausgewählt haben. Die Richtlinie wird aus allen Storage-Objekten, die diese Richtlinie verwenden, entfernt. Sie können auf das Element in der Spalte Associated Objects klicken, um die Objekte anzuzeigen, die diese Richtlinie derzeit verwenden.

Liste der Schwellenwertrichtlinien

- **Policy Name**

  Zeigt den Namen der Schwellenwertrichtlinie an. Sie können Ihren Cursor über den Richtliniennamen positionieren, um die Details der Richtlinie anzuzeigen.

- **Beschreibung**

  Zeigt eine kurze Beschreibung der Schwellenwertrichtlinie an.

- **Erste Bedingung**

  Zeigt die primäre Bedingung für die Schwellenwertrichtlinie an, einschließlich des definierten Performance-Zählers, der Werte für Warnmeldungen und der kritischen Triggerwerte. Sie können den Cursor über den Bedingungsnamen positionieren, um die Details der Bedingung anzuzeigen.

- **Zweiter Zustand**

  Zeigt die Bedingung für die sekundäre Schwellenwertrichtlinie an, falls definiert. Sie können den Cursor über den Bedingungsnamen positionieren, um die Details der Bedingung anzuzeigen. Wenn keine zweite Bedingung definiert ist, ist diese Spalte leer.

  > Wenn eine zweite Bedingung definiert ist, wird ein Ereignis nur erzeugt, wenn beide Bedingungen verletzt werden.

- **Assoziierte Objekte**

  Zeigt den Typ des Speicherobjekts an, auf das die Schwellenwertrichtlinie angewendet werden kann, und die Anzahl der Objekte, die die Richtlinie verwenden. Dieses Feld ist leer, bis Sie die Richtlinie mindestens

einem Objekt zuweisen.

Sie können auf die Spaltenüberschrift klicken, um die Richtlinien nach Objekttyp zu sortieren: Volume, LUN, Aggregat usw. Sie können auf den Richtliniennamen klicken, um die Bestandsseite anzuzeigen, die mit den Objekten ausgefüllt wird, die die Schwellenwertrichtlinie derzeit verwenden.

Seite „Performance Threshold Policy“ erstellen oder klonen

Sie können auf der Seite „Schwellenwertrichtlinie erstellen“ oder auf der Seite „Schwellenwertrichtlinie klonen“ eine neue Richtlinie für Leistungsschwellenwerte erstellen.

Sie können die Felder auf dieser Seite ausfüllen und auf **Speichern** klicken, um eine Richtlinie für Leistungsschwellenwerte hinzuzufügen.

- **Für Objekttyp**

  Wählen Sie den Typ des Speicherobjekts aus, für das Sie eine Schwellenrichtlinie erstellen möchten.

- **Policy Name**

  Geben Sie den Namen der Schwellenwertrichtlinie ein. Der Name wird auf anderen Unified Manager-Seiten angezeigt und sollte eine kurze Beschreibung der Richtlinie enthalten.

- **Beschreibung**

  (Optional) Geben Sie eine detaillierte Beschreibung der Schwellenwertrichtlinie ein.

- **Schwellenwerte**

  Definieren Sie die primäre und optional die sekundäre Schwellwertzählbedingung. Zum Einbeziehen eines sekundären Zählers müssen beide Zähler die Grenzwerte überschreiten, bevor der Schwellenwert als überschritten betrachtet wird.

  - **Wählen Sie einen Zähler**

    Wählen Sie den Zähler aus, für den Sie einen Leistungsschwellenwert festlegen möchten.

  - **Warnung**

    Geben Sie den Grenzwert für den Zähler ein, der als Warnung betrachtet wird.

  - * Kritisch*

    Geben Sie den Grenzwert für den Zähler ein, der als kritisch angesehen wird.

  Gültige Schwellenwerte sind 0.001 bis 10,000,000 für Zahlen, 0.001-100 für Prozentsätze und 0.001-200 für Performance-Kapazität verwendet Prozentwerte.

- **Dauer**

  Wählen Sie die Anzahl der Minuten aus, die der Zählerwert größer sein muss als der Warnwert oder der kritische Grenzwert. Da Unified Manager alle fünf Minuten neue Performance-Zählerwerte erfasst, enthält das Menü basierend auf dem Aktualisierungsintervall Werte in einem Vielfachen von fünf.

Seite „Richtlinie für Leistungsschwellenwert bearbeiten“

Auf der Seite „Schwellenwertrichtlinie bearbeiten“ können Sie eine vorhandene Richtlinie für Leistungsschwellenwerte ändern.

Sie können die Felder auf dieser Seite ändern und auf **Speichern** klicken, um eine Richtlinie für Leistungsschwellenwerte zu ändern. Alle Cluster-Objekte, die derzeit die Schwellenwertrichtlinie verwenden, werden automatisch aktualisiert und verwenden die neue Richtliniendefinition.

- **Für Objekttyp**

  Objekttyp kann nicht geändert werden.

- **Policy Name**

  Ändern Sie den Namen der Schwellenwertrichtlinie.

- **Beschreibung**

  Ändern Sie die detaillierte Beschreibung der Schwellenwertrichtlinie.

- **Schwellenwerte**

  Ändern Sie den primären und optional den sekundären Schwellenwert-Zählerzustand.

  - **Wählen Sie einen Zähler**

    Ändern Sie den Zähler, auf dem Sie einen Performance-Schwellenwert festlegen möchten.

  - **Warnung**

    Geben Sie den Grenzwert für den Zähler ein, der als Warnung betrachtet wird.

  - * Kritisch*

    Geben Sie den Grenzwert für den Zähler ein, der als kritisch angesehen wird.

- **Dauer**

  Ändern Sie die Anzahl der Minuten, die der Zählerwert größer sein muss als der Warnungs- oder der kritische Grenzwert.

Seite „Richtlinie für Leistungsschwellenwert zuweisen“

Auf der Seite „Grenzwertrichtlinie zuweisen“ können Sie einem oder mehreren Speicherobjekten eine Richtlinie für Leistungsschwellenwerte zuweisen.

Die Liste der Richtlinien wird nur mit den Richtlinien ausgefüllt, die für den Storage-Objekttyp gültig sind.

Wählen Sie die Richtlinie aus, die Sie auf das Objekt oder die Objekte anwenden möchten, und klicken Sie dann auf **Richtlinie anwenden**.

Es gibt einige Fälle, in denen beim Versuch, eine Richtlinie anzuwenden, eine Fehlermeldung angezeigt wird:

- Beim Anwenden einer Richtlinie, die die Performance-Kapazität verwendet, wird der Zähler auf einen Node oder Aggregat angewendet, der nicht mit der Software ONTAP 9.0 oder höher installiert ist.

  Versionen der ONTAP Software vor 9.0 unterstützen die Performance-Kapazitäts-Zähler nicht.

- Beim Anwenden einer Kombinationsrichtlinie auf ein FlexGroup Volume, bei dem der zweite Zähler entweder einen Node oder ein Aggregatobjekt beinhaltet.

  Da FlexGroup Volumes über mehrere Nodes und Aggregate verteilt werden können, ist dieser Vorgang nicht zulässig.

Löschen Sie die Seite Richtlinie für Leistungsschwellenwert

Mithilfe der Seite Schwellenwertrichtlinie löschen können Sie eine Performance-Schwellenwertrichtlinie aus einem oder mehreren Storage-Objekten entfernen oder *Clear*.

Die Liste der Richtlinien wird nur mit den Richtlinien ausgefüllt, die im ausgewählten Objekt oder den ausgewählten Objekten verwendet werden.

Wählen Sie die Richtlinie aus, die Sie aus dem Speicherobjekt oder den Objekten entfernen möchten, und klicken Sie dann auf **Richtlinie löschen**.

Analyse von Performance-Ereignissen

Sie können Performance-Ereignisse analysieren, um zu ermitteln, wann sie erkannt wurden, ob sie aktiv (neu oder bestätigt) oder veraltet sind, die betroffenen Workloads und Cluster-Komponenten betroffen sind und die Optionen für die Behebung von Ereignissen selbst verfügbar sind.

Anzeigen von Informationen zu Performance-Ereignissen

Auf der Seite „Ereignisinventar“ können Sie eine Liste aller neuen und veralteten Performanceereignisse auf den von Unified Manager zu überwachenden Clustern anzeigen. Durch die Anzeige dieser Informationen können Sie die kritischsten Ereignisse bestimmen und anschließend detaillierte Informationen abrufen, um die Ursache des Ereignisses zu bestimmen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue oder veraltete Performanceereignisse vorliegen.

Über diese Aufgabe

Die Liste der Ereignisse wird nach festgestellter Zeit sortiert, wobei die letzten Ereignisse zuerst aufgeführt werden. Sie können auf eine Spaltenüberschrift klicken, um die Ereignisse basierend auf dieser Spalte zu sortieren. Beispielsweise können Sie nach der Spalte Status sortieren, um Ereignisse nach dem Schweregrad anzuzeigen. Wenn Sie nach einem bestimmten Ereignis oder nach einem bestimmten Ereignis suchen, können Sie mit den Filter- und Suchmechanismen die Liste der Ereignisse, die in der Liste angezeigt werden,

verfeinern.

Ereignisse aus allen Quellen werden auf dieser Seite angezeigt:

- Benutzerdefinierte Richtlinie für Leistungsschwellenwerte
- Systemdefinierte Performance-Schwellenwertrichtlinie
- Dynamischer Performance-Schwellenwert

Die Spalte Ereignistyp enthält die Quelle des Ereignisses. Sie können ein Ereignis auswählen, um Details zum Ereignis auf der Seite Ereignisdetails anzuzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Events**.
2. Suchen Sie ein Ereignis, das Sie analysieren möchten, und klicken Sie auf den Ereignisnamen.

   Die Detailseite für das Ereignis wird angezeigt.

   Sie können die Detailseite für ein Ereignis auch anzeigen, indem Sie auf der Seite des Performance Explorers auf den Link „Ereignisname“ und aus einer E-Mail-Benachrichtigung klicken.

Analyse von Ereignissen aus benutzerdefinierten Performance-Schwellenwerten

Ereignisse, die aus benutzerdefinierten Schwellenwerten generiert werden, deuten darauf hin, dass ein Performance-Zähler für ein bestimmtes Storage-Objekt, z. B. ein Aggregat oder ein Volume, den in der Richtlinie definierten Schwellenwert überschritten hat. Dies gibt an, dass beim Cluster-Objekt ein Performance-Problem auftritt.

Auf der Seite Ereignisdetails können Sie das Leistungsereignis analysieren und bei Bedarf Korrekturmaßnahmen ergreifen, um die Leistung wieder normal zu machen.

Reaktion auf benutzerdefinierte Performance-Schwellenwertereignisse

Sie können Unified Manager verwenden, um Performance-Ereignisse zu untersuchen, die durch einen Performance-Zähler durch eine benutzerdefinierte Warnung oder einen kritischen Schwellenwert verursacht werden. Sie können auch Unified Manager verwenden, um den Systemzustand der Cluster-Komponente zu überprüfen, um zu ermitteln, ob kürzlich Systemzustandsereignisse auf der Komponente, die zum Performance-Ereignis beigetragen haben, erkannt wurden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue oder veraltete Performanceereignisse vorliegen.

Schritte

1. Rufen Sie die Seite **Event** Details auf, um Informationen zum Event anzuzeigen.

2. Lesen Sie die **Beschreibung**, die die Schwellenverletzung beschreibt, die das Ereignis verursacht hat.

   Beispielsweise hat die Meldung „`Latency value of 456 ms/op hat ein WARNEREIGNIS auf der Grundlage des Schwellenwerts von 400 ms/op` ausgelöst. Dies zeigt an, dass ein Latenzwarnereignis für das Objekt aufgetreten ist.

3. Bewegen Sie den Mauszeiger über den Richtliniennamen, um Details zur Schwellenwertrichtlinie anzuzeigen, die das Ereignis ausgelöst hat.

   Dazu zählen der Richtlinienname, der zu bewertete Performance-Zähler, der Zählerwert, der nicht durchbrochen werden muss, um es als kritisches oder Warnereignis zu betrachten, und die Dauer, bis zu der der Zähler den Wert überschreiten muss.

4. Notieren Sie sich die **Event Trigger Time**, damit Sie untersuchen können, ob gleichzeitig andere Ereignisse aufgetreten sind, die zu diesem Ereignis beigetragen haben könnten.
5. Führen Sie eine der folgenden Optionen aus, um das Ereignis genauer zu untersuchen, um festzustellen, ob Sie Maßnahmen zur Behebung des Leistungsproblems durchführen müssen:

Option	Mögliche Ermittlungsmaßnahmen
Klicken Sie auf den Namen des Quellobjekts, um die Explorer-Seite für dieses Objekt anzuzeigen.	Auf dieser Seite können Sie die Objektdetails anzeigen und dieses Objekt mit anderen ähnlichen Storage-Objekten vergleichen. So wird ersichtlich, ob es bei anderen Storage-Objekten um die gleiche Zeit ein Performance-Problem gibt. Um zum Beispiel zu sehen, ob andere Volumes auf demselben Aggregat auch ein Performance-Problem haben.
Klicken Sie auf den Cluster-Namen, um die Seite „Cluster Summary“ anzuzeigen.	Auf dieser Seite können Sie die Details für den Cluster anzeigen, auf dem dieses Objekt residiert, um zu sehen, ob weitere Performance-Probleme zur gleichen Zeit aufgetreten sind.

Analyse von Ereignissen aus systemdefinierten Performance-Schwellenwerten

Ereignisse, die aus systemdefinierten Performance-Schwellenwerten generiert werden, geben an, dass ein Performance-Zähler oder eine Gruppe von Performance-Zählern für ein bestimmtes Storage-Objekt den Schwellenwert aus einer systemdefinierten Richtlinie überschritten hat. Dies bedeutet, dass es beim Storage-Objekt, z. B. in einem Aggregat oder Node, zu einem Performance-Problem kommt.

Auf der Seite Ereignisdetails können Sie das Leistungsereignis analysieren und bei Bedarf Korrekturmaßnahmen ergreifen, um die Leistung wieder normal zu machen.

Systemdefinierte Schwellenwertrichtlinien sind auf Cloud Volumes ONTAP-, ONTAP Edge- oder ONTAP Select-Systemen nicht aktiviert.

Reaktion auf systemdefinierte Performance-Schwellenwertereignisse

Sie können Unified Manager verwenden, um Performance-Ereignisse zu untersuchen, die durch einen Performance-Zähler einen vom System definierten Warnschwellenwert verursacht werden. Sie können auch den Systemzustand der Cluster-Komponente mit Unified Manager überprüfen, um zu ermitteln, ob kürzlich entdeckte Ereignisse auf der Komponente, die zum Performance-Ereignis beigetragen hat.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue oder veraltete Performanceereignisse vorliegen.

Schritte

1. Rufen Sie die Seite **Event** Details auf, um Informationen zum Event anzuzeigen.
2. Lesen Sie die **Beschreibung**, die die Schwellenverletzung beschreibt, die das Ereignis verursacht hat.

   Beispielsweise hat die Meldung „`Node Auslastungswert von 90 % ein WARNEREIGNIS ausgelöst, basierend auf dem Schwellenwert von 85 %`“ zeigt an, dass ein Warnereignis für die Node-Auslastung des Cluster-Objekts aufgetreten ist.

3. Notieren Sie sich die **Event Trigger Time**, damit Sie untersuchen können, ob gleichzeitig andere Ereignisse aufgetreten sind, die zu diesem Ereignis beigetragen haben könnten.
4. Lesen Sie unter **Systemdiagnose** die kurze Beschreibung des Analysetyps, den die systemdefinierte Richtlinie auf dem Clusterobjekt ausführt.

   Bei einigen Ereignissen wird neben der Diagnose ein grünes oder rotes Symbol angezeigt, um anzugeben, ob bei dieser Diagnose ein Problem gefunden wurde. Für andere Typen von systemdefinierten Ereignistypen wird die Zählerdiagramme für das Objekt angezeigt.

5. Klicken Sie unter **Suggested Actions** auf den Link **Help me do this**, um die vorgeschlagenen Aktionen anzuzeigen, die Sie durchführen können, um das Aufkommen selbst zu lösen.

Reaktion auf Performance-Ereignisse der QoS-Richtliniengruppe

Unified Manager generiert Warnereignisse für die QoS-Richtlinie, wenn der Workload-Durchsatz (IOPS/TB oder MB/s) die festgelegte ONTAP-QoS-Richtlinieneinstellung überschritten hat und die Workload-Latenz sich beeinträchtigt. Diese systemdefinierten Ereignisse bieten die Möglichkeit, potenzielle Performance-Probleme zu beheben, bevor viele Workloads von der Latenz beeinträchtigt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

Über diese Aufgabe

Unified Manager generiert Warnereignisse bei Verstößen gegen QoS-Richtlinien, wenn der Workload-Durchsatz die festgelegte QoS-Richtlinieneinstellung während jeder Performance-Erfassungsfrist für die

vorherige Stunde überschritten hat. Der Workload-Durchsatz kann den QoS-Schwellenwert für nur einen kurzen Zeitraum während des jeweiligen Erfassungszeitraums überschreiten. Unified Manager zeigt jedoch während des Erfassungszeitraums auf dem Diagramm nur den „durchschnittlichen“-Durchsatz an. Aus diesem Grund erhalten Sie unter Umständen QoS-Ereignisse, während der Durchsatz für einen Workload den im Diagramm angegebenen Richtlinienschwellenwert nicht überschritten hat.

Sie können System Manager oder die Befehle ONTAP zum Verwalten von Richtliniengruppen verwenden, einschließlich der folgenden Aufgaben:

- Erstellen einer neuen Richtliniengruppe für den Workload
- Hinzufügen oder Entfernen von Workloads in einer Richtliniengruppe
- Verschieben eines Workloads zwischen Richtliniengruppen
- Ändern der Durchsatzbegrenzung einer Richtliniengruppe
- Verschieben eines Workloads in ein anderes Aggregat oder Node

Schritte

1. Rufen Sie die Seite **Event** Details auf, um Informationen zum Event anzuzeigen.
2. Lesen Sie die **Beschreibung**, die die Schwellenverletzung beschreibt, die das Ereignis verursacht hat.

   Beispielsweise hat die Meldung „IOPS-Wert von 1,352 IOPS auf vol1_NFS1 ein WARNEREIGNIS ausgelöst, um potenzielle Performance-Probleme für den Workload zu identifizieren“ zeigt, dass ein QoS max IOPS-Ereignis auf Volume vol1_NFS1 aufgetreten ist.

3. Lesen Sie den Abschnitt * Ereignisinformationen*, um weitere Informationen darüber zu erhalten, wann das Ereignis eingetreten ist und wie lange das Ereignis aktiv war.

   Außerdem können bei Volumes oder LUNs, die den Durchsatz einer QoS-Richtlinie teilen, die Namen der drei wichtigsten Workloads angezeigt werden, die die meisten IOPS oder MB/s verbrauchen.

4. Überprüfen Sie im Abschnitt **Systemdiagnose** die beiden Diagramme: Eine für den gesamten durchschnittlichen IOPS oder MB/s (je nach Ereignis) und eine für Latenz. Nach Anordnung der Workloads wird ersichtlich, welche Cluster-Komponenten sich am stärksten auf die Latenz auswirken, wenn der Workload zur Markierung für die QoS-Höchstgrenze nähert.

   Bei einem Ereignis einer Shared-QoS-Richtlinie werden die drei wichtigsten Workloads im Durchsatzdiagramm dargestellt. Wenn mehr als drei Workloads die QoS-Richtlinie nutzen, werden in der Kategorie „andere Workloads“ zusätzliche Workloads hinzugefügt. Außerdem zeigt das Latenzdiagramm die durchschnittliche Latenz aller Workloads, die Teil der QoS-Richtlinie sind.

   Beachten Sie, dass bei anpassungsfähigen QoS-Richtlinienereignissen in den Diagrammen für IOPS und MB/s IOPS- oder MB/s-Werte angezeigt werden, die in ONTAP basierend auf der Größe des Volumes aus der zugewiesenen Richtlinie für IOPS/TB-Schwellenwerte konvertiert wurden.

5. Überprüfen Sie im Abschnitt * vorgeschlagene Aktionen* die Vorschläge und bestimmen Sie, welche Maßnahmen Sie durchführen sollten, um eine Erhöhung der Latenz für den Workload zu vermeiden.

   Klicken Sie bei Bedarf auf die Schaltfläche **Hilfe**, um weitere Details zu den vorgeschlagenen Aktionen anzuzeigen, die Sie durchführen können, um das Leistungsereignis zu lösen.

Allgemeines zu Ereignissen durch anpassungsfähige QoS-Richtlinien mit einer definierten Blockgröße

Adaptive QoS-Richtliniengruppen skalieren je nach Volume-Größe automatisch eine Durchsatzdecke oder -Stellfläche und erzielen so bei veränderter Volume-Größe das Verhältnis von IOPS zu TB. Ab ONTAP 9.5 können Sie in der QoS-Richtlinie die Blockgröße festlegen, um einen MB/s-Schwellenwert gleichzeitig effektiv anzuwenden.

Durch die Zuweisung eines IOPS-Schwellenwerts in einer anpassungsfähigen QoS-Richtlinie wird nur die Anzahl der Vorgänge festgelegt, die in jedem Workload ausgeführt werden. Abhängig von der Blockgröße des Clients, die auf dem Client die Workloads generiert, enthalten einige IOPS sehr viel mehr Daten. Die Nodes, die die Vorgänge verarbeiten, werden daher deutlich entlastet.

Der MB/s-Wert für einen Workload wird mithilfe der folgenden Formel generiert:

```
MBps = (IOPS * Block Size) / 1000
```

Wenn ein Workload durchschnittlich 3,000 IOPS ist und die Blockgröße auf dem Client auf 32 KB eingestellt ist, dann sind die effektiven MB/s für diesen Workload 96. Wenn bei diesem gleichen Workload ein Mittelwert von 3,000 IOPS und die Blockgröße auf dem Client auf 48 KB eingestellt ist, dann sind die effektiven MB/s für diese Workload 144. Bei einer größeren Blockgröße verarbeitet der Node 50 % mehr Daten.

Sehen wir uns nun die folgende anpassungsfähige QoS-Richtlinie an, die über eine definierte Blockgröße verfügt und die Art der Auslösung von Ereignissen basierend auf der Blockgröße des Clients.

Erstellen Sie eine Richtlinie und legen Sie den Spitzendurchsatz auf 2,500 IOPS/TB mit einer Blockgröße von 32 KB fest. Dadurch wird der MB/s-Schwellenwert für ein Volumen mit 1 TB Kapazität effektiv auf 80 MBit/s ((2500 IOPS * 32 KB) / 1000) eingestellt. Beachten Sie, dass Unified Manager ein Warnereignis generiert, wenn der Durchsatzwert 10 % unter dem definierten Schwellenwert liegt. Ereignisse werden in den folgenden Situationen erzeugt:

Genutzte Kapazität	**Das Ereignis wird erzeugt, wenn der Durchsatz diese …**
IOPS	MB/Sek.
1 TB	2,250 IOPS
72 Mbit/s	2 TB
4,500 IOPS	144 Mbit/s
5 TB	11,250 IOPS

Wenn das Volume 2 TB des verfügbaren Speicherplatzes verwendet und der IOPS 4,000 beträgt und die QoS-Blockgröße auf 32 KB auf dem Client eingestellt ist, beträgt der MB/s-Durchsatz 128 MB/s ((4,000 IOPS * 32 KB)/1000). In diesem Szenario wird kein Ereignis generiert, da sowohl 4,000 IOPS als auch 128 Mbps unter dem Schwellenwert für ein Volume mit 2 TB Speicherplatz liegen.

Wenn das Volume 2 TB des verfügbaren Speicherplatzes verwendet und der IOPS 4,000 beträgt und die QoS-Blockgröße auf dem Client auf 64 KB gesetzt ist, dann beträgt der MB/s-Durchsatz 256 MB/s ((4,000 IOPS * 64 KB)/1000). In diesem Fall generieren die 4,000 IOPS kein Ereignis, der MB/s-Wert von 256 MB/s liegt

jedoch über dem Schwellenwert von 144 MB/s und ein Ereignis wird generiert.

Wenn aus diesem Grund ein Ereignis aufgrund einer MB/s-Verletzung für eine adaptive QoS-Richtlinie, die die Blockgröße enthält, ausgelöst wird, wird im Abschnitt Systemdiagnose der Seite Ereignisdetails ein MB/s-Diagramm angezeigt. Wenn das Ereignis aufgrund einer Verletzung des IOPS für die Richtlinie zur adaptiven QoS ausgelöst wird, wird im Abschnitt Systemdiagnose ein IOPS-Diagramm angezeigt. Wenn sowohl für IOPS als auch für MB/s eine Sicherheitsverletzung auftritt, erhalten Sie zwei Ereignisse.

Weitere Informationen zum Anpassen der QoS-Einstellungen finden Sie im Power Guide *ONTAP 9 zur Leistungsüberwachung*.

"ONTAP 9 Leistungsüberwachung – Stromversorgungshandbuch"

Reaktion auf Node-Ressourcen überlastete Performance-Ereignisse

Unified Manager generiert zu stark ausgelastete Warnmeldungen bei Node-Ressourcen, wenn ein einzelner Node über die Grenzen seiner betrieblichen Effizienz arbeitet und so die Workload-Latenzen potenziell beeinträchtigen. Diese systemdefinierten Ereignisse bieten die Möglichkeit, potenzielle Performance-Probleme zu beheben, bevor viele Workloads von der Latenz beeinträchtigt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue oder veraltete Performanceereignisse vorliegen.

Über diese Aufgabe

Unified Manager generiert Warnereignisse für überlastete Node-Ressourcen bei Richtlinienverstößen, indem Nodes gesucht werden, die mehr als 30 Minuten lang mehr als 100 % der Performance-Kapazität nutzen.

Sie können diesen Typ eines Performance-Problems mit System Manager oder den Befehlen ONTAP beheben, einschließlich der folgenden Aufgaben:

- Erstellen und Anwenden einer QoS-Richtlinie auf alle Volumes oder LUNs, die die Systemressourcen überbeanspruchen
- Reduzierung des maximalen Durchsatzes bei QoS in einer Richtliniengruppe, auf die Workloads angewendet wurden
- Verschieben eines Workloads in ein anderes Aggregat oder Node
- Erhöhung der Kapazität durch Hinzufügen von Festplatten zum Node oder durch Upgrade auf einen Node mit schnellerer CPU und mehr RAM

Schritte

1. Rufen Sie die Seite **Event** Details auf, um Informationen zum Event anzuzeigen.
2. Lesen Sie die **Beschreibung**, die die Schwellenverletzung beschreibt, die das Ereignis verursacht hat.

   Zum Beispiel die Meldung „`Perf". Die genutzte Kapazität bei der Einfachheit beträgt 139 %.-02 hat ein WARNEREIGNIS ausgelöst, um potenzielle Performance-Probleme in der Datenverarbeitungseinheit zu identifizieren.`“ zeigt an, dass die Performance auf der Einfachheit eines Node 02 überlastet ist und die Node-Performance beeinträchtigt.

3. Lesen Sie im Abschnitt **Systemdiagnose** die drei Diagramme durch: Eins für die auf dem Node genutzte Performance-Kapazität, eins für die durchschnittlichen Storage-IOPS durch die wichtigsten Workloads und eins für die Latenz bei den wichtigsten Workloads. Auf diese Weise sehen Sie, welche Workloads die Ursache der Latenz auf dem Node sind.

   Sie können die QoS-Richtlinien auf welche Workloads angewendet werden und welche nicht, indem Sie den Mauszeiger über das IOPS-Diagramm bewegen.

4. Überprüfen Sie im Abschnitt * vorgeschlagene Aktionen* die Vorschläge und bestimmen Sie, welche Maßnahmen Sie durchführen sollten, um eine Erhöhung der Latenz für den Workload zu vermeiden.

   Klicken Sie bei Bedarf auf die Schaltfläche **Hilfe**, um weitere Details zu den vorgeschlagenen Aktionen anzuzeigen, die Sie durchführen können, um das Leistungsereignis zu lösen.

Analyse von Ereignissen aus dynamischen Leistungsschwellenwerten

Ereignisse, die aus dynamischen Schwellenwerten generiert werden, geben an, dass die tatsächliche Reaktionszeit (Latenz) für einen Workload zu hoch oder zu niedrig ist im Vergleich zum erwarteten Reaktionszeitbereich. Auf der Seite Ereignisdetails können Sie das Leistungsereignis analysieren und bei Bedarf Korrekturmaßnahmen ergreifen, um die Leistung wieder normal zu machen.

Dynamische Performance-Schwellenwerte sind auf Cloud Volumes ONTAP-, ONTAP Edge- oder ONTAP Select-Systemen nicht aktiviert.

Identifizierung der Opfer-Workloads, die an einem dynamischen Performance-Ereignis beteiligt sind

In Unified Manager können Sie ermitteln, welche Volume Workloads die höchste Abweichung der Reaktionszeit (Latenz) aufweisen, die durch eine Storage-Komponente verursacht wurde. Anhand der Identifizierung dieser Workloads können Sie nachvollziehen, warum die Client-Applikationen, auf die sie zugreifen, langsamer als normal ausgeführt wurden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete dynamische Leistungsereignisse vorliegen.

Über diese Aufgabe

Auf der Seite Ereignisdetails wird eine Liste der benutzerdefinierten und systemdefinierten Workloads angezeigt, die nach der höchsten Abweichung von Aktivität oder Auslastung der Komponente oder am stärksten vom Ereignis betroffen sind. Die Werte basieren auf den Peaks, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Aktivität **Opfer-Workloads** aus.
3. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten Workloads

anzuzeigen, die sich auf die Komponente auswirken, und den Namen des Workloads mit dem Opfer anzuzeigen.

Identifizierung problematischer Workloads, die an einem dynamischen Performance-Ereignis beteiligt sind

In Unified Manager können Sie ermitteln, welche Workloads die höchste Nutzungsabweichung einer Clusterkomponente aufweisen. Anhand der Ermittlung dieser Workloads können Sie nachvollziehen, warum bestimmte Volumes des Clusters über langsame Reaktionszeiten (Latenz) verfügen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete dynamische Leistungsereignisse vorliegen.

Über diese Aufgabe

Auf der Seite Ereignisdetails wird eine Liste der benutzerdefinierten und systemdefinierten Workloads angezeigt, die nach der höchsten Nutzung der Komponente oder am stärksten von dem Ereignis betroffen sind. Die Werte basieren auf den Peaks, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Aktivität **Bully Workloads** aus.
3. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten problematischer Workloads anzuzeigen, die sich auf die Komponente auswirken.

Erkennen von Haifischlasten, die an einem dynamischen Performance-Ereignis beteiligt sind

In Unified Manager können Sie ermitteln, welche Workloads die höchste Nutzungsabweichung einer Storage-Komponente aufweisen. Anhand der Identifizierung dieser Workloads können Sie ermitteln, ob diese Workloads in ein weniger ausgelasttes Cluster verschoben werden sollen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es gibt ein neues, anerkanntes oder überholes dynamisches Ereignis für die Leistung.

Über diese Aufgabe

Auf der Seite Ereignisdetails wird eine Liste der benutzerdefinierten und systemdefinierten Workloads angezeigt, die nach der höchsten Nutzung der Komponente oder am stärksten von dem Ereignis betroffen sind. Die Werte basieren auf den Peaks, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Aktivität **Shark-Workloads** aus.
3. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten Workloads anzuzeigen, die sich auf die Komponente auswirken, und den Namen des Haifischarbeitslasts.

Performance-Ereignisanalyse für eine MetroCluster-Konfiguration

Sie können mit Unified Manager ein Performance-Ereignis für eine MetroCluster-Konfiguration analysieren. Sie können die an dem Ereignis beteiligten Workloads ermitteln und die vorgeschlagenen Maßnahmen zur Lösung prüfen.

MetroCluster-Performance-Ereignisse können auf *bully* Workloads zurückzuführen sein, die die Interswitch-Links (ISLs) zwischen den Clustern überlasten oder aufgrund von Systemzustandsproblemen. Unified Manager überwacht jedes Cluster in einer MetroCluster-Konfiguration unabhängig und berücksichtigt dabei nicht die Performance-Ereignisse in einem Partner-Cluster.

Auf der Seite Unified ManagerDashboards/Überblick werden auch Performance-Ereignisse von beiden Clustern in der MetroCluster-Konfiguration angezeigt.Sie können auch die Health-Seiten von Unified Manager anzeigen, um den Zustand der einzelnen Cluster zu überprüfen und ihre Beziehung anzuzeigen.

Analyse eines dynamischen Performance-Ereignisses auf einem Cluster in einer MetroCluster Konfiguration

Sie können Unified Manager verwenden, um das Cluster in einer MetroCluster-Konfiguration zu analysieren, bei der ein Performance-Ereignis erkannt wurde. Sie können den Cluster-Namen, die Ereigniserkennungszeit und die damit verbundenen Workloads *bully* und *victim* identifizieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Für eine MetroCluster-Konfiguration müssen neue, anerkannte oder veraltete Performance-Ereignisse vorliegen.
- Beide Cluster in der MetroCluster-Konfiguration müssen von derselben Instanz von Unified Manager überwacht werden.

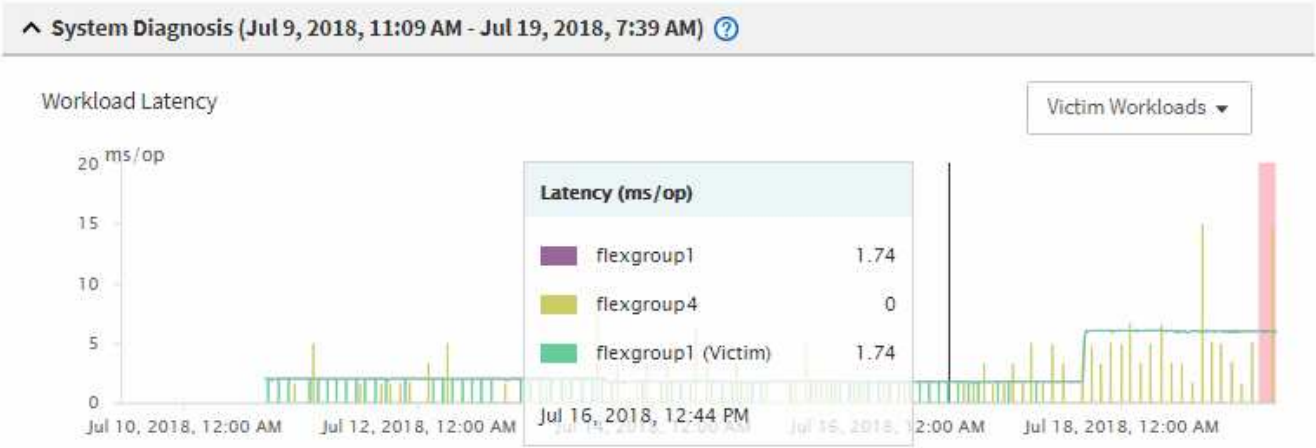
Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Die Ereignisbeschreibung enthält Namen der betroffenen Workloads sowie die Anzahl der betroffenen Workloads.

   In diesem Beispiel ist das Symbol für MetroCluster-Ressourcen rot dargestellt, was bedeutet, dass die MetroCluster-Ressourcen über Konflikte verfügen. Sie positionieren den Cursor über das Symbol, um eine Beschreibung des Symbols anzuzeigen. Oben auf der Seite in der Ereignis-ID identifiziert der Cluster-Name den Namen des Clusters, auf dem das Ereignis erkannt wurde.

3. Notieren Sie sich den Cluster-Namen und die Ereignis-Erkennungszeit, mit der Sie Performance-Ereignisse im Partner-Cluster analysieren können.
4. Überprüfen Sie in den Diagrammen die „_victim_Workloads“, um zu bestätigen, dass ihre Antwortzeiten höher sind als der Performance-Schwellenwert.

   In diesem Beispiel wird der Workload des Opfers im Hover-Text angezeigt. Die Latenzdiagramme werden auf hoher Ebene angezeigt, ein konsistentes Latenzmuster für die betroffenen Opfer-Workloads. Obwohl die anormale Latenz der betroffenen Workloads das Ereignis ausgelöst hat, kann ein konsistentes Latenzmuster darauf hindeuten, dass die Workloads innerhalb des erwarteten Bereichs liegen. Durch einen Spitzen bei den I/O wurde die Latenz erhöht und das Ereignis ausgelöst.



   Falls Sie vor Kurzem eine Applikation auf einem Client installiert haben, der auf diese Volume-Workloads zugreift und die Applikation eine hohe Anzahl an I/O-Vorgängen sendet, kann die Verzögerungen bereits vorwegnehmen. Wenn die Latenz für die Workloads innerhalb des erwarteten Bereichs zurückkehrt, ändert sich der Ereignisstatus zu veraltet und bleibt mehr als 30 Minuten in diesem Status, können Sie das Ereignis wahrscheinlich ignorieren. Wenn das Ereignis andauernde und im neuen Status verbleibt, können Sie es weiter untersuchen, um festzustellen, ob andere Probleme das Ereignis verursacht haben.

5. Wählen Sie im Workload-Durchsatzdiagramm die Option **problematische Workloads** aus, um die problematische Workloads anzuzeigen.

   Die Anwesenheit von problematischer Workloads zeigt an, dass ein Ereignis möglicherweise durch eine oder mehrere Workloads auf dem lokalen Cluster verursacht wurde, bei denen die MetroCluster-Ressourcen überlastet sind. Die anspruchsvollen Workloads weisen eine hohe Abweichung beim Schreibdurchsatz (MB/s) auf.

   Dieses Diagramm wird auf höherer Ebene das Muster des Schreibdurchsatzes (MB/s) für die Workloads angezeigt. Sie können das MB/s-Muster für Schreibvorgänge überprüfen, um einen anormalen Durchsatz zu identifizieren, der darauf hindeutet, dass ein Workload die MetroCluster-Ressourcen übernutzt.

   Wenn an diesem Ereignis keine problematische Workloads beteiligt sind, wurde dieses Ereignis möglicherweise durch ein Systemzustandsproblem mit der Verbindung zwischen den Clustern oder durch

ein Performance-Problem auf dem Partner-Cluster verursacht. Sie können Unified Manager verwenden, um den Systemzustand beider Cluster in einer MetroCluster Konfiguration zu überprüfen. Außerdem können Sie mit Unified Manager Performance-Ereignisse im Partner-Cluster überprüfen und analysieren.

Analyse eines dynamischen Performance-Ereignisses für ein Remote-Cluster auf einer MetroCluster-Konfiguration

Mit Unified Manager können Sie dynamische Performance-Ereignisse auf einem Remote-Cluster in einer MetroCluster-Konfiguration analysieren. Mit der Analyse können Sie ermitteln, ob ein Ereignis im Remote-Cluster ein Ereignis auf seinem Partner-Cluster verursacht hat.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen ein Performance-Ereignis auf einem lokalen Cluster in einer MetroCluster Konfiguration analysiert und die Ereigniserkennungszeit ermittelt haben.
- Sie müssen den Zustand des lokalen Clusters und dessen am Performance-Ereignis beteiligten Partner-Clusters überprüft und den Namen des Partner-Clusters erhalten haben.

Schritte

1. Loggen Sie sich bei der Unified Manager-Instanz ein, die das Partner-Cluster überwacht.
2. Klicken Sie im linken Navigationsbereich auf **Events**, um die Ereignisliste anzuzeigen.
3. Wählen Sie im Auswahlfeld **Zeitbereich** die Option **Letzte Stunde** aus und klicken Sie dann auf **Bereich anwenden**.
4. Wählen Sie im Auswahlfeld **Filterung** im linken Dropdown-Menü die Option **Cluster** aus, geben Sie den Namen des Partner Clusters in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.

   Wenn während der letzten Stunde keine Ereignisse für das ausgewählte Cluster vorhanden sind, zeigt dies an, dass es während des Ereignisses beim Partner keine Performance-Probleme aufgetreten sind.

5. Wenn im ausgewählten Cluster Ereignisse über die letzte Stunde erkannt wurden, vergleichen Sie die Ereignis-Erkennungszeit mit der Ereignis-Erkennungszeit für das Ereignis auf dem lokalen Cluster.

   Wenn diese Ereignisse problematische Workloads verursachen, die zu Konflikten bei der Datenverarbeitungskomponente führen, könnte ein oder mehrere dieser Punkte das Ereignis auf dem lokalen Cluster verursacht haben. Sie können auf das Ereignis klicken, um es zu analysieren und die vorgeschlagenen Aktionen für die Lösung auf der Seite Ereignisdetails zu prüfen.

   Wenn diese Ereignisse keine problematische Workloads betreffen, wurden sie nicht zum Performance-Ereignis auf dem lokalen Cluster verursacht.

Er reagiert auf ein dynamisches Performance-Ereignis, das durch die QoS-Richtliniengruppendrosselung verursacht wird

Mithilfe von Unified Manager können Sie ein Performance-Ereignis untersuchen, das durch eine Richtliniengruppe für Quality of Service (QoS) verursacht wird, die den Workload-Durchsatz (MB/s) drosselt. Die Drosselung hat die Reaktionszeiten (Latenz) von Volume-Workloads in der Richtliniengruppe erhöht. Anhand der Ereignisinformationen können Sie bestimmen, ob neue Grenzen für die

Richtliniengruppen erforderlich sind, um die Drosselung zu stoppen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Lesen Sie die **Beschreibung**, die den Namen der von der Drosselung betroffenen Workloads anzeigt.

   Die Beschreibung kann dieselbe Arbeitslast für das Opfer und den Täter anzeigen, da die Drosselung den Workload zum Opfer selbst macht.

3. Notieren Sie den Namen des Volumes mit einer Anwendung wie einem Texteditor.

   Sie können den Volume-Namen suchen, um ihn später zu finden.

4. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Aktivität **Bully Workloads** aus.
5. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten Workloads anzuzeigen, die sich auf die Richtliniengruppe auswirken.

   Die Arbeitslast oben in der Liste hat die höchste Abweichung und verursacht die Drosselung. Die Aktivität entspricht dem Prozentsatz des von den einzelnen Workloads verwendeten Richtliniengruppenlimits.

6. Navigieren Sie zur Seite **Performance/Volume Details** für den Top Workload.
7. Wählen Sie **Aufbruchdaten nach** aus.
8. Aktivieren Sie das Kontrollkästchen neben **Latenz*****, um alle Latenzdiagramme auszuwählen.
9. Wählen Sie unter **IOPS** die Option **Lese-/Schreibvorgänge/Sonstiges** aus.
10. Klicken Sie Auf **Absenden**.

    Die Aufschlüsselung werden unter dem Latenzdiagramm und dem IOPS-Diagramm angezeigt.

11. Vergleichen Sie das Diagramm **Policy Group Impact** mit dem Diagramm **Latenz**, um zu sehen, welcher Prozentsatz der Drosselung sich zum Zeitpunkt des Ereignisses auf die Latenz ausgewirkt hat.

    Die Richtliniengruppe weist einen maximalen Durchsatz von 1,000 Operationen pro Sekunde (in op/s) auf, die die Workloads in ihr nicht zusammen überschreiten können. Zum Zeitpunkt des Ereignisses führten die Workloads in der Richtliniengruppe einen Gesamtdurchsatz von über 1,200 Op/s durch, sodass die Richtliniengruppe ihre Aktivität wieder auf 1,000 Op/Sek. ausbremsen konnte Das Policy Group Impact-Diagramm zeigt, dass die Drosselung 10 % der gesamten Latenz verursachte und bestätigt, dass die Drosselung das Ereignis verursacht hat.

12. Überprüfen Sie das Diagramm **Cluster Components**, das die gesamte Latenz nach Clusterkomponente anzeigt.

    Die Latenz befindet sich in der Richtliniengruppe am höchsten, was bestätigt, dass die Drosselung das Ereignis verursacht hat.

13. Vergleichen Sie das Diagramm * Lese-/Schreib-Latenz* mit dem Diagramm * Lese-/Schreibvorgänge/anderes*.

Beide Diagramme zeigen eine hohe Anzahl von Leseanforderungen mit einer hohen Latenz, jedoch ist die Anzahl der Anfragen und die Menge der Latenz für Schreibanforderungen niedrig. Anhand dieser Werte können Sie ermitteln, ob ein hoher Durchsatz oder eine höhere Anzahl an Operationen die Latenz erhöht. Sie können diese Werte verwenden, wenn Sie sich entscheiden, ein Richtliniengruppenlimit auf den Durchsatz oder die Operationen zu legen.

14. Verwenden Sie OnCommand System Manager, um die aktuelle Obergrenze für die Richtliniengruppe auf 1,300 Op/Sek. zu erhöhen
15. Kehren Sie nach einem Tag wieder zu Unified Manager zurück, und suchen Sie nach dem Namen des Workloads, den Sie in Schritt 3 aufgenommen haben.

    Die Seite Performance/Volume Details wird angezeigt.

16. Wählen Sie **Aufbrechen von Daten um** > **IOPS**.
17. Klicken Sie Auf **Absenden**.

    Das Diagramm Lese-/Schreibvorgänge/Sonstiges wird angezeigt.

18. Zeigen Sie unten auf der Seite den Cursor auf das Symbol Ereignis ändern ( ) Für die Änderung der Policy-Gruppengrenzen.
19. Vergleichen Sie das Diagramm **Lese/Schreibvorgänge/Sonstiges** mit dem Diagramm **Latenz**.

    Die Lese- und Schreibanfragen sind dieselben, aber die Drosselung hat gestoppt und die Latenz ist gesunken.

Reaktion auf ein dynamisches Performance-Ereignis aufgrund eines Festplattenausfalls

Mit Unified Manager können Sie ein Performance-Ereignis untersuchen, das durch die Überprovisionierung eines Aggregats verursacht wird. Sie können auch Unified Manager verwenden, um den Systemzustand des Aggregats zu überprüfen, um zu ermitteln, ob kürzlich auf dem Aggregat erkannte Systemzustandsereignisse zum Performance-Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Lesen Sie die **Description**, die die Workloads beschreibt, die an dem Ereignis beteiligt sind, und die Clusterkomponente, die mit einem Konflikt verbunden ist.

   Es gibt mehrere Opfer-Volumes, deren Latenz von der Cluster-Komponente mit Konflikten beeinträchtigt wurde. Das Aggregat, das sich in der Mitte eines RAID-Rekonstruktionss befindet, um die ausgefallene Festplatte durch eine Ersatzfestplatte zu ersetzen, ist die Clusterkomponente. Unter „Komponente in Konflikt“ ist das Aggregat-Symbol rot hervorgehoben und der Name des Aggregats wird in Klammern angezeigt.

3. Wählen Sie im Diagramm Workload-Auslastung die Option **Bully Workloads** aus.

4. Bewegen Sie den Mauszeiger über das Diagramm, um die obersten Workloads anzuzeigen, die sich auf die Komponente auswirken.

   Die wichtigsten Workloads mit der höchsten Spitzenauslastung seit dem Erkennen des Ereignisses werden oben in der Tabelle angezeigt. Einer der wichtigsten Workloads ist der durch das System definierte Workload Disk Health, der auf eine RAID-Rekonstruktion hinweist. Eine Rekonstruktion ist der interne Prozess zur Wiederherstellung des Aggregats mit der freien Platte. Der Disk Health Workload und die anderen Workloads im Aggregat verursachten wahrscheinlich die Konflikte im Aggregat und das zugehörige Ereignis.

5. Nachdem Sie bestätigt haben, dass die Aktivitäten des Festplatten-Status-Workloads das Ereignis verursacht haben, warten Sie ca. 30 Minuten, bis die Rekonstruktion abgeschlossen ist, und warten Sie, bis Unified Manager das Ereignis analysiert und erkennt, ob es noch im Aggregat zu Konflikten kommt.
6. Suchen Sie in Unified Manager nach der Ereignis-ID, die Sie in Schritt 2 aufgezeichnet haben.

   Das Ereignis für den Festplattenausfall wird auf der Seite „Ereignisdetails“ angezeigt. Überprüfen Sie nach Abschluss der RAID-Rekonstruktion, ob der Status veraltet ist, und geben Sie an, dass das Ereignis behoben ist.

7. Wählen Sie im Workload-Auslastungsdiagramm **Bully Workloads** aus, um die Workloads auf dem Aggregat nach Spitzenauslastung zu sehen.
8. Navigieren Sie zur Seite **Performance/Volume Details** für den Top Workload.
9. Klicken Sie auf **1d**, um die letzten 24 Stunden (1 Tag) der Daten für das ausgewählte Volumen anzuzeigen.

   Im Latenzdiagramm ist ein roter Punkt (🔴) Gibt an, wann das Ereignis des Festplattenfehlers aufgetreten ist.

10. Wählen Sie **Aufbruchdaten nach** aus.
11. Wählen Sie unter **Components** die Option **Disk Utiation**.
12. Klicken Sie Auf **Absenden**.

    Das Diagramm zur Festplattenauslastung zeigt ein Diagramm aller Lese- und Schreibanforderungen vom ausgewählten Workload bis zu den Festplatten des Zielaggregats an.

13. Vergleichen Sie die Daten im Diagramm **Disk Utiation** mit den Daten zum Zeitpunkt des Ereignisses im Diagramm **Latenz**.

    Zum Zeitpunkt des Ereignisses zeigt die Plattenauslastung einen hohen Anteil an Lese- und Schreibvorgängen durch die RAID-Rekonstruktionsprozesse an, was die Latenz des ausgewählten Volumes erhöht. Einige Stunden nach dem Ereignis waren sowohl die Lese- als auch die Schreibvorgänge sowie die Latenz gesunken, sodass die Konflikte zwischen dem Aggregat nicht mehr bestehen.

Er reagiert auf ein dynamisches Performance-Ereignis, das durch HA Takeover verursacht wird

Mit Unified Manager können Sie ein Performance-Ereignis anhand hoher Datenverarbeitung auf einem Cluster Node in einem Hochverfügbarkeitspaar (HA-Paar) untersuchen. Sie können auch Unified Manager verwenden, um den Systemzustand der Nodes zu überprüfen, ob kürzlich entdeckte Systemzustandsereignisse auf den Nodes, die zum Performance-Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Lesen Sie die **Description**, die die Workloads beschreibt, die an dem Ereignis beteiligt sind, und die Clusterkomponente, die mit einem Konflikt verbunden ist.

   Es gibt ein Opfer-Volume, dessen Latenz von der Cluster-Komponente im Konflikt beeinträchtigt wurde. Der Datenverarbeitungs-Node, der alle Workloads vom Partner-Node übernommen hat, ist die Cluster-Komponente im Konflikt. Unter Komponente in Konflikt wird das Symbol für die Datenverarbeitung rot markiert und der Name des Node, der zum Zeitpunkt des Ereignisses die Datenverarbeitung verarbeitet hat, wird in Klammern angezeigt.

3. Klicken Sie in der **Beschreibung** auf den Namen des Opfervolumens.

   Die Seite Performance/Volume Details wird angezeigt. Im unteren Bereich der Seite in der Zeile Ereignisse Zeit wird ein Symbol für das Ereignis ändern ( ) Gibt die Zeit an, zu der Unified Manager den Start der HA-Übernahme erkannt hat.

4. Zeigen Sie den Cursor auf das Änderungsereignis-Symbol für die HA-Übernahme.

   Details zum HA Takeover werden in der Tabelle „Ereignisse“ angezeigt. Im Latenzdiagramm zeigt ein Ereignis an, dass das ausgewählte Volume aufgrund einer hohen Latenz um die gleiche Zeit wie das HA-Takeover den Performance-Schwellenwert überschritten hat.

5. Wählen Sie **Aufbruchdaten nach** aus.
6. Wählen Sie unter **Latenz Cluster-Komponenten** aus.
7. Klicken Sie Auf **Absenden**.

   Das Diagramm Cluster-Komponenten wird angezeigt. Im Diagramm wird die gesamte Latenz nach Clusterkomponente unterteilt.

8. Zeigen Sie unten auf der Seite den Mauszeiger auf das Symbol für das Änderungsereignis zum Beginn der HA-Übernahme.
9. Vergleichen Sie im Diagramm **Cluster Components** die Latenz für die Datenverarbeitung mit der gesamten Latenz im Diagramm * Latenz*.

   Zum Zeitpunkt der HA-Übernahme betrug die Datenverarbeitung aufgrund der steigenden Workload-Anforderungen am Datenverarbeitungs-Node eine Spitze. Die höhere CPU-Auslastung steigerte die Latenz und löste das Ereignis aus.

10. Nach der Behebung des fehlerhaften Knotens führt OnCommand System Manager ein HA-Giveback durch, wodurch die Workloads vom Partner-Node zum festgelegten Node verschoben werden.
11. Nachdem die HA-Rückübertragung abgeschlossen ist, suchen Sie im Unified Manager nach der Ereignis-ID, die Sie in Schritt 2 aufgezeichnet haben.

    Das durch die HA-Übernahme ausgelöste Ereignis wird auf der Seite Ereignisdetails angezeigt. Das Ereignis weist nun einen Status veraltet auf, was darauf hinweist, dass das Ereignis gelöst wurde.

12. Klicken Sie in der **Beschreibung** auf den Namen des Opfervolumens.

    Die Seite Performance/Volume Details wird angezeigt. Im unteren Bereich der Seite wird in der Zeile Ereignisse die Zeit angezeigt, in der Unified Manager den Abschluss des HA-Giveback erkannt hat, ein Symbol für ein Änderungsereignis.

13. Wählen Sie **Aufbruchdaten nach** aus.
14. Wählen Sie unter **Latenz Cluster-Komponenten** aus.

    Das Diagramm Cluster-Komponenten wird angezeigt.

15. Zeigen Sie unten auf der Seite den Cursor auf das Symbol für das Änderungsereignis für das HA-Giveback.

    Das Änderungereignis wird in der Tabelle „Ereignisliste“ hervorgehoben und gibt an, dass die HA-Rückgabe erfolgreich abgeschlossen wurde.

16. Vergleichen Sie im Diagramm **Cluster Components** die Latenz für die Datenverarbeitung mit der gesamten Latenz im Diagramm * Latenz*.

    Die Latenz der Komponente für die Datenverarbeitung wurde herabgesetzt, wodurch die gesamte Latenz verringert wurde. Der Node, den das ausgewählte Volume jetzt zur Datenverarbeitung verwendet, hat das Ereignis aufgelöst.

Lösen von Leistungsereignissen

Sie können die vorgeschlagenen Aktionen verwenden, um selbst Leistungsereignisse zu lösen. Die ersten drei Vorschläge werden immer angezeigt, und die Aktionen unter dem vierten Vorschlag sind spezifisch für die Art des angezeigten Ereignisses.

Die **help me do this** Links bieten zusätzliche Informationen zu jeder vorgeschlagenen Aktion, einschließlich Anweisungen zur Durchführung einer bestimmten Aktion. Einige der Aktionen können die Verwendung von Unified Manager, OnCommand System Manager, OnCommand Workflow Automation, ONTAP CLI-Befehlen oder einer Kombination dieser Tools umfassen.

Bestätigung, dass die Latenz im erwarteten Bereich liegt

Wenn eine Cluster-Komponente im Konflikt ist, können Volume-Workloads, die diese verwenden, kürzere Reaktionszeiten (Latenz) haben. Sie können die Latenz der einzelnen Opfer-Workloads auf der Komponente mit Konflikten überprüfen, um zu bestätigen, dass die tatsächliche Latenz innerhalb des erwarteten Bereichs liegt. Sie können auch auf einen Volume-Namen klicken, um die historischen Daten für das Volume anzuzeigen.

Wenn das Performance-Ereignis den Status „veraltet“ aufweist, wurde die Latenz jedes betroffenen Opfers innerhalb des erwarteten Bereichs zurückgegeben.

Prüfen Sie die Auswirkungen von Konfigurationsänderungen auf die Workload Performance

Konfigurationsänderungen auf dem Cluster, z. B. Festplatte ausgefallen, HA-Failover oder ein verschobene Volume, können sich negativ auf die Volume Performance auswirken und zu einer höheren Latenz führen.

In Unified Manager können Sie die Seite Performance/Volume Details überprüfen, um zu sehen, wann eine kürzlich erfolgte Konfigurationsänderung aufgetreten ist, und diese mit den Vorgängen und Latenz (Reaktionszeit) vergleichen, um zu prüfen, ob eine Aktivität für den ausgewählten Volume-Workload geändert wurde.

Die Performance-Seiten von Unified Manager können nur eine begrenzte Anzahl von Änderungsereignissen erkennen. Die Systemzustandsseiten bieten Meldungen für andere Ereignisse, die durch Konfigurationsänderungen verursacht wurden. Sie können in Unified Manager nach dem Volume suchen, um den Ereignisverlauf anzuzeigen.

Optionen zur Verbesserung der Workload Performance von Client-Seite

Sie können Ihre Client-Workloads, z. B. Applikationen oder Datenbanken, prüfen, die I/O-Vorgänge an Volumes senden, die an einem Performance-Ereignis beteiligt sind, um zu ermitteln, ob eine Client-seitige Änderung das Ereignis möglicherweise korrigiert.

Wenn Clients, die mit Volumes in einem Cluster verbunden sind, ihre I/O-Anforderungen erhöhen, muss das Cluster schwieriger arbeiten, die Anforderungen zu erfüllen. Wenn Sie wissen, welche Clients eine hohe Anzahl von I/O-Anforderungen an ein bestimmtes Volume im Cluster haben, können Sie die Cluster-Performance verbessern, indem Sie die Anzahl der Clients, die auf das Volume zugreifen, anpassen oder die I/O-Menge an diesem Volume verringern. Sie können auch eine Obergrenze für die QoS-Richtliniengruppe festlegen, deren Mitglied das Volume ist.

Sie können Clients und deren Applikationen untersuchen, um festzustellen, ob die Clients mehr I/O als gewöhnlich senden, was zu Konflikten bei einer Cluster-Komponente führen kann. Auf der Seite Ereignisdetails werden im Abschnitt Systemdiagnose die wichtigsten Volume-Workloads unter Verwendung der zu verstrittenden Komponente angezeigt. Wenn Sie wissen, welcher Client auf ein bestimmtes Volume zugreift, können Sie auf den Client zugreifen, um zu ermitteln, ob die Client-Hardware oder eine Anwendung nicht wie erwartet funktioniert oder mehr Arbeit geleistet hat als sonst.

In einer MetroCluster-Konfiguration werden Schreibanforderungen an ein Volume in einem lokalen Cluster auf einem Volume im Remote-Cluster gespiegelt. Wenn das Quell-Volume auf dem lokalen Cluster synchron mit dem Ziel-Volume auf dem Remote-Cluster gehalten werden soll, kann auch der Bedarf beider Cluster in der MetroCluster Konfiguration erhöht werden. Indem die Schreibvorgänge auf diese gespiegelten Volumes reduziert werden, führen die Cluster weniger Synchronisierungsvorgänge aus, wodurch die Auswirkungen auf die Performance anderer Workloads reduziert werden.

Prüfen Sie auf Client- oder Netzwerkprobleme

Wenn Clients, die mit Volumes in einem Cluster verbunden sind, ihre I/O-Anforderungen erhöhen, muss das Cluster schwieriger arbeiten, die Anforderungen zu erfüllen. Der erhöhte Bedarf an dem Cluster kann eine Komponente in Konflikt stellen, die Latenz von Workloads erhöhen, die es verwenden, und ein Ereignis in Unified Manager auslösen.

Auf der Seite Ereignisdetails werden im Abschnitt Systemdiagnose die wichtigsten Volume-Workloads unter

Verwendung der zu verstrittenden Komponente angezeigt. Wenn Sie wissen, welcher Client auf ein bestimmtes Volume zugreift, können Sie auf den Client zugreifen, um zu ermitteln, ob die Client-Hardware oder eine Anwendung nicht wie erwartet funktioniert oder mehr Arbeit geleistet hat als sonst. Wenden Sie sich eventuell an Ihren Client-Administrator oder den Anwendungsanbieter, um Unterstützung zu erhalten.

Sie können Ihre Netzwerkinfrastruktur überprüfen, um festzustellen, ob es Hardware-Probleme, Engpässe oder konkurrierende Workloads gibt, die möglicherweise I/O-Anfragen zwischen dem Cluster und den verbundenen Clients verursacht haben, um langsamer als erwartet durchzuführen. Wenden Sie sich möglicherweise an Ihren Netzwerkadministrator, um Hilfe zu erhalten.

Überprüfen Sie, ob die anderen Volumes in der QoS-Richtliniengruppe eine ungewöhnlich hohe Aktivität haben

Sie können die Workloads in der Richtliniengruppe Quality of Service (QoS) mit der höchsten Änderung der Aktivität überprüfen, um zu ermitteln, ob mehrere Workloads das Ereignis verursacht haben. Sie können auch feststellen, ob andere Workloads das festgelegte Durchsatzlimit immer noch überschreiten oder ob sie sich innerhalb des erwarteten Aktivitätsbereichs befinden.

Auf der Seite Ereignisdetails im Abschnitt Systemdiagnose können Sie die Workloads nach Spitzenabweichungen in der Aktivität sortieren, um die Workloads mit der höchsten Aktivitätsänderung oben in der Tabelle anzuzeigen. Bei diesen Workloads handelt es sich möglicherweise um „`bullies`“, deren Aktivität den festgelegten Grenzwert überschritten hat und möglicherweise das Ereignis verursacht hat.

Sie können zur Seite Performance/Volume-Details für jeden Volume-Workload im Diagramm navigieren, um seine IOPS-Aktivität zu überprüfen. Wenn der Workload Perioden mit sehr hoher Betriebstätigkeit ausweist, war er möglicherweise an dem Ereignis beteiligt. Sie können die Richtliniengruppeneinstellungen für den Workload ändern oder den Workload in eine andere Richtliniengruppe verschieben.

Sie können zum Managen von Richtliniengruppen OnCommand System Manager oder die CLI-Befehle von ONTAP verwenden:

- Erstellen einer Richtliniengruppe
- Hinzufügen oder Entfernen von Workloads in einer Richtliniengruppe
- Verschieben Sie einen Workload zwischen Richtliniengruppen.
- Ändern Sie das Durchsatzlimit einer Richtliniengruppe.

Verschieben von logischen Schnittstellen (LIFs)

Das Verschieben von logischen Schnittstellen (LIFs) auf einen weniger ausgelasteten Port kann den Lastausgleich verbessern, Wartungsaufgaben und Performance-Tuning unterstützen und den indirekten Zugriff verringern.

Durch indirekten Zugriff kann die Systemeffizienz gesenkt werden. Ein Volume-Workload nutzt verschiedene Nodes für die Netzwerkverarbeitung und Datenverarbeitung. Um den indirekten Zugriff zu verringern, können Sie LIFs neu anordnen. Dabei werden LIFs verschoben, sodass derselbe Node für die Netzwerkverarbeitung und Datenverarbeitung verwendet wird. Sie können den Lastausgleich so konfigurieren, dass ONTAP überlastete LIFs automatisch zu einem anderen Port verschieben oder Sie eine LIF manuell verschieben können.

Vorteile
• Verbesserung des Lastausgleichs: • Verringern Sie den indirekten Zugriff.
Überlegungen
Wenn ein LIF verschoben wird, das mit CIFS-Freigaben verbunden ist, werden Clients, die auf CIFS-Freigaben zugreifen, getrennt. Sämtliche Lese- oder Schreibanfragen an die CIFS-Freigaben werden unterbrochen.

Sie verwenden die ONTAP-Befehle zum Konfigurieren des Lastausgleichs. Weitere Informationen finden Sie in der ONTAP Netzwerkdokumentation.

Sie verwenden OnCommand System Manager und die CLI-Befehle von ONTAP, um LIFs manuell zu verschieben.

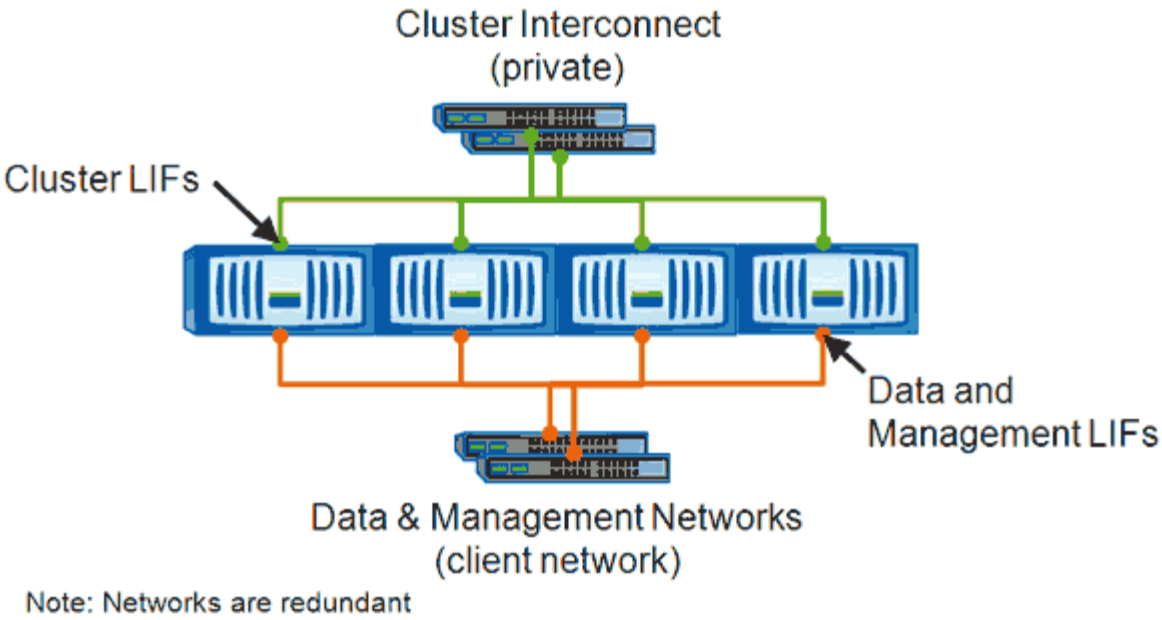
LIFs werden manuell verschoben

Storage Virtual Machines (SVMs) enthalten Daten-Volumes und eine oder mehrere logische Schnittstellen (LIFs), über die die SVM den Clients Daten zur Verfügung stellt. Sie können Daten-LIFs innerhalb derselben SVM von einem physischen Port zu einem anderen verschieben. Möglicherweise möchten Sie dies zum Lastausgleich verbessern oder bei Wartungsarbeiten und Performance-Tuning unterstützen.

Über diese Aufgabe

Es gibt die folgenden Typen von LIFs:

- Daten-LIFs: Sind einer SVM zugeordnet und zur Kommunikation mit den Clients verwendet.
- Cluster-Management-LIFs: Werden zum Verwalten von Nodes, SVMs und dem Cluster selbst verwendet.
- Cluster-LIFs: Werden für den Intracluster-Datenverkehr verwendet.
- Intercluster LIFs: Werden für die Kommunikation zwischen Clustern verwendet.
- Intracluster LIFs: Wird für die Kommunikation zwischen HA-Paaren verwendet.
- SVM-Management-LIFs: Daten-LIFs, die einer SVM zugeordnet und zum Management dieser SVM verwendet werden.



In diesem Workflow wird das Verschieben von Daten-LIFs beschrieben. Dies gilt für NAS (NFS und CIFS) LIFs, nicht jedoch für SAN-LIFs (FC und iSCSI).

Wenn ein LIF verschoben wird, das mit CIFS-Freigaben verbunden ist, wird die Verbindung von Clients, die auf CIFS-Freigaben zugreifen, getrennt. Sämtliche Lese- oder Schreibanfragen an die CIFS-Freigaben werden unterbrochen.

Informationen zum Verschieben anderer Arten von LIFs, einschließlich Details zum Verschieben VON LIFS über verbundene CIFS-Freigaben, finden Sie in der ONTAP-Netzwerkdokumentation.

Sie können die folgenden grundlegenden Aktionen in Bezug auf Daten-LIFs ausführen:

- Zeigt alle Daten-LIFs an.
- Identifizieren der am stärksten ausgelasteten LIFs
- Ermitteln Sie den besten Node zur Annahme einer überlasteten LIF.
- Ändern Sie den Home-Port oder Node für eine LIF, um ihren bevorzugten Speicherort im Cluster zu ändern.

  Sie sollten stattdessen eine LIF verschieben, anstatt eine LIF zu migrieren, um eine dauerhafte Änderung zu erzielen. Um zum ursprünglichen Home Port zurückzukehren, sollten Sie das LIF zurücksetzen.

- Eine Daten-LIF zu einem anderen Port migrieren, um eine temporäre Änderung vorzunehmen, die verwendet werden kann, wenn der Home Port oder Node ein Problem aufweist oder eine geplante Wartung durchgeführt wird.
- Zurücksetzen einer Daten-LIF auf ihren Home-Port

Was LIFs sind

Eine LIF (logische Schnittstelle) ist eine IP-Adresse oder WWPN mit entsprechenden Merkmalen, wie z. B. eine Rolle, ein Home-Port, ein Home-Node, eine Liste von Failover-Ports auf sowie eine Firewall-Richtlinie. Sie können LIFs an Ports konfigurieren, über die

das Cluster Kommunikation über das Netzwerk sendet und empfängt.

LIFs können an folgenden Ports gehostet werden:

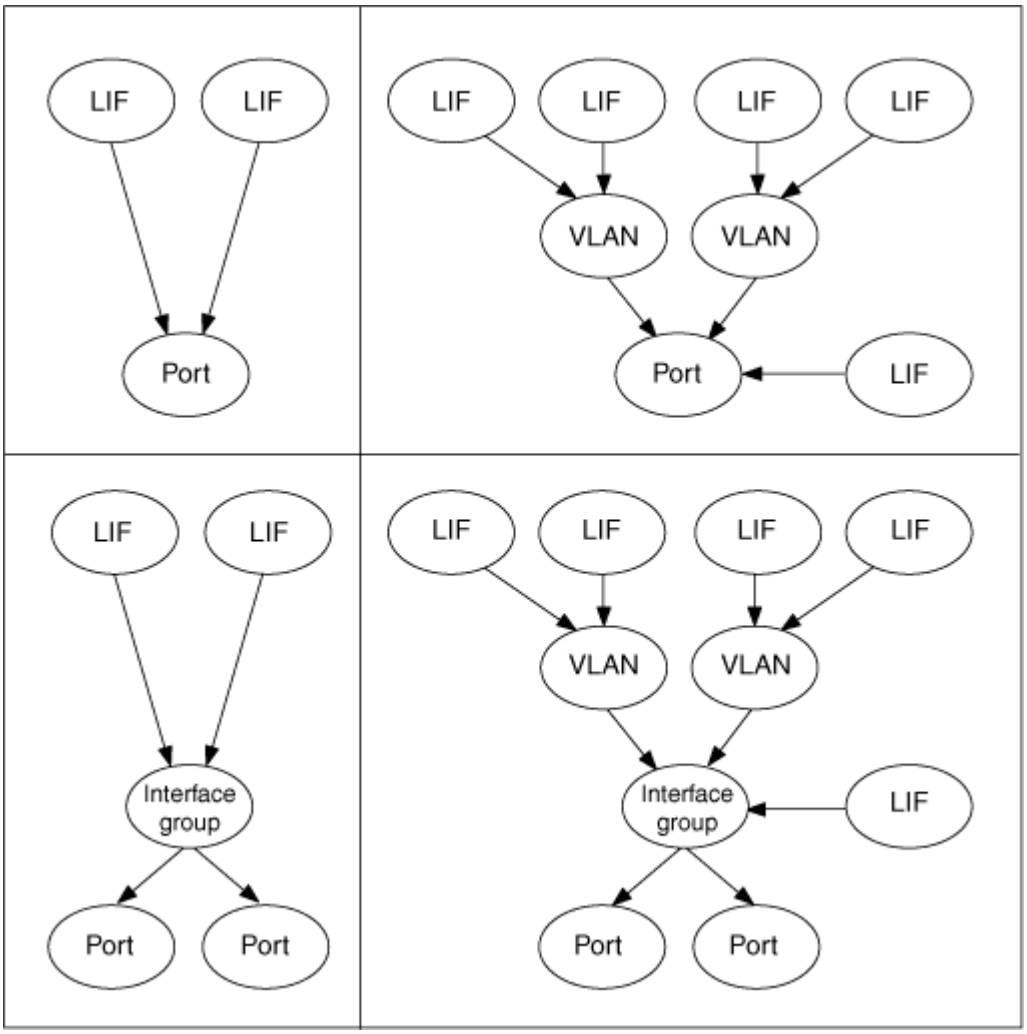
- Physische Ports, die nicht zu Interface Groups gehören
- Interface Groups
- VLANs
- Physische Ports oder Schnittstellengruppen, die VLANs hosten
- Virtuelle IP-Ports (VIP)

  Ab ONTAP 9.5 werden VIP LIFs unterstützt und auf VIP-Ports gehostet.

Während der Konfiguration von SAN-Protokollen, z. B. FC, auf einer logischen Schnittstelle wird sie einem WWPN zugewiesen.

"ONTAP 9 – Systemadministrationshandbuch"

In der folgenden Abbildung wird die Porthierarchie in einem ONTAP-System dargestellt:



Anzeigen aller LIFs in einer SVM mithilfe der CLI

Sie können Informationen zu allen LIFs in einer SVM anzeigen. Möglicherweise möchten Sie alle LIFs anzeigen, bevor Sie bestimmen, welche LIFs möglicherweise ausgelastet sind und verschoben werden sollten.

Über diese Aufgabe

Der Betriebsstatus einer LIF wird dadurch bestimmt, ob sie auf einem bestimmten Port konfiguriert wurde und Daten bereitstellen kann. Wenn eine SVM angehalten wird, können die zugeordneten Daten-LIFs und SVM-Management-LIFs keine Daten mehr bereitstellen. Der Betriebsstatus dieser LIFs ändert sich in `down`.

Schritte

1. Um Informationen zu allen LIFs in einer SVM anzuzeigen, geben Sie den folgenden Befehl ein: `network interface show -vserver vserver_name`

   Mit dem Befehl werden die folgenden Informationen angezeigt:

   - Dem LIF zugeordneten Node oder SVM
   - LIF-Name
   - Administrations- und Betriebsstatus
   - IP-Adresse
   - Netzmaske
   - Node und Port, auf dem die LIF konfiguriert ist

     Ein Home Server kann ein Node oder eine SVM sein.

     Wenn keine Daten für ein Feld verfügbar sind (z. B. die Betriebs-Duplexkonfiguration und die Geschwindigkeit für einen inaktiven Port), wird das Feld als undef angezeigt.

     > Sie können alle verfügbaren Informationen abrufen, indem Sie die angeben `-instance` Parameter.

     Im folgenden Beispiel werden allgemeine Informationen zu allen LIFs einer SVM angezeigt:

```
vs1::> network interface show -vserver vs1
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs1
            lif1         up/up    192.0.2.253/24     node-01       e0b
false
            d2           up/up    192.0.2.252/21     node-01       e0d
true
            data3        up/up    192.0.2.251/20     node-02       e0c
true
```

Identifizierung von LIFs mit den meisten Verbindungen mithilfe der CLI

Möglicherweise möchten Sie eine Daten-LIF migrieren, wenn Sie eine hohe Last oder einen hohen Durchsatz aufweist. Um zu entscheiden, ob eine LIF migriert werden soll, können Sie die Last auf LIFs, die Anzahl der Verbindungen am Port, den Durchsatz und die CPU-Zyklen auf dem Node anzeigen.

Schritte

1. Greifen Sie als Cluster-Administrator auf die CLI zu.
2. Stellen Sie die Berechtigungsebene auf „Advanced“ ein, indem Sie den folgenden Befehl eingeben: `set -privilege advanced`

   Informationen zur Verwendung der CLI im erweiterten Modus finden Sie in der Referenz *Systemadministration*.

3. Geben Sie den folgenden Befehl ein, um das Gewicht der einzelnen LIFs zu ermitteln: `network interface lif-weights show`

   Eine überlastete LIF ist eines mit dem niedrigsten Gewicht.

4. Geben Sie den folgenden Befehl ein, um die aktiven Verbindungen auf einem Node zu suchen: `network connections active show-clients`

   Beachten Sie die höchste Anzahl von Clients pro Node.

```
cluster1::> network connections active show-clients
Node    Client IP Address     Count
------  -----------------     ------
node1   192.0.2.253              12
        192.0.2.252               9
        192.0.2.251              12

node2   192.0.2.250              12
        192.0.2.252               9
        192.0.2.253               9

node3   customer.example.com       2
        customer.example.net       2
        customer.example.org       2
```

5. Geben Sie den folgenden Befehl ein, um die aktiven Verbindungen nach LIF auf einem Node und einer SVM zu finden: `network connections active show-lifs`

   Beachten Sie die höchste Anzahl von Clients pro LIF.

```
cluster1::> network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node1
          vs1           clus1              30

node2
          vs2           clus1              30

node3
          vs3           lif1                2
          vs4           clus1              30
```

6. Überprüfen Sie die LIFs, die sich denselben Home-Port und denselben Home-Node teilen, um die LIFs mit den meisten Verbindungen zu identifizieren.
7. Um den besten Datenport auszuwählen, geben Sie Folgendes ein: `statistics show -object port`

   Der Statistik-Befehl liefert Durchsatz- und Bandbreiteninformationen für Ethernet-Ports. Jede Zeile enthält einen separaten Zähler eindeutiger Informationen. Wert ist der Wert für den Objekttyp seit dem letzten Löschen des Zählers (seit ONTAP zuletzt gestartet wurde).

```
cluster1::> statistics show -object port
Object: port
Instance: e0a
Start-time: 10/11/2013 13:51:41
End-time: 10/11/2013 13:51:41
Node: node1

    Counter                                                     Value
    -------------------------------------------------------- --------
    recv-data                                                      0B
    recv-packets                                                    0
    recv-mcasts                                                     0
    recv-errors                                                     0
    recv-dropped                                                    0
    sent-data                                                      0B
    sent-packets                                                    0
    sent-mcasts                                                     0
    sent-errors                                                     0
    collisions                                                      0
```

Ermitteln des besten Node für eine überlastete LIF mithilfe der CLI

Sie können Informationen zu allen Ports in einem Cluster anzeigen. Sie können Informationen anzeigen, z. B. die Netzwerkport-Rolle (Cluster, Daten oder Node-Management), den Link-Status, die MTU (Maximum Transmission Unit), die Geschwindigkeitseinstellung und den Betriebsstatus sowie die Schnittstellengruppe des Ports.

Schritte

1. Geben Sie zum Anzeigen von Portinformationen den folgenden Befehl ein: `network port show`

   Im folgenden Beispiel werden Informationen zu Netzwerkports angezeigt, die eine Datenrolle aufweisen und sich im Cluster befinden:

```
cluster1::> network port show  -role data -link up
                                    Auto-Negot Duplex      Speed (Mbps)
Node Port Role         Link  MTU    Admin/Oper Admin/Oper  Admin/Oper
---- ---- -----        ----  ----   ---------- ----------  ----------
node1
     e0M  data         up    1500   true/true  full/full   auto/100
     e0b  data         up    1500   true/true  full/full   auto/1000

node2
     e0b  data         up    1500   true/true  full/full   auto/1000
```

2. Überprüfen Sie, ob sich die Zielanschlüsse im gleichen Netzwerk befinden wie der Startport des Quell- und der Home-Node-Ports.

   Beispielsweise sollten sich der Home-Port des Ziels und der Home-Node gegebenenfalls auf demselben VLAN befinden.

3. Um den am wenigsten ausgelasteten Port zu identifizieren, wählen Sie einen Datenport mit der geringsten Anzahl von Verbindungen aus.

Ermitteln des besten Nodes für eine überlastete LIF mithilfe von OnCommand System Manager

Sie können Informationen zu allen Ports in einem Cluster anzeigen. Sie können Informationen anzeigen, z. B. die Netzwerkport-Rolle (Cluster, Daten oder Node-Management), den Link-Status, die MTU (Maximum Transmission Unit), die Geschwindigkeitseinstellung und den Betriebsstatus sowie die Schnittstellengruppe des Ports.

Schritte

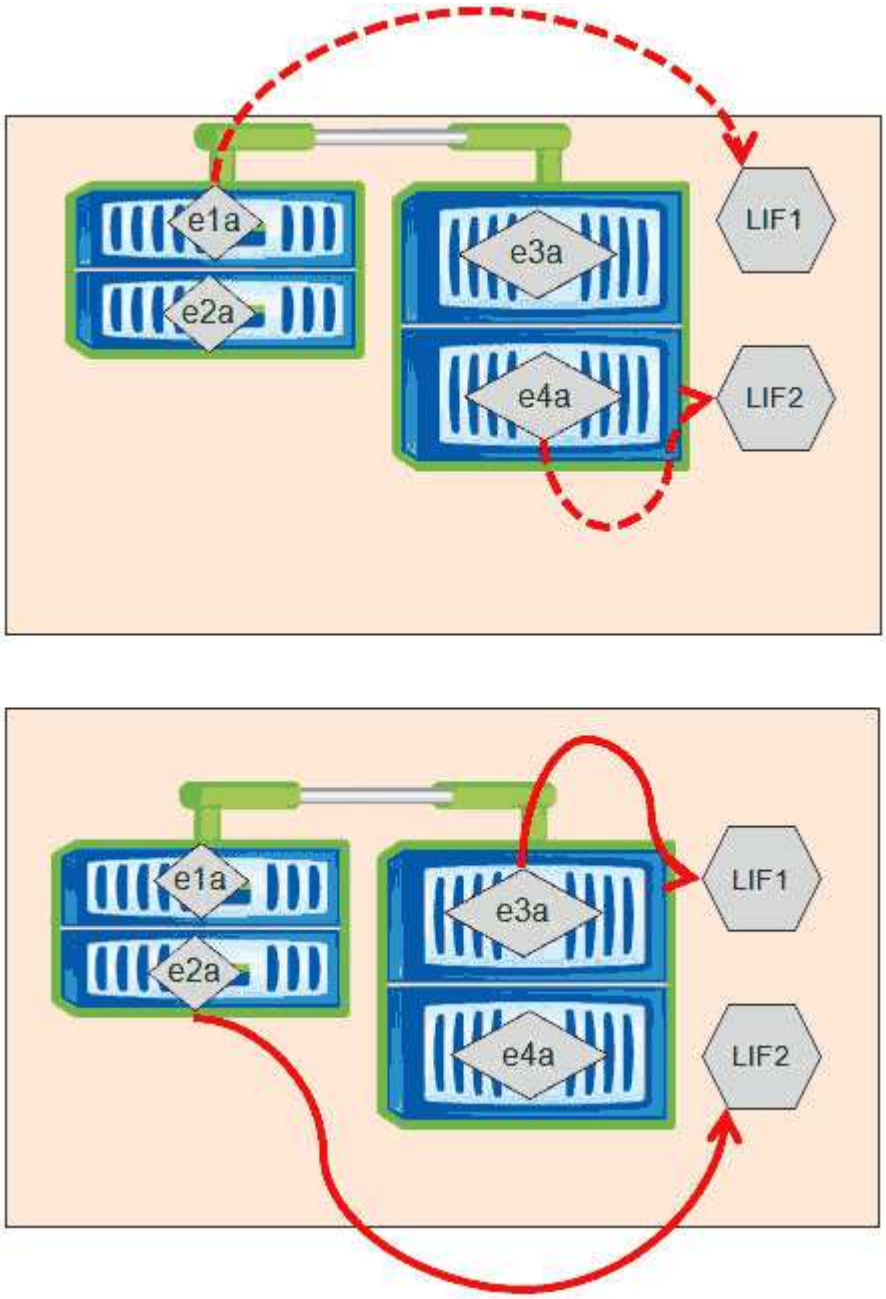
1. Öffnen Sie den OnCommand System Manager.
2. Doppelklicken Sie auf der Registerkarte **Home** auf das Speichersystem.
3. Erweitern Sie im Navigationsbereich die Hierarchie **Nodes**.
4. Um die aktiven Verbindungen auf einem Knoten zu finden, wählen Sie im Navigationsbereich das Symbol für einen Knoten aus.
5. Klicken Sie auf den Namenslink eines Knotens und dann auf **Konfiguration** > **Ports/Adapter**.
6. Beachten Sie die höchste Anzahl von Clients pro Node.

Ändern des Home-Ports und der Nodes für eine LIF mit OnCommand System Manager

Sie können den bevorzugten Speicherort einer logischen Schnittstelle ändern, indem Sie den Home-Port und den Home-Node ändern. Dies ist eine dauerhafte Konfiguration als die Migration einer logischen Schnittstelle, mit der üblicherweise eine LIF vorübergehend auf einen anderen Node während geplanter Wartungsarbeiten verschoben wird.

Über diese Aufgabe

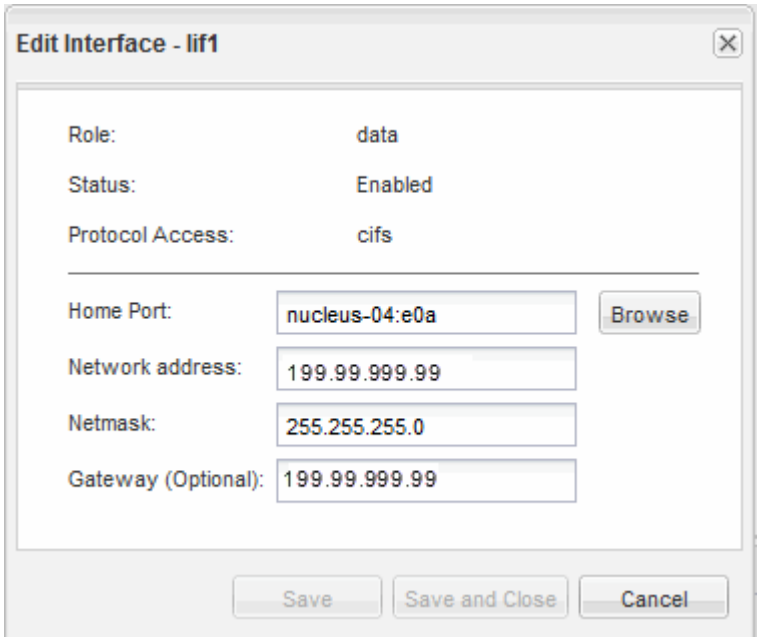
Das folgende Image zeigt den ursprünglichen LIF-Startport und -Node sowie den Home-Port und den Node nach der Änderung. Der ursprüngliche LIF1-Startanschluss wurde von e1a auf e3a umgestellt und LIF2 wurde von e4a in e2a geändert.



Schritte

1. Öffnen Sie den OnCommand System Manager.
2. Doppelklicken Sie auf der Registerkarte **Home** auf das Speichersystem.
3. Erweitern Sie im Navigationsbereich die Hierarchie **SVMs**.
4. Wählen Sie im Navigationsbereich die SVMs aus und klicken Sie auf **Konfiguration** > **Netzwerkschnittstellen**.
5. Wählen Sie das LIF aus und klicken Sie auf **Bearbeiten**.

6. Geben Sie im Dialogfeld Schnittstelle bearbeiten** den Home-Port und die Netzwerkadresse des Ziel-Ports ein.



In ONTAP 8.2 ist das Feld Home-Port deaktiviert.

7. Klicken Sie auf **Speichern und Schließen**.

Zurücksetzen eines LIF auf seinen Home Port mithilfe von OnCommand System Manager

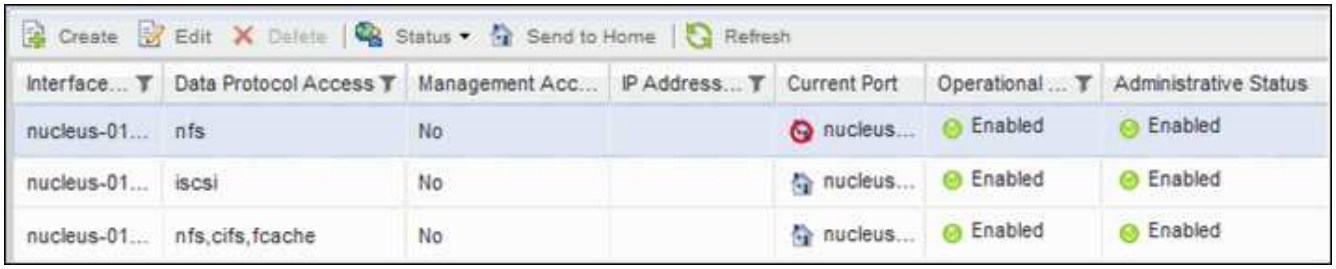
Sie können eine LIF nach einem Failover von ihrem aktuellen Port auf ihren Home Port zurücksetzen oder sie wird entweder manuell oder automatisch zu einem anderen Port migriert. Dies ist mit OnCommand System Manager möglich.

Über diese Aufgabe

Beim Erstellen einer logischen Schnittstelle gibt der Administrator einen Home Port und einen Home Node an, der als bevorzugter Speicherort der logischen Schnittstelle verwendet werden soll. Wenn der Home-Node nicht verfügbar ist oder der Home-Port einen physischen Linkausfall hat, wird die LIF automatisch zu einem neuen Speicherort migriert. Der neue Speicherort wird in OnCommand System Manager z. B. als aktueller Port für die LIF gemeldet. Sofern die Option zur automatischen Wiederherstellung nicht aktiviert ist, bleibt die LIF an diesem neuen Speicherort, bis sie zurückgesetzt wird.

Schritte

1. Öffnen Sie den OnCommand System Manager.
2. Doppelklicken Sie auf der Registerkarte **Home** auf das Speichersystem.
3. Erweitern Sie im Navigationsbereich die Hierarchie **Storage Virtual Machines**.
4. Wählen Sie im Navigationsbereich die SVM aus und klicken Sie auf **Konfiguration** > **Netzwerkschnittstellen**.
5. Suchen Sie nach Daten-LIFs, die ein Haus-Symbol mit einem roten Kreuz in der Spalte **Current Port** anzeigen, wie im folgenden Bild.



6. Wählen Sie das LIF aus und klicken Sie auf **an die Startseite senden**.

   Diese Option ist nur aktiviert, wenn die ausgewählte Schnittstelle auf einem nicht-Home-Port gehostet wird und wenn der Home-Port verfügbar ist.

Kontrolle des Workload-Durchsatzes durch Storage-QoS

Sie können eine Richtliniengruppe für Quality of Service (QoS) erstellen oder bearbeiten, um das Limit für I/O pro Sekunde (IOPS) oder den Durchsatz (MB/s) für die in ihnen enthaltenen Workloads zu steuern. Wenn sich die Workloads in einer Richtliniengruppe ohne festgelegte Grenzwerte befinden, wie z. B. in der Standardrichtlinie, oder das festgelegte Limit Ihren Anforderungen nicht entspricht, können Sie die Obergrenze erhöhen oder die Workloads in eine neue oder vorhandene Richtliniengruppe verschieben, die das gewünschte Limit hat.

QoS-Richtliniengruppen mit „`standard`“ können individuellen Workloads zugewiesen werden, zum Beispiel einzelnen Volumes oder LUNs. In diesem Fall kann der Workload das volle Durchsatzlimit verwenden. QoS-Richtliniengruppen können zudem mehreren Workloads zugewiesen werden. In diesem Fall wird das Durchsatzlimit von den Workloads gemeinsam genutzt. Beispielsweise würde ein QoS-Limit von 9,000 IOPS, das drei Workloads zugewiesen ist, die kombinierten IOPS von über 9,000 IOPS einschränken.

„`Adaptive`“ QoS-Richtliniengruppen können auch einzelnen Workloads oder mehreren Workloads zugewiesen werden. Allerdings erhält jeder Workload bei der Zuweisung zu mehreren Workloads das volle Durchsatzlimit, anstatt gemeinsam mit anderen Workloads auf den Durchsatzwert zu zugreifen. Zudem passen anpassungsfähige QoS-Richtlinien die Durchsatzeinstellung automatisch basierend auf der Volume-Größe pro Workload an. So erhält das Verhältnis von IOPS zu Terabyte bei sich änderender Volume aufrecht. Wenn beispielsweise der Spitzenwert in der Richtlinie für anpassungsfähige QoS auf 5,000 IOPS/TB festgelegt ist, dann hat ein 10-TB-Volume eine Durchsatzobergrenze von 50,000 IOPS. Wenn die Größe des Volumes später auf 20 TB geändert wird, passt die anpassungsfähige QoS die Obergrenze an 100,000 IOPS an.

Ab ONTAP 9.5 können Sie die Blockgröße einschließen, wenn Sie eine anpassungsfähige QoS-Richtlinie definieren. Dadurch wird die Richtlinie für Fälle, in denen Workloads sehr große Blockgrößen verwenden und letztendlich einen hohen Prozentsatz an Durchsatz verbrauchen, effektiv von einem Schwellenwert für IOPS/TB in einen MB/s-Schwellenwert konvertiert.

Wenn bei QoS-Richtlinien für Shared-Gruppen die IOPS oder MB/s aller Workloads in einer Richtliniengruppe das festgelegte Limit überschreitet, drosselt die Richtliniengruppe die Workloads, um ihre Aktivitäten zu beschränken. Dies kann die Performance aller Workloads in der Richtliniengruppe beeinträchtigen. Wenn ein dynamisches Ereignis durch die Richtliniengruppendrosselung generiert wird, zeigt die Ereignisbeschreibung den Namen der beteiligten Richtliniengruppe an.

Auf der Seite „Performance/Volumes Inventory“ können Sie die betroffenen Volumes nach IOPS und MB/s sortieren, um zu sehen, welche Workloads die höchste Auslastung aufweisen und welche dazu möglicherweise beigetragen haben. Wählen Sie auf der Seite „Performance/Volumes Explorer“ andere

Volumes oder LUNs aus, um sie mit den betroffenen Workload-IOPS oder dem Durchsatz des MB/s zu vergleichen.

Durch die Zuweisung von Workloads, die die Node-Ressourcen zu einer restriktiveren Richtliniengruppeneinstellung überbeanspruchen, drosselt die Richtliniengruppe die Workloads, um ihre Aktivitäten zu beschränken. Dadurch wird die Nutzung der Ressourcen auf diesem Node verringert. Wenn der Workload jedoch mehr Node-Ressourcen nutzen soll, kann der Wert der Richtliniengruppe erhöht werden.

Sie können System Manager oder die Befehle ONTAP zum Verwalten von Richtliniengruppen verwenden, einschließlich der folgenden Aufgaben:

- Erstellen einer Richtliniengruppe
- Hinzufügen oder Entfernen von Workloads in einer Richtliniengruppe
- Verschieben eines Workloads zwischen Richtliniengruppen
- Ändern der Durchsatzbegrenzung einer Richtliniengruppe
- Workloads werden in ein anderes Aggregat und/oder Node verschoben

Führen Sie Storage-Effizienzvorgänge zu weniger geschäftigen Zeiten aus

Sie können die Richtlinie oder den Zeitplan ändern, die Storage-Effizienzvorgänge zur Ausführung verarbeiten, wenn die betroffenen Volume-Workloads weniger beschäftigt sind.

Storage-Effizienzvorgänge können viele Cluster-CPU-Ressourcen beanspruchen und zu den Volumes, auf denen die Operationen ausgeführt werden, als problematischer werden. Wenn die Opfer-Volumes gleichzeitig bei Ausführung der Storage-Effizienz-Vorgänge eine hohe Aktivität aufweisen, kann sich ihre Latenz erhöhen und ein Ereignis auslösen.

Auf der Seite Ereignisdetails werden im Abschnitt Systemdiagnose Workloads in der Richtliniengruppe QoS anhand von Spitzenzeiten angezeigt, um die problematische Workload zu identifizieren. Wenn „`sStorage Efficiency`“ oben in der Tabelle angezeigt wird, werden diese Vorgänge die Opfer-Workloads Mobbing. Durch Ändern der Effizienzrichtlinie oder des Zeitplans, die für die Ausführung dieser Workloads weniger stark sind, können Sie verhindern, dass Storage-Effizienz-Vorgänge Konflikte auf einem Cluster verursachen.

Mit OnCommand System Manager managen Sie Effizienzrichtlinien. Sie können die ONTAP-Befehle verwenden, um Effizienzrichtlinien und Zeitpläne zu managen.

Was ist Storage-Effizienz

Storage-Effizienzfunktionen ermöglichen Ihnen, die maximale Datenmenge zu den geringstmöglichen Kosten zu speichern, ermöglichen schnelles Datenwachstum und belegen gleichzeitig weniger Speicherplatz. Die Strategie von NetApp für Storage-Effizienz basiert auf einer integrierten Grundlage aus Storage-Virtualisierung und Unified Storage, die durch das zentrale ONTAP Betriebssystem und das WAFL Filesystem (Write Anywhere File Layout) bereitgestellt werden.

Storage-Effizienz beinhaltet Technologien wie Thin Provisioning, Snapshot-Kopie, Deduplizierung, Datenkomprimierung, FlexClone, Thin Replication mit SnapVault und Volume SnapMirror, RAID-DP, Flash Cache, Flash Pool Aggregat und FabricPool-fähigen Aggregaten, die die Storage-Auslastung erhöhen und die Storage-Kosten senken.

Die Unified Storage-Architektur ermöglicht eine effiziente Konsolidierung eines Storage Area Network (SAN), Network-Attached Storage (NAS) und sekundären Storage auf einer einzigen Plattform.

Ultrakompakte Festplatten, wie z. B. SATA-Laufwerke (Serial Advanced Technology Attachment), die innerhalb von Flash Pool Aggregaten oder mit Flash Cache und RAID-DP Technologie konfiguriert sind, steigern die Effizienz ohne Auswirkungen auf Performance und Resiliency.

Ein FabricPool-fähiges Aggregat umfasst ein reines SSD-Aggregat als Performance-Tier und einen Objektspeicher, den Sie als Cloud-Tier angeben. Bei der Konfiguration von FabricPool kann gemanagt werden, auf welchen Storage-Tiers (der lokale Performance-Tier oder das Cloud-Tier) Daten gespeichert werden sollen, basierend darauf, ob häufig auf den Daten zugegriffen wird.

Technologien wie Thin Provisioning, Snapshot Kopien, Deduplizierung, Datenkomprimierung, Thin Replication mit SnapVault und Volume SnapMirror sowie FlexClone bieten bessere Einsparungen. Sie können diese Technologien einzeln oder in Kombination verwenden, um maximale Storage-Effizienz zu erzielen.

Fügen Sie Festplatten hinzu und weisen Sie Daten erneut zu

Sie können einem Aggregat Festplatten hinzufügen, um die Storage-Kapazität und Performance dieses Aggregats zu erhöhen. Nach dem Hinzufügen von Festplatten wird die Lese-Performance nur verbessert, wenn die Daten über die hinzugefügten Festplatten verteilt werden.

Sie können diese Anweisungen verwenden, wenn Unified Manager aggregierte Ereignisse erhalten hat, die durch dynamische Schwellenwerte oder durch vom System definierte Performance-Schwellenwerte ausgelöst wurden:

- Wenn Sie ein dynamisches Schwellenwertereignis erhalten haben, wird auf der Seite „Ereignisdetails“ das Symbol für die Clusterkomponente, das das „Aggregat mit Konflikten“ darstellt, rot hervorgehoben.

  Unter dem Symbol in Klammern steht der Name des Aggregats, das das Aggregat identifiziert, zu dem Sie Festplatten hinzufügen können.

- Wenn Sie ein systemdefiniertes Schwellenwertereignis erhalten haben, wird auf der Seite Ereignisdetails der Text für die Ereignisbeschreibung den Namen des Aggregats mit dem Problem aufgeführt.

  Sie können Platten hinzufügen und Daten zu diesem Aggregat neu zuweisen.

Die Festplatten, die Sie dem Aggregat hinzufügen, müssen bereits im Cluster vorhanden sein. Wenn auf dem Cluster keine zusätzlichen Festplatten verfügbar sind, müssen Sie sich möglicherweise an den Administrator wenden oder weitere Festplatten erwerben. Mit OnCommand System Manager oder den ONTAP-Befehlen können Sie einem Aggregat Festplatten hinzufügen.

Sie sollten Daten nur bei Nutzung von HDD- und Flash Pool-Aggregaten neu zuweisen. Weisen Sie Daten nicht auf SSD- oder FabricPool-Aggregaten neu zu.

Aktivierung von Flash Cache auf einem Node kann die Workload-Performance verbessern

Sie können die Workload-Performance verbessern, indem Sie Flash Cache™ intelligentes Daten-Caching auf jedem Node im Cluster aktivieren.

Ein Flash Cache Modul, das Performance Acceleration Module PCIe-basiertes Speichermodul, optimiert die Performance von Random Read-intensiven Workloads, indem es als intelligenter externer Read-Cache fungiert. Diese Hardware arbeitet zusammen mit der WAFL Software-Komponente für externen Cache von ONTAP.

In Unified Manager wird auf der Seite „Ereignisdetails“ das Symbol für die Cluster-Komponente, das das von Konflikten gemachte Aggregat darstellt, rot hervorgehoben. Unter dem Symbol in Klammern steht der Name des Aggregats, der das Aggregat identifiziert. Sie können Flash Cache auf dem Node aktivieren, auf dem sich das Aggregat befindet.

Sie können mit dem OnCommand System Manager oder den ONTAP-Befehlen herausfinden, ob Flash Cache installiert oder aktiviert ist, und ihn aktivieren, wenn er noch nicht aktiviert ist. Mit dem folgenden Befehl wird angegeben, ob Flash Cache auf einem bestimmten Node aktiviert ist: `cluster::> run local options flexscale.enable`

Weitere Informationen über Flash Cache und die Anforderungen für deren Verwendung finden Sie im folgenden technischen Bericht:

"Technischer Bericht 3832: Flash Cache Best Practices Guide"

Die Aktivierung von Flash Pool auf einem Storage-Aggregat kann die Workload-Performance verbessern

Sie können die Workload-Performance durch Aktivierung der Flash Pool Funktion auf einem Aggregat verbessern. Ein Flash Pool ist ein Aggregat, das sowohl HDDs als auch SSDs umfasst. Die HDDs werden im primären Storage eingesetzt und die SSDs bieten einen hochperformanten Lese- und Schreib-Cache, um die Aggregat-Performance zu steigern.

In Unified Manager wird auf der Seite „Event Details“ der Name des Aggregats mit Konflikten angezeigt. Sie können mit OnCommand System Manager oder mit den ONTAP-Befehlen herausfinden, ob Flash Pool für ein Aggregat aktiviert ist. Wenn SSDs installiert sind, kann sie über die Befehlszeilenschnittstelle aktiviert werden. Wenn SSDs installiert sind, können Sie mit dem folgenden Befehl auf dem Aggregat feststellen, ob Flash Pool aktiviert ist: `cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled`

In diesem Befehl `aggr_name` Ist der Name des Aggregats, z. B. das Aggregat, das über Konflikte verfügt.

Weitere Informationen zu Flash Pool und den jeweiligen Anforderungen finden Sie im *Clustered Data ONTAP Leitfaden zum Management von physischem Storage*.

Zustandsprüfung der MetroCluster Konfiguration

Mit Unified Manager können Sie den Zustand der Cluster in einer MetroCluster-Konfiguration überprüfen. Anhand des Integritätsstatus und der Ereignisse können Sie ermitteln, ob es Hardware- oder Softwareprobleme gibt, die die Performance Ihrer Workloads beeinträchtigen können.

Wenn Sie Unified Manager so konfigurieren, dass E-Mail-Alarme gesendet werden, können Sie Ihre E-Mail auf Probleme mit dem Systemzustand im lokalen oder Remote-Cluster prüfen, die möglicherweise zu einem Performance-Ereignis beigetragen haben. In der Benutzeroberfläche von Unified Manager können Sie **Ereignisse** auswählen, um eine Liste aktueller Ereignisse anzuzeigen. Anschließend können Sie mit den

Filtern nur MetroCluster-Konfigurationsereignisse anzeigen.

Überprüfung der MetroCluster-Konfiguration

Sie können Performance-Probleme bei gespiegelten Workloads in einer MetroCluster-Konfiguration vermeiden, indem Sie sicherstellen, dass die MetroCluster-Konfiguration korrekt eingerichtet ist. Sie können außerdem die Workload-Performance verbessern, indem Sie die Konfiguration ändern oder Software- oder Hardware-Komponenten aktualisieren.

Das *MetroCluster Installations- und Konfigurationshandbuch* enthält Anweisungen zum Einrichten der Cluster in der MetroCluster-Konfiguration, einschließlich der Fibre Channel (FC)-Switches, Kabel und Inter-Switch-Links (ISLs). Darüber hinaus unterstützt Sie die Konfiguration der MetroCluster Software, sodass die lokalen und Remote Cluster mit gespiegelten Volume-Daten kommunizieren können.

Sie können Ihre MetroCluster Konfiguration mit den Anforderungen im *MetroCluster Installations- und Konfigurationsleitfaden* vergleichen, um zu ermitteln, ob ein Ändern oder Aktualisieren von Komponenten in Ihrer MetroCluster-Konfiguration die Workload-Performance verbessern könnte. Dieser Vergleich hilft Ihnen bei der Beantwortung der folgenden Fragen:

- Sind die Controller für Ihre Workloads geeignet?
- Müssen Sie Ihre ISL-Bundles auf eine höhere Bandbreite aktualisieren, um einen höheren Durchsatz zu bewältigen?
- Können Sie die Buffer-to-Buffer Credits (BBC) auf Ihren Switches anpassen, um die Bandbreite zu erhöhen?
- Wenn Ihre Workloads einen hohen Schreibdurchsatz auf SSD-Storage (Solid State Drive) aufweisen, müssen Sie Ihre FC-to-SAS-Bridges aktualisieren, um den Durchsatz zu bewältigen?

Informationen zum Austauschen oder Aktualisieren von MetroCluster-Komponenten finden Sie im *MetroCluster-Servicehandbuch*.

Verschieben von Workloads in ein anderes Aggregat

Mithilfe von Unified Manager können Sie ein Aggregat identifizieren, das weniger ausgelastet ist als das Aggregat, in dem Ihre Workloads sich befinden. Anschließend können Sie ausgewählte Volumes oder LUNs zu diesem Aggregat verschieben. Durch die Verschiebung hochperformanter Workloads in ein weniger ausgelastete Aggregat oder ein Aggregat mit aktiviertem Flash-Storage können die Workloads effizienter arbeiten.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den Namen des Aggregats aufgezeichnet haben, das derzeit ein Performance-Problem hat.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu der das Aggregat das Ereignis erhalten hat.
- Sie müssen die Ereignis-ID z. B. aufgezeichnet haben"` p-sdt-clue1-ag-2542`".
- Unified Manager muss einen Monat oder mehrere Performance-Daten erfasst und analysiert haben.

Über diese Aufgabe

Anhand dieser Schritte werden die folgenden Ressourcen ermittelt, damit Sie hochperformante Workloads in ein weniger ausgelasttes Aggregat verschieben können:

- Die Aggregate auf demselben Cluster, die weniger genutzt werden
- Die Volumes mit der höchsten Performance im aktuellen Aggregat

Schritte

1. Identifizieren Sie das Aggregat im Cluster, das am wenigsten genutzt wird:
   a. Klicken Sie auf der Seite **Event** Details auf den Namen des Clusters, auf dem sich das Aggregat befindet.

      Die Cluster-Details werden auf der Landing Page Performance/Cluster angezeigt.

   b. Klicken Sie auf der Seite **Zusammenfassung** im Bereich **verwaltete Objekte** auf **Aggregate**.

      Die Liste der Aggregate auf diesem Cluster wird angezeigt.

   c. Klicken Sie auf die Spalte **Nutzung**, um die Aggregate nach den am wenigsten verwendeten Aggregaten zu sortieren.

      Sie können auch jene Aggregate identifizieren, die die größte **freie Kapazität** haben. Diese Liste enthält potenzielle Aggregate, zu denen Workloads verschoben werden können.

   d. Notieren Sie sich den Namen des Aggregats, zu dem Sie die Workloads verschieben möchten.
2. Ermitteln Sie die hochperformanten Volumes des Aggregats, das das Ereignis erhalten hat:
   a. Klicken Sie auf das Aggregat mit der Leistungsfrage.

      Die Aggregatdetails werden auf der Seite „Performance/Aggregate Explorer“ angezeigt.

   b. Wählen Sie im Auswahlfeld **Zeitbereich** die Option **Letzte 30 Tage** aus und klicken Sie dann auf **Bereich anwenden**.

      So können Sie einen längeren Performance-Verlauf anzeigen als die Standarddauer von 72 Stunden. Sie möchten ein Volume verschieben, das viele Ressourcen auf einer konsistenten Basis verwendet, und nicht nur in den letzten 72 Stunden.

   c. Wählen Sie im Steuerelement **Ansicht und Vergleich Volumen auf diesem Aggregat** aus.

      Es wird eine Liste der FlexVol Volumes und FlexGroup-zusammengehörigen Volumes auf diesem Aggregat angezeigt.

   d. Sortieren Sie die Volumes nach den höchsten MB/s und dann nach den höchsten IOPS, um die Volumes mit der höchsten Performance zu sehen.
   e. Notieren Sie sich die Namen der Volumes, die Sie in ein anderes Aggregat verschieben möchten.
3. Verschieben Sie die hochperformanten Volumes auf das identifizierte Aggregat mit niedriger Auslastung.

   Sie können die Schritte für die Verschiebung mit OnCommand System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools ausführen.

Nachdem Sie fertig sind

Prüfen Sie nach einigen Tagen, ob Sie dieselbe Art von Ereignissen von diesem Node oder Aggregat erhalten.

Workloads werden auf einen anderen Node verschoben

Mithilfe von Unified Manager können Sie ein Aggregat auf einem anderen Node identifizieren, der weniger ausgelastet ist als der Node, auf dem Ihre Workloads derzeit ausgeführt werden. Anschließend können Sie ausgewählte Volumes zu diesem Aggregat verschieben. Durch die Migration hochperformanter Workloads auf ein Aggregat auf einem weniger ausgelasteten Node können die Workloads auf beiden Nodes effizienter ausgeführt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den Namen des Node notiert haben, der derzeit ein Performance-Problem hat.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu der der Node das Performance-Ereignis erhalten hat.
- Sie müssen die Ereignis-ID—zum Beispiel „`p-sdt-clus1-nod-6982`“ aufgezeichnet haben.
- Unified Manager muss Performance-Daten für einen Monat oder länger erfassen und analysieren haben.

Über diese Aufgabe

Mithilfe dieses Verfahrens können Sie die folgenden Ressourcen ermitteln, um hochperformante Workloads auf einen weniger ausgelasteten Node zu verschieben:

- Die Nodes in demselben Cluster verfügen über die höchste freie Performance-Kapazität
- Die Aggregate auf dem neuen Node mit der höchsten freien Performance-Kapazität
- Die Volumes mit der höchsten Performance auf dem aktuellen Node

Schritte

1. Ermitteln Sie einen Node im Cluster mit der größten freien Performance-Kapazität:
   a. Klicken Sie auf der Seite **Event Details** auf den Namen des Clusters, auf dem sich der Knoten befindet.

      Die Cluster-Details werden auf der Landing Page Performance/Cluster angezeigt.

   b. Klicken Sie auf der Registerkarte **Übersicht** im Bereich **verwaltete Objekte** auf **Knoten**.

      Die Liste der Nodes auf diesem Cluster wird angezeigt.

   c. Klicken Sie auf die Spalte **verwendete Performance-Kapazität**, um die Knoten nach dem geringsten Prozentsatz zu sortieren.

      Diese enthält eine Liste potenzieller Nodes, zu die Sie Workloads verschieben können.

   d. Notieren Sie sich den Namen des Node, auf den Sie die Workloads verschieben möchten.

2. Identifizieren Sie ein Aggregat auf dem neuen Node, der am wenigsten genutzt wird:
   a. Klicken Sie im linken Navigationsbereich auf **Leistung** > **Aggregate**.

      Die Seite Performance/Aggregate wird angezeigt.

   b. Klicken Sie im linken Dropdown-Menü auf **Filterung**, wählen Sie **Knoten** aus, geben Sie den Namen des Knotens in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.

      Die Seite Performance/Aggregate wird mit der Liste der auf diesem Node verfügbaren Aggregate neu angezeigt.

   c. Klicken Sie auf die Spalte **Performance Capacity Used**, um die Aggregate nach den am wenigsten verwendeten Aggregaten zu sortieren.

      Diese Liste enthält potenzielle Aggregate, zu denen Workloads verschoben werden können.

   d. Notieren Sie sich den Namen des Aggregats, zu dem Sie die Workloads verschieben möchten.
3. Ermitteln Sie die hochperformanten Workloads vom Node, der das Ereignis erhalten hat:
   a. Kehren Sie zur Seite **Veranstaltungsdetails** für die Veranstaltung zurück.
   b. Klicken Sie im Feld **Betroffene Volumes** auf den Link für die Anzahl der Volumes.

      Die Seite Performance/Volumes wird mit einer gefilterten Liste der Volumes auf diesem Node angezeigt.

   c. Klicken Sie auf die Spalte **Gesamtkapazität**, um die Volumes nach dem größten zugewiesenen Speicherplatz zu sortieren.

      Hier wird eine Liste potenzieller Volumes angezeigt, die Sie möglicherweise verschieben möchten.

   d. Notieren Sie sich die Namen der Volumes, die Sie verschieben möchten, sowie die Namen der aktuellen Aggregate, auf denen sich diese befinden.
4. Verschieben Sie die Volumes zu den Aggregaten, die Sie als größte freie Performance-Kapazität auf dem neuen Node identifiziert haben.

   Sie können die Schritte für die Verschiebung mit OnCommand System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools ausführen.

Nachdem Sie fertig sind

Nach einigen Tagen können Sie überprüfen, ob Sie von diesem Node bzw. Aggregat dieselbe Art von Ereignissen erhalten.

Verschieben von Workloads in ein Aggregat auf einem anderen Node

Mithilfe von Unified Manager können Sie ein Aggregat auf einem anderen Node identifizieren, der weniger ausgelastet ist als der Node, auf dem Ihre Workloads gerade ausgeführt werden. Anschließend können Sie ausgewählte Volumes zu diesem Aggregat verschieben. Durch die Migration hochperformanter Workloads auf ein Aggregat auf einem weniger ausgelasteten Node können Workloads auf beiden Nodes effizienter ausgeführt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den Namen des Node notiert haben, der derzeit ein Performance-Problem hat.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu der der Node das Performance-Ereignis erhalten hat.
- Sie müssen die Ereignis-ID z. B. „`p-sdt-clus1-nod-6982`“ aufgezeichnet haben.
- Unified Manager muss einen Monat oder mehrere Performance-Daten erfasst und analysiert haben.

Über diese Aufgabe

Anhand dieser Schritte werden die folgenden Ressourcen ermittelt, damit Sie hochperformante Workloads auf einen weniger ausgelasteten Node verschieben können:

- Die Nodes auf demselben Cluster, die weniger genutzt werden
- Die Aggregate auf dem neuen Node, die am wenigsten genutzt werden
- Die Volumes mit der höchsten Performance auf dem aktuellen Node

Schritte

1. Identifizieren Sie einen Knoten im Cluster, der am wenigsten genutzt wird:
   a. Klicken Sie auf der Seite **Event** Details auf den Namen des Clusters, auf dem sich der Knoten befindet.

      Die Cluster-Details werden auf der Landing Page Performance/Cluster angezeigt.

   b. Klicken Sie auf der Seite **Übersicht** im Bereich **verwaltete Objekte** auf **Knoten**.

      Die Liste der Nodes auf diesem Cluster wird angezeigt.

   c. Klicken Sie auf die Spalte **Auslastung**, um die Knoten nach der geringsten Auslastung zu sortieren.

      Sie können auch die Knoten identifizieren, die die größte **freie Kapazität** haben. Diese enthält eine Liste potenzieller Nodes, zu die Sie Workloads verschieben können.

   d. Notieren Sie sich den Namen des Node, auf den Sie die Workloads verschieben möchten.
2. Identifizieren Sie ein Aggregat auf dem neuen Node, der am wenigsten genutzt wird:
   a. Klicken Sie im linken Navigationsbereich auf **Leistung** > **Aggregate**.

      Die Seite Performance/Aggregate wird angezeigt.

   b. Klicken Sie im linken Dropdown-Menü auf **Filterung**, wählen Sie **Knoten** aus, geben Sie den Namen des Knotens in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.

      Die Performance/Aggregate werden mit der Liste der auf diesem Node verfügbaren Aggregate neu angezeigt.

   c. Klicken Sie auf die Spalte **Nutzung**, um die Aggregate nach den am wenigsten verwendeten Aggregaten zu sortieren.

      Sie können auch jene Aggregate identifizieren, die die größte **freie Kapazität** haben. Diese Liste enthält potenzielle Aggregate, zu denen Workloads verschoben werden können.

d. Notieren Sie sich den Namen des Aggregats, zu dem Sie die Workloads verschieben möchten.

3. Ermitteln Sie die hochperformanten Workloads vom Node, der das Ereignis erhalten hat:
   a. Kehren Sie zur Seite **Event**-Details für die Veranstaltung zurück.
   b. Klicken Sie im Feld **Betroffene Volumes** auf den Link für die Anzahl der Volumes.

      Die Seite Performance/Volumes wird mit einer gefilterten Liste der Volumes auf diesem Node angezeigt.

   c. Klicken Sie auf die Spalte **Gesamtkapazität**, um die Volumes nach dem größten zugewiesenen Speicherplatz zu sortieren.

      Hier wird eine Liste potenzieller Volumes angezeigt, die Sie möglicherweise verschieben möchten.

   d. Notieren Sie sich die Namen der Volumes, die Sie verschieben möchten, sowie die Namen der aktuellen Aggregate, auf denen sich diese befinden.
4. Verschieben Sie die Volumes zu den Aggregaten, die Sie als niedrige Auslastung auf dem neuen Node angegeben haben.

   Sie können die Schritte für die Verschiebung mit OnCommand System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools ausführen.

Nachdem Sie fertig sind

Prüfen Sie nach einigen Tagen, ob Sie dieselbe Art von Ereignissen von diesem Node oder Aggregat erhalten.

Workloads werden in einen Node in einem anderen HA-Paar verschoben

Sie können Unified Manager verwenden, um ein Aggregat auf einem Node in einem anderen HA-Paar zu identifizieren, das über mehr freie Performance-Kapazität verfügt als das HA-Paar, in dem Ihre Workloads derzeit ausgeführt werden. Anschließend können Sie ausgewählte Volumes auf dem neuen HA-Paar in Aggregate verschieben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Ihr Cluster muss aus mindestens zwei HA-Paaren bestehen

  Diese Problembehebung ist nicht möglich, wenn nur ein HA-Paar im Cluster vorhanden ist.

- Sie müssen die Namen der beiden Nodes im HA-Paar, bei dem derzeit ein Performance-Problem aufgetreten ist, notiert haben.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu der die Nodes das Performance-Ereignis erhalten haben.
- Sie müssen die Ereignis-ID—zum Beispiel „`p-sdt-clus1-nod-6982`“ aufgezeichnet haben.
- Unified Manager muss Performance-Daten für einen Monat oder länger erfassen und analysieren haben.

Über diese Aufgabe

Durch die Verschiebung hochperformanter Workloads auf ein Aggregat auf einen Node mit einer höheren

freien Performance-Kapazität können Workloads auf beiden Nodes effizienter ausgeführt werden. Mithilfe dieses Verfahrens können Sie die folgenden Ressourcen ermitteln, um hochperformante Workloads auf einen Node mit mehr freier Performance-Kapazität auf einem anderen HA-Paar zu verschieben:

- Die Nodes in einem anderen HA-Paar auf demselben Cluster mit der größten freien Performance-Kapazität
- Die Aggregate auf den neuen Nodes mit der höchsten freien Performance-Kapazität
- Auf den aktuellen Nodes höchste Performance

Schritte

1. Identifizieren Sie die Nodes, die zu einem anderen HA-Paar auf demselben Cluster gehören:
   a. Klicken Sie auf der Seite **Event Details** auf den Namen des Clusters, auf dem sich die Knoten befinden.

      Die Cluster-Details werden auf der Landing Page Performance/Cluster angezeigt.

   b. Klicken Sie auf der Seite **Übersicht** im Bereich **verwaltete Objekte** auf **Knoten**.

      Die Liste der Nodes in diesem Cluster wird auf der Seite Performance/Nodes angezeigt.

   c. Notieren Sie sich die Namen der Nodes, die sich in verschiedenen HA-Paaren vom HA-Paar befinden, das derzeit ein Performance-Problem aufweist.
2. Identifizierung eines Node im neuen HA-Paar mit der größten freien Performance-Kapazität:
   a. Klicken Sie auf der Seite **Performance/Nodes** auf die Spalte **Performance Capacity used**, um die Knoten nach dem geringsten Prozentsatz zu sortieren.

      Diese enthält eine Liste potenzieller Nodes, zu die Sie Workloads verschieben können.

   b. Notieren Sie sich den Namen des Node auf einem anderen HA-Paar, auf das Sie die Workloads verschieben möchten.
3. Ermitteln Sie auf dem neuen Node ein Aggregat mit der höchsten freien Performance-Kapazität:
   a. Klicken Sie auf der Seite **Leistung/Knoten** auf den Knoten.

      Auf der Seite Performance/Node Explorer werden die Node-Details angezeigt.

   b. Wählen Sie im Menü **Ansicht und Vergleich Aggregate auf diesem Knoten** aus.

      Die Aggregate auf diesem Node werden im Raster angezeigt.

   c. Klicken Sie auf die Spalte **Performance Capacity Used**, um die Aggregate nach den am wenigsten verwendeten Aggregaten zu sortieren.

      Diese Liste enthält potenzielle Aggregate, zu denen Workloads verschoben werden können.

   d. Notieren Sie sich den Namen des Aggregats, zu dem Sie die Workloads verschieben möchten.
4. Identifizieren Sie die hochperformanten Workloads der Nodes, die das Ereignis erhalten haben:
   a. Kehren Sie zur Seite **Event**-Details für die Veranstaltung zurück.
   b. Klicken Sie im Feld **Betroffene Volumes** auf den Link für die Anzahl der Volumes des ersten Knotens.

      Die Seite Performance/Volumes wird mit einer gefilterten Liste der Volumes auf diesem Node angezeigt.

c. Klicken Sie auf die Spalte **Gesamtkapazität**, um die Volumes nach dem größten zugewiesenen Speicherplatz zu sortieren.

   Hier erhalten Sie eine Liste potenzieller Volumes, die Sie verschieben möchten.

d. Notieren Sie sich die Namen der Volumes, die Sie verschieben möchten, sowie die Namen der aktuellen Aggregate, auf denen sich diese befinden.

e. Führen Sie für den zweiten Knoten, der zu diesem Ereignis gehörte, Schritte 4c und 4d aus, um mögliche Volumes zu identifizieren, die auch von diesem Knoten verschoben werden sollen.

5. Verschieben Sie die Volumes zu den Aggregaten, die Sie als größte freie Performance-Kapazität auf dem neuen Node identifiziert haben.

   Sie können die Schritte für die Verschiebung mit OnCommand System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools ausführen.

Nachdem Sie fertig sind

Nach einigen Tagen können Sie überprüfen, ob Sie von diesem Node bzw. Aggregat dieselbe Art von Ereignissen erhalten.

Workloads werden in einem anderen HA-Paar auf einen anderen Node verschoben

Mithilfe von Unified Manager können Sie ein Aggregat auf einem Node in einem anderen HA-Paar identifizieren, das weniger beschäftigt ist als das HA-Paar, in dem Ihre Workloads derzeit ausgeführt werden. Anschließend können Sie ausgewählte Volumes auf dem neuen HA-Paar in Aggregate verschieben. Durch die Migration hochperformanter Workloads auf ein Aggregat auf einem weniger ausgelasteten Node können Workloads auf beiden Nodes effizienter ausgeführt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Der Cluster muss aus mindestens zwei HA-Paaren bestehen. Diese Problembehebung ist nicht möglich, wenn im Cluster nur ein HA-Paar vorhanden ist.
- Sie müssen die Namen der beiden Nodes im HA-Paar, in dem derzeit das Performance-Problem aufgetreten ist, notiert haben.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu der die Nodes das Performance-Ereignis erhalten haben.
- Sie müssen die Ereignis-ID z. B. „`p-sdt-clus1-nod-6982`“ aufgezeichnet haben.
- Unified Manager muss einen Monat oder mehrere Performance-Daten erfasst und analysiert haben.

Über diese Aufgabe

Anhand dieser Schritte werden die folgenden Ressourcen ermittelt, damit Sie hochperformante Workloads auf einen weniger ausgelasteten Node in einem anderen HA-Paar verschieben können:

- Die Nodes in einem anderen HA-Paar auf demselben Cluster, das weniger genutzt wird
- Die Aggregate auf den neuen Nodes, die am wenigsten genutzt werden

- Auf den aktuellen Nodes höchste Performance

Schritte

1. Identifizieren Sie die Nodes, die zu einem anderen HA-Paar auf demselben Cluster gehören:
   a. Klicken Sie im linken Navigationsbereich auf **Leistung** > **Cluster**.

      Die Seite Performance/Cluster wird angezeigt.

   b. Klicken Sie im Feld **Knotenanzahl** für den aktuellen Cluster auf die Zahl.

      Die Seite Leistung/Knoten wird angezeigt.

   c. Notieren Sie sich die Namen der Nodes, die sich in verschiedenen HA-Paaren vom HA-Paar befinden, das derzeit ein Performance-Problem aufweist.
2. Identifizieren Sie einen Node im neuen HA-Paar, der am wenigsten genutzt wird:
   a. Klicken Sie auf die Spalte **Auslastung**, um die Knoten nach der geringsten Auslastung zu sortieren.

      Sie können auch die Knoten identifizieren, die die größte **freie Kapazität** haben. Diese enthält eine Liste potenzieller Nodes, zu die Sie Workloads verschieben können.

   b. Notieren Sie sich den Namen des Node, auf den Sie die Workloads verschieben möchten.
3. Identifizieren Sie ein Aggregat auf dem neuen Node, der am wenigsten genutzt wird:
   a. Klicken Sie im linken Navigationsbereich auf **Leistung** > **Aggregate**.

      Die Seite Performance/Aggregate wird angezeigt.

   b. Klicken Sie im linken Dropdown-Menü auf **Filterung**, wählen Sie **Knoten** aus, geben Sie den Namen des Knotens in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.

      Die Seite Performance/Aggregate wird mit der Liste der auf diesem Node verfügbaren Aggregate neu angezeigt.

   c. Klicken Sie auf die Spalte **Nutzung**, um die Aggregate nach den am wenigsten verwendeten Aggregaten zu sortieren.

      Sie können auch jene Aggregate identifizieren, die die größte **freie Kapazität** haben. Diese Liste enthält potenzielle Aggregate, zu denen Workloads verschoben werden können.

   d. Notieren Sie sich den Namen des Aggregats, zu dem Sie die Workloads verschieben möchten.
4. Identifizieren Sie die hochperformanten Workloads der Nodes, die das Ereignis erhalten haben:
   a. Kehren Sie zur Seite **Event**-Details für die Veranstaltung zurück.
   b. Klicken Sie im Feld **Betroffene Volumes** auf den Link für die Anzahl der Volumes des ersten Knotens.

      Die Seite Performance/Volumes wird mit einer gefilterten Liste der Volumes auf diesem Node angezeigt.

   c. Klicken Sie auf die Spalte **Gesamtkapazität**, um die Volumes nach dem größten zugewiesenen Speicherplatz zu sortieren.

      Hier erhalten Sie eine Liste potenzieller Volumes, die Sie verschieben möchten.

d. Notieren Sie sich die Namen der Volumes, die Sie verschieben möchten, sowie die Namen der aktuellen Aggregate, auf denen sich diese befinden.

e. Führen Sie für den zweiten Knoten, der zu diesem Ereignis gehörte, Schritte 4c und 4d aus, um mögliche Volumes zu identifizieren, die auch von diesem Knoten verschoben werden sollen.

5. Verschieben Sie die Volumes zu den Aggregaten, die Sie als niedrige Auslastung auf dem neuen Node angegeben haben.

   Sie können die Schritte für die Verschiebung mit OnCommand System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools ausführen.

Nachdem Sie fertig sind

Prüfen Sie nach einigen Tagen, ob Sie dieselbe Art von Ereignissen von diesem Node oder Aggregat erhalten.

Setzen Sie QoS-Richtlinieneinstellungen ein, um die Arbeit an diesem Node zu priorisieren

Sie können eine Obergrenze für eine QoS-Richtliniengruppe festlegen, um das Durchsatzlimit für I/O pro Sekunde (IOPS) oder MB/s für die in ihr enthaltenen Workloads zu steuern. Wenn sich Workloads in einer Richtliniengruppe ohne festgelegte Grenzwerte befinden, wie z. B. in der Standardrichtliniengruppe oder das festgelegte Limit Ihren Anforderungen nicht entspricht, können Sie das festgelegte Limit erhöhen oder die Workloads in eine neue oder vorhandene Richtliniengruppe mit dem gewünschten Limit verschieben.

Wenn ein Performance-Ereignis auf einem Node durch eine Überlastung der Node-Ressourcen verursacht wird, zeigt die Ereignisbeschreibung auf der Seite Ereignisdetails einen Link zur Liste der betroffenen Volumes an. Auf der Seite „Performance/Volumes“ können die betroffenen Volumes nach IOPS und MB/s sortiert werden, um zu sehen, welche Workloads die höchste Auslastung aufweisen, die möglicherweise an dem Ereignis beigetragen hat.

Durch die Zuweisung von Volumes, die die Node-Ressourcen überbeanspruchen, zu einer restriktiveren Richtliniengruppeneinstellung drosselt die Richtliniengruppe die Workloads, um ihre Aktivität zu beschränken. Dadurch wird die Nutzung der Ressourcen auf diesem Node verringert.

Sie können OnCommand System Manager oder die ONTAP Befehle zum Verwalten von Richtliniengruppen verwenden, einschließlich der folgenden Aufgaben:

- Erstellen einer Richtliniengruppe
- Hinzufügen oder Entfernen von Workloads in einer Richtliniengruppe
- Verschieben eines Workloads zwischen Richtliniengruppen
- Ändern der Durchsatzbegrenzung einer Richtliniengruppe

Entfernen Sie inaktive Volumes und LUNs

Wenn der freie Speicherplatz des Aggregats als Problem identifiziert wurde, können Sie nach nicht verwendeten Volumes und LUNs suchen und diese aus dem Aggregat löschen. Dies kann dazu beitragen, dass weniger Speicherplatz erforderlich ist.

Wenn ein Performance-Ereignis auf einem Aggregat durch geringen Festplattenspeicher verursacht wird, gibt es einige Möglichkeiten, Sie festzustellen, welche Volumes und LUNs nicht mehr verwendet werden.

So identifizieren Sie ungenutzte Volumes:

- Auf der Seite Ereignisdetails wird im Feld * Betroffene Objekte Anzahl* ein Link angezeigt, der die Liste der betroffenen Volumes anzeigt.

  Klicken Sie auf den Link, um die Volumes auf der Seite Performance/Volumes anzuzeigen. Dort können Sie die betroffenen Volumes nach **IOPS** sortieren, um zu sehen, welche Volumen nicht aktiv waren.

So identifizieren Sie ungenutzte LUNs:

1. Notieren Sie auf der Seite Ereignisdetails den Namen des Aggregats, auf dem das Ereignis aufgetreten ist.
2. Klicken Sie im linken Navigationsbereich auf **Leistung** > **LUNs**.
3. Klicken Sie im linken Dropdown-Menü auf **Filter**, wählen Sie **Aggregat** aus, geben Sie den Namen des Aggregats in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.
4. Sortieren Sie die resultierende Liste der betroffenen LUNs nach **IOPS**, um die LUNs anzuzeigen, die nicht aktiv sind.

Nachdem Sie die nicht verwendeten Volumes und LUNs ermittelt haben, können Sie diese Objekte mit dem OnCommand System Manager oder mit den ONTAP-Befehlen löschen.

Fügen Sie Festplatten hinzu und führen Sie die Rekonstruktion des Aggregat-Layouts durch

Sie können einem Aggregat Festplatten hinzufügen, um die Storage-Kapazität und Performance dieses Aggregats zu erhöhen. Nach dem Hinzufügen der Platten sehen Sie nur eine Verbesserung der Performance nach dem Rekonstruieren des Aggregats.

Wenn Sie auf der Seite Ereignisdetails ein systemdefiniertes Schwellenwertereignis erhalten, enthält der Text für die Ereignisbeschreibung den Namen des Aggregats, dessen Problem aufgetreten ist. Sie können in diesem Aggregat Festplatten hinzufügen und Daten rekonstruieren.

Die Festplatten, die Sie dem Aggregat hinzufügen, müssen bereits im Cluster vorhanden sein. Wenn auf dem Cluster keine zusätzlichen Festplatten verfügbar sind, müssen Sie sich möglicherweise an den Administrator wenden oder weitere Festplatten erwerben. Mit OnCommand System Manager oder den ONTAP-Befehlen können Sie einem Aggregat Festplatten hinzufügen.

"Technischer Bericht 3838: Konfigurationsleitfaden Für Storage-Subsysteme"

Management von Kontingenten

Mit Benutzer- und Gruppenquoten lässt sich die Menge an Festplattenspeicher oder die Anzahl der Dateien begrenzen, die ein Benutzer oder eine Benutzergruppe verwenden kann. Sie können Quota-Informationen für Benutzer und Benutzergruppen anzeigen, z. B. die Festplatten- und Dateiverwendung und die verschiedenen auf Festplatten festgelegten Grenzwerte.

Welche Kontingentbeschränkungen sind

Einschränkungen der Benutzerkontingente sind Werte, die der Unified Manager-Server verwendet, um zu bewerten, ob sich der Speicherplatzbedarf eines Benutzers dem Limit nähert oder das vom Kontingent des Benutzers festgelegte Limit erreicht hat. Wenn das Softlimit überschritten wird oder das harte Limit erreicht wird, generiert der Unified Manager-Server Benutzer-Quota-Ereignisse.

Standardmäßig sendet der Unified Manager-Server eine Benachrichtigungs-E-Mail an Benutzer, die das Softlimit für Quotengrenzen überschritten oder das endgültige Kontingent erreicht haben und für die Benutzer-Quota-Ereignisse konfiguriert werden. Der OnCommand-Administrator kann Warnungen konfigurieren, die die angegebenen Empfänger der Benutzer- oder Benutzergruppen-Quota-Ereignisse benachrichtigen.

Sie können die Kontingentgrenze entweder mit OnCommand System Manager oder mit der ONTAP CLI festlegen.

Anzeigen von Benutzer- und Benutzergruppenkontingenten

Auf der Seite Health/Storage Virtual Machines Inventory werden Informationen über die auf der SVM konfigurierten Benutzer- und Benutzergruppenkontingente angezeigt. Sie können den Namen des Benutzers oder der Benutzergruppe, die auf Festplatten und Dateien festgelegten Grenzen, den verwendeten Festplatten- und Dateispeicherplatz und die E-Mail-Adresse für Benachrichtigungen anzeigen.

Bevor Sie beginnen

Sie müssen eine der folgenden Rollen haben, um diese Aufgabe auszuführen: Operator, OnCommand Administrator oder Storage Administrator.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory eine SVM aus und klicken Sie dann auf die Registerkarte **Benutzer- und Gruppenkontingente**.

Erstellen von Regeln zum Generieren von E-Mail-Adressen

Sie können Regeln erstellen, um die E-Mail-Adresse auf der Grundlage des mit Clustern, Storage Virtual Machines (SVMs), Volumes, qtrees, Benutzern oder Benutzergruppen verbundenen Benutzerkontingente anzugeben. Bei einer Quota-Verletzung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Richtlinien auf der Seite Regeln zur Erstellung von Benutzer- und Gruppenkontingente-E-Mail-Adresse geprüft haben.

Über diese Aufgabe

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

- Bei (€ QTREE ==’qtre1’) dann qtree1@xyz.com
- Bei (€ QTREE == *) dann admin@xyz.com

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

WENN (US-DOLLAR USER_OR_GROUP == *) DANN USD USER_OR_GROUP@ USD DOMAIN

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Setup-Menü auf **Quota Email**.
2. Klicken Sie auf der Seite **Setup** Optionen auf **Adressregeln** und geben Sie dann die Regel basierend auf Ihren Kriterien ein.
3. Klicken Sie auf **Validieren**, um die Syntax der Regel zu validieren.

   Wenn die Syntax der Regel nicht korrekt ist, wird eine Fehlermeldung angezeigt. Sie müssen die Syntax korrigieren und erneut auf **Validieren** klicken.
4. Klicken Sie auf **Speichern und Schließen**.
5. Überprüfen Sie, ob die von Ihnen erstellte E-Mail-Adresse auf der Seite * Health/Storage Virtual Machine* Details auf der Registerkarte **Benutzer- und Gruppenquoten** angezeigt wird.

Erstellen eines E-Mail-Benachrichtigungsformats für Benutzer- und Benutzergruppenkontingente

Sie können ein Benachrichtigungsformat für E-Mails erstellen, die an einen Benutzer oder eine Benutzergruppe gesendet werden, wenn ein mit Quota zusammenhängendes Problem vorliegt (weiche Obergrenze oder harte Grenze erreicht).

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Setup-Menü auf **Quota Email**.
2. Klicken Sie auf der Seite **Setup** Optionen auf **Benachrichtigungsformat** und geben Sie dann die Details in die Felder **von**, **Betreff** und **E-Mail-Details** ein.
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 ggf. den Inhalt der E-Mail-Benachrichtigung.
6. Klicken Sie auf **Speichern und Schließen**.

Bearbeiten der E-Mail-Adressen für Benutzer- und Gruppenkontingente

Sie können die E-Mail-Adressen basierend auf den mit Clustern verbundenen Benutzerkontingenten, Storage Virtual Machines (SVMs), Volumes, qtrees, Benutzern oder Benutzergruppen ändern. Sie können die E-Mail-Adresse ändern, wenn Sie die E-Mail-Adresse überschreiben möchten, die durch Regeln generiert wurde, die im Dialogfeld „Regeln zum Generieren von Benutzer- und Gruppenkontingente-E-Mail-Adresse“ angegeben sind.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den geprüft haben Richtlinien zur Erstellung von Regeln.

Über diese Aufgabe

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory eine SVM aus und klicken Sie dann auf die Registerkarte **Benutzer- und Gruppenkontingente**.
3. Klicken Sie unter der Zeile der Registerkarten 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 von den 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 durch die angegebene Regel generierte E-Mail-Adresse wird im Feld * E-Mail-Adresse* angezeigt.
Sie möchten Benachrichtigungen an eine bestimmte E-Mail-Adresse senden	a. Ändern Sie die E-Mail-Adresse im Feld * E-Mail-Adresse*. b. Klicken Sie Auf **Speichern**. Die Regeln zur Generierung der Benutzer- und Gruppenkontingente-E-Mail-Adressen gelten nicht mehr für die Quote.

Allgemeines zu Kontingenten

Wenn Sie die Konzepte zu Kontingenten verstehen, können Sie Ihre Benutzerquoten und Benutzergruppenkontingente effizient managen.

Überblick über den Quotenprozess

Kontingente können „weich“ oder „hart“ sein. Wenn festgelegte Grenzwerte überschritten werden, sorgt eine Soft Quota dafür, dass ONTAP eine Benachrichtigung sendet, wohingegen eine Hard Quota in diesem Fall einen Schreibvorgang fehlschlagen lässt.

Wenn ONTAP von einem Benutzer oder einer Benutzergruppe eine Schreibanforderung für ein FlexVol Volume erhält, wird überprüft, ob für dieses Volume für diesen Benutzer oder diese Benutzergruppe Quoten aktiviert wurden, und Folgendes bestimmt:

- Ob die harte Grenze erreicht wird

  Wenn ja, schlägt der Schreibvorgang fehl, wenn das harte Limit erreicht ist und die Benachrichtigung über harte Quota gesendet wird.

- Gibt an, ob das weiche Limit verletzt wird

  Wenn ja, ist der Schreibvorgang erfolgreich, wenn die weiche Grenze überschritten wird und die Soft Quota Benachrichtigung gesendet wird.

- Gibt an, ob ein Schreibvorgang den Softlimit nicht überschreitet

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

Über Kontingente

Quoten bieten eine Möglichkeit, den Festplattenspeicherplatz und die Anzahl der Dateien zu beschränken, die von einem Benutzer, einer Gruppe oder einem qtree verwendet werden. Sie geben Quoten mit an `/etc/quotas` Datei: Sie werden auf ein bestimmtes Volume oder einen bestimmten qtree angewendet.

Warum man Quoten verwendet

Mithilfe von Quotas lässt sich die Ressourcennutzung in FlexVol Volumes begrenzen, Benachrichtigungen bereitstellen, wenn die Ressourcenauslastung bestimmte Level erreicht oder die Ressourcenauslastung nachverfolgt.

Sie geben aus folgenden Gründen ein Kontingent an:

- Um die Menge an Festplattenspeicher oder die Anzahl der Dateien zu begrenzen, die von einem Benutzer oder einer Gruppe verwendet werden können oder die von einem qtree enthalten sein können
- Um den von einem Benutzer, einer Gruppe oder einem qtree verwendeten Dateispeicherplatz oder die Anzahl der Dateien zu verfolgen, ohne dass ein Limit gesetzt wird
- Um Anwender bei einer hohen Festplatten- oder Dateiennutzung zu warnen

Beschreibung der Dialogfelder Quotas

Sie können die entsprechende Option auf der Registerkarte Benutzer- und Gruppenkontingente auf der Seite Health/Storage Virtual Machines Inventory verwenden, um das Format der E-Mail-Benachrichtigung zu konfigurieren, die bei Auftreten eines quotenbezogenen Problems gesendet wird, und um Regeln zur Angabe von E-Mail-Adressen basierend auf dem Benutzerkontingent zu konfigurieren.

Seite „Format für E-Mail-Benachrichtigungen“

Auf der Seite „E-Mail-Benachrichtigungsformat“ werden die Regeln der E-Mail angezeigt, die an einen Benutzer oder eine Benutzergruppe gesendet werden, wenn ein quota-bezogenes Problem vorliegt (Soft Limit missachtet oder Hard Limit erreicht).

Die E-Mail-Benachrichtigung wird nur gesendet, wenn die folgenden Kontingentereignisse für Benutzer oder Benutzergruppen generiert werden: Benutzerkontingente oder Gruppenkontingente Festplattenplatzweiche Grenze überschritten, Benutzer- oder Gruppenkontingente Dateianzahl weiche Grenze überschritten, Benutzer- oder Gruppenkontingente Festplattenspeicherplatz-Limit erreicht oder Benutzer- oder Gruppenkontingente Dateianzahl erreicht.

- * Von*

  Zeigt die E-Mail-Adresse an, von der die E-Mail gesendet wird, die Sie bearbeiten können. Standardmäßig handelt es sich hierbei um die E-Mail-Adresse, die die Seite „Setup/Benachrichtigungen“ angegeben ist.

- **Betreff**

  Zeigt den Betreff der Benachrichtigungs-E-Mail an.

- **E-Mail-Details**

  Zeigt den Text der Benachrichtigungs-E-Mail an. Sie können den Text entsprechend Ihren Anforderungen ändern. Sie können beispielsweise Informationen zu den Quota-Attributen bereitstellen und die Anzahl der Schlüsselworte 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.

  - US-DOLLAR QUOTA_TARGET

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

  - US-DOLLAR QUOTA_USED_PERCENT

    Gibt den Prozentsatz des Festplattenlimits, des Soft-Limits der Festplatte, des Dateihartes oder des vom Benutzer oder der Benutzergruppe verwendeten Soft-Limits an.

  - US-DOLLAR QUOTA_LIMIT

    Gibt das Festplatten-Hard-Limit oder das Limit für die Datei an, das vom Benutzer oder der Benutzergruppe erreicht wird und eines der folgenden Ereignisse generiert wird:

        - Hard Limit für Speicherplatz für Benutzer- oder Gruppenkontingente erreicht
        - Speicherplatz-Soft-Limit für Benutzer- oder Gruppenkontingente erreicht
        - Harte Grenze für die Anzahl der Benutzer- oder Gruppenkontingente erreicht
        - Dateianzahl Benutzer- oder Gruppenkontingente Soft-Limit erreicht
    - QUOTE_USED

      Gibt den verwendeten Festplattenspeicher oder die Anzahl der Dateien an, die vom Benutzer oder der Benutzergruppe erstellt wurden.

    - US-DOLLAR QUOTA_USER

      Gibt den Benutzer- oder Benutzergruppennamen an.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die Änderungen im Benachrichtigungsformat für E-Mail-Nachrichten anzeigen, speichern oder abbrechen:

- **Vorschau**

  Zeigt eine Vorschau der Benachrichtigungs-E-Mail an.

- **Wiederherstellen auf Werkseinstellungen**

  Ermöglicht die Wiederherstellung des Benachrichtigungsformats auf die werkseitigen Standardwerte.

- **Speichern**

  Speichert die Änderungen im Benachrichtigungsformat.

Regeln zum Erstellen der E-Mail-Adresse für Benutzer- und Gruppenkontingente

Auf der Seite „Regeln zum Generieren von E-Mail-Adressen für Benutzer- und Gruppenkontingente“ können Sie Regeln erstellen, um E-Mail-Adressen basierend auf dem Benutzerkontingent festzulegen, das mit Clustern, SVMs, Volumes, qtrees, Benutzern, Oder Benutzergruppen. Bei Überschreitung einer Quote wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

Regelbereich

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

Wie Sie Regeln definieren

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 enthält eine separate Regel. Die Standardregel ist die letzte Regel in der Liste. Sie können die Prioritätenreihenfolge von Regeln ändern. Sie können jedoch die Reihenfolge der Standardregel nicht ändern.

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

- Bei (€ QTREE ==‘qtre1‘) dann qtree1@xyz.com
- Bei (€ QTREE == *) dann admin@xyz.com

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

WENN (US-DOLLAR USER_OR_GROUP == *) DANN USD USER_OR_GROUP@ USD DOMAIN

Wenn mehrere Benutzer dieselbe Quote haben, werden die Namen der Benutzer als kommagetrennte Werte angezeigt und die Regeln gelten nicht für die Quote.

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 auflistet.

Regelsyntax

Die Syntax der Regel muss eine der folgenden sein:

- Wenn (*gültige Variable**Operator* *) dann *email ID@Domain Name*

  `if` Ist ein Schlüsselwort und ist in Kleinbuchstaben. Der Operator lautet ==. Die E-Mail-ID kann jedes beliebige Zeichen, die gültigen Variablen €USER_OR_GROUP, US-Dollar USER oder USD GROUP oder eine Kombination von Zeichen und den gültigen Variablen €USER_OR_GROUP, USD USER oder USD GROUP enthalten. Der Domainname kann jedes beliebige Zeichen, die gültige Variable USD DOMAIN oder eine Kombination eines beliebigen Zeichens und der gültigen Variable USD DOMAIN enthalten. Gültige Variablen können groß oder klein sein, dürfen aber keine Kombination aus beiden sein. Beispielsweise sind DomänenanDollar und US-Dollar-DOMAINS gültig, eine gültige Variable in US-Dollar jedoch nicht.

- Wenn (*gültige Variable**Operator* '*string* ') dann *email ID@Domain Name*

  `if` Ist ein Schlüsselwort und ist klein geschrieben. Der Bediener kann sein `contains` Oder ==. Die E-Mail-ID kann jedes beliebige Zeichen, die gültigen Variablen €USER_OR_GROUP, US-Dollar USER oder USD GROUP oder eine Kombination von Zeichen und den gültigen Variablen €USER_OR_GROUP, USD USER oder USD GROUP enthalten. Der Domainname kann jedes beliebige Zeichen, die gültige Variable USD DOMAIN oder eine Kombination eines beliebigen Zeichens und der gültigen Variable USD DOMAIN enthalten. Gültige Variablen können groß oder klein sein, dürfen aber keine Kombination aus beiden sein. Beispielsweise sind DomänenanDollar und US-Dollar-DOMAINS gültig, eine gültige Variable in US-Dollar jedoch nicht.

Befehlsschaltflächen

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

- **Validieren**

  Überprüft die Syntax der erstellten Regel. Wenn während der Validierung Fehler auftreten, wird die Regel, die den Fehler generiert, zusammen mit einer Fehlermeldung angezeigt.

- **Wiederherstellen auf Werkseinstellungen**

  Ermöglicht Ihnen, die Adressregeln auf die werkseitigen Standardwerte wiederherzustellen.

- **Speichern**

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

Verwalten und Überwachen der Cluster- und Cluster-Objektintegrität

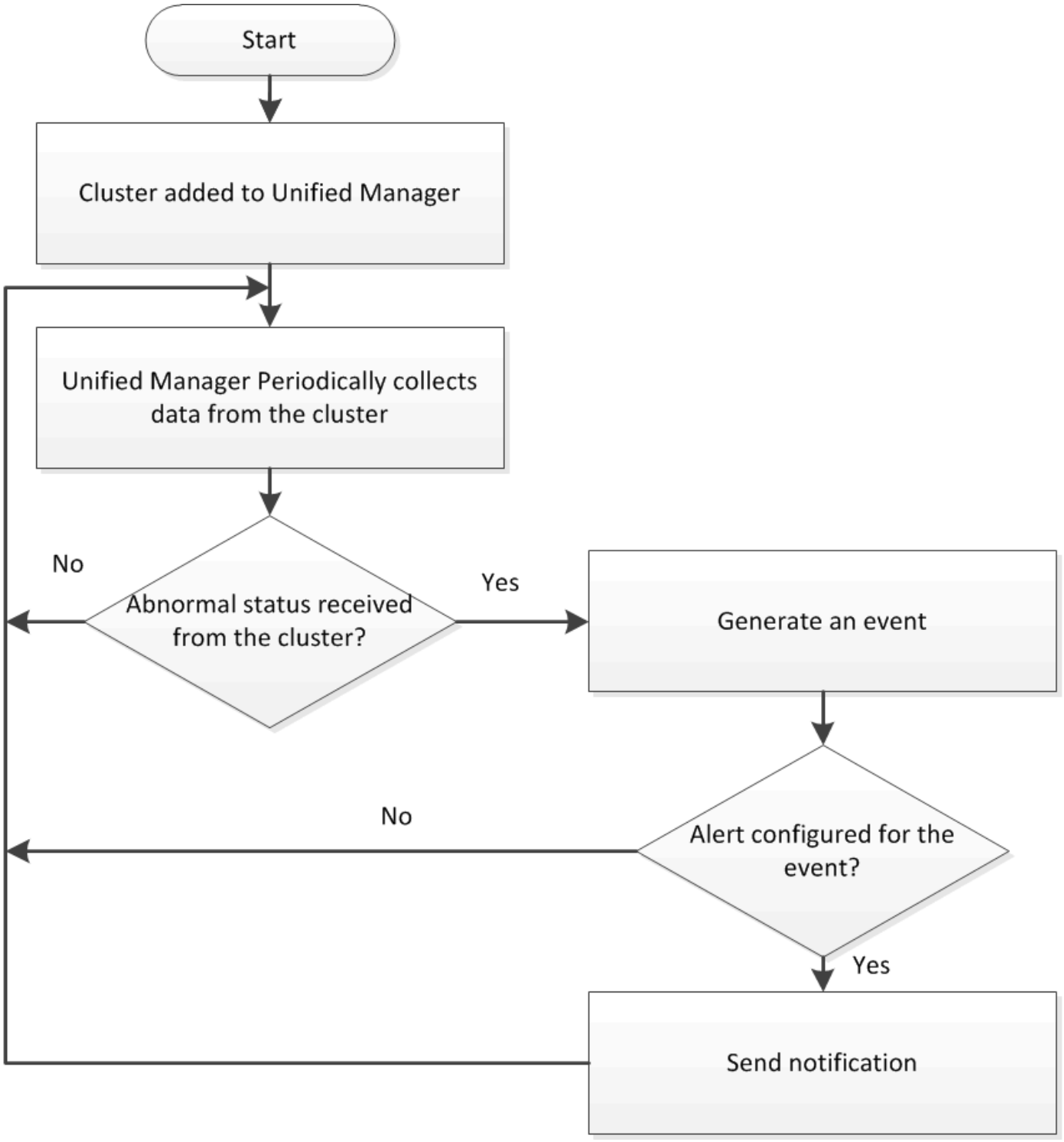
Unified Manager verwendet regelmäßige API-Abfragen und eine Datenerfassungs-Engine, um Daten aus den Clustern zu erfassen. Durch das Hinzufügen von Clustern zur Unified Manager-Datenbank können diese Cluster hinsichtlich Verfügbarkeit und Kapazität überwacht und gemanagt werden.

Allgemeines zum Cluster-Monitoring

Sie können der Unified Manager Datenbank Cluster hinzufügen, um Cluster zu überwachen, um Verfügbarkeit, Kapazität und andere Details wie CPU-Nutzung, Schnittstellenstatistiken, freien Festplattenspeicher, qtree-Nutzung und Chassis-Umgebung zu überwachen.

Ereignisse werden generiert, wenn der Status anormal ist oder wenn ein vordefinierter Schwellenwert überschritten wird. Bei entsprechender Konfiguration sendet Unified Manager eine Benachrichtigung an einen bestimmten Empfänger, wenn ein Ereignis eine Warnmeldung auslöst.

Das folgende Flussdiagramm zeigt den Monitoring-Prozess von Unified Manager:



Allgemeines zu Root-Volumes von Nodes

Sie können das Root-Volume des Nodes mithilfe von Unified Manager überwachen. Als Best Practice wird empfohlen, dass das Node-Root-Volume über ausreichende Kapazitäten verfügen sollte, um zu verhindern, dass der Node ausfällt.

Wenn die verwendete Kapazität des Node-Root-Volumes 80 Prozent der Gesamt-Root-Volume-Kapazität des Nodes überschreitet, wird das Ereignis Node Root Volume Space fast Full generiert. Sie können eine Meldung für das Ereignis konfigurieren, um eine Benachrichtigung zu erhalten. Sie können geeignete Maßnahmen ergreifen, um zu verhindern, dass der Node unter Verwendung von OnCommand System Manager oder der

ONTAP CLI ausfällt.

Allgemeines zu Ereignissen und Schwellenwerten für Root-Aggregate von Nodes

Sie können das Root-Aggregat des Nodes mithilfe von Unified Manager überwachen. Als Best Practice empfiehlt es sich, das Root-Volumen im Root-Aggregat stark bereitzustellen, um zu verhindern, dass der Knoten angehalten wird.

Standardmäßig werden Kapazitäts- und Performance-Ereignisse nicht für die Root-Aggregate generiert. Darüber hinaus gelten die von Unified Manager verwendeten Schwellenwertwerte nicht für die Root-Aggregate der Nodes. Nur ein Mitarbeiter des technischen Supports kann die Einstellungen für diese zu erstellenden Ereignisse ändern. Wenn die Einstellungen vom technischen Supportmitarbeiter geändert werden, werden die Kapazitätsschwellenwerte auf das Root-Aggregat des Nodes angewendet.

Sie können geeignete Maßnahmen ergreifen, um zu verhindern, dass der Node mit OnCommand System Manager oder der ONTAP CLI angehalten wird.

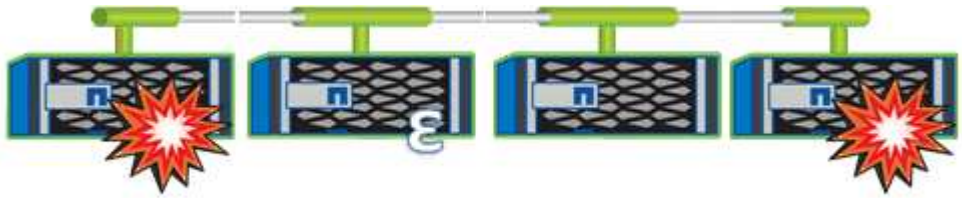
Verständnis von Quorum und Epsilon

Quorum und Epsilon sind wichtige Kennzahlen für den Clusterzustand und die Funktion, die gemeinsam zeigen, wie Cluster potenzielle Herausforderungen bei Kommunikation und Konnektivität bewältigen.

Quorum ist eine Voraussetzung für ein voll funktionsfähiges Cluster. Wenn ein Cluster Quorum aufweist, sind die meisten Knoten in einem ordnungsgemäßen Zustand und können miteinander kommunizieren. Wenn das Quorum verloren geht, verliert das Cluster die Möglichkeit, normale Cluster-Vorgänge zu erledigen. Es kann jederzeit nur eine Sammlung von Knoten Quorum enthalten, da alle Knoten gemeinsam eine Ansicht der Daten teilen. Wenn zwei nicht kommunizierende Knoten die Daten auf unterschiedliche Weise ändern dürfen, ist es daher nicht mehr möglich, die Daten in einer einzigen Datenansicht zu vergleichen.

Jeder Knoten im Cluster nimmt an einem Abstimmprotokoll Teil, das einen Knoten *Master* wählt; jeder verbleibende Knoten ist ein *secondary*. Der Master-Node ist für die Synchronisierung von Informationen im gesamten Cluster verantwortlich. Wenn Quorum gebildet wird, wird es durch ständige Abstimmung beibehalten. Wenn der Hauptknoten offline geht und sich das Cluster noch im Quorum befindet, wird ein neuer Master von den Knoten ausgewählt, die online bleiben.

Da es die Möglichkeit einer Krawatte in einem Cluster mit einer geraden Anzahl von Knoten gibt, hat ein Knoten eine zusätzliche fraktionale Abstimmungsgewichtung namens *epsilon*. Wenn die Konnektivität zwischen zwei gleichen Teilen eines großen Clusters ausfällt, bleibt die Gruppe der Nodes mit epsilon ein Quorum, vorausgesetzt, dass alle Nodes ordnungsgemäß sind. Die folgende Abbildung zeigt beispielsweise ein Cluster mit vier Nodes, in dem zwei der Nodes ausgefallen sind. Da einer der verbliebenen Nodes jedoch Epsilon enthält, bleibt das Cluster im Quorum, auch wenn es nicht die einfache Mehrheit der gesunden Knoten gibt.



Epsilon wird beim Erstellen des Clusters automatisch dem ersten Knoten zugewiesen. Wenn der Node, auf dem Epsilon steht, ungesund wird, seinen Hochverfügbarkeits-Partner übernimmt oder vom

Hochverfügbarkeitspartner übernommen wird, wird Epsilon automatisch einem gesunden Node in einem anderen HA-Paar neu zugewiesen.

Wenn ein Node offline geschaltet wird, kann sich dies darauf auswirken, dass das Cluster im Quorum bleibt. Daher gibt ONTAP eine Warnmeldung aus, wenn Sie versuchen, einen Vorgang durchzuführen, der entweder das Cluster aus dem Quorum entfernt, oder wenn es ein Ausfall von dem Verlust des Quorums entfernt wird. Sie können die Quorum-Warnmeldungen mit deaktivieren `cluster quorum-service options modify` Befehl auf der erweiterten Berechtigungsebene

Angenommen, die zuverlässige Konnektivität zwischen den Knoten des Clusters ist, ist ein größerer Cluster im Allgemeinen stabiler als ein kleinerer Cluster. Das Quorum, das die einfache Mehrheit der halben Nodes plus Epsilon erfordert, ist auf einem Cluster mit 24 Nodes einfacher zu warten als bei einem Cluster mit zwei Nodes.

Ein Cluster mit zwei Nodes stellt die Beibehaltung von Quorum vor besondere Herausforderungen. Cluster mit zwei Nodes verwenden *Cluster HA*, bei dem keines der Nodes Epsilon enthält. Stattdessen werden beide Nodes fortlaufend abgefragt, um sicherzustellen, dass bei einem Node ein voller Lese-/Schreibzugriff auf die Daten sowie Zugriff auf logische Schnittstellen und Managementfunktionen sichergestellt ist.

Anzeigen der Cluster-Liste und der Details

Sie können die Seite „Health/Clusters Inventory“ verwenden, um Ihr Clusterinventar anzuzeigen. Auf der Seite „Systemzustand/Cluster Storage Summary“ können in allen Clustern zusammengefasste Informationen zur Storage-Kapazität und -Auslastung angezeigt werden.

Bevor Sie beginnen

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

Über diese Aufgabe

Sie können auch Details für einzelne Cluster anzeigen, beispielsweise für den Zustand des Clusters, die Kapazität, die Konfiguration, LIFs, Nodes, Und Festplatten in diesem Cluster verwenden Sie die Seite „Systemzustand/Cluster-Details“.

Die Details auf der Seite „Health/Clusters Inventory“, „Health/Clusters Storage Summary“ und die Seite „Health/Cluster Details“ unterstützen Sie bei der Planung Ihres Speichers. Vor dem Bereitstellen eines neuen Aggregats können Sie beispielsweise auf der Seite „Systemzustand/Cluster-Inventar“ ein bestimmtes Cluster auswählen und Kapazitätsdetails erhalten, um zu ermitteln, ob der Cluster über den erforderlichen Speicherplatz verfügt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Gesundheit** > **Cluster**.
2. Wählen Sie im Menü **Ansicht** die Option **Speicherzusammenfassung** aus, um Details zur Speicherkapazität und Auslastung in allen Clustern anzuzeigen
3. Zeigen Sie die vollständigen Details des Clusters auf der Seite **Systemzustand/Cluster** Details an, indem Sie auf den Cluster-Namen klicken.

Überprüfen des Systemzustands von Clustern in einer MetroCluster-Konfiguration

Mit Unified Manager können Sie den Betriebszustand der Cluster und ihrer Komponenten

in einer MetroCluster-Konfiguration überprüfen. Wenn die Cluster an einem von Unified Manager erkannten Performance-Ereignis beteiligt waren, kann der Integritätsstatus Ihnen dabei helfen festzustellen, ob ein Hardware- oder Softwareproblem zu dem Ereignis beigetragen hat.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen ein Performance-Ereignis für eine MetroCluster-Konfiguration analysiert und den Namen des betroffenen Clusters erhalten haben.
- Beide Cluster in der MetroCluster-Konfiguration müssen von derselben Instanz von Unified Manager überwacht werden.

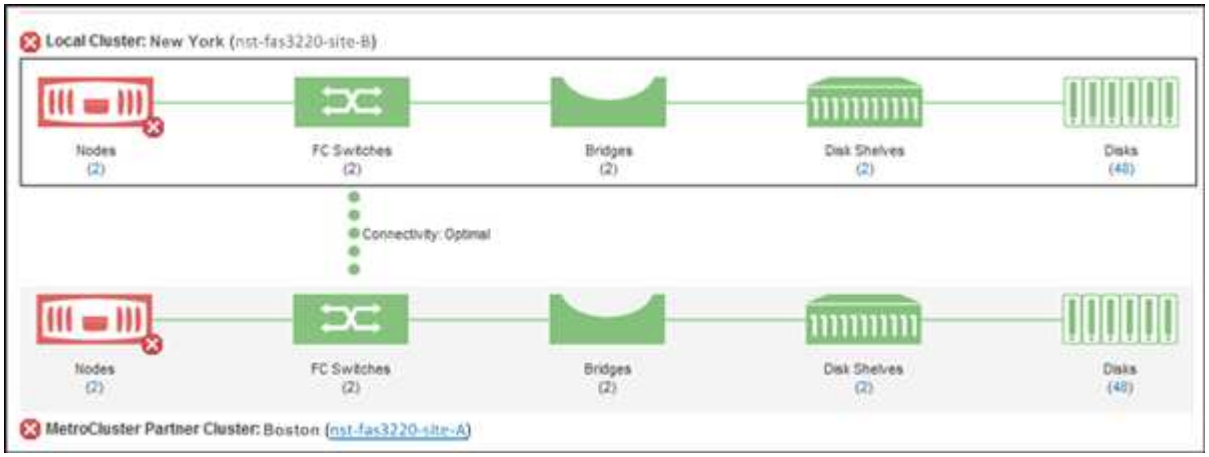
Schritte

1. Klicken Sie im linken Navigationsbereich auf **Events**, um die Ereignisliste anzuzeigen.
2. Wählen Sie im Filter-Panel alle MetroCluster-Filter unter der Kategorie **Quelltyp** aus.
3. Klicken Sie neben einem MetroCluster-Ereignis auf den Namen des Clusters.

   Die Seite „Systemzustand/Cluster-Bestand“ wird mit detaillierten Informationen zum Ereignis angezeigt.

   Wenn keine MetroCluster-Ereignisse angezeigt werden, können Sie mithilfe der Suchleiste nach dem Namen des Clusters suchen, das am Performance-Ereignis beteiligt ist.

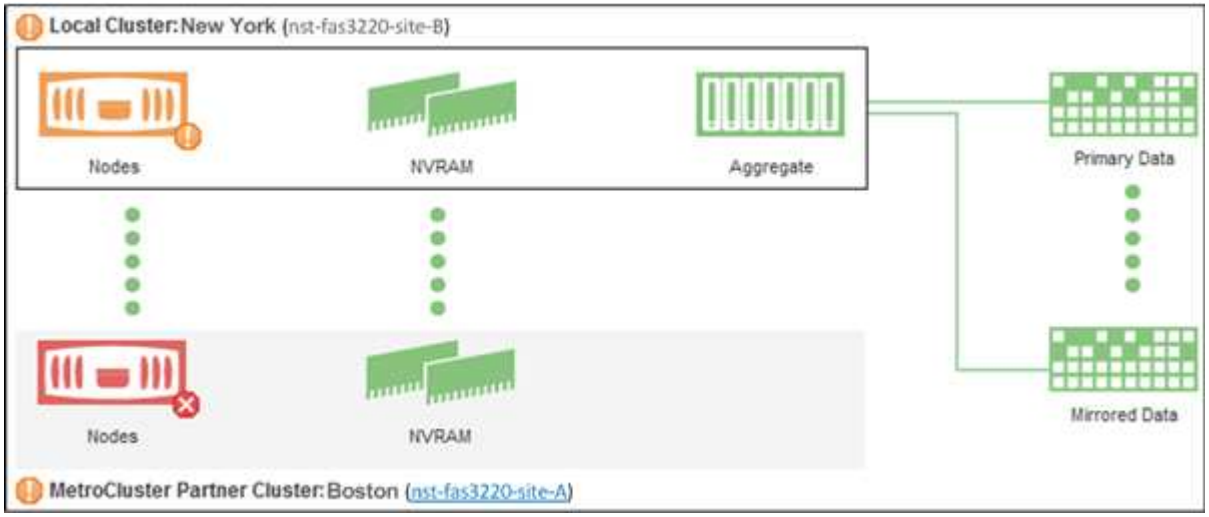
4. Wählen Sie die Registerkarte **MetroCluster Connectivity** aus, um den Zustand der Verbindung zwischen dem ausgewählten Cluster und seinem Partner-Cluster anzuzeigen.



In diesem Beispiel werden die Namen und die Komponenten des lokalen Clusters und dessen Partner-Cluster angezeigt. Ein gelbes oder rotes Symbol bedeutet, dass für die markierte Komponente ein Systemzustandsereignis angezeigt wird. Das Verbindungssymbol stellt die Verbindung zwischen den Clustern dar. Sie können mit dem Mauszeiger auf ein Symbol zeigen, um Ereignisinformationen anzuzeigen, oder auf das Symbol klicken, um die Ereignisse anzuzeigen. Möglicherweise hat ein Systemzustandsproblem auf einem der Cluster zum Performance-Ereignis beigetragen.

Unified Manager überwacht die NVRAM-Komponente der Verbindung zwischen den Clustern. Wenn das FC-Switch-Symbol im lokalen Cluster oder Partner-Cluster oder das Konnektivitätssymbol rot ist, könnte ein Systemzustandsproblem möglicherweise das Performance-Ereignis verursacht haben.

5. Wählen Sie die Registerkarte **MetroCluster-Replikation** aus.



Wenn in diesem Beispiel das NVRAM-Symbol auf dem lokalen oder Partner-Cluster gelb oder rot ist, hat möglicherweise ein Systemzustandsproblem im NVRAM das Performance-Ereignis verursacht. Wenn auf der Seite keine roten oder gelben Symbole angezeigt werden, hat möglicherweise ein Performance-Problem auf dem Partner-Cluster das Performance-Ereignis verursacht.

Anzeigen der Node-Liste und der Details

Auf der Seite „Systemzustand/Knoten-Inventar“ können Sie die Liste der Knoten in Ihren Clustern anzeigen. Auf der Seite „Systemzustand/Cluster-Details“ können Sie detaillierte Informationen zu Nodes anzeigen, die Teil des überwachten Clusters sind.

Bevor Sie beginnen

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

Über diese Aufgabe

Sie können Details wie den Node-Status, den Cluster mit dem Node, die zusammengefasste Kapazität (verwendet und insgesamt) und Details zur Rohkapazität (nutzbar, frei und insgesamt) anzeigen. Zudem erhalten Sie Informationen über HA-Paare, Festplatten-Shelfs und Ports.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Gesundheit** > **Knoten**.
2. Klicken Sie auf der Seite **Health/Nodes** Inventory auf den Knoten, dessen Details Sie anzeigen möchten.

   Die detaillierten Informationen für den ausgewählten Node werden auf der Seite „Systemzustand/Cluster-Details“ angezeigt. Im linken Teilfenster wird die Liste der HA-Paare angezeigt. Standardmäßig sind die HA-Details geöffnet, in denen Details zum HA-Status und Ereignisse im Zusammenhang mit dem ausgewählten HA-Paar angezeigt werden.

3. Um weitere Details zum Knoten anzuzeigen, führen Sie die entsprechende Aktion aus:

Anzeigen…	Klicken Sie Auf…
Informationen zu Platten-Shelves	**Platten-Shelves**.
Port-bezogene Informationen	**Ports**.

Anzeigen der SVM-Liste und der Details

Über die Seite „Systemzustand“/„Storage Virtual Machines Inventory“ können Sie Ihr Inventar an Storage Virtual Machines (SVMs) überwachen. Mithilfe der Detailseite „Systemzustand/Storage Virtual Machine“ können Sie detaillierte Informationen zu überwachten SVMs anzeigen.

Bevor Sie beginnen

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

Über diese Aufgabe

Sie können SVM-Details anzeigen, beispielsweise die Kapazität, Effizienz und Konfiguration einer SVM. Sie können auch Informationen zu zugehörigen Geräten und zugehörigen Warnmeldungen für diese SVM anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie eine der folgenden Möglichkeiten, um die SVM-Details anzuzeigen:
   - Wenn Sie minimale Details anzeigen möchten, positionieren Sie den Cursor über den SVM-Namen.
   - Um die vollständigen Details anzuzeigen, klicken Sie auf den SVM-Namen.

     Sie können die vollständigen Details auch anzeigen, indem Sie im Dialogfeld mit den minimalen Details auf **Details anzeigen** klicken.
3. Zeigen Sie die Objekte an, die mit der SVM in Verbindung stehen, indem Sie im Dialogfeld mit den minimalen Details auf **View Related** klicken.

Anzeigen der Aggregatliste und der Details

Über die Seite „Systemzustand/Aggregate Inventory“ können Sie das Inventar Ihrer Aggregate überwachen. Auf der Seite Systemzustand/Aggregate Kapazität und Auslastung können Sie Informationen über die Kapazität und Auslastung von Aggregaten in allen Clustern anzeigen.

Bevor Sie beginnen

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

Über diese Aufgabe

Sie können Details wie Aggregatskapazität und -Konfiguration sowie Festplatteninformationen über die Detailseite „Systemzustand/Aggregat“ anzeigen. Sie können diese Details verwenden, bevor Sie die Schwellenwerteinstellungen konfigurieren, falls erforderlich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **Aggregate**.
2. Wählen Sie eine der folgenden Möglichkeiten, um die Aggregatdetails anzuzeigen:
   - Um Informationen über die Kapazität und Auslastung aller Aggregate in allen Clustern anzuzeigen, wählen Sie im Menü Ansicht die Option **Aggregatskapazität und -Auslastung** aus.
   - Um minimale Details anzuzeigen, positionieren Sie den Cursor über den Aggregatnamen.
   - Um die vollständigen Details anzuzeigen, klicken Sie auf den Aggregatnamen.

     Sie können die vollständigen Details auch anzeigen, indem Sie im Dialogfeld mit den minimalen Details auf **Details anzeigen** klicken.
3. Zeigen Sie die Objekte an, die mit dem Aggregat zusammenhängen, indem Sie im Dialogfeld mit den minimalen Details auf **Related** klicken.

Anzeigen von Details zum Speicherpool

Sie können Details zum Speicherpool anzeigen, um den Zustand des Speicherpools, den gesamten und verfügbaren Cache sowie die verwendeten und verfügbaren Zuweisungen zu überwachen.

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **Aggregate**.
2. Klicken Sie auf den Aggregatnamen.

   Die Details zum ausgewählten Aggregat werden angezeigt.
3. Klicken Sie auf die Registerkarte **Disk Information**.

   Detaillierte Laufwerksinformationen werden angezeigt.

   Die Cache-Tabelle wird nur angezeigt, wenn das ausgewählte Aggregat einen Speicherpool verwendet.
4. Bewegen Sie in der Cache-Tabelle den Zeiger über den Namen des erforderlichen Storage Pools.

   Die Details des Speicherpools werden angezeigt.

Anzeigen der Volume-Liste und der Details

Auf der Seite „Status/Volume Inventory“ können Sie das Inventar der Volumes überwachen. Auf der Seite Systemzustand/Volumes Kapazität und Auslastung werden Informationen über die Kapazität und Auslastung der Volumes in einem Cluster angezeigt.

Bevor Sie beginnen

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

Über diese Aufgabe

Auf der Seite „Systemzustand/Volume-Details“ finden Sie zudem detaillierte Informationen zu überwachten Volumes, darunter Kapazität, Effizienz, Konfiguration und Sicherung der Volumes. Sie können auch Informationen zu den zugehörigen Geräten und zugehörigen Warnmeldungen für ein bestimmtes Volume anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **Volumes**.
2. Es gibt folgende Möglichkeiten, die Volume-Details anzuzeigen:
   - Um detaillierte Informationen zur Kapazität und Auslastung von Volumes in einem Cluster anzuzeigen, wählen Sie im Menü Ansicht die Option **Volume-Kapazität und -Auslastung**.
   - Um minimale Details anzuzeigen, positionieren Sie den Cursor über den Namen der Lautstärke.
   - Klicken Sie zum Einblenden der vollständigen Details auf den Volume-Namen.

     Sie können die vollständigen Details auch anzeigen, indem Sie im Dialogfeld mit den minimalen Details auf **Details anzeigen** klicken.
3. Zeigen Sie die Objekte an, die mit dem Volumen in Verbindung stehen, indem Sie im Dialogfeld mit den minimalen Details auf **Related** klicken.

Anzeigen der CIFS-Freigaben

Auf der Seite Health/Storage Virtual Machine Details können Sie detaillierte Informationen über die CIFS-Freigabe anzeigen, die von der ausgewählten SVM (Storage Virtual Machine) gehostet wird. Sie können Details anzeigen, wie z. B. den Freigabennamen, den Verbindungspfad, Objekte, Sicherheitseinstellungen und die für die Freigabe definierten Richtlinien exportieren.

Bevor Sie beginnen

- Die CIFS-Lizenz muss auf dem Cluster aktiviert sein.
- Es müssen logische Schnittstellen, die die CIFS-Freigaben erfüllen, konfiguriert werden.
- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Freigaben in Ordnern werden auf der Registerkarte CIFS-Freigaben nicht angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie die SVM aus, für die Sie die Details der CIFS-Freigabe anzeigen möchten.
3. Klicken Sie auf der Seite **Health/Storage Virtual Machine** Details auf die Registerkarte **CIFS Shares**.

Anzeigen von Informationen zur FabricPool-Kapazität

Sie können FabricPool Kapazitätsinformationen für Cluster, Aggregate und Volumes auf den Seiten „Health Inventory“ und „Details“ für diese Objekte anzeigen. Sie können auch FabricPool-Informationen im Bericht über Aggregatskapazität und -Auslastung anzeigen.

Über diese Aufgabe

Auf diesen Seiten werden Informationen angezeigt, beispielsweise die verfügbare Kapazität auf der lokalen Performance-Tier und auf der Cloud-Tier. Sie erfahren, wie viel Kapazität in beiden Tiers verwendet wird, welche Aggregate an ein Cloud-Tier angebunden sind. Welche Volumes die Funktionen von FabricPool implementieren, indem bestimmte Informationen in das Cloud-Tier verschoben werden

Schritte

1. Führen Sie einen der folgenden Schritte aus:

So zeigen Sie Kapazitätsinformationen für…	Tun Sie das…
Cluster	a. Klicken Sie auf der Seite „Systemzustand/Cluster-Inventar“ auf ein Cluster. b. Klicken Sie auf der Seite Health/Cluster Details auf die Registerkarte **Konfiguration**. Auf der Anzeige werden die Namen aller Cloud-Tiers angezeigt, mit denen dieses Cluster verbunden ist.

So zeigen Sie Kapazitätsinformationen für…	Tun Sie das…
Aggregate	a. Klicken Sie auf der Seite „Systemzustand/Aggregate Inventory“ auf ein Aggregat, in dem das Feld Typ „`SSD (FabricPool)`“ anzeigt. b. Klicken Sie auf der Detailseite „Systemzustand/Aggregat“ auf die Registerkarte **Kapazität**. Das Display zeigt die Gesamtkapazität sowie den belegten und freien Speicherplatz im Cloud-Tier an. c. Klicken Sie auf die Registerkarte **Disk Information**. Das Display zeigt den Namen der Cloud-Tier und den verfügbaren Speicherplatz an. d. Klicken Sie auf die Registerkarte **Konfiguration**. Das Display zeigt den Namen der Cloud-Tier sowie weitere detaillierte Informationen zum Objektspeicher an.
Volumes	a. Klicken Sie auf der Seite „System/Volume-Inventar“ auf ein Volume, auf dem im Feld „`Tiering Policy`“ ein Richtlinienname angezeigt wird. b. Klicken Sie auf der Seite Health/Volume Details auf die Registerkarte **Konfiguration**. Auf der Anzeige wird der Name der FabricPool-Tiering-Richtlinie angezeigt, die dem Volume zugewiesen ist.

Nachdem Sie fertig sind

Weitere Informationen zu FabricPool-Aggregaten finden Sie im Power Guide_ „ _ONTAP 9 Festplatten und Aggregate“.

"ONTAP 9 Festplatten und Aggregate Power Guide"

Anzeigen der Liste der Snapshot Kopien

Sie können die Liste der Snapshot Kopien für ein ausgewähltes Volume anzeigen. Mithilfe der Liste der Snapshot Kopien lässt sich die Menge an Festplattenspeicher berechnen, die zurückgewonnen werden kann, wenn eine oder mehrere Snapshot

Kopien gelöscht werden. Außerdem können Sie die Snapshot Kopien bei Bedarf löschen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Das Volume, das die Snapshot Kopien enthält, muss online sein.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **Volumes**.
2. Wählen Sie auf der Seite **Systemzustand/Volumes** Inventar das Volume aus, das die Snapshot Kopien enthält, die Sie anzeigen möchten.
3. Klicken Sie auf der Seite **Health/Volume** Details auf die Registerkarte **Capacity**.
4. Klicken Sie im Fensterbereich **Details** der Registerkarte **Kapazität** im Abschnitt Weitere Details auf den Link neben **Snapshot Kopien**.

   Die Anzahl der Snapshot Kopien ist ein Link, der die Liste der Snapshot Kopien anzeigt.

Snapshot Kopien werden gelöscht

Sie können eine Snapshot-Kopie löschen, um Speicherplatz zu sparen oder um freien Speicherplatz zu freizugeben. Oder Sie können die Snapshot-Kopie löschen, wenn sie nicht mehr benötigt wird.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Das Volume muss sich online sein.

Um eine Snapshot Kopie zu löschen, die besetzt oder gesperrt ist, müssen Sie die Snapshot Kopie aus der Anwendung freigegeben haben, die sie verwendet hat.

Über diese Aufgabe

- Die Basis-Snapshot Kopie in einem übergeordneten Volume kann nicht gelöscht werden, wenn ein FlexClone Volume diese Snapshot Kopie nutzt.

  Die Snapshot Basis-Kopie ist die Snapshot Kopie, die zur Erstellung des FlexClone Volume verwendet wird und den Status anzeigt `Busy` Und Anwendungsabhängigkeit als `Busy,Vclone` Im übergeordneten Volume.

- Sie können keine gesperrte Snapshot Kopie löschen, die in einer SnapMirror Beziehung verwendet wird.

  Die Snapshot Kopie ist gesperrt und für das nächste Update erforderlich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **Volumes**.
2. Wählen Sie auf der Seite **Systemzustand/Volumes** Inventar das Volume aus, das die Snapshot Kopien

enthält, die Sie anzeigen möchten.

Die Liste der Snapshot Kopien wird angezeigt.

3. Klicken Sie auf der Seite **Health/Volume** Details auf die Registerkarte **Capacity**.
4. Klicken Sie im Fensterbereich **Details** der Registerkarte **Kapazität** im Abschnitt Weitere Details auf den Link neben **Snapshot Kopien**.

   Die Anzahl der Snapshot Kopien ist ein Link, der die Liste der Snapshot Kopien anzeigt.

5. Wählen Sie in der Ansicht **Snapshot Kopien** die Snapshot Kopien aus, die Sie löschen möchten, und klicken Sie dann auf **Ausgewählte löschen**.

Berechnung des nicht anforderbaren Speicherplatzes für Snapshot Kopien

Sie können den Speicherplatz berechnen, den zurückgewonnen werden kann, wenn eine oder mehrere Snapshot-Kopien gelöscht werden.

Bevor Sie beginnen

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

Das Volume muss sich online sein.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **Volumes**.
2. Wählen Sie auf der Seite **Systemzustand/Volumes** Inventar das Volume aus, das die Snapshot Kopien enthält, die Sie anzeigen möchten.

   Die Liste der Snapshot Kopien wird angezeigt.

3. Klicken Sie auf der Seite **Health/Volume** Details auf die Registerkarte **Capacity**.
4. Klicken Sie im Fensterbereich **Details** der Registerkarte **Kapazität** im Abschnitt Weitere Details auf den Link neben **Snapshot Kopien**.

   Die Anzahl der Snapshot Kopien ist ein Link, der die Liste der Snapshot Kopien anzeigt.

5. Wählen Sie in der Ansicht **Snapshot Kopien** die Snapshot Kopien aus, für die Sie den zurückforderbaren Speicherplatz berechnen möchten.
6. Klicken Sie Auf **Berechnen**.

   Der zurückforderbare Speicherplatz (in Prozent und KB, MB, GB usw.) auf dem Volume wird angezeigt.

7. Um den wieder einzuforderbaren Speicherplatz neu zu berechnen, wählen Sie die erforderlichen Snapshot Kopien aus, und klicken Sie auf **Neu berechnen**.

Beschreibung der Fenster und Dialogfelder für Cluster-Objekte

Sie können alle Cluster- und Cluster-Objekte auf der jeweiligen Storage-Objektseite anzeigen. Sie können die Details auch auf der entsprechenden Seite mit den Details des Speicherobjekts anzeigen.

„Systemzustand“/„Cluster Inventory“-Seite

Auf der Seite „Health/Clusters Inventory“ können Sie Cluster hinzufügen und detaillierte Informationen zu den von Ihnen überwachten Clustern anzeigen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Befehlsschaltflächen

- **Überwachungsstatus Anzeigen**

  Hier können Sie den Überwachungsstatus der ausgewählten Cluster anzeigen, indem Sie zur Seite Configuration/Cluster Data Sources navigieren.

- **Anmerkung**

  Ermöglicht Ihnen, das ausgewählte Cluster mit Anmerkungen zu versehen.

- **Liste Aktualisieren**

  Aktualisiert die Cluster-Liste und die dem Cluster zugeordneten Eigenschaften.

- **Export**

  Ermöglicht das Exportieren der Details aller überwachten Cluster in kommagetrennte Werte (`.csv`) Datei.

Cluster-Tabelle

In der Tabelle Cluster werden die Eigenschaften aller erkannten Cluster angezeigt. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen:

- **Status**

  Ein Symbol, das den aktuellen Status des Clusters angibt. Der Status kann kritisch sein (), Fehler (), Warnung (Oder normal ()).

  Sie können Ihren Mauszeiger über das Symbol positionieren, um weitere Informationen über das Ereignis oder die für das Cluster generierten Ereignisse anzuzeigen.

  Wenn der Status des Clusters auf einem einzelnen Ereignis basiert, können Sie Informationen wie den Ereignisnamen, die Zeit und das Datum, an dem das Ereignis generiert wurde, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Sie können auf die Schaltfläche **Details anzeigen** klicken, um weitere Informationen über die Veranstaltung anzuzeigen.

  Wenn der Status des Clusters auf mehreren Ereignissen des gleichen Schweregrads basiert, werden die drei wichtigsten Ereignisse zusammen mit Informationen wie dem Ereignisnamen, der Zeit und dem Datum, an dem die Ereignisse generiert werden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link**Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

- * Cluster*

  Der Name des Clusters.

- **Kommunikationsstatus**

  Gibt an, ob das Cluster erreichbar ist oder nicht.

  Der Status wird als gut angezeigt, wenn das Cluster erreichbar ist. Wenn das Cluster nicht erreichbar ist oder die Anmeldeinformationen ungültig sind, wird der Status als nicht erreichbar angezeigt.

- **Systemzustand**

  Allgemeine Informationen zum Status des Clusters, die anhand des Status verschiedener Cluster-Subsysteme berechnet werden.

  Mögliche Werte sind OK, OK mit Unterdrückten, herabgestuft und Komponenten nicht erreichbar. Diese Werte werden von den Zustandsüberwachungen in der ONTAP Software bestimmt.

- **Hostname oder IP-Adresse**

  Der FQDN, der Kurzname oder die IP-Adresse der Cluster-Management-LIF, die zur Verbindung mit dem Cluster verwendet wird.

- **FQDN**

  Der vollständig qualifizierte Domänenname (FQDN) des Clusters.

- **Betriebssystemversion**

  Die ONTAP Version, in der das Cluster ausgeführt wird.

  Wenn im Cluster die Nodes unterschiedliche Versionen von ONTAP ausführen, wird die früheste ONTAP-Version angezeigt.

- **Anzahl Knoten**

  Anzahl der Nodes, die zum Cluster gehören.

- **Letzte Aktualisierte Zeit**

  Der Zeitstempel, an dem die Überwachungsmuster des Clusters zuletzt erfasst wurden.

- **Seriennummer**

  Die Seriennummer des Clusters.

- **Kontakt**

  Die Kontaktinformationen des Clusters.

- **Lage**

  Der Speicherort des Clusters.

- **FIPS aktiviert**

  Gibt an, ob der FIPS-Modus auf dem Cluster aktiviert ist

Bereich Filter

Im Bereich Filter können Sie Filter festlegen, um die Anzeige von Informationen in der Cluster-Liste anzupassen. Sie können Filter in den Spalten Status, Kommunikationsstatus, Systemintegrität und Anmerkung auswählen.

Die im Fensterbereich Filter angegebenen Filter überschreiben die Filter, die für die Spalten in der Clusterliste angegeben sind.

Systemzustand/Cluster-Storage-Übersicht

Auf der Seite „Systemzustand/Cluster Storage Summary“ können in allen Clustern zusammengefasste Informationen zur Storage-Kapazität und -Auslastung angezeigt werden. Anhand dieser Informationen werden mögliche Kapazitätsrisiken identifiziert und die Workloads neu ausgerichtet.

Verwenden Sie die Schaltfläche **Export**, um die Details aller überwachten Cluster in kommagetrennte Werte zu exportieren (`.csv`) Datei.

- * Cluster*

  Der Cluster-Name.

- **HA-Paar**

  Der HA-Paar-Wert, der durch die Bildung von zwei Nodes ermittelt wird.

- **Modell/Familie**

  Modell oder Familienname des Clusters.

- **Betriebssystemversion**

  Die auf dem System installierte ONTAP-Version.

- **Gesamtbruttokapazität**

  Zeigt die gesamte physische Kapazität aller Festplatten im Array an.

- **Unkonfigurierte Rohkapazität**

  Die nicht konfigurierte Kapazität von Festplatten, deren Containertyp nicht aggregiert, beschädigt, frei oder freigegeben ist. Diese Kapazität ist immer höher als die physische Kapazität der Festplatte in ONTAP. Nehmen Sie beispielsweise eine 2-TB-Festplatte in Betracht. Die physische Kapazität der Festplatte beträgt 1.6 TB in ONTAP, während die nicht konfigurierte Rohkapazität in Unified Manager 1.8 TB beträgt.

- **Gesamtkapazität**

  Die Gesamtgröße der verfügbaren Aggregate für den Benutzer. Dies schließt die Snapshot Kopie-Reserve ein.

- **Verwendete Gesamtkapazität**

  Die Kapazität, die bereits in Aggregaten verwendet wird. Dies schließt die Kapazität ein, die von Volumes,

LUNs und anderen Technologieköpfen für Storage-Effizienz verbraucht wird.

- * Nicht Genutzte Kapazität Aggregieren*

  Die Kapazität, die möglicherweise zum Speichern zusätzlicher Daten im Aggregat verfügbar ist. Dies schließt die Snapshot Kopie-Reserve ein.

- **Zugewiesene LUN-Kapazität**

  Die Kapazität der zugeordneten LUNs.

- **Nicht zugewiesene LUN-Kapazität**

  Die Kapazität aller LUNs, die dem Host nicht zugeordnet sind.

- **Volumen Gesamtkapazität**

  Die Gesamtkapazität der Volumes (genutzt plus nicht genutzt).

- **Volumen Genutzte Kapazität**

  Verwendete Kapazität der Volumes.

- **Volumen Ungenutzte Kapazität**

  Die ungenutzte Kapazität der Volumes.

- **Volume Protection Kapazität**

  Die Kapazität der Volumes mit SnapMirror und SnapVault ist aktiviert.

- * Cluster Lizenzierte Cloud Stufe Gesamt*

  Die Gesamtkapazität, die in der Cloud-Tier lizenziert wurde. Dieses Feld wird für Storage-Provider angezeigt, die eine FabricPool-Lizenz benötigen, z. B. Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage oder Alibaba Cloud Object Storage.

- * Clusterlizenzierte Cloud-Stufe Verwendet*

  Der von Daten im Cloud-Tier verwendete Speicherplatz für Storage-Provider, die eine FabricPool Lizenz benötigen.

- **Verwendete Cluster-StorageGRID-Kapazität**

  Von Daten in der Cloud-Tier verwendeter Speicherplatz für Storage-Provider, die keine FabricPool-Lizenz benötigen, beispielsweise StorageGRID.

„Systemzustand/Cluster-Details“-Seite

Auf der Seite Systemzustand/Cluster-Details finden Sie ausführliche Informationen über ein ausgewähltes Cluster, z. B. Angaben zu Systemzustand, Kapazität und Konfiguration. Sie können außerdem Informationen zu den logischen Schnittstellen (LIFs), Nodes, Festplatten, zugehörigen Geräten und zugehörigen Warnmeldungen für das Cluster anzeigen.

Der Status neben dem Cluster-Namen, z. B. (gut), stellt den Kommunikationsstatus dar, ob Unified Manager mit dem Cluster kommunizieren kann. Er stellt nicht den Failover-Status oder den Gesamtstatus des Clusters dar.

Befehlsschaltflächen

Mit den Schaltflächen des Befehls können Sie die folgenden Aufgaben für das ausgewählte Cluster ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Hier können Sie zur Seite Performance/Cluster-Details navigieren.

-

  Hiermit können Sie den ausgewählten Cluster zum Dashboard „Favoriten“ hinzufügen.

- **Aktionen**

  - Alarm hinzufügen: Öffnet das Dialogfeld Alarm hinzufügen, in dem Sie dem ausgewählten Cluster eine Warnung hinzufügen können.
  - Erneut entdecken: Initiiert eine manuelle Aktualisierung des Clusters, sodass Unified Manager die neuesten Änderungen am Cluster erkennen kann.

    Bei Kombination von Unified Manager mit OnCommand Workflow Automation erfasst der Wiederauffindungvorgang ggf. auch zwischengespeicherte Daten von WFA.

  Nachdem der Vorgang zur erneuten Erkennung initiiert wurde, wird ein Link zu den zugehörigen Jobdetails angezeigt, um die Nachverfolgung des Jobstatus zu ermöglichen.

  - Anmerkungen: Ermöglicht es Ihnen, das ausgewählte Cluster zu kommentieren.

- **Cluster Anzeigen**

  Hier können Sie zur Seite „Health/Clusters Inventory“ navigieren.

Registerkarte Systemzustand

Zeigt detaillierte Informationen zur Datenverfügbarkeit und zu Kapazitätsproblemen der verschiedenen Cluster-Objekte wie Nodes, SVMs und Aggregate an. Verfügbarkeitsprobleme hängen von der Datenserverfunktion der Cluster-Objekte ab. Kapazitätsprobleme stehen im Zusammenhang mit der Datenspeicherfunktion der Cluster-Objekte.

Sie können auf das Diagramm eines Objekts klicken, um eine gefilterte Liste der Objekte anzuzeigen. Beispielsweise können Sie auf das SVM-Kapazitätsdiagramm klicken, in dem Warnungen angezeigt werden, um eine gefilterte Liste der SVMs anzuzeigen. Diese Liste enthält SVMs mit Volumes oder qtrees, deren Kapazitätsprobleme mit einem Schweregrad von Warnung auftreten. Sie können auch auf das Diagramm „SVMs Verfügbarkeit“ klicken, in dem Warnungen angezeigt werden, um die Liste der SVMs mit Verfügbarkeitsproblemen und einem Schweregrad „Warnung“ anzuzeigen.

- **Verfügbarkeitsprobleme**

  Grafische Darstellung der Gesamtzahl an Objekten, einschließlich Objekten mit Verfügbarkeitsproblemen und Objekten, bei denen keine Probleme mit der Verfügbarkeit auftreten Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten

Details zu Verfügbarkeitsproblemen, die sich auf die Verfügbarkeit von Daten im Cluster auswirken oder bereits davon betroffen sein können. Beispielsweise werden Informationen über Festplatten-Shelfs angezeigt, die ausgefallen sind und Aggregate, die offline sind.

Die für das SFO-Balkendiagramm angezeigten Daten basieren auf dem HA-Status der Nodes. Die für alle anderen Balkendiagramme angezeigten Daten werden auf Grundlage der generierten Ereignisse berechnet.

- **Kapazitätsprobleme**

  Grafische Darstellung der Gesamtzahl an Objekten, einschließlich Objekten mit Kapazitätsproblemen und Objekten, die keine Kapazitätsprobleme haben. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Kapazitätsproblemen, die sich auf die Kapazität von Daten im Cluster auswirken oder bereits sie beeinträchtigen können. Beispielsweise werden Informationen zu Aggregaten angezeigt, die mit hoher Wahrscheinlichkeit die festgelegten Schwellenwerte überschreiten.

Registerkarte „Kapazität“

Zeigt detaillierte Informationen zur Kapazität des ausgewählten Clusters an.

- * Kapazität*

  Zeigt das Datenkapazitätsdiagramm zu der genutzten Kapazität und der verfügbaren Kapazität aus allen zugewiesenen Aggregaten an:

  - Gesamtkapazität

    Zeigt die Gesamtkapazität des Clusters an. Dies schließt nicht die Kapazität ein, die Parität zugewiesen ist.

  - Verwendet

    Zeigt die Kapazität an, die von Daten verwendet wird. Dies schließt nicht die Kapazität ein, die für Parität, richtige Dimensionierung und Reservierung verwendet wird.

  - Verfügbar

    Zeigt die für Daten verfügbare Kapazität an.

  - Ersatzteile

    Zeigt die verfügbare Speicherkapazität für die Speicherung aller freien Festplatten an.

  - Provisioniert

    Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

- * Cloud Tier*

  Zeigt Kapazitätsdetails über das Cloud-Tier für FabricPool-fähige Aggregate auf dem Cluster an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

  - Verwendet

Zeigt den Speicherplatz an, der von Daten in konfigurierten Cloud-Tiers verwendet wird.

- Datendiagramm

  Bei Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage oder Alibaba Cloud Object Storage werden die Gesamtkapazität, die von diesem Cluster lizenziert wurde, und die von Aggregaten verwendete Menge angezeigt.

Bei einer StorageGRID wird im Diagramm nur die Gesamtkapazität angezeigt, die von Aggregaten verwendet wird.

- **Details**

  Zeigt detaillierte Informationen zur verwendeten und verfügbaren Kapazität an.

  - Gesamtkapazität

    Zeigt die Gesamtkapazität des Clusters an. Dies schließt nicht die Kapazität ein, die Parität zugewiesen ist.

  - Verwendet

    Zeigt die Kapazität an, die von Daten verwendet wird. Dies schließt nicht die Kapazität ein, die für Parität, richtige Dimensionierung und Reservierung verwendet wird.

  - Verfügbar

    Zeigt die für Daten verfügbare Kapazität an.

  - Provisioniert

    Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

  - Ersatzteile

    Zeigt die verfügbare Speicherkapazität für die Speicherung aller freien Festplatten an.

  - Cloud-Tier

    Zeigt den Speicherplatz an, der von Daten in konfigurierten Cloud-Tiers verwendet wird. Bei Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage oder Alibaba Cloud Object Storage wird auch die Gesamtkapazität, die von diesem Cluster lizenziert wurde, angezeigt.

- **Kapazität Breakout nach Datenträgertyp**

  Im Bereich Capacity Breakout nach Disk Type werden ausführliche Informationen zur Festplattenkapazität der verschiedenen Festplattentypen im Cluster angezeigt. Durch Klicken auf den Festplattentyp werden weitere Informationen zum Festplattentyp auf der Registerkarte Laufwerke angezeigt.

  - Nutzbare Gesamtkapazität –

    Zeigt die verfügbare Kapazität und freie Kapazität der Datenfestplatten an.

  - HDD

    Grafische Darstellung der verwendeten Kapazität und der verfügbaren Kapazität aller Festplatten im

Cluster. Die gestrichelte Linie stellt die freie Kapazität der Datenfestplatten dar.

- Flash
  - SSD-Daten

    Grafische Darstellung der verwendeten Kapazität und der verfügbaren Kapazität der SSD-Datenfestplatten im Cluster

  - SSD Cache

    Zeigt grafisch die speicherbare Kapazität der SSD-Cache-Laufwerke im Cluster an.

  - SSD Spare

    Grafische Darstellung der freien Kapazität der SSD-, Daten- und Cache-Festplatten im Cluster

- Nicht Zugewiesene Festplatten

  Zeigt die Anzahl der nicht zugewiesenen Festplatten im Cluster an.

- **Aggregate mit Kapazitätsprobleme Liste**

  Zeigt Details zur verwendeten Kapazität und zur verfügbaren Kapazität der Aggregate mit Kapazitätsproblemen in Tabellenform an.

  - Status

    Zeigt an, dass das Aggregat ein kapazitätsbezogenes Problem mit einem bestimmten Schweregrad hat.

    Sie können den Zeiger auf den Status verschieben, um weitere Informationen zu dem für das Aggregat generierten Ereignis oder Ereignissen anzuzeigen.

    Wenn der Status des Aggregats durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen wurde, und die Ursache des Ereignisses anzeigen. Sie können auf die Schaltfläche **Details anzeigen** klicken, um weitere Informationen über die Veranstaltung anzuzeigen.

    Wenn der Status des Aggregats durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen angezeigt, z. B. Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst werden, und der Name des Administrators, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

    > Ein Aggregat kann mehrere kapazitätsbezogene Ereignisse vom gleichen Schweregrad oder verschiedene Schweregrade aufweisen. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Aggregat zwei Ereignisse mit dem Schweregrad „Fehler“ und „kritisch“ hat, wird nur der Schweregrad „kritisch“ angezeigt.

  - Aggregat

    Zeigt den Namen des Aggregats an.

- Genutzte Datenkapazität

  Grafische Anzeige von Informationen zur Kapazitätsauslastung des Aggregats (in Prozent)

- Tage voll

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor die volle Kapazität des Aggregats erreicht ist.

Registerkarte Konfiguration

Zeigt Details zum ausgewählten Cluster an, z. B. IP-Adresse, Seriennummer, Kontakt und Standort:

- **Cluster Übersicht**
  - Management-LIF

    Zeigt die Cluster-Management-LIF an, die Unified Manager zum Herstellen einer Verbindung mit dem Cluster verwendet. Der Betriebsstatus der LIF wird ebenfalls angezeigt.

  - Host-Name oder IP-Adresse

    Zeigt den FQDN, den Kurznamen oder die IP-Adresse der Clusterverwaltungs-LIF an, die Unified Manager zur Verbindung mit dem Cluster verwendet.

  - FQDN

    Zeigt den vollständig qualifizierten Domänennamen (FQDN) des Clusters an.

  - Betriebssystemversion

    Zeigt die ONTAP-Version an, die das Cluster ausführt. Wenn im Cluster die Nodes unterschiedliche Versionen von ONTAP ausführen, wird die früheste ONTAP-Version angezeigt.

  - Seriennummer

    Zeigt die Seriennummer des Clusters an.

  - Kontakt

    Zeigt Details zum Administrator an, an den Sie bei Cluster-Problemen wenden sollten.

  - Standort

    Zeigt den Speicherort des Clusters an.

- **Remote Cluster Übersicht**

  Enthält Details zum Remote-Cluster in einer MetroCluster-Konfiguration. Diese Informationen werden nur für MetroCluster-Konfigurationen angezeigt.

  - Cluster

    Zeigt den Namen des Remote-Clusters an. Sie können auf den Cluster-Namen klicken, um zur Detailseite des Clusters zu navigieren.

- Hostname oder IP-Adresse

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Remote-Clusters an.

- Seriennummer

  Zeigt die Seriennummer des Remote-Clusters an.

- Standort

  Zeigt den Speicherort des Remote-Clusters an.

- **MetroCluster Übersicht**

  Bietet Details zum lokalen Cluster in einer MetroCluster Konfiguration. Diese Informationen werden nur für MetroCluster-Konfigurationen angezeigt.

  - Typ

    Zeigt an, ob es sich bei dem MetroCluster-Typ um zwei oder vier Nodes handelt.

  - Konfiguration

    Zeigt die MetroCluster-Konfiguration an, die die folgenden Werte aufweisen kann:

    - Stretch-Konfiguration mit SAS-Kabeln
    - Stretch-Konfiguration mit FC-SAS Bridge
    - Fabric-Konfiguration mit FC Switches

    Bei einem MetroCluster mit vier Nodes wird nur eine Fabric-Konfiguration mit FC-Switches unterstützt.

  +

  - Automatisiertes ungeplantes Switchover (AUSO)

    Zeigt an, ob das automatisierte ungeplante Switchover für das lokale Cluster aktiviert ist. Standardmäßig ist AUSO für alle Cluster in einer MetroCluster-Konfiguration mit zwei Knoten in Unified Manager aktiviert. Sie können die AUSO-Einstellung über die Befehlszeilenschnittstelle ändern.

- **Knoten**
  - Gesteigerte

    Zeigt die Anzahl der Knoten an, die aktiv sind (Oder runter ( ) Im Cluster.

  - Betriebssystemversionen

    Zeigt die ONTAP-Versionen, die die Nodes ausführen, sowie die Anzahl der Nodes, auf denen eine bestimmte Version von ONTAP ausgeführt wird. Beispielsweise gibt 9.0 (2), 8.3 (1) an, dass zwei Nodes ONTAP 9.0 ausführen und auf einem Node ONTAP 8.3 ausgeführt wird.

- **Storage Virtual Machines**
  - Gesteigerte

Zeigt die Anzahl der SVMs an, die aktiv sind (Oder runter ( ) Im Cluster.

- **LIFs**
  - Gesteigerte

    Zeigt die Anzahl der nicht-Daten-LIFs an, die in der aktiv sind (Oder runter ( ) Im Cluster.

  - Cluster-Management-LIFs

    Zeigt die Anzahl der Cluster-Management-LIFs an.

  - Node-Management-LIFs

    Zeigt die Anzahl der LIFs für das Node-Management an.

  - Cluster-LIFs

    Zeigt die Anzahl der Cluster-LIFs an.

  - Intercluster LIFs

    Zeigt die Anzahl der Intercluster-LIFs an.

- **Protokolle**
  - Datenprotokolle

    Zeigt die Liste der lizenzierten Datenprotokolle an, die für den Cluster aktiviert sind. Datenprotokolle sind iSCSI, CIFS, NFS, NVMe und FC/FCoE.

- **Cloud-Tiers**

  In sind die Namen der Cloud-Tiers aufgeführt, mit denen dieses Cluster verbunden ist. Außerdem werden die Typen (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Alibaba Cloud Object Storage oder StorageGRID) und die Status der Cloud-Tiers (verfügbar oder nicht verfügbar) aufgelistet.

Registerkarte MetroCluster-Konnektivität

Zeigt die Probleme und den Konnektivitätsstatus der Clusterkomponenten der MetroCluster Konfiguration an. Ein Cluster wird in einem roten Feld angezeigt, wenn der Disaster-Recovery-Partner des Clusters Probleme hat.

Die Registerkarte MetroCluster-Konnektivität wird nur für Cluster angezeigt, die sich in einer MetroCluster-Konfiguration befinden.

Sie können zur Detailseite eines Remote-Clusters navigieren, indem Sie auf den Namen des Remote-Clusters klicken. Sie können die Details der Komponenten auch anzeigen, indem Sie auf den Zähllink einer Komponente klicken. Wenn Sie beispielsweise auf den Zähllink des Node im Cluster klicken, wird auf der Detailseite des Clusters die Registerkarte Node angezeigt. Wenn Sie auf den Link Zählen der Festplatten im Remote-Cluster klicken, wird die Registerkarte Festplatte auf der Detailseite des Remote-Clusters angezeigt.

Beim Verwalten einer MetroCluster Konfiguration mit acht Nodes wird durch Klicken auf den Zähllink der Komponente Platten-Shelfs nur die lokalen Shelfs des Standard-HA-Paars angezeigt. Es gibt auch keine Möglichkeit, die lokalen Shelfs auf dem anderen HA-Paar anzuzeigen.

Sie können den Mauszeiger über die Komponenten bewegen, um bei jedem Problem die Details und den Konnektivitätsstatus der Cluster anzuzeigen. Außerdem werden weitere Informationen zu dem für das Problem erzeugten Ereignis oder Ereignissen angezeigt.

Wenn der Status des Verbindungsproblem zwischen den Komponenten durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugeordnet ist, und die Ursache des Ereignisses anzeigen. Die Schaltfläche Details anzeigen enthält weitere Informationen zum Ereignis.

Wenn der Status des Verbindungsproblem zwischen den Komponenten durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum bei Auslösung der Ereignisse und dem Namen des Administrators angezeigt, dem das Ereignis zugeordnet ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

Registerkarte „MetroCluster-Replikation“

Zeigt den Status der Daten an, die repliziert werden. Sie können die Registerkarte MetroCluster-Replikation verwenden, um die Datensicherung durch synchrones Spiegeln der Daten mit den bereits Peering-Clustern zu gewährleisten. Ein Cluster wird in einem roten Feld angezeigt, wenn der Disaster-Recovery-Partner des Clusters Probleme hat.

Die Registerkarte MetroCluster-Replikation wird nur für Cluster angezeigt, die sich in einer MetroCluster-Konfiguration befinden.

In einer MetroCluster-Umgebung können Sie diese Registerkarte verwenden, um die logischen Verbindungen und Peering des lokalen Clusters mit dem Remote-Cluster zu überprüfen. Sie können die objektive Darstellung der Cluster-Komponenten mit ihren logischen Verbindungen anzeigen. Dadurch werden Probleme identifiziert, die bei der Spiegelung von Metadaten und Daten auftreten können.

Auf der Registerkarte MetroCluster-Replikation bietet das lokale Cluster eine detaillierte grafische Darstellung des ausgewählten Clusters. MetroCluster-Partner bezieht sich auf das Remote-Cluster.

Registerkarte LIFs

Zeigt Details zu allen nicht-Daten-LIFs an, die auf dem ausgewählten Cluster erstellt wurden.

- **LIF**

  Zeigt den Namen der logischen Schnittstelle an, die im ausgewählten Cluster erstellt wird.

- **Betriebsstatus**

  Zeigt den Betriebsstatus der logischen Schnittstelle an. Diese kann im aktiv sein (), Down (Oder Unbekannt (). Der Betriebsstatus einer logischen Schnittstelle wird vom Status ihrer physischen Ports bestimmt.

- **Verwaltungsstatus**

Zeigt den Administrationsstatus der logischen Schnittstelle an. Dieser kann im aktiv sein (), Down (Oder Unbekannt ()). Sie können den Administrationsstatus einer logischen Schnittstelle steuern, wenn Sie Änderungen an der Konfiguration oder während der Wartung vornehmen. Der Administrationsstatus kann sich vom Betriebsstatus unterscheiden. Wenn jedoch der Administrationsstatus eines LIF „Inaktiv“ lautet, ist der Betriebsstatus standardmäßig „Inaktiv“.

- **IP-Adresse**

  Zeigt die IP-Adresse des LIF an.

- * Rolle*

  Zeigt die Rolle des LIF an. Mögliche Rollen sind Cluster-Management-LIFs, Node-Management-LIFs, Cluster-LIFs und Intercluster-LIFs.

- * Home Port*

  Zeigt den physischen Port an, dem die LIF ursprünglich zugeordnet war.

- **Aktueller Port**

  Zeigt den physischen Port an, dem das LIF derzeit zugeordnet ist. Nach der LIF-Migration kann sich der aktuelle Port vom Home Port unterscheiden.

- **Failover-Richtlinie**

  Zeigt die für das LIF konfigurierte Failover-Richtlinie an.

- **Routing-Gruppen**

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

  Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt. Daher wird für diese Cluster eine leere Spalte angezeigt.

- **Failover-Gruppe**

  Zeigt den Namen der Failover-Gruppe an.

Registerkarte Knoten

Zeigt Informationen zu Nodes im ausgewählten Cluster an. Sie können ausführliche Informationen zu HA-Paaren, Festplatten-Shelfs und Ports anzeigen:

- **HA Details**

  Stellt eine bildliche Darstellung des HA-Status und des Integritätsstatus der Nodes im HA-Paar bereit. Der Integritätsstatus des Node wird durch die folgenden Farben angezeigt:

  - **Grün**

    Der Node befindet sich in einem Betriebszustand.

  - **Gelb**

Der Node hat den Partner-Node übernommen oder der Node weist einige Umgebungsprobleme auf.

- * Rot*

  Der Node ist ausgefallen.

  Sie können Informationen zur Verfügbarkeit des HA-Paars anzeigen und erforderliche Maßnahmen ergreifen, um Risiken zu vermeiden. Im Fall eines möglichen Übernahmevorgangs wird beispielsweise die folgende Meldung angezeigt: `Storage failover possible`.

  Sie können eine Liste der Ereignisse anzeigen, die zum HA-Paar und seiner Umgebung betreffen, z. B. Lüfter, Netzteile, NVRAM-Batterie, Flash-Karten, Serviceprozessor und Verbindung von Festplatten-Shelfs: Sie können auch die Uhrzeit anzeigen, zu der die Ereignisse ausgelöst wurden.

  Sie können weitere Informationen zu Nodes anzeigen, z. B. die Modellnummer und die Seriennummer.

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

- **Platten-Shelves**

  Zeigt Informationen über die Festplatten-Shelfs im HA-Paar an.

  Sie können auch Ereignisse anzeigen, die für die Festplatten-Shelfs und die Umgebungskomponenten generiert wurden, sowie die Zeit, zu der die Ereignisse ausgelöst wurden.

  - **Regal-ID**

    Zeigt die ID des Shelf an, in dem sich die Festplatte befindet.

  - **Komponentenstatus**

    Zeigt Umgebungsdetails der Festplatten-Shelfs an, z. B. Netzteile, Lüfter, Temperatursensor, aktuelle Sensoren, Festplattenkonnektivität. Und Spannungssensoren. Die Umgebungsdetails werden als Symbole in den folgenden Farben angezeigt:

    - **Grün**

      Die Umgebungskomponenten funktionieren ordnungsgemäß.

    - **Grau**

      Für die Umgebungskomponenten sind keine Daten verfügbar.

    - * Rot*

      Einige Umgebungskomponenten sind nicht verfügbar.

  - **Bundesland**

    Zeigt den Status des Festplatten-Shelf an. Mögliche Status sind Offline, Online, kein Status, Initialisierung erforderlich, fehlt, Und Unbekannt.

  - **Modell**

    Zeigt die Modellnummer des Festplatten-Shelf an.

- **Lokales Festplatten-Shelf**

  Gibt an, ob sich das Festplatten-Shelf auf dem lokalen Cluster oder dem Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

- * Unique ID*

  Zeigt die eindeutige ID des Festplatten-Shelf an.

- **Firmware-Version**

  Zeigt die Firmware-Version des Festplatten-Shelf an.

- **Ports**

Zeigt Informationen zu den zugehörigen FC-, FCoE- und Ethernet-Ports an. Sie können Details zu den Ports und den zugehörigen LIFs anzeigen, indem Sie auf die Port-Symbole klicken.

Sie können auch die für die Ports generierten Ereignisse anzeigen.

Sie können folgende Portdetails anzeigen:

- Port-ID

  Zeigt den Namen des Ports an. Die Port-Namen können beispielsweise E0M, e0a und e0b sein.

- Rolle

  Zeigt die Rolle des Ports an. Mögliche Rollen sind Cluster, Data, Intercluster, Node-Management und Undefined.

- Typ

  Zeigt das Protokoll der physischen Schicht an, das für den Port verwendet wird. Mögliche Typen sind Ethernet, Fibre Channel und FCoE.

- WWPN

  Zeigt den WWPN (World Wide Port Name) des Ports an.

- Firmware-Version

  Zeigt die Firmware-Version des FC/FCoE-Ports an.

- Status

  Zeigt den aktuellen Status des Ports an. Mögliche Zustände sind up, Down, Link not connected. Oder Unbekannt ( ).

Sie können die portbezogenen Ereignisse in der Ereignisliste anzeigen. Sie können auch die zugehörigen LIF-Details anzeigen, z. B. LIF-Name, Betriebsstatus, IP-Adresse oder WWPN, Protokolle, den Namen der zu dieser LIF gehörenden SVM, den aktuellen Port, die Failover-Richtlinie und die Failover-Gruppe.

Registerkarte „Festplatten“

Zeigt Details zu den Festplatten im ausgewählten Cluster an. Sie können Festplatten-bezogene Informationen wie die Anzahl der verwendeten Festplatten, Ersatzfestplatten, fehlerhafte Festplatten und nicht zugewiesene Laufwerke anzeigen. Sie können auch weitere Details anzeigen, z. B. den Festplattennamen, den Festplattentyp und den Besitzer-Node der Festplatte.

- **Disk Pool Zusammenfassung**

  Zeigt die Anzahl der Laufwerke an, die nach effektiven Typen (FCAL, SAS, SATA, MSATA, SSD, Array-LUN und VMDISK) und der Zustand der Festplatten. Sie können auch andere Details anzeigen, wie z. B. die Anzahl der Aggregate, freigegebenen Festplatten, Ersatzfestplatten, defekte Festplatten, nicht zugewiesene Laufwerke, Und nicht unterstützten Festplatten. Wenn Sie auf den Link zur Anzahl der effektiven Festplattentypen klicken, werden Festplatten mit dem ausgewählten Status und dem effektiven Typ angezeigt. Wenn Sie beispielsweise auf den Zähllink für den Festplattenstatus „beschädigt“ und „effektiver Typ SAS“ klicken, werden alle Festplatten mit dem Festplattenstatus „beschädigt“ und „effektiver Typ „SAS“ angezeigt.

- **Datenträger**

  Zeigt den Namen der Festplatte an.

- **RAID-Gruppen**

  Zeigt den Namen der RAID-Gruppe an.

- **Owner Node**

  Zeigt den Namen des Node an, zu dem die Festplatte gehört. Wenn die Festplatte nicht zugewiesen ist, wird in dieser Spalte kein Wert angezeigt.

- **Bundesland**

  Zeigt den Status der Festplatte an: Aggregate, Shared, Spare, broken, Unassigned, Nicht unterstützt oder Unbekannt. Standardmäßig wird diese Spalte sortiert, um die Status in der folgenden Reihenfolge anzuzeigen: Gebrochen, nicht zugewiesen, nicht unterstützt, Spare, Aggregat, Und Shared IT.

- **Lokaler Datenträger**

  Zeigt entweder Ja oder Nein an, um anzugeben, ob sich das Laufwerk im lokalen Cluster oder im Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

- **Position**

  Zeigt die Position des Laufwerks basierend auf seinem Container-Typ an, z. B. Kopieren, Daten oder Parität. Standardmäßig ist diese Spalte ausgeblendet.

- **Betroffene Aggregate**

  Zeigt die Anzahl der Aggregate an, die aufgrund der ausgefallenen Festplatte betroffen sind. Sie können den Mauszeiger über den Zähllink verschieben, um die betroffenen Aggregate anzuzeigen. Klicken Sie dann auf den Aggregatnamen, um Details zum Aggregat anzuzeigen. Sie können auch auf die Aggregatanzahl klicken, um die Liste der betroffenen Aggregate auf der Seite „Systemzustand/Aggregate Inventory“ anzuzeigen.

  In dieser Spalte wird für die folgenden Fälle kein Wert angezeigt:

- Für fehlerhafte Festplatten, wenn ein Cluster mit solchen Festplatten zu Unified Manager hinzugefügt wird
- Wenn keine ausgefallenen Festplatten vorhanden sind

- **Speicherpool**

  Zeigt den Namen des Speicherpools an, zu dem die SSD gehört. Sie können den Zeiger über den Speicherpool verschieben, um Details des Speicherpools anzuzeigen.

- **Speicherbare Kapazität**

  Zeigt die verfügbare Festplattenkapazität an.

- **Rohkapazität**

  Zeigt die Kapazität der unformatierten RAW-Festplatte vor der richtigen Dimensionierung und RAID-Konfiguration an. Standardmäßig ist diese Spalte ausgeblendet.

- **Typ**

  Zeigt die Festplattentypen an, z. B. ATA, SATA, FCAL oder VMDISK.

- * Effektiver Typ*

  Zeigt den von ONTAP zugewiesenen Festplattentyp an.

  Bestimmte ONTAP-Festplattentypen werden als gleichbedeutend mit dem Erstellen und Hinzufügen zu Aggregaten und mit Ersatzmanagement angesehen. ONTAP weist jedem Festplattentyp einen effektiven Festplattentyp zu.

- **Spare Blocks Verbraucht %**

  Zeigt in Prozent die Spare-Blöcke an, die in der SSD-Festplatte verbraucht werden. Diese Spalte ist bei anderen Festplatten als SSD-Festplatten leer.

- **Bewertete Lebensdauer %**

  Zeigt prozentual eine Schätzung der verwendeten SSD-Lebensdauer an, basierend auf der tatsächlichen SSD-Nutzung und der Vorhersage der SSD-Lebensdauer des Herstellers. Ein Wert größer als 99 zeigt an, dass die geschätzte Haltbarkeit verbraucht wurde, weist aber möglicherweise nicht auf einen SSD-Ausfall hin. Wenn der Wert unbekannt ist, wird die Platte weggelassen.

- **Firmware**

  Zeigt die Firmware-Version der Festplatte an.

- **U/MIN**

  Zeigt die Umdrehungen pro Minute (U/min) der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

- **Modell**

  Zeigt die Modellnummer der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

- * Anbieter*

Zeigt den Namen des Festplattenanbieters an. Standardmäßig ist diese Spalte ausgeblendet.

- **Regal-ID**

  Zeigt die ID des Shelf an, in dem sich die Festplatte befindet.

- **Bucht**

  Zeigt die ID des Einschubschachts an, in dem sich die Festplatte befindet.

Bereich „Verwandte Anmerkungen“

Hiermit können Sie die mit dem ausgewählten Cluster verknüpften Anmerkungsdetails anzeigen. Die Details umfassen den Anmerkungsnamen und die auf das Cluster angewandten Anmerkungswerte. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Mit dieser Option können Sie Gerätedetails anzeigen, die mit dem ausgewählten Cluster verknüpft sind.

Zu den Details gehören Eigenschaften des mit dem Cluster verbundenen Geräts, wie z. B. Gerätetyp, Größe, Anzahl und Integritätsstatus. Sie können auf den Zähllink klicken, um weitere Analysen zu diesem Gerät durchzuführen.

Mithilfe des Teilfensters MetroCluster können Sie Anzahl und auch Details zum Remote MetroCluster Partner sowie zu den zugehörigen Cluster-Komponenten wie Nodes, Aggregaten und SVMs abrufen. Das Teilfenster „MetroCluster Partner“ wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

Im Bereich „Verwandte Geräte“ können Sie die Nodes, SVMs und Aggregate anzeigen und navigieren, die mit dem Cluster in Verbindung stehen:

- **MetroCluster Partner**

  Zeigt den Integritätsstatus des MetroCluster Partners an. Über den Link „count“ können Sie weitere Informationen über Zustand und Kapazität der Cluster-Komponenten abrufen.

- **Knoten**

  Zeigt die Anzahl, die Kapazität und den Systemzustand der Nodes an, die zum ausgewählten Cluster gehören. Kapazität gibt die nutzbare Gesamtkapazität über die verfügbare Kapazität an.

- **Storage Virtual Machines**

  Zeigt die Anzahl der SVMs an, die zum ausgewählten Cluster gehören.

- **Aggregate**

  Zeigt die Anzahl, Kapazität und den Systemzustand der Aggregate an, die zum ausgewählten Cluster gehören.

Bereich „Verwandte Gruppen“

Mit können Sie die Liste der Gruppen anzeigen, die den ausgewählten Cluster enthalten.

Bereich „Verwandte Warnungen“

Im Teilfenster „Related Alerts“ können Sie die Liste der Meldungen für das ausgewählte Cluster anzeigen. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Systemzustand/Knoten-Inventar Seite

Auf der Seite „Systemzustand/Nodes-Inventar“ können Sie detaillierte Informationen zu den Nodes in einem ausgewählten Cluster anzeigen.

Befehlsschaltfläche

- **Export**

  Ermöglicht das Exportieren der Details aller überwachten Knoten in kommagetrennte Werte (`.csv`) Datei.

Liste der Knoten

In der Liste Nodes werden die Eigenschaften aller erkannten Nodes in einem Cluster angezeigt. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen.

- **Status**

  Ein Symbol, das den aktuellen Status des Knotens identifiziert. Der Status kann kritisch sein (), Fehler (), Warnung (Oder normal ().

  Sie können den Mauszeiger über das Symbol positionieren, um weitere Informationen zu dem für den Node generierten Ereignis oder Ereignis anzuzeigen.

- **Knoten**

  Der Name des Node.

- **Bundesland**

  Der Status des Node. Der Status kann aktiv oder Inaktiv sein.

- **HA-Zustand**

  Der Status des HA-Paars. Der Status kann „Fehler“, „Warnung“, „Normal“ oder „nicht zutreffend“ lauten.

- **Stillzeit**

  Die verstrichene Zeit oder der Zeitstempel seit dem Offline-Status des Node. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel des Offline-Status des Node angezeigt.

- * Cluster*

  Der Name des Clusters, zu dem der Node gehört.

- **Modell**

  Das Modell des Node.

- **Betriebssystemversion**

  Die Softwareversion von ONTAP, auf der der Node ausgeführt wird.

- * All Flash Optimiert*

  Gibt an, ob der Node nur für die Unterstützung von Solid State-Laufwerken (SSDs) optimiert ist

- **Seriennummer**

  Die Seriennummer des Node.

- **Firmware-Version**

  Die Versionsnummer der Firmware des Node.

- **Eigentümer**

  Der Name des Eigentümers des Node.

- **Lage**

  Der Speicherort des Node.

- **Verwendete Gesamtkapazität**

  Die Menge an Speicherplatz, der in den Aggregaten des Node für Daten verwendet wird.

- **Gesamtkapazität**

  Der insgesamt für Daten in den Aggregaten des Node verfügbare Speicherplatz.

- **Nutzbare Ersatzkapazität**

  Die Menge an verfügbarem Speicherplatz im Node, der zur Verbesserung der Aggregatskapazität verwendet werden kann.

- **Nutzbare Rohkapazität**

  Die Menge an Speicherplatz, der im Node nutzbar ist.

- **Gesamtbruttokapazität**

  Die Kapazität jeder nicht formatierten Festplatte im Knoten vor der richtigen Dimensionierung und RAID-Konfiguration.

- **SVM-Anzahl**

  Die Anzahl der SVMs im Cluster

- * FC Port Anzahl*

  Die Anzahl der vom Node enthaltenen FC-Ports.

- **FCoE Port Anzahl**

Die Anzahl der vom Node enthaltenen FCoE-Ports.

- * Anzahl Ethernet-Ports*

  Die Anzahl der vom Node enthaltenen ethernet-Ports.

- **Flash-Kartengröße**

  Die Größe der auf dem Node installierten Flash-Karten.

- * Anzahl Der Flash-Karten*

  Die Anzahl der auf dem Node installierten Flash-Karten.

- * Anzahl Festplatten-Shelfs*

  Die Anzahl der vom Node enthaltenen Platten-Shelfs.

- * Datenträgeranzahl*

  Die Anzahl der Festplatten im Node.

Bereich Filter

Im Bereich Filter können Sie Filter einstellen, um die Art und Weise anzupassen, wie Informationen in der Liste der Knoten angezeigt werden. Sie können Filter für die Spalten Status, Zustand und HA-Status auswählen.

Die im Fensterbereich Filter angegebenen Filter überschreiben die Filter, die für die Spalten in der Liste Knoten angegeben sind.

Systemzustand/Aggregate Inventarseite

Auf der Seite „Systemzustand/Aggregate Inventory“ werden Informationen zu den überwachten Aggregaten angezeigt und Sie können die Schwellenwerteinstellungen anzeigen und ändern.

Befehlsschaltflächen

- **Schwellenwerte Bearbeiten**

  Zeigt das Dialogfeld „Aggregat-Schwellenwerte bearbeiten“ an, in dem Sie die Schwellenwerteinstellungen für einen oder mehrere Aggregate bearbeiten können.

- **Export**

  Ermöglicht das Exportieren der Details aller überwachten Aggregate in kommagetrennte Werte (`.csv`) Datei.

Aggregatliste

Zeigt die Eigenschaften aller erkannten Aggregate im Tabellenformat an. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen:

- **Status**

  Der aktuelle Status des Aggregats. Der Status kann kritisch sein (), Fehler (), Warnung (Oder normal ()).

  Sie können den Zeiger auf den Status verschieben, um weitere Informationen zu dem für das Aggregat generierten Ereignis oder Ereignissen anzuzeigen.

  Wenn der Status des Aggregats durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen wurde, und die Ursache des Ereignisses anzeigen. Sie können auf die Schaltfläche **Details anzeigen** klicken, um weitere Informationen über die Veranstaltung anzuzeigen.

  Wenn der Status des Aggregats durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen angezeigt, z. B. Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst werden, und der Name des Administrators, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

- * Aggregat*

  Der Name des Aggregats.

  Sie können den Zeiger auf ein Aggregat verschieben, um Informationen wie das letzte erzeugte Ereignis, den Node mit Aggregat, RAID-Typ, Snapshot Reserve, Snapshot Kopien und dem im Aggregat zugewiesenen Speicherplatz anzuzeigen. Sie können auch die Anzahl der derzeit laufenden Volume-Verschiebungen anzeigen.

- **Bundesland**

  Der aktuelle Status des Aggregats:

  - Offline

    Lese- oder Schreibzugriff ist nicht zulässig.

  - Online

    Lese- und Schreibzugriff auf Volumes in diesem Aggregat ist zulässig.

  - Eingeschränkt

    Begrenzte Vorgänge, wie etwa die Paritätsrekonstruktion, sind zulässig, der Datenzugriff jedoch nicht.

  - Wird Erstellt

    Das Aggregat wird erstellt.

  - Zerstören

    Das Aggregat wird zerstört.

  - Fehlgeschlagen

Das Aggregat kann nicht online gebracht werden.

- Eingefroren

  Das Aggregat bedient (vorübergehend) keine Anforderungen.

- Uneinheitlich

  Das Aggregat wurde als beschädigt markiert; wenden Sie sich an den technischen Support.

- Eisenbeschränkungen

  Diagnosetools können nicht auf dem Aggregat ausgeführt werden.

- Montage

  Das Aggregat wird angehängt.

- Teilweise

  Mindestens eine Festplatte für das Aggregat gefunden wurde, aber zwei oder mehr Disketten fehlen.

- Stillgelegt

  Das Aggregat wird stillgelegt.

- Wird Stillgelegt

  Das Aggregat wird stillgelegt.

- Umgekehrt

  Die Umkehroperation des Aggregats ist abgeschlossen.

- Nicht Abgehängt

  Das Aggregat ist offline.

- Entmounten

  Das Aggregat wird offline geschaltet.

- Unbekannt

  Gibt an, dass das Aggregat erkannt wird, die Aggregatinformationen jedoch noch nicht vom Unified Manager-Server abgerufen werden.

- **Knoten**

  Der Name des Storage Controllers, der das Aggregat enthält.

- **Spiegelstatus**

  Der Mirror-Status des Aggregats:

  - Gespiegelt

Die aggregierten Plex-Daten werden gespiegelt.

- Spiegelung beeinträchtigt

  Die aggregierten Plex-Daten können nicht gespiegelt werden.

- Spiegelung wird neu synchronisiert

  Die aggregierten Plex-Daten werden gespiegelt.

- Fehlgeschlagen

  Die Plex-Datenspiegelung des Aggregats ist fehlgeschlagen.

- Ungültige Konfiguration

  Der anfängliche Status, bevor ein Aggregat erstellt wird.

- Nicht Initialisiert

  Das Aggregat wird erstellt.

- Nicht Gespiegelt

  Das Aggregat wird nicht gespiegelt.

- CP-Zählprüfung wird durchgeführt

  Das Aggregat wurde assimiliert und Unified Manager prüft, ob die CP für die Plexe ähnlich ist.

- Limbo

  Es gibt ein Problem mit den Aggregat-Etiketten. Das ONTAP System erkennt das Aggregat, kann aber das Aggregat nicht genau assimilieren.

- Erfordert eine CP-Zählprüfung

  Das Aggregat ist assimiliert, aber die CP wird auf beiden Plexen gezählt, noch nicht.

Wenn sich ein Aggregat im Status „Mirror_Resynchronisierung“ befindet, wird zudem der Resynchronisierungsprozentsatz angezeigt.

- * Im Übergang*

  Ob die Migration im Aggregat abgeschlossen ist oder nicht.

- **Typ**

  Der Aggregattyp:

  - HDD
  - Hybrid

    Kombiniert HDDs und SSDs, aber Flash Pool wurde nicht aktiviert.

- Hybrid (Flash Pool)

  Kombiniert HDDs und SSDs und ermöglicht die Aktivierung von Flash Pool.

- SSD
- SSD (FabricPool)

  Kombiniert SSDs mit einer Cloud-Tier

- VMDisk (SDS)

  Virtuelle Laufwerke innerhalb einer virtuellen Maschine

- VMDisk (FabricPool)

  Kombiniert virtuelle Festplatten mit einer Cloud-Tier

- LUN (FlexArray) bei Standardfestplatten und SSD-Festplatten ist diese Spalte leer, wenn auf dem überwachten Speichersystem eine ONTAP-Version vor 8.3 ausgeführt wird.

- **SnapLock Typ**

  Der SnapLock-Typ für das Aggregat. Mögliche Werte sind Compliance, Enterprise, Non-SnapLock.

- **Genutzte Datenkapazität**

  Die Menge an Speicherplatz, der für Daten im Aggregat verwendet wird.

- **Verwendete Daten %**

  Der Prozentsatz des für Daten im Aggregat genutzten Speicherplatzes.

- **Verfügbare Datenkapazität**

  Die Menge an Speicherplatz, der für Daten im Aggregat verfügbar ist.

- * Verfügbare Daten %*

  Der Prozentsatz des verfügbaren Speicherplatzes für Daten im Aggregat.

- **Gesamtkapazität Der Daten**

  Die Gesamtdatengröße des Aggregats.

- * Engagierte Kapazität*

  Den insgesamt für alle Volumes im Aggregat zugesagt wurde.

  Wenn Autogrow auf Volumes im Aggregat aktiviert ist, basiert die engagierte Kapazität auf der maximal zulässigen Volume-Größe, die mit Autogrow festgelegt ist, nicht auf der ursprünglichen Volume-Größe. Bei FabricPool Aggregaten ist dieser Wert nur für die lokale oder Performance-Ebene bzw. Kapazität relevant. Der im Cloud-Tier verfügbare Speicherplatz wird in diesem Wert nicht berücksichtigt.

- **Speicherersparnis**

  Das Storage-Effizienz-Verhältnis basiert auf dem logischen Gesamtspeicherplatz, der zum Speichern der

Daten verwendet wird, und dem physischen Speicherplatz, der zum Speichern der Daten unter Einsatz der ONTAP Storage-Effizienztechnologien erforderlich wäre.

Dieses Feld wird nur dann befüllt, wenn auf dem überwachten Speichersystem ONTAP Version 9.0 oder höher ausgeführt wird, und nur für Aggregate ohne Root-Root.

- **RAID-Typ**

  Der RAID-Konfigurationstyp:

  - RAID 0: Alle RAID-Gruppen sind vom Typ RAID 0.
  - RAID 4: Alle RAID Gruppen sind vom Typ RAID 4.
  - RAID-DP: Alle RAID-Gruppen vom Typ RAID-DP.
  - RAID-TEC: Alle RAID Gruppen sind vom Typ RAID-TEC.
  - Gemischtes RAID: Das Aggregat enthält RAID-Gruppen unterschiedlicher RAID-Typen (RAID 0, RAID 4, RAID-DP und RAID-TEC).

- **Cloud Tier Verwendeter Platz**

  Der Speicherplatz, der im Cloud-Tier verwendet wird; wenn das Aggregat ein FabricPool Aggregat ist.

Bereich Filter

Mit können Sie Filter festlegen, um die Art und Weise anzupassen, wie Informationen in der Liste der Aggregate angezeigt werden. Sie können Filter für die Spalte Status auswählen.

Die im Fensterbereich Filter angegebenen Filter überschreiben die für die Spalten in der Liste Aggregate angegebenen Filter.

Systemzustand/Aggregate Kapazitäts- und Auslastungsseite

Auf der Seite Systemzustand/Aggregate Kapazität und Auslastung können Sie Informationen über die Kapazität und Auslastung von Aggregaten in allen Clustern anzeigen. Diese Informationen geben Ihnen die Möglichkeit, mögliche Kapazitätsrisiken zu verstehen und die konfigurierte, genutzte und nicht genutzte Kapazität von Aggregaten anzuzeigen.

Verwenden Sie die Schaltfläche **Export**, um die Details aller überwachten Aggregate in kommagetrennte Werte zu exportieren (`.csv`) Datei.

- * Cluster*

  Der Cluster-Name.

- **HA-Paar**

  Der HA-Paar-Wert, der durch die Bildung von zwei Nodes ermittelt wird.

- * Aggregat*

  Der Name des Aggregats.

- **Gesamtkapazität Der Daten**

  Die Gesamtkapazität (genutzter plus verfügbarer) Daten.

- **Genutzte Datenkapazität**

  Der verwendeten Datenkapazität.

- **Verwendete Daten %**

  Die genutzte Datenkapazität als Prozentsatz.

- **Verfügbare Datenkapazität**

  Die verfügbare Datenkapazität.

- * Verfügbare Daten %*

  Die verfügbare Datenkapazität als Prozentsatz.

- * Tägliche Zuwachsrate %*

  Die Wachstumsrate, die alle 24 Stunden im Aggregat stattfindet.

- **Tage Bis Voll**

  Die geschätzte Anzahl der verbleibenden Tage, bevor das Aggregat die volle Kapazität erreicht.

- **Space Full Threshold %**

  Der Prozentsatz, an dem ein Aggregat als voll erachtet wird.

- **Space Fast Voll Schwellenwert %**

  Der Prozentsatz, bei dem ein Aggregat als fast voll erachtet wird.

- **Schwellenwert Der Wachstumsrate**

  Die Wachstumsrate des Aggregats, die als normal angesehen wird, bevor das System ein ungewöhnliches Ereignis für die aggregierte Wachstumsrate generiert.

- **Schwellenwert Für Die Empfindlichkeit Der Wachstumsrate**

  Der Faktor, der auf die Standardabweichung der Wachstumsrate eines Aggregats angewendet wird. Wenn die Wachstumsrate die faktorierte Standardabweichung überschreitet, wird ein ungewöhnliches Ereignis für die aggregierte Wachstumsrate generiert.

- **Tage Bis Zur Vollständigen Schwelle**

  Die Anzahl der verbleibenden Tage, bevor das Aggregat die volle Kapazität erreicht.

- **Snapshot Reserve Gesamtkapazität**

  Die Gesamtkapazität der Snapshot-Reserve des Aggregats.

- **Verwendete Snapshot-Reserve Kapazität**

Die Menge an Speicherplatz, der von Snapshot-Kopien aus der Snapshot Reserve verwendet wird.

- **Snapshot Reserve Verwendet %**

  Die Menge an Speicherplatz, den Snapshot Kopien aus der Snapshot Reserve als Prozentsatz verwendet haben.

- **Snapshot Reserve Verfügbare Kapazität**

  Die Menge an Speicherplatz, der für Snapshot-Kopien verfügbar ist.

- **Snapshot Reserve Verfügbar %**

  Die Menge an Speicherplatz, die für Snapshot Kopien als Prozentsatz verfügbar ist.

- **Snapshot Kopien Reservieren Voller Schwellenwert %**

  Der Prozentsatz, an dem ein Aggregat seinen gesamten reservierten Speicherplatz für Snapshot Kopien verbraucht hat.

- **Überengagierte Kapazität %**

  Die Gesamtüberbelegung als Prozentsatz.

- **Überbeplante Schwelle %**

  Der Prozentsatz, an dem ein Aggregat als überengagiert erachtet wird.

- **Nahezu Überhöhte Schwelle %**

  Der Prozentsatz, an dem ein Aggregat als nahezu überengagiert angesehen wird.

- **Aggregattyp**

  Der Aggregattyp:

  - HDD
  - Hybrid

    Kombiniert HDDs und SSDs, aber Flash Pool wurde nicht aktiviert.

  - Hybrid (Flash Pool)

    Kombiniert HDDs und SSDs und ermöglicht die Aktivierung von Flash Pool.

  - SSD
  - SSD (FabricPool)

    Kombiniert SSDs mit einer Cloud-Tier

  - VMDisk (SDS)

    Virtuelle Laufwerke innerhalb einer virtuellen Maschine

  - VMDisk (FabricPool)

Kombiniert virtuelle Festplatten mit einer Cloud-Tier

- LUN (FlexArray) bei Standardfestplatten und SSD-Festplatten ist diese Spalte leer, wenn auf dem überwachten Speichersystem eine ONTAP-Version vor 8.3 ausgeführt wird.

- **RAID-Typ**

  Der RAID-Konfigurationstyp.

- **Gesamtzustand**

  Der aktuelle Status des Aggregats.

- **SnapLock Typ**

  Gibt an, ob es sich um ein SnapLock Aggregat oder ein nicht-SnapLock Aggregat handelt.

- **Cloud Tier Verwendeter Platz**

  Die Datenmenge, die aktuell im Cloud-Tier verwendet wird.

- * Cloud Tier*

  Der Name des Cloud-Tier-Objektspeichers beim Erstellen von ONTAP.

Angaben zum Systemzustand/Aggregat

Sie können auf der Seite „Systemzustand/Aggregat-Details“ detaillierte Informationen über das ausgewählte Aggregat anzeigen, z. B. Kapazität, Festplatteninformationen, Konfigurationsdetails und erzeugte Ereignisse. Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für das Aggregat anzeigen.

Befehlsschaltflächen

> Bei der Überwachung eines FabricPool-fähigen Aggregats gelten die überzugesund auf dieser Seite überzuschichtenden Werte nur für die lokale Kapazität oder das Performance-Tier. Der auf dem Cloud-Tier verfügbare Speicherplatz wird nicht in den überengagierten Werten dargestellt. Ebenso gelten die Werte für die Aggregatschwellenwerte nur für die lokale Performance-Tier.

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

- **Wechseln Sie zur Leistungsansicht**

  Ermöglicht Ihnen die Navigation zur Seite mit den Details zu Performance/Aggregat.

-

  Ermöglicht Ihnen das Hinzufügen des ausgewählten Aggregats zum Favoriten-Dashboard.

- **Aktionen**
  - Alarm Hinzufügen

    Ermöglicht Ihnen das Hinzufügen einer Warnung zum ausgewählten Aggregat.

◦ Schwellenwerte Bearbeiten

Ermöglicht Ihnen das Ändern der Schwellenwerteinstellungen für das ausgewählte Aggregat.

- **Aggregate Anzeigen**

Ermöglicht Ihnen die Navigation zur Seite „Bestandsaufnahme“/„Systemzustand“/„Aggregate“.

Registerkarte „Kapazität“

Auf der Registerkarte Kapazität werden ausführliche Informationen zum ausgewählten Aggregat, z. B. Kapazität, Schwellenwerte und tägliche Wachstumsrate, angezeigt.

Standardmäßig werden Kapazitätsereignisse nicht für die Root-Aggregate generiert. Darüber hinaus gelten die von Unified Manager verwendeten Schwellenwertwerte nicht für die Root-Aggregate der Nodes. Nur ein Mitarbeiter des technischen Supports kann die Einstellungen für diese zu erstellenden Ereignisse ändern. Wenn die Einstellungen von einem Mitarbeiter des technischen Supports geändert werden, werden die Schwellenwerte auf das Root-Aggregat des Nodes angewendet.

- * Kapazität*

Zeigt das Datenkapazitätsdiagramm und das Diagramm Snapshot Kopien an, in dem Kapazitätsdetails zum Aggregat angezeigt werden:

◦ Verwendet

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

◦ Überengagiert

Gibt an, dass der Speicherplatz im Aggregat zu hoch belegt ist.

◦ Warnung

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

◦ Fehler

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

◦ Datendiagramm

Zeigt die Gesamtkapazität und die genutzte Datenkapazität des Aggregats an. Wenn das Aggregat zu hoch eingestellt ist, wird ein Flag mit der überzuviel Kapazität angezeigt.

◦ Diagramm Snapshot Kopien

Dieses Diagramm wird nur angezeigt, wenn die verwendete Snapshot-Kapazität oder die Snapshot-Reserve nicht null ist.

Beide Diagramme zeigen die Kapazität an, in der die Snapshot-Kapazität die Snapshot-Reserve überschreitet, wenn die genutzte Snapshot-Kapazität die Snapshot-Reserve überschreitet.

- * Cloud Tier*

  Zeigt Kapazitätsdetails über das Cloud-Tier für FabricPool-fähige Aggregate an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

  - Verwendet

    Zeigt den Speicherplatz an, der von Daten im Cloud-Tier verwendet wird.

  - Nicht Verfügbar

    Zeigt den Speicherplatz in der Cloud-Tier für ein Objekt aus Amazon S3, Microsoft Azure Cloud FabricPool oder IBM Cloud Object Storage an, das nicht verwendet werden kann. Dieser Speicherplatz kann mit einem anderen FabricPool-fähigen Aggregat gemeinsam genutzt werden.

  - Datendiagramm

    Bei Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage oder Alibaba Cloud Object Storage werden die Gesamtkapazität, die von diesem Cluster lizenziert wurde, die von diesem Aggregat verwendete Menge und die nicht nutzbare Menge von anderen Aggregaten, die die Cloud-Tier verwenden, in der Übersicht angezeigt.

  Bei einer StorageGRID wird nur die von diesem Aggregat genutzte Gesamtkapazität angezeigt.

- **Details**

  Zeigt detaillierte Informationen zur Kapazität an.

  - Gesamtkapazität

    Zeigt die Gesamtkapazität im Aggregat an.

  - Datenkapazität

    Zeigt den vom Aggregat (genutzte Kapazität) verwendeten Speicherplatz und die Menge des verfügbaren Speicherplatzes im Aggregat an (freie Kapazität).

  - Snapshot-Reserve

    Zeigt die verwendete und freie Snapshot Kapazität des Aggregats an.

  - Überzuviel Kapazität

    Zeigt die Überbelegung des Aggregats an. Aufgrund einer Überbelegung von Aggregaten bieten Sie mehr Storage, als tatsächlich in einem bestimmten Aggregat verfügbar ist, sofern nicht alle Storage-Ressourcen derzeit verwendet werden. Bei Nutzung von Thin Provisioning kann die Gesamtgröße der Volumes im Aggregat die Gesamtkapazität des Aggregats überschreiten.

    > Wenn Sie Ihr Aggregat zu hoch ansetzen, müssen Sie den verfügbaren Speicherplatz sorgfältig überwachen und Storage nach Bedarf hinzufügen, um Schreibfehler aufgrund von unzureichendem Speicherplatz zu vermeiden.

  - Cloud-Tier

    Bei Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage oder Alibaba Cloud Object Storage

werden die gesamte lizenzierte Kapazität, die durch dieses Aggregat benötigte Menge, die in anderen Aggregaten benötigte Menge und die freie Kapazität für das Cloud-Tier angezeigt. Bei einer StorageGRID wird nur die von diesem Aggregat genutzte Gesamtkapazität angezeigt.

- Cache-Speicherplatz Insgesamt

  Zeigt den gesamten Speicherplatz der Solid State-Laufwerke (SSDs) bzw. Zuweisungseinheiten an, die einem Flash Pool Aggregat hinzugefügt werden. Wenn Sie Flash Pool für ein Aggregat aktiviert, aber keine SSDs hinzugefügt haben, wird der Cache-Speicherplatz als 0 KB angezeigt.

  Dieses Feld ist ausgeblendet, wenn Flash Pool für ein Aggregat deaktiviert ist.

- Schwellenwerte Für Aggregate

  Zeigt die folgenden Kapazitätsschwellenwerte für das Aggregat an:

  - Nahezu Vollständig. Schwellenwert

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

  - Vollständiger Schwellenwert

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

  - Nahezu Überbeanspruchung Des Schwellenwerts

    Gibt den Prozentsatz an, mit dem ein Aggregat fast überbelegt ist.

  - Überbeanspruchung Des Schwellenwerts

    Gibt den Prozentsatz an, zu dem ein Aggregat überengagiert ist.

- Weitere Details: Tägliche Wachstumsrate

  Zeigt den im Aggregat verwendeten Festplattenspeicher an, wenn die Änderungsrate zwischen den letzten beiden Proben 24 Stunden andauert.

  Wenn ein Aggregat beispielsweise 10 GB Festplattenspeicher bei 2:00 Uhr und 12 GB bei 6:00 Uhr nutzt, beträgt die tägliche Wachstumsrate (GB) für dieses Aggregat 2 GB.

- Volume-Verschiebung

  Zeigt die Anzahl der aktuell laufenden Volume-Move-Vorgänge an:

  - Volumes Aus

    Zeigt die Anzahl und Kapazität der Volumes an, die aus dem Aggregat verschoben werden.

  Über den Link können Sie weitere Details anzeigen, beispielsweise den Volume-Namen, die Aggregate, zu denen das Volume verschoben wird, den Status der Verschiebung eines Volumes und die geschätzte Endzeit.

  - Volumes In

    Zeigt die Anzahl und die verbleibende Kapazität der Volumes an, die in das Aggregat verschoben werden.

Über den Link können Sie weitere Details anzeigen, beispielsweise den Volume-Namen, das Aggregat, aus dem das Volume verschoben wird, den Status der Verschiebung des Volumes und die geschätzte Endzeit.

  - Geschätzte genutzte Kapazität nach der Verschiebung eines Volumes

    Zeigt den geschätzten belegten Speicherplatz (in Prozent und in KB, MB, GB usw.) im Aggregat an, nachdem die Verschiebevorgänge des Volumes abgeschlossen sind.

- **Kapazitätsüberblick - Volumen**

  Zeigt Diagramme an, die Informationen zur Kapazität der Volumes im Aggregat enthalten sind. Es wird die Menge an Speicherplatz angezeigt, die vom Volume (genutzte Kapazität) und die Menge des verfügbaren Speicherplatzes (freie Kapazität) im Volume verwendet wird. Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, wird die vom Volume verwendete Menge an Speicherplatz (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht verwendet werden kann (nicht nutzbare Kapazität), da die Kapazität des Aggregats angezeigt wird.

  Sie können das anzuangezeigte Diagramm in den Dropdown-Listen auswählen. Sie können die im Diagramm angezeigten Daten sortieren, um Details wie die genutzte Größe, die bereitgestellte Größe, die verfügbare Kapazität, die schnellste tägliche Wachstumsrate und die langsamste Wachstumsrate anzuzeigen. Sie können die Daten auf Grundlage der Storage Virtual Machines (SVMs) filtern, die die Volumes im Aggregat enthalten. Sie können auch Details zu Volumes anzeigen, die über Thin Provisioning bereitgestellt wurden. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den Bereich von Interesse positionieren. Standardmäßig werden im Diagramm die Top 30 der gefilterten Volumes im Aggregat angezeigt.

Registerkarte „Festplatteninformationen“

Zeigt detaillierte Informationen zu den Festplatten im ausgewählten Aggregat an, einschließlich RAID-Typ und -Größe sowie Typ der im Aggregat verwendeten Festplatten. Auf der Registerkarte werden auch die RAID-Gruppen und die verwendeten Festplatten (z. B. SAS, ATA, FCAL, SSD oder VMDISK) grafisch dargestellt. Weitere Informationen, wie z. B. der Schacht, das Shelf und die Drehgeschwindigkeit der Festplatte, können Sie mit dem Cursor über die Parity-Festplatten und die Daten-Festplatten anzeigen.

- * Daten*

  Grafische Anzeige von Details zu dedizierten Datenträgern, freigegebenen Datenträgern oder beidem. Wenn die Datenfestplatten freigegebene Laufwerke enthalten, werden grafische Details der freigegebenen Laufwerke angezeigt. Wenn die Datenfestplatten dedizierte Laufwerke und freigegebene Festplatten enthalten, werden grafische Details sowohl der dedizierten Datenlaufwerke als auch der freigegebenen Datenträger angezeigt.

  - **RAID-Details**

    RAID-Details werden nur für dedizierte Festplatten angezeigt.

    - Typ

      Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

    - Gruppengröße

      Zeigt die maximale Anzahl an Laufwerken an, die in der RAID-Gruppe zulässig sind.

        - Gruppen

          Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

    - **Verwendete Festplatten**
        - Effektiver Typ

          Zeigt die Typen der Datenfestplatten an (z. B. ATA, SATA, FCAL, SSD, Oder VMDISK) im Aggregat.

        - Datenfestplatten

          Zeigt die Anzahl und Kapazität der Datenfestplatten an, die einem Aggregat zugewiesen sind. Details zur Datenfestplatte werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Festplatten enthält.

        - Parity-Festplatten

          Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat zugewiesen werden. Details zur Parity-Festplatte werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Festplatten enthält.

        - Gemeinsame Festplatten

          Zeigt die Anzahl und Kapazität der freigegebenen Datenfestplatten an, die einem Aggregat zugewiesen sind. Details zu gemeinsam genutzten Festplatten werden nur angezeigt, wenn das Aggregat freigegebene Festplatten enthält.

    - **Ersatzfestplatten**

      Zeigt den effektiven Typ, die Nummer und die Kapazität der Ersatzfestplatten an, die für den Knoten im ausgewählten Aggregat verfügbar sind.

      Bei einem Failover eines Aggregats an den Partner-Node zeigt Unified Manager nicht alle freien Festplatten an, die mit dem Aggregat kompatibel sind.

- **SSD Cache**

  Enthält Details zu dedizierten Cache-SSD-Festplatten und Shared Cache SSD-Festplatten.

  Für die dedizierten Cache-SSD-Festplatten werden folgende Details angezeigt:

    - **RAID-Details**
        - Typ

          Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

        - Gruppengröße

          Zeigt die maximale Anzahl an Laufwerken an, die in der RAID-Gruppe zulässig sind.

        - Gruppen

          Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

- **Verwendete Festplatten**
  - Effektiver Typ

    Gibt an, dass die Festplatten, die für den Cache im Aggregat verwendet werden, vom Typ SSD sind.

  - Datenfestplatten

    Zeigt die Anzahl und Kapazität der Datenfestplatten an, die einem Aggregat für den Cache zugewiesen werden.

  - Parity-Festplatten

    Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat für den Cache zugewiesen werden.

- **Ersatzfestplatten**

  Zeigt den effektiven Typ, die Nummer und die Kapazität der Ersatzfestplatten an, die für den Knoten im ausgewählten Aggregat für den Cache verfügbar sind.

  Bei einem Failover eines Aggregats an den Partner-Node zeigt Unified Manager nicht alle freien Festplatten an, die mit dem Aggregat kompatibel sind.

  Enthält die folgenden Details für den gemeinsamen Cache:

- **Speicherpool**

  Zeigt den Namen des Speicherpools an. Sie können den Zeiger über den Speicherpool-Namen verschieben, um folgende Details anzuzeigen:

  - Status

    Zeigt den Status des Speicherpools an, der gesund oder ungesund sein kann.

  - Gesamtzuweisungen

    Zeigt die Gesamtzuordnungseinheiten und die Größe im Speicherpool an.

  - Größe Der Zuordnungseinheit

    Zeigt den minimalen Speicherplatz im Speicherpool an, der einem Aggregat zugewiesen werden kann.

  - Festplatten

    Zeigt die Anzahl der Laufwerke an, die zum Erstellen des Speicherpools verwendet werden. Wenn die Anzahl der Laufwerke in der Spalte „Speicherpool“ und die Anzahl der Festplatten, die auf der Registerkarte „Laufwerksinformationen“ für diesen Speicherpool angezeigt werden, nicht übereinstimmen, zeigt dies an, dass eine oder mehrere Festplatten beschädigt sind und der Speicherpool ungesund ist.

  - Zuweisung Verwendet

    Zeigt Anzahl und Größe der von den Aggregaten verwendeten Zuordnungseinheiten an. Sie

können auf den Aggregatnamen klicken, um Details zum Aggregat anzuzeigen.

- Verfügbare Zuweisung

  Zeigt die Anzahl und Größe der für die Nodes verfügbaren Zuweisungseinheiten an. Sie können auf den Node-Namen klicken, um weitere Details zum Aggregat anzuzeigen.

- **Zugewiesener Cache**

  Zeigt die Größe der vom Aggregat verwendeten Zuordnungseinheiten an.

- **Zuordnungseinheiten**

  Zeigt die Anzahl der vom Aggregat verwendeten Zuordnungseinheiten an.

- **Festplatten**

  Zeigt die Anzahl der Festplatten im Speicherpool an.

- **Details**
  - Storage-Pool

    Zeigt die Anzahl der Speicherpools an.

  - Gesamtgröße

    Zeigt die Gesamtgröße der Speicherpools an.

- * Cloud Tier*

  Zeigt den Namen des Cloud-Tiers an, sofern Sie ein FabricPool-fähiges Aggregat konfiguriert haben und die gesamte lizenzierte Kapazität für Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage oder Alibaba Cloud Object Storage Objekte anzeigt.

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration werden Details zum ausgewählten Aggregat angezeigt, z. B. hinsichtlich seines Cluster-Nodes, des Blocktyps, des RAID-Typs, der RAID-Größe und der Anzahl der RAID-Gruppen:

- **Übersicht**
  - Knoten

    Zeigt den Namen des Node an, der das ausgewählte Aggregat enthält.

  - Blocktyp

    Zeigt das Blockformat des Aggregats an: Entweder 32-Bit oder 64-Bit.

  - RAID-Typ

    Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP, RAID-TEC oder gemischtes RAID).

  - RAID-Größe

    Zeigt die Größe der RAID-Gruppe an.

- RAID-Gruppen

  Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

- SnapLock-Typ

  Zeigt den SnapLock-Typ des Aggregats an.

- * Cloud Tier*

  Wenn es sich um ein FabricPool-fähiges Aggregat handelt, werden die Details für den Objektspeicher angezeigt. Je nach Speicheranbieter sind einige Felder unterschiedlich:

  - Name

    Zeigt den Namen des Objektspeichers an, als er von ONTAP erstellt wurde.

  - Objekt-Storage-Provider

    Zeigt den Namen des Storage-Providers an, z. B. StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud oder Alibaba Cloud Object Storage.

  - Objektspeichername (FQDN) oder Servername

    Zeigt den FQDN des Objektspeichers an.

  - Auf Schlüssel oder Konto zugreifen

    Zeigt den Zugriffsschlüssel oder das Konto für den Objektspeicher an.

  - Bucket-Name oder Container-Name

    Zeigt den Bucket- oder Container-Namen des Objektspeichers an.

  - SSL

    Zeigt an, ob die SSL-Verschlüsselung für den Objektspeicher aktiviert ist.

Historienbereich

Im Bereich Verlauf werden Diagramme angezeigt, die Informationen über die Kapazität des ausgewählten Aggregats enthalten. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Verlaufsdiagramme können Ihnen bei der Identifizierung von Trends helfen: Wenn beispielsweise die Aggregatnutzung konsistent den Schwellenwert „nahezu voll“ überschreitet, können Sie die entsprechenden Maßnahmen ergreifen.

Verlaufsdiagramme zeigen folgende Informationen an:

- **Verwendete Aggregatskapazität (%)**

  Zeigt die verwendete Kapazität im Aggregat und den Trend in der Art und Weise an, wie die aggregierte

Kapazität basierend auf dem Nutzungsverlauf als Liniendiagramme in Prozentsätzen auf der vertikalen (y) Achse verwendet wird. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Kapazität verwendet“ klicken, wird die Diagramm-Zeile mit der verwendeten Kapazität ausgeblendet.

- **Verwendete Aggregatskapazität vs Gesamtkapazität**

  Zeigt den Trend in der Verwendung der Aggregatskapazität basierend auf dem Nutzungsverlauf sowie der verwendeten Kapazität und der Gesamtkapazität als Liniendiagramme in Byte, Kilobyte, Megabyte, Und so weiter, auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „verwendete Trend-Kapazität“ klicken, wird das Diagramm „verwendete Trendkapazität“ ausgeblendet.

- **Verwendete Aggregatskapazität (%) gegenüber dem Einsatz (%)**

  Zeigt den Trend an, wie die aggregierte Kapazität basierend auf dem Nutzungsverlauf verwendet wird, sowie den belegten Speicherplatz als Liniendiagramme in Prozent auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Space engagierte“ klicken, wird die Zeile „Space engagierte“ ausgeblendet.

Ereignisliste

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

- **Severity**

  Zeigt den Schweregrad des Ereignisses an.

- **Veranstaltung**

  Zeigt den Ereignisnamen an.

- **Auslösezeit**

  Zeigt die Zeit an, die seit der Erzeugung des Ereignisses verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel für den Zeitpunkt angezeigt, zu dem das Ereignis generiert wurde.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie den Clusterknoten, Volumes und Festplatten anzeigen, die mit dem Aggregat in Verbindung stehen:

- **Knoten**

Zeigt die Kapazität und den Integritätsstatus des Node an, der das Aggregat enthält. Kapazität gibt die nutzbare Gesamtkapazität über die verfügbare Kapazität an.

- **Aggregate im Knoten**

  Zeigt die Anzahl und Kapazität aller Aggregate im Cluster-Node an, der das ausgewählte Aggregat enthält. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt. Wenn z. B. ein Cluster-Node zehn Aggregate enthält, von denen fünf den Warnstatus und die verbleibenden fünf den kritischen Status anzeigen, ist der angezeigte Status „kritisch“.

- **Bände**

  Zeigt die Anzahl und Kapazität der FlexVol Volumes und FlexGroup Volumes im Aggregat an. Die Anzahl umfasst keine FlexGroup-Komponenten. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt.

- **Ressourcen-Pool**

  Zeigt die mit dem Aggregat verbundenen Ressourcen-Pools an.

- **Festplatten**

  Zeigt die Anzahl der Festplatten im ausgewählten Aggregat an.

Bereich „Verwandte Warnungen“

Im Bereich „Related Alerts“ können Sie die Liste der Warnmeldungen anzeigen, die für das ausgewählte Aggregat erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Inventarseite für den Status/Speicher virtueller Maschinen

Auf der Seite „Systemzustand“/„Storage Virtual Machines Inventory“ können Sie detaillierte Informationen zu den von Ihnen überwachten Storage Virtual Machines (SVMs) anzeigen.

Befehlsschaltflächen

- **Export**

  Ermöglicht es Ihnen, die Details aller überwachten SVMs in kommagetrennte Werte zu exportieren (`.csv`) Datei.

- **Anmerkung**

  Hiermit können Sie die ausgewählte Storage Virtual Machine (SVM) kommentieren.

SVMs-Liste

Die Liste der SVMs wird im Tabellenformat die Eigenschaften aller erkannten SVMs angezeigt. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen:

- **Status**

Der aktuelle Status der SVM. Der Status kann kritisch sein (), Fehler (), Warnung (Oder normal ().

Sie können den Zeiger auf den Status verschieben, um weitere Informationen zu dem für die SVM generierten Ereignis oder Ereignissen anzuzeigen.

Wenn der Status der SVM durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugeordnet ist, und die Ursache des Ereignisses anzeigen. Sie können auf die Schaltfläche Details anzeigen klicken, um weitere Informationen zum Ereignis anzuzeigen.

Wenn der Status der SVM durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen angezeigt, z. B. Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst werden, und der Name des Administrators, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link Alle Ereignisse anzeigen klicken, um die Liste der generierten Ereignisse anzuzeigen.

- **Storage Virtual Machine**

  Der Name der SVM.

  Sie können den Zeiger auf jede SVM verschieben, um Informationen wie das letzte erzeugte Ereignis, das Cluster, zu dem die SVM gehört, den Volume-Typ der SVM, die zulässigen Protokolle und den in der SVM zugewiesenen Speicherplatz anzuzeigen. Sie können auch Details zu verwandten Objekten anzeigen, z. B. den Cluster, zu dem die SVM gehört, alle SVMs, die zum Cluster gehören, und die Volumes, die zur SVM gehören.

- **Bundesland**

  Der aktuelle Administrationsstatus der SVM Der Status kann ausgeführt, angehalten, gestartet oder angehalten werden.

- * Cluster*

  Der Name des Clusters, zu dem die SVM gehört.

- **Zulässiger Volumentyp**

  Der Typ des Volumes, der in der SVM erstellt werden kann. Der Typ kann InfiniteVol, FlexVol oder FlexVol/FlexGroup sein.

  Der FlexGroup-Typ ist bei Verwendung von ONTAP 9.1 oder höher zulässig.

- **Verfügbare Datenkapazität**

  Die verfügbare Datenkapazität aller Volumes in der SVM.

- **Gesamtkapazität Der Daten**

  Die Gesamtkapazität aller Volumes in der SVM.

- **Root Volume**

  Der Name des Root-Volumes der SVM.

- **NIS-Status**

  Der Status des Network Information Service (NIS). Der Status kann aktiviert, deaktiviert oder nicht konfiguriert werden.

- **NIS-Domäne**

  Der NIS-Domain-Name. Diese Spalte ist leer, wenn der NIS-Server deaktiviert oder nicht konfiguriert ist.

- **DNS-Status**

  Der Status des Domain Name System (DNS). Der Status kann aktiviert, deaktiviert oder nicht konfiguriert werden.

- **DNS-Domäne**

  Der DNS-Domain-Name.

- **Name Service Switch**

  Der von Hosts gesammelte Informationstyp. Mögliche Werte sind Datei, LDAP oder NIS.

- **LDAP aktiviert**

  Gibt an, ob das LDAP-Protokoll aktiviert ist oder nicht.

- **Erlaubte Protokolle**

  Der Typ der Protokolle, der auf der SVM konfiguriert werden kann. Verfügbare Protokolle sind FC/FCoE, iSCSI, HTTP, NDMP, NVMe, NFS und CIFS.

- **Maximal Zulässige Volumen**

  Die maximal zulässigen Volumes, die auf der SVM konfiguriert werden können.

- **Anzahl Der Volumes**

  Anzahl der Volumes in der SVM

Bereich Filter

Im Bereich Filter können Sie Filter festlegen, um die Art und Weise anzupassen, in der Liste SVMs angezeigt wird. Sie können Filter für die Spalten Status, Zustand und Anmerkung auswählen.

Die im Fensterbereich Filter angegebenen Filter überschreiben die Filter, die für die Spalten in der Liste SVMs angegeben sind.

Detailseite „Systemzustand/Speicher-Virtual Machine“

Auf der Seite Systemzustand/Storage Virtual Machine-Details können Sie detaillierte Informationen zur ausgewählten SVM anzeigen, z. B. Systemzustand, Kapazität, Konfiguration, Datenrichtlinien, logische Schnittstellen (LIFs), LUNs, qtrees sowie Benutzer- und Gruppenkontingente. Sie können auch Informationen zu verwandten

Objekten und zugehörigen Warnmeldungen für die SVM anzeigen.

Es können nur Data SVMs überwacht werden.

Befehlsschaltflächen

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

- **Wechseln Sie zur Leistungsansicht**

  Hiermit können Sie zur Detailseite zu Performance/SVM navigieren.

- **Aktionen**

  - Alarm Hinzufügen

    Hiermit können Sie eine Warnung zur ausgewählten SVM hinzufügen.

  - Schwellenwerte Bearbeiten

    Ermöglicht Ihnen das Bearbeiten der SVM-Schwellenwerte.

    Diese Schaltfläche ist nur aktiviert, wenn sie auf der Registerkarte qtrees oder für eine SVM mit Infinite Volume angezeigt wird.

  - Anmerkungen Hinzufügen

    Ermöglicht Ihnen, die ausgewählte SVM zu kommentieren.

- **Storage Virtual Machines Anzeigen**

  Hier können Sie zur Seite „Health/Storage Virtual Machines Inventory“ navigieren.

Registerkarte Systemzustand

Auf der Registerkarte Systemzustand werden detaillierte Informationen zur Datenverfügbarkeit, Datenkapazität und Sicherung verschiedener Objekte wie Volumes, Aggregate, NAS LIFs, SAN LIFs, LUNs, angezeigt. Protokolle, Services, NFS-Exporte und CIFS-Freigaben.

Sie können auf das Diagramm eines Objekts klicken, um die gefilterte Liste der Objekte anzuzeigen. Beispielsweise können Sie auf das Diagramm für die Volume-Kapazität klicken, das Warnungen anzeigt, um die Liste der Volumes mit Kapazitätsproblemen mit dem Schweregrad „Warnung“ anzuzeigen.

- **Verfügbarkeitsprobleme**

  Zeigt als Diagramm die Gesamtzahl der Objekte an, einschließlich Objekten mit Verfügbarkeitsproblemen und Objekten, die keine Probleme mit der Verfügbarkeit haben. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Verfügbarkeitsproblemen, die sich auf die Verfügbarkeit von Daten in der SVM auswirken oder bereits davon betroffen sein können. Beispielsweise werden Informationen zu den NAS-LIFs und den SAN-LIFs angezeigt, die ausgefallen sind und die Volumes offline sind.

  Sie können auch Informationen zu aktuell ausgeführten Protokollen und Services sowie zur Anzahl und dem Status von NFS-Exporten und CIFS-Freigaben anzeigen.

Wenn es sich bei der ausgewählten SVM um eine SVM mit Infinite Volume handelt, können Sie Verfügbarkeitsinformationen über das Infinite Volume anzeigen.

- **Kapazitätsprobleme**

  Zeigt als Diagramm die Gesamtzahl der Objekte an, einschließlich Objekten mit Kapazitätsproblemen und Objekten, die keine Kapazitätsprobleme haben. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die nachfolgende Grafik liefert Details zu Kapazitätsproblemen, die sich auf die Kapazität der Daten der SVM auswirken oder bereits beeinträchtigen können. Beispielsweise werden Informationen zu Aggregaten angezeigt, die mit hoher Wahrscheinlichkeit die festgelegten Schwellenwerte überschreiten.

  Wenn es sich bei der ausgewählten SVM um eine SVM mit Infinite Volume handelt, können Sie die Kapazitätsdetails über das Infinite Volume anzeigen.

- **Schutzprobleme**

  Er bietet eine schnelle Übersicht über den Schutz der SVM, indem die Gesamtzahl der Beziehungen, einschließlich Beziehungen mit Schutzproblemen und Beziehungen, bei denen keine Sicherungsprobleme auftreten, als Diagramm angezeigt werden. Wenn nicht geschützte Volumes vorhanden sind, führt ein Klick auf den Link zur Seite Systemzustand/Volumes-Inventar, auf der eine gefilterte Liste der nicht geschützten Volumes in der SVM angezeigt werden kann. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Durch Klicken auf ein Diagramm gelangen Sie zur Seite „Schutz/Volume-Beziehungen“, auf der eine gefilterte Liste mit Details zu den Schutzbeziehungen angezeigt werden kann. Die nachfolgenden Informationen enthalten Details zu Sicherungsproblemen, die sich auf den Schutz der Daten in der SVM auswirken oder bereits beeinträchtigen können. Beispielsweise werden Informationen über Volumes angezeigt, die eine Snapshot Kopie-Reserve haben, die fast voll ist, oder über Probleme mit der SnapMirror Beziehungs-Verzögerung.

  Wenn die ausgewählte SVM eine Repository-SVM ist, wird der Schutzbereich nicht angezeigt.

Registerkarte „Kapazität“

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

Folgende Informationen werden für eine SVM mit FlexVol-Volume oder FlexGroup-Volume angezeigt:

- * Kapazität*

  Im Kapazitätsbereich werden Details zur verwendeten und verfügbaren Kapazität angezeigt, die aus allen Volumes zugewiesen sind:

  - Gesamtkapazität

    Zeigt die Gesamtkapazität (in MB, GB usw.) der SVM an.

  - Verwendet

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

  - Garantiert Verfügbar

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

◦ Nicht Garantiert

Zeigt den verfügbaren Speicherplatz für Daten an, die in der SVM für Thin Provisioning Volumes zugewiesen sind.

- **Volumen mit Kapazitätsproblemen**

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

◦ Status

Zeigt an, dass das Volumen ein kapazitätsbezogenes Problem mit einem angezeigten Schweregrad hat.

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

Wenn der Status des Volumes durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen wurde, und die Ursache des Ereignisses anzeigen. Sie können die Schaltfläche **Details anzeigen** verwenden, um weitere Informationen über die Veranstaltung anzuzeigen.

Wenn der Status des Volumes durch mehrere Ereignisse desselben Schweregrades bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

Ein Volume kann mehrere Ereignisse desselben Schweregrades oder unterschiedlicher Schweregrade aufweisen. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Volume zwei Ereignisse mit Schweregraden für Fehler und Warnung enthält, wird nur der Schweregrad Fehler angezeigt.

◦ Datenmenge

Zeigt den Namen des Volumes an.

◦ Genutzte Datenkapazität

Zeigt als Diagramm Informationen zur Auslastung der Volume-Kapazität (in Prozent) an.

◦ Tage voll

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

◦ Thin Provisioning

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

◦ Aggregate

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

Für eine SVM mit Infinite Volume werden folgende Informationen angezeigt:

- * Kapazität*

  Zeigt die folgenden kapazitätsbezogenen Details an:

  - Prozentsatz der genutzten und freien Datenkapazität
  - Prozentsatz der genutzten und freien Snapshot-Kapazität
  - Snapshot-Überlauf

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

  - Verwendet

    Zeigt den Speicherplatz an, der von Daten in der SVM mit Infinite Volume genutzt wird.

  - Warnung

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

  - Fehler

    Zeigt an, dass der Speicherplatz in der SVM mit Infinite Volume, falls voll, verfügbar ist. Wird dieser Schwellenwert nicht erreicht, wird das Ereignis „Space Full“ generiert.

- **Weitere Details**
  - Gesamtkapazität

    Zeigt die Gesamtkapazität in der SVM mit Infinite Volume an.

  - Datenkapazität

    Zeigt die genutzte Datenkapazität, verfügbare Datenkapazität und Details zur Snapshot Überlaufkapazität der SVM mit Infinite Volume an.

  - Snapshot-Reserve

    Zeigt die verwendeten und freien Details der Snapshot-Reserve an.

  - Systemkapazität

    Zeigt die genutzte Systemkapazität und die verfügbare Systemkapazität der SVM mit Infinite Volume an.

  - Schwellenwerte

    Zeigt die nahezu vollständigen und vollständigen Schwellenwerte der SVM mit Infinite Volume an.

- **Storage Class Capacity Details**

Zeigt Informationen zur Kapazitätsauslastung in Ihren Speicherklassen an. Diese Informationen werden nur angezeigt, wenn Sie Storage-Klassen für Ihre SVM mit Infinite Volume konfiguriert haben.

- **Storage Virtual Machine Storage Class Schwellenwerte**

  Zeigt die folgenden Schwellenwerte (in Prozent) Ihrer Speicherklassen an:

  - Nahezu Vollständig. Schwellenwert

    Gibt den Prozentsatz an, bei dem eine Storage-Klasse in einer SVM mit Infinite Volume als nahezu voll erachtet wird.

  - Vollständiger Schwellenwert

    Gibt den Prozentsatz an, bei dem die Storage-Klasse in einer SVM mit Infinite Volume als voll erachtet wird.

  - Limit Der Snapshot-Nutzung

    Gibt das Limit in Prozent im Speicherplatz an, der für Snapshot Kopien in der Storage-Klasse reserviert ist.

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration werden Konfigurationsdetails zu der ausgewählten SVM, z. B. Cluster, Root-Volume, die enthaltenen Volumes (Infinite Volume oder FlexVol Volumes) und die auf der SVM erstellten Richtlinien angezeigt:

- **Übersicht**
  - Cluster

    Zeigt den Namen des Clusters an, zu dem die SVM gehört.

  - Zulässiger Volume-Typ

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

  - Root-Volume

    Zeigt den Namen des Root-Volumes der SVM an.

  - Zulässige Protokolle

    Zeigt den Typ der Protokolle an, die für die SVM konfiguriert werden können. Außerdem gibt an, ob ein Protokoll aktiv ist ( ), unten ( ), oder ist nicht konfiguriert ( ).

- **Daten-LIFs**
  - NAS

    Zeigt die Anzahl der NAS-LIFs an, die der SVM zugeordnet sind. Außerdem gibt an, ob die LIFs aktiv sind (Oder runter ( ).

  - San

Zeigt die Anzahl der SAN-LIFs an, die der SVM zugeordnet sind. Außerdem gibt an, ob die LIFs aktiv sind (Oder runter ().

- FC-NVMe

  Zeigt die Anzahl der FC-NVMe LIFs an, die der SVM zugeordnet sind. Außerdem gibt an, ob die LIFs aktiv sind (Oder runter ().

- Verbindungspfad

  Zeigt den Pfad an, auf dem das Infinite Volume gemountet ist. Für eine SVM wird nur ein Verbindungspfad mit Infinite Volume angezeigt.

- Speicherklassen

  Zeigt die Storage-Klassen an, die der ausgewählten SVM mit Infinite Volume zugeordnet sind. Es werden nur Storage-Klassen für eine SVM mit Infinite Volume angezeigt.

- **Management-LIFs**
  - Gesteigerte

    Zeigt die Anzahl der Management-LIFs an, die der SVM zugeordnet sind. Außerdem gibt an, ob die Management-LIFs aktiv sind (Oder runter ().

- **Richtlinien**
  - Snapshots

    Zeigt den Namen der Snapshot-Richtlinie an, die auf der SVM erstellt wurde.

  - Exportrichtlinien

    Zeigt entweder den Namen der Exportrichtlinie an, wenn eine einzelne Richtlinie erstellt wird, oder zeigt die Anzahl der Exportrichtlinien an, wenn mehrere Richtlinien erstellt werden.

  - Datenrichtlinie

    Zeigt an, ob eine Datenrichtlinie für die ausgewählte SVM mit Infinite Volume konfiguriert ist.

- **Services**
  - Typ

    Zeigt den Service-Typ an, der für die SVM konfiguriert ist. Der Typ kann Domain Name System (DNS) oder Network Information Service (NIS) sein.

  - Bundesland

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

  - Domain-Name

    Zeigt die vollständig qualifizierten Domänennamen (FQDNs) des DNS-Servers für die DNS-Dienste oder NIS-Server für die NIS-Dienste an. Wenn der NIS-Server aktiviert ist, wird der aktive FQDN des NIS-Servers angezeigt. Wenn der NIS-Server deaktiviert ist, wird die Liste aller FQDNs angezeigt.

- IP-Adresse

  Zeigt die IP-Adressen des DNS- oder NIS-Servers an. Wenn der NIS-Server aktiviert ist, wird die aktive IP-Adresse des NIS-Servers angezeigt. Wenn der NIS-Server deaktiviert ist, wird die Liste aller IP-Adressen angezeigt.

Registerkarte LIFs

Die Registerkarte LIFs zeigt Details zu den Daten-LIFs an, die auf der ausgewählten SVM erstellt wurden:

- **LIF**

  Zeigt den Namen der logischen Schnittstelle an, die auf der ausgewählten SVM erstellt wird.

- **Betriebsstatus**

  Zeigt den Betriebsstatus der logischen Schnittstelle an. Diese kann im aktiv sein ( ), Down (Oder Unbekannt ( ). Der Betriebsstatus einer logischen Schnittstelle wird vom Status ihrer physischen Ports bestimmt.

- **Verwaltungsstatus**

  Zeigt den Administrationsstatus der logischen Schnittstelle an. Dieser kann im aktiv sein ( ), Down (Oder Unbekannt ( ). Der Administrationsstatus einer LIF wird vom Storage-Administrator gesteuert, um Änderungen an der Konfiguration oder zu Wartungszwecken vorzunehmen. Der Administrationsstatus kann sich vom Betriebsstatus unterscheiden. Wenn jedoch der Administrationsstatus eines LIF „Inaktiv“ lautet, ist der Betriebsstatus standardmäßig „Inaktiv“.

- **IP-Adresse / WWPN**

  Zeigt die IP-Adresse für Ethernet LIFs und den World Wide Port Name (WWPN) für FC LIFs an.

- **Protokolle**

  Zeigt die Liste der für das LIF angegebenen Datenprotokolle an, z. B. CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe und FlexCache. Bei Infinite Volume sind die SAN-Protokolle nicht anwendbar.

- * Rolle*

  Zeigt die LIF-Rolle an. Die Rollen können Daten oder Management sein.

- * Home Port*

  Zeigt den physischen Port an, dem die LIF ursprünglich zugeordnet war.

- **Aktueller Port**

  Zeigt den physischen Port an, dem das LIF derzeit zugeordnet ist. Wenn das LIF migriert wird, unterscheidet sich der aktuelle Port möglicherweise vom Home Port.

- **Portsatz**

  Zeigt den Port-Satz an, dem das LIF zugeordnet ist.

- **Failover-Richtlinie**

Zeigt die für das LIF konfigurierte Failover-Richtlinie an. Für LIFs für NFS, CIFS und FlexCache ist die standardmäßige Failover-Richtlinie Next verfügbar. Failover-Richtlinie gilt nicht für FC- und iSCSI-LIFs.

- **Routing-Gruppen**

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

  Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt. Daher wird für diese Cluster eine leere Spalte angezeigt.

- **Failover-Gruppe**

  Zeigt den Namen der Failover-Gruppe an.

Registerkarte „qtrees“

Auf der Registerkarte qtrees werden Details zu qtrees und ihren Kontingenten angezeigt. Sie können auf die Schaltfläche **Schwellenwerte bearbeiten** klicken, wenn Sie die gesundheitlichen Schwellenwerte für qtree-Kapazität für eine oder mehrere qtrees bearbeiten möchten.

Verwenden Sie die Schaltfläche **Exportieren**, um einen kommagetrennten Wert zu erstellen (`.csv`) Datei mit den Details aller überwachten qtrees. Beim Export in eine CSV-Datei können Sie wahlweise einen qtrees-Bericht für die aktuelle SVM, für alle SVMs im aktuellen Cluster oder alle SVMs für alle Cluster in Ihrem Datacenter erstellen. In der exportierten CSV-Datei werden einige zusätzliche Felder „qtrees“ angezeigt.

Die Registerkarte „qtrees“ wird für eine SVM mit Infinite Volume nicht angezeigt.

- **Status**

  Zeigt den aktuellen Status des qtree an. Der Status kann kritisch sein (), Fehler (), Warnung (Oder normal ().

  Sie können den Mauszeiger über das Statussymbol bewegen, um weitere Informationen zu dem für den qtree generierten Ereignis oder Ereignissen anzuzeigen.

  Wenn der Status des qtree durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Sie können **Details anzeigen** verwenden, um weitere Informationen über die Veranstaltung anzuzeigen.

  Wenn der Status des qtree durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch **Alle Ereignisse anzeigen** verwenden, um die Liste der generierten Ereignisse anzuzeigen.

  Ein qtree kann mehrere Ereignisse des gleichen Schweregrads oder unterschiedlicher Schweregrade aufweisen. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn ein qtree z. B. zwei Ereignisse mit Schweregraden für Fehler und Warnung hat, wird nur der Schweregrad „Fehler“ angezeigt.

- **Qtree**

  Zeigt den Namen des qtree an.

- * Cluster*

  Zeigt den Namen des Clusters an, der den qtree enthält. Wird nur in der exportierten CSV-Datei angezeigt.

- **Storage Virtual Machine**

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

- **Lautstärke**

  Zeigt den Namen des Volume an, das den qtree enthält.

  Sie können den Zeiger über den Volume-Namen verschieben, um weitere Informationen zum Volume anzuzeigen.

- **Quota Set**

  Gibt an, ob ein Kontingent aktiviert oder auf dem qtree deaktiviert ist.

- **Quotentyp**

  Gibt an, ob das Kontingent für einen Benutzer, eine Benutzergruppe oder einen qtree ist. Wird nur in der exportierten CSV-Datei angezeigt.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Für jeden Benutzer und jede Benutzergruppe werden mehrere Zeilen angezeigt. Wenn der Kontingenttyp qtree ist oder nicht festgelegt ist, ist die Spalte leer. Wird nur in der exportierten CSV-Datei angezeigt.

- **Verwendete Festplatte %**

  Zeigt den Prozentsatz des verwendeten Festplattenspeichers an. Wenn ein Festplattenlimit festgelegt ist, basiert dieser Wert auf dem Festplattenlimit. Wenn das Kontingent ohne Festplattenlimit festgelegt wird, basiert der Wert auf dem Volume-Datenraum. Wenn das Kontingent nicht festgelegt ist oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört, wird „`not anwendbare`“ auf der Grid-Seite angezeigt und das Feld in den CSV-Exportredaten leer ist.

- **Festplatten-Hard-Limit**

  Zeigt die maximale Menge an Festplattenspeicher an, die für den qtree zugewiesen ist. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht wird und keine weiteren Festplattenschreibvorgänge mehr zulässig sind. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein Festplattenlimit gesetzt wird, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört.

- **Soft Limit Für Festplatten**

  Zeigt die Menge an Festplattenspeicher an, die dem qtree zugewiesen ist, bevor ein Warnereignis generiert wird. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein Disk-Softlimit gesetzt wird, wenn das Kontingent nicht festgelegt ist, oder wenn

Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört. Standardmäßig ist diese Spalte ausgeblendet.

- **Datenträgerschwellenwert**

  Zeigt den Schwellenwert an, der für den Festplattenspeicher festgelegt wurde. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein Festplattenschwellenwert eingestellt ist, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im qtree verwendeten Dateien an. Wenn das harte Limit für die Datei festgelegt ist, basiert dieser Wert auf dem harten Limit der Datei. Es wird kein Wert angezeigt, wenn das Kontingent ohne harte Dateibegrenzung festgelegt ist. Wenn das Kontingent nicht festgelegt ist oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört, wird „`not anwendbare`“ auf der Grid-Seite angezeigt und das Feld in den CSV-Exportredaten leer ist.

- **Harte Dateibegrenzung**

  Zeigt das endgültige Limit für die Anzahl der Dateien an, die auf den qtrees zulässig sind. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne eine feste Dateibegrenzung festgelegt wird, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört.

- **Soft Limit Für Dateien**

  Zeigt den Softlimit für die Anzahl der Dateien an, die auf qtrees zulässig sind. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein Datei-Softlimit gesetzt wird, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört. Standardmäßig ist diese Spalte ausgeblendet.

Registerkarte „Benutzer- und Gruppenkontingente“

Zeigt Details zu den Quoten für Benutzer und Benutzergruppen für die ausgewählte SVM an. Sie können Informationen wie den Status des Kontingents, den Namen des Benutzers oder der Benutzergruppe, die auf den Festplatten und Dateien festgelegten Soft- und Hard-Limits, den Speicherplatz und die Anzahl der verwendeten Dateien sowie den Schwellenwert für die Festplatte anzeigen. Sie können auch die E-Mail-Adresse ändern, die einem Benutzer oder einer Benutzergruppe zugeordnet ist.

- **Schaltfläche 'Email-Adresse bearbeiten'**

  Öffnet das Dialogfeld E-Mail-Adresse bearbeiten, in dem die aktuelle E-Mail-Adresse des ausgewählten Benutzers oder der ausgewählten Benutzergruppe angezeigt wird. Sie können die E-Mail-Adresse ändern. Wenn das Feld**E-Mail-Adresse bearbeiten** leer ist, wird die Standardregel verwendet, um eine E-Mail-Adresse für den ausgewählten Benutzer oder die ausgewählte Benutzergruppe zu generieren.

  Wenn mehrere Benutzer das gleiche Kontingent haben, werden die Namen der Benutzer als kommagetrennte Werte angezeigt. Außerdem wird die Standardregel nicht verwendet, um die E-Mail-Adresse zu generieren; Sie müssen daher die erforderliche E-Mail-Adresse angeben, damit Benachrichtigungen gesendet werden können.

- **Schaltfläche E-Mail-Regeln konfigurieren**

  Mit dieser Option können Sie Regeln erstellen oder ändern, um eine E-Mail-Adresse für die auf der SVM

konfigurierten Benutzer- oder Benutzergruppen-Quoten zu generieren. Bei einer Quota-Verletzung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

- **Status**

  Zeigt den aktuellen Status des Kontingents an. Der Status kann kritisch sein (), Warnung (Oder normal ().

  Sie können den Zeiger über das Statussymbol verschieben, um weitere Informationen über das Ereignis oder die Ereignisse anzuzeigen, die für das Kontingent generiert wurden.

  Wenn der Status des Kontingents durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugeordnet ist, und die Ursache des Ereignisses anzeigen. Sie können **Details anzeigen** verwenden, um weitere Informationen über die Veranstaltung anzuzeigen.

  Wenn der Status des Kontingents durch mehrere Ereignisse desselben Schweregrades bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum angezeigt, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch **Alle Ereignisse anzeigen** verwenden, um die Liste der generierten Ereignisse anzuzeigen.

  > Eine Quote kann mehrere Ereignisse desselben Schweregrades oder unterschiedlicher Schweregrade haben. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Kontingent zwei Ereignisse mit Schweregraden für Fehler und Warnung enthält, wird nur der Schweregrad „Fehler“ angezeigt.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Wenn mehrere Benutzer das gleiche Kontingent haben, werden die Namen der Benutzer als kommagetrennte Werte angezeigt.

  Der Wert wird als „`Unbekannt`“ angezeigt, wenn ONTAP aufgrund von SECD-Fehlern keinen gültigen Benutzernamen liefert.

- **Typ**

  Gibt an, ob das Kontingent für einen Benutzer oder eine Benutzergruppe gilt.

- **Volumen oder Qtree**

  Zeigt den Namen des Volume oder qtree an, auf dem das Benutzer- oder Benutzergruppenkontingent angegeben ist.

  Sie können den Mauszeiger über den Namen des Volume oder qtree bewegen, um weitere Informationen zum Volume oder qtree anzuzeigen.

- **Verwendete Festplatte %**

  Zeigt den Prozentsatz des verwendeten Festplattenspeichers an. Der Wert wird als „`not anwendbares`“ angezeigt, wenn das Kontingent ohne Festplattenlimit festgelegt wird.

- **Festplatten-Hard-Limit**

Zeigt den maximalen Speicherplatz an, der dem Kontingent zugewiesen ist. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht wird und keine weiteren Festplattenschreibvorgänge mehr zulässig sind. Der Wert wird als „`Unlimited`“ angezeigt, wenn das Kontingent ohne Festplattenlimit festgelegt wird.

- **Soft Limit Für Festplatten**

  Zeigt die Menge an Festplattenspeicher an, die für das Kontingent zugewiesen ist, bevor ein Warnereignis generiert wird. Der Wert wird als „`Unlimited`“ angezeigt, wenn das Kontingent ohne Laufwerk-Softlimit festgelegt wird. Standardmäßig ist diese Spalte ausgeblendet.

- **Datenträgerschwellenwert**

  Zeigt den Schwellenwert an, der für den Festplattenspeicher festgelegt wurde. Der Wert wird als „`Unlimited`“ angezeigt, wenn das Kontingent ohne Datenträgerschwellenwert eingestellt ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im qtree verwendeten Dateien an. Der Wert wird als „`not anwendbares`“ angezeigt, wenn das Kontingent ohne harte Dateibegrenzung festgelegt ist.

- **Harte Dateibegrenzung**

  Zeigt das harte Limit für die Anzahl der Dateien an, die auf dem Kontingent zulässig sind. Der Wert wird als „`Unlimited`“ angezeigt, wenn das Kontingent ohne hartes Dateilimit festgelegt wird.

- **Soft Limit Für Dateien**

  Zeigt das Softlimit für die Anzahl der Dateien an, die auf dem Kontingent zulässig sind. Der Wert wird als „`Unlimited`“ angezeigt, wenn das Kontingent ohne DateiSoftlimit festgelegt wird. Standardmäßig ist diese Spalte ausgeblendet.

- **E-Mail-Adresse**

  Zeigt die E-Mail-Adresse des Benutzers oder der Benutzergruppe an, an die Benachrichtigungen gesendet werden, wenn eine Verletzung der Quoten vorhanden ist.

Registerkarte NFS Exporte

Auf der Registerkarte NFS-Exporte werden Informationen zu NFS-Exporten angezeigt, z. B. sein Status, der dem Volume zugeordnete Pfad (Infinite Volumes, FlexGroup Volumes oder FlexVol-Volumes), die Zugriffsebenen von Clients auf die NFS-Exporte und die für die exportierten Volumes definierte Exportrichtlinie. NFS-Exporte werden unter den folgenden Bedingungen nicht angezeigt: Wenn das Volume nicht angehängt ist oder wenn die mit der Exportrichtlinie für das Volume verknüpften Protokolle keine NFS-Exporte enthalten.

Verwenden Sie die Schaltfläche **Exportieren**, um einen kommagetrennten Wert zu erstellen (`.csv`) Datei mit den Details aller überwachten NFS-Exporte. Beim Export in eine CSV-Datei können Sie wählen, einen NFS Exports-Bericht für die aktuelle SVM, für alle SVMs im aktuellen Cluster oder für alle SVMs für alle Cluster in Ihrem Datacenter zu erstellen. In der exportierten CSV-Datei werden einige zusätzliche Felder für die Exportrichtlinie angezeigt.

- **Status**

  Zeigt den aktuellen Status des NFS-Exports an. Der Status kann „Fehler“ sein ( ) Oder normal ( ).

- **Verbindungspfad**

  Zeigt den Pfad an, auf den das Volume angehängt ist. Wird auf einen qtree eine explizite NFS Exportrichtlinie angewendet, zeigt die Spalte den Pfad des Volume an, über das auf den qtree zugegriffen werden kann.

- **Verbindungspfad Aktiv**

  Zeigt an, ob der Pfad für den Zugriff auf das bereitgestellte Volume aktiv oder inaktiv ist.

- **Volumen oder Qtree**

  Zeigt den Namen des Volumes oder qtree an, auf das die NFS-Exportrichtlinie angewendet wird. Bei Infinite Volumes wird der Name der SVM mit dem Infinite Volume angezeigt. Wenn eine NFS-Exportrichtlinie auf einen qtree im Volume angewendet wird, werden in der Spalte sowohl die Namen des Volume als auch der qtree angezeigt.

  Sie können auf den Link klicken, um Details zum Objekt auf der entsprechenden Detailseite anzuzeigen. Wenn es sich bei dem Objekt um einen qtree handelt, werden sowohl für den qtree als auch für das Volume Links angezeigt.

- * Cluster*

  Zeigt den Namen des Clusters an. Wird nur in der exportierten CSV-Datei angezeigt.

- **Storage Virtual Machine**

  Zeigt den Namen der SVM mit NFS-Exportrichtlinien an. Wird nur in der exportierten CSV-Datei angezeigt.

- **Volume-Status**

  Zeigt den Status des Volumes an, das exportiert wird. Der Status kann Offline, Online, eingeschränkt oder gemischt sein.

  - Offline

    Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

  - Online

    Lese- und Schreibzugriff auf das Volume ist zulässig.

  - Eingeschränkt

    Begrenzte Vorgänge, wie etwa die Paritätsrekonstruktion, sind zulässig, der Datenzugriff jedoch nicht.

  - Gemischt

    Die Komponenten eines FlexGroup-Volumes sind nicht alle im selben Zustand.

- **Sicherheitsstil**

  Zeigt die Zugriffsberechtigung für die exportierten Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder gemischt sein.

  - UNIX (NFS-Clients)

Dateien und Verzeichnisse im Volume haben UNIX Berechtigungen.

- Virtualisierung

  Dateien und Verzeichnisse im Volume weisen einen einheitlichen Sicherheitsstil auf.

- NTFS (CIFS-Clients)

  Dateien und Verzeichnisse im Volume haben Windows NTFS-Berechtigungen.

- Gemischt

  Dateien und Verzeichnisse auf dem Volume können entweder UNIX Berechtigungen oder Windows NTFS Berechtigungen haben.

- **UNIX-Erlaubnis**

  Zeigt die UNIX-Berechtigungsbits in einem Oktal-String-Format an, das für die exportierten Volumes festgelegt ist. Es ähnelt den Berechtigungsbits im UNIX-Stil.

- **Exportrichtlinie**

  Zeigt die Regeln an, die die Zugriffsberechtigung für exportierte Volumes definieren. Sie können auf den Link klicken, um Details zu den Regeln anzuzeigen, die mit der Exportrichtlinie verknüpft sind, z. B. die Authentifizierungsprotokolle und die Zugriffsberechtigung.

  Wenn Sie einen Bericht für die Seite NFS-Exporte erstellen, werden alle Regeln, die zur Exportrichtlinie gehören, in die CSV-Datei exportiert. Wenn z. B. zwei Regeln in der Exportrichtlinie enthalten sind, sehen Sie nur eine Zeile in der NFS-Export-Grid-Seite, die exportierten Daten haben jedoch zwei Zeilen, die den beiden Regeln entsprechen.

- **Regelindex**

  Zeigt die Regeln an, die der Exportrichtlinie zugeordnet sind, z. B. die Authentifizierungsprotokolle und die Zugriffsberechtigung. Wird nur in der exportierten CSV-Datei angezeigt.

- **Zugriffsprotokolle**

  Zeigt die Protokolle an, die für die Regeln für die Exportrichtlinie aktiviert sind. Wird nur in der exportierten CSV-Datei angezeigt.

- * Client Match*

  Zeigt die Clients an, die über die Berechtigung zum Zugriff auf Daten auf den Volumes verfügen. Wird nur in der exportierten CSV-Datei angezeigt.

- **Nur-Lese-Zugriff**

  Zeigt das Authentifizierungsprotokoll an, das zum Lesen von Daten auf den Volumes verwendet wird. Wird nur in der exportierten CSV-Datei angezeigt.

- **Schreibzugriff Lesen**

  Zeigt das Authentifizierungsprotokoll an, das zum Lesen oder Schreiben von Daten auf den Volumes verwendet wird. Wird nur in der exportierten CSV-Datei angezeigt.

Registerkarte CIFS Shares

Zeigt Informationen zu den CIFS-Freigaben auf der ausgewählten SVM an. Sie können Informationen anzeigen, wie z. B. den Status der CIFS-Freigabe, den Freigabennamen, den mit der SVM verknüpften Pfad, den Status des Verbindungspfads der Freigabe, das Objekt enthält, den Status des enthaltenden Volumes, die Sicherheitsdaten der Freigabe und die für die Freigabe definierten Exportrichtlinien. Sie können auch feststellen, ob ein äquivalenter NFS-Pfad für die CIFS-Freigabe vorhanden ist.

Freigaben in Ordnern werden auf der Registerkarte CIFS-Freigaben nicht angezeigt.

- **Befehlsschaltfläche Benutzerzuordnung anzeigen**

  Öffnet das Dialogfeld Benutzerzuordnung.

  Sie können sich die Details der Benutzerzuordnung für die SVM anzeigen lassen.

- **ACL-Befehlstaste anzeigen**

  Öffnet das Dialogfeld „Zugriffskontrolle“ für die Freigabe.

  Sie können Benutzer- und Berechtigungsdetails für die ausgewählte Freigabe anzeigen.

- **Status**

  Zeigt den aktuellen Status der Freigabe an. Der Status kann Normal ( ) Oder Fehler ( ).

- **Name Der Weitergabe**

  Zeigt den Namen der CIFS-Freigabe an.

- **Pfad**

  Zeigt den Verbindungspfad an, auf dem die Freigabe erstellt wird.

- **Verbindungspfad Aktiv**

  Zeigt an, ob der Pfad für den Zugriff auf die Freigabe aktiv oder inaktiv ist.

- **Objekt**

  Zeigt den Namen des enthaltenden Objekts an, zu dem die Freigabe gehört. Das zugehörige Objekt kann ein Volume oder ein qtree sein.

  Durch Klicken auf den Link können Sie auf der entsprechenden Detailseite Details über das zugehörige Objekt anzeigen. Wenn es sich bei dem enthaltenen Objekt um einen qtree handelt, werden sowohl für qtree als auch für das Volume Links angezeigt.

- **Volume-Status**

  Zeigt den Status des Volumes an, das exportiert wird. Der Status kann Offline, Online, eingeschränkt oder gemischt sein.

  - Offline

    Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

- Online

  Lese- und Schreibzugriff auf das Volume ist zulässig.

- Eingeschränkt

  Begrenzte Vorgänge, wie etwa die Paritätsrekonstruktion, sind zulässig, der Datenzugriff jedoch nicht.

- Gemischt

  Die Komponenten eines FlexGroup-Volumes sind nicht alle im selben Zustand.

- **Sicherheit**

  Zeigt die Zugriffsberechtigung für die exportierten Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder gemischt sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume haben UNIX Berechtigungen.

  - Virtualisierung

    Dateien und Verzeichnisse im Volume weisen einen einheitlichen Sicherheitsstil auf.

  - NTFS (CIFS-Clients)

    Dateien und Verzeichnisse im Volume haben Windows NTFS-Berechtigungen.

  - Gemischt

    Dateien und Verzeichnisse auf dem Volume können entweder UNIX Berechtigungen oder Windows NTFS Berechtigungen haben.

- **Exportrichtlinie**

  Zeigt den Namen der Exportrichtlinie an, die für die Freigabe gilt. Wenn keine Exportrichtlinie für die SVM angegeben ist, wird der Wert als nicht aktiviert angezeigt.

  Sie können auf den Link klicken, um Details zu den Regeln anzuzeigen, die der Exportrichtlinie zugeordnet sind, z. B. Zugriffsprotokolle und Berechtigungen. Die Verknüpfung ist deaktiviert, wenn die Exportrichtlinie für die ausgewählte SVM deaktiviert ist.

- **NFS-Äquivalent**

  Gibt an, ob ein Äquivalent zu NFS für die Freigabe vorhanden ist.

REGISTERKARTE „SAN“

Zeigt Details zu LUNs, Initiatorgruppen und Initiatoren für die ausgewählte SVM an. Standardmäßig wird die Ansicht LUNs angezeigt. Sie können Details zu den Initiatorgruppen auf der Registerkarte Initiatorgruppen und Details zu Initiatoren auf der Registerkarte Initiatoren anzeigen.

- **LUNs-Registerkarte**

  Zeigt Details zu den LUNs an, die zur ausgewählten SVM gehören. Sie können Informationen anzeigen,

wie z. B. den LUN-Namen, den LUN-Zustand (online oder offline), den Namen des Filesystems (Volume oder qtree), das die LUN enthält, den Typ des Host-Betriebssystems, die Gesamtkapazität und die Seriennummer der LUN. Sie können auch anzeigen, ob Thin Provisioning auf der LUN aktiviert ist und ob die LUN einer Initiatorgruppe zugeordnet ist.

Sie können auch die Initiatorgruppen und Initiatoren anzeigen, die der ausgewählten LUN zugeordnet sind.

- **Registerkarte Initiatorgruppen**

  Zeigt Details zu Initiatorgruppen an. Sie können Details anzeigen, z. B. den Namen der Initiatorgruppe, den Zugriffsstatus, den Typ des Host-Betriebssystems, das von allen Initiatoren in der Gruppe verwendet wird, und das unterstützte Protokoll. Wenn Sie in der Spalte Zugriffsstatus auf den Link klicken, können Sie den aktuellen Zugriffsstatus der Initiatorgruppe anzeigen.

  - **Normal**

    Die Initiatorgruppe ist mit mehreren Zugriffspfaden verbunden.

  - * Einzelner Pfad*

    Die Initiatorgruppe ist mit einem einzelnen Zugriffspfad verbunden.

  - **Keine Pfade**

    Es ist kein Zugriffspfad mit der Initiatorgruppe verbunden.

    Sie können anzeigen, ob Initiatorgruppen über einen Port-Satz allen LIFs oder spezifischen LIFs zugeordnet werden. Wenn Sie in der Spalte zugewiesene LIFs auf den Link zum Zählen klicken, werden entweder alle LIFs angezeigt oder bestimmte LIFs für einen Port-Satz angezeigt. LIFs, die über das Zielportal zugeordnet sind, werden nicht angezeigt. Es wird die Gesamtzahl der Initiatoren und LUNs angezeigt, die einer Initiatorgruppe zugeordnet sind.

  Sie können auch die LUNs und Initiatoren anzeigen, die der ausgewählten Initiatorgruppe zugeordnet sind.

- **Registerkarte Initiatoren**

  Zeigt den Namen und Typ des Initiators und die Gesamtzahl der Initiatorgruppen an, die diesem Initiator für die ausgewählte SVM zugeordnet sind.

  Sie können auch die LUNs und Initiatorgruppen anzeigen, die der ausgewählten Initiatorgruppe zugeordnet sind.

Datenrichtlinie

Auf der Registerkarte Datenrichtlinie können Sie eine oder mehrere Regeln in einer Datenrichtlinie erstellen, ändern, aktivieren oder löschen. Sie können die Datenrichtlinie auch in die Unified Manager-Datenbank importieren und die Datenrichtlinie auf Ihren Computer exportieren:

Die Registerkarte Datenrichtlinie wird nur für SVMs mit Infinite Volume angezeigt.

- **Regelliste**

  Zeigt die Liste der Regeln an. Wenn Sie die Regel erweitern, können Sie die entsprechenden übereinstimmenden Kriterien der Regel und der Speicherklasse anzeigen, in der der Inhalt auf der Grundlage der Regel platziert wird.

Die Standardregel ist die letzte Regel in der Liste. Sie können die Reihenfolge der Standardregel nicht ändern.

- Übereinstimmende Kriterien

  Zeigt die Bedingungen für die Regel an. Eine Regel kann z. B. „`Dateipfad beginnt mit `/eng/Nightly`“ lauten.

  Der Dateipfad muss immer mit einem Verbindungspfad beginnen.

- Platzierung Von Inhalten

  Zeigt die entsprechende Speicherklasse für die Regel an.

- **Regelfilter**

Mit dieser Funktion können Sie Regeln filtern, die einer bestimmten Speicherklasse zugeordnet sind, die in der Liste aufgeführt ist.

- **Aktionsschaltflächen**
  - Erstellen

    Öffnet das Dialogfeld Regel erstellen, in dem Sie eine neue Regel für Ihre Datenrichtlinie erstellen können.

  - Bearbeiten

    Öffnet das Dialogfeld Regel bearbeiten, in dem Sie Regeleigenschaften wie Verzeichnispfade, Dateitypen und Eigentümer ändern können.

  - Löschen

    Löscht die ausgewählte Regel.

  - Nach Oben

    Verschiebt die ausgewählte Regel in der Liste nach oben. Sie können die Standardregel jedoch nicht in der Liste nach oben verschieben.

  - Nach Unten Verschieben

    Verschiebt die ausgewählte Regel nach unten in der Liste. Sie können die Standardregel jedoch nicht nach unten in der Liste verschieben.

  - Aktivieren

    Aktiviert die Regeln und Änderungen an der Datenrichtlinie in der SVM mit Infinite Volume.

  - Zurücksetzen

    Setzt alle Änderungen zurück, die an der Konfiguration der Datenrichtlinien vorgenommen wurden.

  - Importieren

    Importiert eine Konfiguration der Datenrichtlinien aus einer Datei.

◦ Exportieren

Exportiert eine Konfiguration von Datenrichtlinien in eine Datei.

Bereich für zugehörige Geräte

Im Bereich „Verwandte Geräte“ können Sie LUNs, CIFS Shares und die Quoten für Benutzer und Benutzergruppen anzeigen und navigieren, die mit dem qtree in Verbindung stehen:

- **LUNs**

  Zeigt die Gesamtzahl der LUNs an, die dem ausgewählten qtree zugeordnet sind.

- **NFS-Exporte**

  Zeigt die Gesamtzahl der NFS-Exportrichtlinien an, die mit dem ausgewählten qtree verknüpft sind.

- **CIFS-Freigaben**

  Zeigt die Gesamtzahl der CIFS-Shares an, die mit dem ausgewählten qtree verbunden sind.

- **Benutzer- und Gruppenquoten**

  Zeigt die Gesamtzahl der Benutzer- und Benutzergruppenkontingente an, die mit dem ausgewählten qtree verknüpft sind. Auf der Grundlage des höchsten Schweregrads wird auch der Integritätsstatus der Kontingente von Benutzern und Benutzergruppen angezeigt.

Bereich „Verwandte Anmerkungen“

Im Fensterbereich Verwandte Anmerkungen können Sie die mit der ausgewählten SVM verknüpften Anmerkungsdetails anzeigen. Details umfassen den Anmerkungsnamen und die auf die SVM angewandten Anmerkungswerte. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie Cluster, Aggregate und Volumes anzeigen, die mit der SVM in Verbindung stehen:

- * Cluster*

  Zeigt den Integritätsstatus des Clusters an, zu dem die SVM gehört.

- **Aggregate**

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

- * Zugewiesene Aggregate*

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

- **Bände**

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

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ können Sie eine Liste der Gruppen anzeigen, die der ausgewählten SVM zugeordnet sind.

Bereich „Verwandte Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnmeldungen anzeigen, die für die ausgewählte SVM erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link **Alarm hinzufügen** klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Namen der Warnmeldung klicken.

Dialogfeld „Speicherpool“

Das Dialogfeld Storage Pool ermöglicht Ihnen, Details zum dedizierten Cache von SSDs anzuzeigen, auch unter dem Namen „ *Storage Pools*“ bekannt. Sie können die Storage-Pools überwachen und Details anzeigen, wie z. B. den Storage-Pool-Zustand, den gesamten und verfügbaren Cache sowie die im Speicherpool verwendeten und verfügbaren Zuweisungen.

Sie können die folgenden Speicher-Pool-Details anzeigen:

- **Status**

  Zeigt den Status des Speicherpools an, der gesund oder ungesund sein kann.

- **Gesamtzuweisungen**

  Zeigt die Gesamtzuordnungseinheiten und die Größe im Speicherpool an.

- **Größe Der Zuordnungseinheit**

  Zeigt den minimalen Speicherplatz im Speicherpool an, der einem Aggregat zugewiesen werden kann.

- **Festplatten**

  Zeigt die Anzahl der Laufwerke an, die zum Erstellen des Speicherpools verwendet werden. Wenn die Anzahl der Laufwerke in der Spalte „Speicherpool“ und die Anzahl der Festplatten, die auf der Registerkarte „Laufwerksinformationen“ für diesen Speicherpool angezeigt werden, nicht übereinstimmen, zeigt dies an, dass eine oder mehrere Festplatten beschädigt sind und der Speicherpool ungesund ist.

- **Cache-Zuweisungen**
  - Verwendete Zuweisungen

    Zeigt Anzahl und Größe der von den Aggregaten verwendeten Zuordnungseinheiten an. Sie können auf den Aggregatnamen klicken, um Details zum Aggregat anzuzeigen.

◦ Verfügbare Zuordnungen

Zeigt die Anzahl und Größe der für die Nodes verfügbaren Zuweisungseinheiten an. Sie können auf den Node-Namen klicken, um weitere Details zum Aggregat anzuzeigen.

Integrität/Volumen-Inventarseite

Auf der Seite „Systemzustand/Volume-Bestand“ werden Informationen zu den Volumes in den überwachten Speichersystemen angezeigt und Sie können die Schwellwerteinstellungen des Volumes ändern.

Befehlsschaltflächen

- **Schwellenwerte Bearbeiten**

  Zeigt das Dialogfeld Schwellenwerte bearbeiten an, in dem Sie die Einstellungen für den Integritätsschwellenwert für ein oder mehrere Volumes bearbeiten können.

- **Schutz**

  Zeigt die folgenden Untermenüs an:

  ◦ SnapMirror

  Ermöglicht Ihnen, eine SnapMirror Beziehung für die ausgewählten Volumes zu erstellen.

  ◦ SnapVault

  Ermöglicht Ihnen, eine SnapVault-Beziehung für die ausgewählten Volumes zu erstellen.

- **Wiederherstellen**

  Zeigt das Dialogfeld Wiederherstellen an, in dem Sie Verzeichnisse oder Dateien von einem Volume gleichzeitig wiederherstellen können.

  Diese Schaltfläche ist deaktiviert, wenn mehrere Volumes ausgewählt sind, oder wenn ein FlexGroup-Volume ausgewählt ist oder ein für SnapMirror Synchronous konfiguriertes Volume ausgewählt ist.

- **Anmerkung**

  Ermöglicht Ihnen, das ausgewählte Volume mit Anmerkungen zu versehen.

- **Export**

  Ermöglicht das Exportieren der Details aller überwachten Volumes in kommagetrennte Werte (`.csv`) Datei. Bei der Anzeige von Infinite Volumes werden die Infinite Volume Komponenten exportiert.

Volumes Übersicht

Die Tabelle Volumes zeigt die Eigenschaften aller erkannten Volumes an. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen:

- **Status**

Der aktuelle Status eines Volumes. Der Status kann kritisch sein (), Fehler (), Warnung (Oder normal ()).

Sie können den Zeiger über den Status verschieben, um weitere Informationen zu dem für das Volume generierten Ereignis oder Ereignissen anzuzeigen.

Wenn der Status des Volumes durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen wurde, und die Ursache des Ereignisses anzeigen. Sie können auf den Link **Details anzeigen** klicken, um weitere Informationen über die Veranstaltung anzuzeigen.

Wenn der Status des Volumes durch mehrere Ereignisse desselben Schweregrades bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum beim Auslösen der Ereignisse und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

- **Lautstärke**

  Der Name des Volume.

  Sie können den Mauszeiger über ein Volume bewegen, um Informationen wie den im Volume zugewiesenen Speicherplatz für das qtree-Kontingent, den Status der letzten Verschiebung des Volumes und den dem Volume zugewiesenen Speicherplatz anzuzeigen. Sie können auch Details zu verwandten Objekten wie z.B. die SVM anzeigen, zu der das Volume gehört, das Aggregat, zu dem das Volume gehört, und alle Volumes, die zu diesem Aggregat gehören.

  Wenn eine SVM mit Infinite Volume überwacht wird, können Sie Details zu den drei Typen von Komponenten (Daten, Namespace und Namespace-Spiegelung) in der SVM mit Infinite Volume anzeigen. Zu den Angaben zu den Komponenten zählen folgende Informationen:

  - Name der Komponente
  - Zustand der Komponente
  - Name der SVM mit Infinite Volume, zu der die Komponente gehört
  - Verbindungspfad der Komponente
  - Name des Aggregats, in dem die Komponente enthalten ist
  - Verfügbare, genutzte und Gesamtkapazität der Komponente der Daten
- **Bundesland**

  Der aktuelle Status des Volumes:

  - Offline

    Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

  - Online

    Lese- und Schreibzugriff auf das Volume ist zulässig.

  - Eingeschränkt

Begrenzte Vorgänge, wie etwa die Paritätsrekonstruktion, sind zulässig, der Datenzugriff jedoch nicht.

- Gemischt

  Die Komponenten eines FlexGroup-Volumes sind nicht alle im selben Zustand.

- **Verbindungspfad**

  Der Pfad, auf den das Volume angehängt ist.

- **Storage Virtual Machine**

  Der SVM, die das Volume enthält.

- **Aggregate**

  Der Name des Aggregats, auf dem sich das Volume befindet, oder die Anzahl der Aggregate, auf denen sich das FlexGroup Volume befindet.

  Sie können auf den Namen klicken, um Details auf der Seite „Aggregatdetails“ anzuzeigen. Bei FlexGroup Volumes können Sie auf die Nummer klicken, um die Aggregate anzuzeigen, die in der FlexGroup auf der Seite Aggregate verwendet werden.

- **Tiering-Richtlinie**

  Die Tiering-Richtlinie für das Volume. Die Richtlinie wirkt sich nur dann aus, wenn das Volume auf einem FabricPool Aggregat bereitgestellt wird:

  - Keine. Die Daten für dieses Volume verbleiben immer auf der Performance-Tier.
  - Nur Snapshot: Nur Snapshot Daten werden automatisch in die Cloud-Tier verschoben. Alle anderen Daten verbleiben in der Performance-Tier.
  - Backup: Bei Datensicherungs-Volumes werden alle übertragenen Benutzerdaten in der Cloud-Tier gestartet, aber bei späteren Client-Lesevorgängen kann es dazu kommen, heiße Daten in die Performance-Tier zu verschieben.
  - Automatisch. Daten auf diesem Volume werden automatisch zwischen Performance-Tier und Cloud-Tier verschoben, wenn ONTAP feststellt, dass die Daten „`Hot`“ oder „`Cold`“ sind.

- **SnapLock Typ**

  Der SnapLock-Typ des Aggregats, der das Volume enthält. Verfügbare Optionen sind Compliance, Enterprise, Non-SnapLock.

- * Im Übergang*

  Ob die Transition des Volume abgeschlossen ist oder nicht.

- **Schutzrolle**

  Die Schutzrolle eines Volumens:

  - Ungesichert

    Lese-/Schreib-Volume ohne ausgehende oder eingehende SnapMirror- oder SnapVault-Beziehungen

  - Geschützt

Lese-/Schreib-Volume mit einer ausgehenden SnapMirror oder SnapVault Beziehung

- Ziel

  Datensicherung (DP)-Volume oder Lese-/Schreib-Volume mit einer eingehenden SnapMirror oder SnapVault Beziehung

- Keine Angabe

  Ein Volume, für das keine Sicherungsrollen gelten, wie z. B. ein Volume zur Lastenteilung, eine Datenkomponente oder ein temporäres Volume

  Sie können Ihren Zeiger über die Schutzrolle eines Volumes verschieben, um eine grafische Darstellung der Schutztopologie für das ausgewählte Volume anzuzeigen. Dazu können das Quell-Volume, die Gesamtzahl der ausgehenden synchronen und asynchronen SnapMirror Beziehungen und die Gesamtzahl der ausgehenden SnapVault Beziehungen gehören. Die blaue Markierung um die Lautstärke zeigt die ausgewählte Lautstärke an.

Durch Klicken auf **Anzeigen von Schutzdetails** wird die Registerkarte Schutz auf der Seite Daten zum Zustand/Volumen angezeigt.

- **Thin Provisioning**

  Gibt an, ob die Platzgarantie für das ausgewählte Volume festgelegt ist. Gültige Werte sind Ja und Nein

- **Verfügbare Datenkapazität**

  Die Menge an physischem Speicherplatz, der derzeit für Daten im Volume verfügbar ist.

- * Verfügbare Daten %*

  Der Prozentsatz des derzeit für Daten im Volume verfügbaren physischen Speicherplatzes.

- **Genutzte Datenkapazität**

  Die Menge an physischem Speicherplatz, der von Daten im Volume genutzt wird

- **Verwendete Daten %**

  Der Prozentsatz des physischen Speicherplatzes, der von Daten im Volume genutzt wird, basierend auf der insgesamt verfügbaren Datenkapazität.

- **Logischer Raum Verwendet %**

  Der Prozentsatz des logischen Speicherplatzes, der von Daten im Volume genutzt wird, basierend auf der insgesamt verfügbaren Datenkapazität.

- **Logical Space Reporting**

  Gibt an, ob das Volume über einen konfigurierten logischen Speicherplatz verfügt. Der Wert kann aktiviert, deaktiviert oder nicht zutreffend sein.

  Logischer Speicherplatz gibt die tatsächliche Größe der Daten an, die auf dem Volume gespeichert werden, ohne die Einsparungen durch ONTAP Storage-Effizienztechnologien zu verwenden.

- **Gesamtkapazität Der Daten**

Der insgesamt für Daten auf dem Volume verfügbare physische Speicherplatz.

- **Storage-Klasse**

  Der Name der Speicherklasse. Diese Spalte wird nur für Infinite Volume angezeigt.

- **Konstituierende Rolle**

  Der Rollenname der Komponente. Als Rollen können Namespace, Daten oder Namespace-Spiegelung genutzt werden. Diese Spalte wird nur für Infinite Volumes angezeigt.

- **Status Verschieben**

  Der aktuelle Status der Volume-Verschiebung. Der Status kann „in Bearbeitung“, „Pause“, „Fehlgeschlagen“ oder „Abgeschlossen“ sein.

  Sie können den Mauszeiger über den Status bewegen, um weitere Informationen zum Vorgang der Volume-Verschiebung anzuzeigen, z. B. Quelle, Ziel, Startzeit des Vorgangs, Ende des Vorgangs, aktuelle Phase der Volume-Verschiebung, die gerade ausgeführt wird, Status (in Prozent) und geschätzte Endzeit.

- **Caching-Richtlinie**

  Die dem ausgewählten Volume zugeordnete Caching-Richtlinie Die Richtlinie bietet Informationen darüber, wie das Flash Pool Caching für das Volume stattfindet.

Cache-Richtlinie	Beschreibung
Automatisch	Lese-Cache speichert alle Metadaten-Blöcke und liest zufällig gelesene Benutzerdatenblöcke im Cache und schreibt alle zufällig überschreibbaren Datenblöcke für Benutzer im Cache.
Keine	Keine Benutzerdaten oder Metadatenblöcke im Cache.
Alle	Lese-Caches mit allen Benutzerdaten, die gelesen und geschrieben werden Die Richtlinie führt kein Schreib-Caching durch.
Zufälliger Schreibzugriff	Diese Richtlinie ist eine Kombination aus den Richtlinien All und No Read-Random Write und führt die folgenden Aktionen durch: • Lese-Caches mit allen Benutzerdaten, die gelesen und geschrieben werden • Der Schreib-Cache speichert alle zufällig überschreibenden Benutzerdatenblöcke.
Alle Gelesen	Lese-Caches für alle Metadaten, zufällig gelesene und sequenziell gelesene Benutzerdatenblöcke

Cache-Richtlinie	Beschreibung
Alle Lese-Random-Schreibvorgänge	Diese Richtlinie ist eine Kombination aus den Richtlinien All Read und No Read-Random Write und führt die folgenden Aktionen durch: • Lese-Caches für alle Metadaten, zufällig gelesene und sequenziell gelesene Benutzerdatenblöcke • Der Schreib-Cache speichert alle zufällig überschreibenden Benutzerdatenblöcke.
Zufälliger Lesezugriff	Lese-Caches für alle Metadaten, zufällig gelesene, sequenziell gelesene und zufällig geschriebene Datenblöcke der Benutzer
Zufälliger Lesezugriff Mit Schreibzugriff	Diese Richtlinie besteht aus einer Kombination der Richtlinien All Read Random Write und No Read-Random Write. Sie führt Folgendes aus: • Lesen Sie den Cache aller Metadaten, zufällig gelesene und sequenziell gelesene sowie zufällig geschriebene Datenblöcke für die Benutzerdaten. • Der Schreib-Cache speichert alle zufällig überschreibenden Benutzerdatenblöcke.
Meta	Lesezugriffe erfolgen nur durch Metadaten-Blöcke.
Zufälliger Meta-Schreibvorgang	Diese Richtlinie ist eine Kombination aus Meta und No Read-Random Write und führt Folgendes aus: Nur Lese-Caches
Kein Lese-Random-Schreibvorgang	Der Schreib-Cache speichert alle zufällig überschreibenden Benutzerdatenblöcke. Die Richtlinie führt kein Lese-Caching durch.
Zufälliges Lesen	Lese-Caches für alle Metadaten-Blöcke und zufällig gelesene Benutzerdatenblöcke
Random-Read-Write	Der Lese-Cache speichert alle Metadaten, zufällig gelesene und zufällig geschriebene Datenblöcke der Benutzer.

Cache-Richtlinie	Beschreibung
Random-Read-Write – Zufällige Schreibzugriffe	Diese Richtlinie ist eine Kombination aus den Richtlinien für zufällige Schreibvorgänge und Schreibvorgänge ohne Lese-/Schreibzugriff. Folgende Schritte werden vorgenommen: • Der Lese-Cache speichert alle Metadaten im Cache, Lesezugriffe erfolgen nach dem Zufallsprinzip, und die Datenblöcke werden zufällig überschrieben. • Der Schreib-Cache speichert alle zufällig überschreibenden Benutzerdatenblöcke.

- **Cache-Aufbewahrungspriorität**

  Die Priorität für die Cache-Aufbewahrung für das Volume. Eine Priorität für die Cache-Aufbewahrung definiert, wie lange die Blöcke eines Volumes sich im Cache-Status befinden, sobald sie „kalt“ sind.

  ◦ Niedrig

  Speichern Sie das kalte Volume zum geringstmöglichen Zeitpunkt

  ◦ Normal

  Speichern Sie das kalte Volume-Blocks zum Standardzeitpunkt

  ◦ Hoch

  Speichern Sie das kalte Volume für höchste Zeit

- **Komprimierung**

  Gibt an, ob die Komprimierung für das Volume aktiviert ist In der Spalte wird entweder aktiviert oder deaktiviert angezeigt.

- **Deduplizierung**

  Gibt an, ob die Deduplizierung für das Volume aktiviert ist In der Spalte wird entweder aktiviert oder deaktiviert angezeigt.

- **Stil**

  Stil des Volumes: FlexVol oder FlexGroup.

- **Typ**

  Der Volume-Typ. Der Volume-Typ kann Lese-, Schreib- und Datenschutz, Lastverteilung oder Daten-Cache sein.

- * Cluster*

  Den Cluster, der das Ziel-Volume enthält. Sie können weitere Details zum Cluster anzeigen, indem Sie auf den Cluster-Namen klicken.

- **Cluster-Knoten**

  Der Name des Node, zu dem das Volume gehört, oder die Anzahl der Nodes, auf denen sich das FlexGroup Volume befindet. Weitere Details zum Cluster-Node können Sie anzeigen, indem Sie auf den Node-Namen klicken.

  Sie können auf den Node-Namen klicken, um Details auf der Seite „Node Details“ anzuzeigen. Für FlexGroup Volumes können Sie auf die Zahl klicken, um die Knoten anzuzeigen, die in der FlexGroup auf der Seite Knoten verwendet werden.

- **Lokale Snapshot-Richtlinie**

  Richtlinien für lokale Snapshot Kopien für die aufgeführten Volumes. Der Standardrichtlinienname ist Standard.

Bereich Filter

Im Bereich Filter können Sie Filter festlegen, um die Art und Weise anzupassen, wie Informationen in der Liste Volumes angezeigt werden. Sie können Filter auswählen, die sich auf die Spalten Volume Status, Status und Anmerkung beziehen.

Die im Fensterbereich Filter angegebenen Filter überschreiben die Filter, die für die Spalten in der Liste Volumes angegeben sind.

System-/Volume-Kapazität und Auslastungsseite

Auf der Seite Systemzustand/Volumes Kapazität und Auslastung werden Informationen über die Kapazität und Auslastung der Volumes in einem Cluster angezeigt. Diese Informationen geben Ihnen die Möglichkeit, mögliche Kapazitätsrisiken zu verstehen und die konfigurierte, verwendete und nicht genutzte Kapazität von Volumes anzuzeigen. Darüber hinaus können Sie mit diesen Informationen Entscheidungen zum Aktivieren speicherplatzsparender Funktionen wie Deduplizierung und Thin Provisioning treffen.

Verwenden Sie die Schaltfläche **Export**, um die Details aller überwachten Volumes in kommagetrennte Werte zu exportieren (`.csv`) Datei.

- * Cluster*

  Der Cluster-Name.

- **SVM**

  Der Name der Storage Virtual Machine (SVM), die das Volume enthält.

- **Lautstärke**

  Der Name des Volume.

- **Gesamtkapazität Der Daten**

  Die Gesamtkapazität (genutzter plus verfügbarer) Daten in einem Volume.

- **Genutzte Datenkapazität**

Der genutzten Datenkapazität in einem Volume.

- **Verwendete Daten %**

  Die verwendeten Daten in einem Volume als Prozentsatz.

- **Verfügbare Datenkapazität**

  Die verfügbare Datenkapazität in einem Volume.

- * Verfügbare Daten %*

  Die verfügbare Datenkapazität in einem Volume als Prozentsatz.

- * Tägliche Zuwachsrate %*

  Die Wachstumsrate, die alle 24 Stunden im Volumen stattfindet.

- **Tage Bis Voll**

  Die geschätzte Anzahl der verbleibenden Tage, bis die volle Kapazität des Volume erreicht ist.

- **Space Full Threshold %**

  Der Prozentsatz des im Volume verwendeten Speicherplatzes, der als voll betrachtet wird.

- **Space Fast Voll Schwellenwert %**

  Der Prozentsatz des im Volume genutzten Speicherplatzes, der als fast voll angesehen wird.

- **Wachstumsquote Schwellenwert %**

  Die Wachstumsrate des Volumes, die als normal angesehen wird, bevor das System ein anormales Ereignis für die Volume-Wachstumsrate generiert.

- **Schwellenwert Für Die Empfindlichkeit Der Wachstumsrate**

  Der Faktor, der auf die Standardabweichung der Wachstumsrate eines Volumens angewendet wird. Wenn die Wachstumsrate die faktorierte Standardabweichung überschreitet, wird ein ungewöhnliches Ereignis der Volumenwachstumsrate generiert.

- **Tage Bis Zur Vollständigen Schwelle**

  Die Anzahl der verbleibenden Tage, bevor die volle Kapazität erreicht wurde.

- **Snapshot-Überlauf %**

  Der Prozentsatz des Speicherplatzes, der von Snapshot Kopien verbraucht wird.

- **Verwendete Snapshot-Reserve Kapazität**

  Die Menge an Speicherplatz, der von Snapshot Kopien im Volume verwendet wird.

- **Snapshot Reserve Verwendet %**

  Die Menge an Speicherplatz, der von Snapshot Kopien im Volume als Prozentsatz verwendet wird.

- **Snapshot Reserve Verfügbare Kapazität**

  Die Menge an Speicherplatz, der für Snapshot Kopien im Volume verfügbar ist.

- **Snapshot Reserve Verfügbar %**

  Die Menge an Speicherplatz, die als Prozentsatz für Snapshot Kopien im Volume verfügbar ist.

- **Snapshot Reserve Gesamtkapazität**

  Zeigt die Gesamtkapazität der Snapshot Kopien im Volume an.

- **Snapshot Kopien Reservieren Voller Schwellenwert %**

  Der Prozentsatz, bei dem der für Snapshot Kopien reservierte Speicherplatz voll ist, gilt.

- **Schwellenwert Für Anzahl Der Snapshot-Kopien**

  Die Anzahl der Snapshot Kopien auf einem Volume, die als zu viele Kopien gelten.

- **Snapshot Kopiert Tage Bis Vollschwellenwert**

  Die Anzahl der verbleibenden Tage, bis der für Snapshot-Kopien reservierte Speicherplatz voll ist, erreicht die volle Kapazität.

- * Anzahl Inodes*

  Die Anzahl der Inodes im Volume.

- **Auslastung Von Nodes %**

  Der Prozentsatz des in dem Volume verwendeten Inode-Speicherplatzes.

- **Inodes Full Threshold %**

  Der Prozentsatz, bei dem ein Volume als verbraucht betrachtet wird, alle Inodes verbraucht zu haben.

- **Inodes Nahezu Vollen Schwellenwert %**

  Der Prozentsatz, bei dem ein Volumen betrachtet wird, um den Großteil seiner Inodes verbraucht zu haben.

- **Quote Zugesagt Kapazität**

  Der Speicherplatz, der für Kontingente im Volume reserviert ist.

- **Quote Überzuviel Kapazität**

  Die Menge an Speicherplatz, die für Quoten verwendet werden kann, bevor das System das überzustrapaziertes Ereignis des Volume Quota generiert.

- **Überschreitungsschwellenwert Für Quote %**

  Der Prozentsatz, bei dem der Platz für die Quoten auf dem Volumen genutzt wird, wird als überengagiert betrachtet.

- **Quote Nahezu Überfordert Schwellenwert %**

  Der Prozentsatz, bei dem der Platz für die Quoten auf dem Volumen genutzt wird, wird als fast übertrieben betrachtet.

- **Snapshot Autodelete**

  Gibt an, ob das automatische Löschen von Snapshot Kopien aktiviert oder deaktiviert ist.

- **Deduplizierung**

  Gibt an, ob die Deduplizierung für das Volume aktiviert oder deaktiviert ist

- **Deduplizierungseinsparungen**

  Die Menge an Speicherplatz, die durch die Deduplizierung in einem Volume eingespart wurde

- **Komprimierung**

  Gibt an, ob die Komprimierung für das Volume aktiviert oder deaktiviert ist

- **Komprimierung Raumeinsparungen**

  Die Menge an Speicherplatz, die durch Komprimierung in einem Volume eingespart wurde

- **Caching-Richtlinie**

  Die dem ausgewählten Volume zugeordnete Caching-Richtlinie

  Diese Richtlinie gibt Informationen darüber, wie Flash Pool Caching für das Volume stattfindet. Weitere Informationen zu Caching-Richtlinien finden Sie auf der Seite „Systemzustand/Volumes-Inventar“.

- **Cache-Aufbewahrungspriorität**

  Die Priorität, die für die Aufbewahrung von zwischengespeicherten Pools verwendet wird.

- **Thin Provisioning**

  Gibt an, ob die Platzgarantie für das ausgewählte Volume festgelegt ist. Gültige Werte sind Ja und Nein

- **Autogrow**

  Gibt an, ob das Volume automatisch mit der Größe wächst, wenn der Speicherplatz erschöpft ist

- * Raumgarantie*

  Die Storage-Garantie-Option, die für das Volume erforderlich ist.

- **Schutzrolle**

  Die Schutzrolle, die für das Volume festgelegt ist.

- **Bundesland**

  Der Status des zu exportierenden Volumes.

- **SnapLock Typ**

  Gibt an, ob es sich um ein SnapLock-Volume oder ein nicht-SnapLock-Volume handelt.

- **SnapLock Ablaufdatum**

  Das Verfalldatum des SnapLock.

- **Tiering-Richtlinie**

  Die Tiering-Richtlinie für das Volume. Gültig bei Implementierung nur in FabricPool-fähigen Aggregaten

Angaben zum Zustand/Volumen

Auf der Seite „Systemzustand/Volume-Details“ werden ausführliche Informationen zu einem ausgewählten Volume angezeigt, beispielsweise Kapazität, Storage-Effizienz, Konfiguration, Sicherung, Kommentare und erzeugte Ereignisse. Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für dieses Volume anzeigen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Befehlsschaltflächen

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

- **Wechseln Sie zur Leistungsansicht**

  Hier können Sie zur Seite Performance/Volume Details navigieren.

-

  Ermöglicht das Hinzufügen der ausgewählten Lautstärke zum Favoriten-Dashboard.

- **Aktionen**
  - Alarm Hinzufügen

    Ermöglicht das Hinzufügen einer Warnmeldung zum ausgewählten Volume.

  - Schwellenwerte Bearbeiten

    Ermöglicht das Ändern der Schwellenwerteinstellungen für das ausgewählte Volume.

  - Anmerkungen Hinzufügen

    Ermöglicht Ihnen, das ausgewählte Volume mit Anmerkungen zu versehen.

  - Sichern

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

  - Beziehung

Ermöglicht Ihnen die Ausführung folgender Sicherungsbeziehungsvorgänge:

- Bearbeiten

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

- Abbrechen

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

- Stilllegen

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

- Pause

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

- Entfernen

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

- Fortsetzen

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

- Neu Synchronisieren

  Ermöglicht Ihnen die Neusynchronisierung einer zuvor unterbrochenen Beziehung.

- Initialisierung/Aktualisierung

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

- Reverse Resync

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

◦ Wiederherstellen

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

Die Schaltfläche „Wiederherstellen“ und die Schaltflächen für den Beziehungsvorgang stehen nicht für FlexGroup-Volumes oder für Volumes mit synchronem Schutz zur Verfügung.

- **View Volumes**

  Hier können Sie zur Seite „Health/Volumes Inventory“ navigieren.

Registerkarte „Kapazität“

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

- **Kapazität Physisch**

  Detaillierte Informationen zur physischen Kapazität des Volumes:

  - Snapshot-Überlauf

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

  - Verwendet

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

  - Warnung

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

  - Fehler

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

  - Nicht Nutzbar

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

  - Datendiagramm

    Zeigt die Gesamtkapazität und die genutzte Datenkapazität des Volume an.

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

    - Tatsächliche Datenkapazität des Volumes für die folgenden Bedingungen:
      - Autogrow ist deaktiviert.

        - Das autogrow-fähige Volume hat die maximale Größe erreicht.
        - Autogrow-aktivierte Volumes mit Thick Provisioning können nicht weiter wachsen.
      - Datenkapazität des Volumes unter Berücksichtigung der maximalen Volume-Größe (für Volumes mit Thin Provisioning und für Thick Provisioning Volumes, wenn das Aggregat über genügend Platz für das Volume verfügt, um die maximale Größe zu erreichen)
      - Datenkapazität des Volumes nach Berücksichtigung der nächsten möglichen Autogrow Größe (für Thick Provisioning Volumes, die einen Autogrow-Prozentwert haben)
    - Diagramm Snapshot Kopien

      Dieses Diagramm wird nur angezeigt, wenn die verwendete Snapshot-Kapazität oder die Snapshot-Reserve nicht null ist.

  Beide Diagramme zeigen die Kapazität an, um die die Snapshot-Kapazität die Snapshot-Reserve überschreitet, wenn die verwendete Snapshot-Kapazität die Snapshot-Reserve überschreitet.

- **Kapazität Logisch**

  Zeigt die logischen Platzeigenschaften des Volumes an. Der logische Speicherplatz gibt die tatsächliche Größe der auf Festplatte gespeicherten Daten an, ohne dabei die Einsparungen durch die ONTAP Storage-Effizienztechnologien zu verwenden.

    - Bericht Zu Logischem Speicherplatz

      Zeigt an, ob für das Volume ein Bericht über den logischen Speicherplatz konfiguriert ist. Der Wert kann aktiviert, deaktiviert oder nicht zutreffend sein. „`not anwendbare`“ wird für Volumes auf älteren ONTAP-Versionen oder auf Volumes angezeigt, die kein logisches Speicherplatz-Reporting unterstützen.

    - Verwendet

      Zeigt die Menge des logischen Speicherplatzes an, der von Daten im Volume verwendet wird, und den Prozentsatz des logischen Speicherplatzes, der basierend auf der Gesamtkapazität genutzt wird.

    - Verfügbar

      Zeigt die Menge des logischen Speicherplatzes an, der noch für Daten im Volume verfügbar ist, und den Prozentsatz des verfügbaren logischen Speicherplatzes basierend auf der Gesamtkapazität.

    - Durchsetzung Des Logischen Speicherplatzes

      Zeigt an, ob die Durchsetzung des logischen Speicherplatzes für über Thin Provisioning bereitgestellte Volumes konfiguriert ist. Bei Einstellung auf aktiviert kann die verwendete logische Größe des Volumes nicht größer sein als die aktuell eingestellte physische Volume-Größe.

- **Autogrow**

  Zeigt an, ob das Volumen automatisch wächst, wenn es nicht mehr genügend Speicherplatz hat.

- * Raumgarantie*

  Zeigt die FlexVol-Lautstärkeregelung an, wenn ein Volume freie Blöcke aus einem Aggregat entfernt. Diese Blöcke sind dann garantiert für Schreibvorgänge auf Dateien im Volume verfügbar. Die Speicherplatzgarantie kann auf eine der folgenden gesetzt werden:

- Keine

  Es wurde keine Speicherplatzzusage für das Volume konfiguriert.

- Datei

  Die vollständige Größe von dünn geschriebenen Dateien (zum Beispiel LUNs) ist garantiert.

- Datenmenge

  Die volle Größe des Volumens wird garantiert.

- Teilweise

  Das FlexCache-Volume reserviert basierend auf seiner Größe Speicherplatz. Wenn die Größe des FlexCache-Volumes 100 MB oder mehr ist, ist die Mindestplatzgarantie standardmäßig auf 100 MB gesetzt. Wenn die Größe des FlexCache-Volumes weniger als 100 MB ist, wird die Mindestplatzgarantie auf die Größe des FlexCache-Volumes gesetzt. Wenn die Größe des FlexCache-Volumes später erhöht wird, wird die Mindestplatzgarantie nicht erhöht.

  Die Speicherplatzzusage ist ein Teil, wenn es sich um ein Volume vom Typ Data-Cache handelt.

- **Details (Physisch)**

  Zeigt die physischen Merkmale des Volumes an.

- **Gesamtkapazität**

  Zeigt die gesamte physische Kapazität im Volume an.

- **Datenkapazität**

  Zeigt den vom Volume genutzten physischen Speicherplatz (genutzte Kapazität) und die Menge an verfügbarem (freier Kapazität) physischen Speicherplatz im Volume an. Diese Werte werden auch als Prozentsatz der gesamten physischen Kapazität angezeigt.

  Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, wird die vom Volume verwendete Menge an Speicherplatz (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht verwendet werden kann (nicht nutzbare Kapazität), da die Kapazität des Aggregats angezeigt wird.

- **Snapshot Reserve**

  Zeigt die Menge an Speicherplatz an, der von den Snapshot Kopien verwendet (genutzte Kapazität) und die Menge an Speicherplatz, die für Snapshot Kopien verfügbar ist (freie Kapazität) im Volume an. Diese Werte werden auch als Prozentsatz der gesamten Snapshot-Reserve angezeigt.

  Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, dann wird die Menge an Speicherplatz, der von den Snapshot Kopien verwendet wird (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht für die Erstellung von Snapshot Kopien verwendet werden kann (nicht nutzbare Kapazität). Aufgrund von Aggregat-Kapazitätsproblemen wird angezeigt.

- **Volumenschwellwerte**

Zeigt die folgenden Schwellenwerte für die Volume-Kapazität an:

- Nahezu Vollständig. Schwellenwert

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

- Vollständiger Schwellenwert

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

- **Weitere Details**
  - Autogrow Maximalgröße

    Zeigt die maximale Größe an, bis die Lautstärke automatisch erweitert werden kann. Der Standardwert ist 120 % der Volume-Größe bei der Erstellung. Dieses Feld wird nur angezeigt, wenn Autogrow für das Volume aktiviert ist.

  - Der Qtree Kontingent Verplante Kapazität

    Zeigt den Speicherplatz an, der in den Quoten reserviert wurde.

  - Qtree-Kontingent Überbeansprucht Kapazität

    Zeigt die Menge an Speicherplatz an, die verwendet werden kann, bevor das System das überverplante Ereignis des Volume Qtree-Kontingents generiert.

  - Fraktionale Reserve

    Steuert die Größe der Überschreibungsreserve. Standardmäßig ist die fraktionale Reserve auf 100 festgelegt und gibt an, dass 100 Prozent des erforderlichen reservierten Speicherplatzes reserviert werden, damit die Objekte für Überschreibungen vollständig gesichert sind. Wenn die fraktionale Reserve weniger als 100 Prozent beträgt, wird der reservierte Speicherplatz für alle platzreservierten Dateien in diesem Volume auf den Prozentsatz der fraktionalen Reserve reduziert.

  - Tägliche Snapshot Wachstumsrate

    Zeigt die Änderung an (in Prozent oder in KB, MB, GB usw.), die alle 24 Stunden in den Snapshot Kopien des ausgewählten Volumes stattfindet.

  - Snapshot Tage voll belegt

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

    Das Feld „Snapshot Days to Full“ zeigt einen nicht anwendbaren Wert an, wenn das Wachstum der Snapshot-Kopien im Volume null oder negativ ist oder wenn es keine Daten zur Berechnung der Wachstumsrate gibt.

  - Snapshot Automatisch Löschen

    Gibt an, ob Snapshot Kopien automatisch in freien Speicherplatz gelöscht werden, wenn ein Schreibvorgang auf ein Volume aufgrund von fehlendem Speicherplatz im Aggregat ausfällt.

  - Snapshots

Zeigt Informationen über die Snapshot-Kopien im Volume an.

Die Anzahl der Snapshot Kopien auf dem Volume wird als Link angezeigt. Wenn Sie auf den Link klicken, werden die Snapshot Kopien in dem Dialogfeld Volume geöffnet, in dem Details zu den Snapshot Kopien angezeigt werden.

Die Anzahl der Snapshot Kopien wird etwa jede Stunde aktualisiert. Die Liste der Snapshot-Kopien wird jedoch zu dem Zeitpunkt aktualisiert, zu dem Sie auf das Symbol klicken. Dies kann zu einem Unterschied zwischen der in der Topologie angezeigten Anzahl der Snapshot Kopien und der Anzahl der aufgelisteten Snapshot Kopien führen, wenn Sie auf das Symbol klicken.

- **Volume Move**

  Zeigt den Status der aktuellen oder der letzten Volume-Verschiebung an, die am Volume durchgeführt wurde, und weitere Details an, z. B. die aktuelle Phase der Verschiebung eines Volumes – im Gange ist, das Quellaggregat, das Zielaggregat, die Startzeit, die Endzeit, Und die geschätzte Endzeit.

  Zeigt außerdem die Anzahl der Vorgänge zum Verschieben von Volumes an, die auf dem ausgewählten Volume ausgeführt werden. Weitere Informationen über die Vorgänge zum Verschieben von Volumes erhalten Sie, indem Sie auf den Link **Protokoll zum Verschieben von Volumes** klicken.

„Effizienz“

Die Registerkarte „Effizienz“ zeigt Informationen über den in den Volumes gespeicherten Speicherplatz mithilfe von Storage-Effizienzfunktionen wie Deduplizierung, Komprimierung und FlexClone Volumes an.

- **Deduplizierung**
  - Aktiviert

    Gibt an, ob die Deduplizierung auf einem Volume aktiviert oder deaktiviert ist.

  - Speicherersparnis

    Zeigt die Menge an gespeichertem Speicherplatz (in Prozent oder in KB, MB, GB usw.) in einem Volume mithilfe der Deduplizierung an.

  - Letzter Lauf

    Zeigt die Zeit an, die seit dem letzten Deduplizierungsvorgang verstrichen ist. Außerdem gibt an, ob der Deduplizierungsvorgang erfolgreich war.

  Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, der den Zeitpunkt der Durchführung des Vorgangs darstellt.

  - Modus

    Gibt an, ob der auf einem Volume aktivierte Deduplizierungsvorgang ein manueller, geplanter oder richtlinienbasierter Vorgang ist. Wenn der Modus auf „geplant“ eingestellt ist, wird der Betriebsplan angezeigt, und wenn der Modus auf eine Richtlinie festgelegt ist, wird der Richtlinienname angezeigt.

  - Status

    Zeigt den aktuellen Status des Deduplizierungsvorgangs an. Der Status kann „Idle“, „Initialisieren“, „aktiv“, „Rückgängig“, „Ausstehend“, „Ausstehend“ sein. Downgrade oder deaktiviert.

◦ Typ

Gibt den Typ des Deduplizierungsvorgangs an, der auf dem Volume ausgeführt wird. Wenn das Volume eine SnapVault-Beziehung hat, wird als SnapVault angezeigt. Für jedes andere Volumen wird der Typ als normal angezeigt.

- **Komprimierung**
  - Aktiviert

    Gibt an, ob die Komprimierung auf einem Volume aktiviert oder deaktiviert ist.

  - Speicherersparnis

    Zeigt den eingesparten Speicherplatz (in Prozent oder in KB, MB, GB usw.) in einem Volume mithilfe der Komprimierung an.

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration werden Details zum ausgewählten Volume angezeigt, z. B. Richtlinie für den Export, RAID-Typ, Kapazität und Storage-Effizienz-Funktionen des Volumes:

- **Übersicht**
  - Vollständiger Name

    Zeigt den vollständigen Namen des Volumes an.

  - Aggregate

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

  - Tiering-Richtlinie

    Zeigt die Tiering-Richtlinie für das Volume an; wenn das Volume auf einem FabricPool-fähigen Aggregat implementiert wird. Die Richtlinie kann „Keine“, „nur Snapshot“, „Backup“ oder „automatisch“ lauten.

  - Storage Virtual Machine

    Zeigt den Namen der Storage Virtual Machine (SVM) an, die das Volume enthält.

  - Verbindungspfad

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

  - Exportrichtlinie

    Zeigt den Namen der Exportrichtlinie an, die für das Volume erstellt wurde. Über den Link können Sie Details zu den Exportrichtlinien, den Authentifizierungsprotokollen und den aktivierten Zugriff auf die Volumes anzeigen, die zu der SVM gehören.

  - Stil

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

- Typ

  Zeigt den Typ des ausgewählten Volumens an. Der Volume-Typ kann Lese-/Schreibvorgänge, Lastverteilung, Datensicherung, Daten-Cache oder temporär sein.

- RAID-Typ

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

  > Es können mehrere RAID-Typen für FlexGroup Volumes angezeigt werden, da sich die zusammengehörigen Volumes für FlexGroups auf Aggregaten unterschiedlicher Typen sein können.

- SnapLock-Typ

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

- SnapLock Expiry

  Zeigt das Ablaufdatum des SnapLock-Volume an.

- * Kapazität*
  - Thin Provisioning

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

  - Autogrow

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

  - Snapshot Automatisch Löschen

    Gibt an, ob Snapshot Kopien automatisch in freien Speicherplatz gelöscht werden, wenn ein Schreibvorgang auf ein Volume aufgrund von fehlendem Speicherplatz im Aggregat ausfällt.

  - Kontingente

    Gibt an, ob die Quoten für das Volume aktiviert sind.

- * Effizienz*
  - Deduplizierung

    Gibt an, ob die Deduplizierung für das ausgewählte Volume aktiviert oder deaktiviert ist.

  - Komprimierung

    Gibt an, ob die Komprimierung für das ausgewählte Volume aktiviert oder deaktiviert ist.

- **Schutz**
  - Snapshots

Gibt an, ob die automatischen Snapshot Kopien aktiviert oder deaktiviert sind.

Registerkarte „Schutz“

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

- **Zusammenfassung**

  Zeigt die Eigenschaften von SnapMirror- und SnapVault-Beziehungen für ein ausgewähltes Volume an. Für einen anderen Beziehungstyp wird nur die Eigenschaft Beziehungstyp angezeigt. Wenn ein primäres Volume ausgewählt wird, werden nur die Richtlinie für verwaltete und lokale Snapshot-Kopien angezeigt. Für SnapMirror und SnapVault Beziehungen werden folgende Eigenschaften angezeigt:

  - Quell-Volume

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

  - Verzögerungsstatus

    Zeigt den Status der Update- oder Transferverzögerungen für eine Schutzbeziehung an. Der Status kann „Fehler“, „Warnung“ oder „kritisch“ sein.

    Der lag-Status gilt nicht für synchrone Beziehungen.

  - Verzögerungsdauer

    Zeigt die Zeit an, mit der die Daten auf dem Spiegel hinter der Quelle liegen.

  - Letzte Erfolgreiche Aktualisierung

    Zeigt Datum und Uhrzeit der letzten erfolgreichen Schutzaktualisierung an.

    Die letzte erfolgreiche Aktualisierung gilt nicht für synchrone Beziehungen.

  - Storage Service-Mitglied

    Zeigt entweder Ja oder Nein an, um anzugeben, ob das Volume zu einem Storage-Service gehört und von diesem gemanagt wird.

  - Versionsflexible Replizierung

    Zeigt entweder Ja, Ja mit Sicherungsoption oder Keine an. Ja zeigt an, dass die SnapMirror Replizierung möglich ist, auch wenn auf Quell- und Ziel-Volumes unterschiedliche Versionen der ONTAP Software ausgeführt werden. Ja, mit der Backup-Option bezeichnet die Implementierung von SnapMirror Sicherung mit der Möglichkeit, mehrere Versionen von Backup-Kopien auf dem Zielsystem aufzubewahren. Keine gibt an, dass die Version Flexible Replikation nicht aktiviert ist.

  - Beziehungsfähigkeit

    Zeigt die ONTAP-Funktionen an, die für die Sicherungsbeziehung verfügbar sind.

  - Protection Service

    Zeigt den Namen des Schutzdienstes an, wenn die Beziehung von einer Schutzpartneranwendung

verwaltet wird.

- Beziehungstyp

  Zeigt alle Beziehungstypen an, einschließlich Asynchronous Mirror, Asynchronous Vault, StrictSync und Sync.

- Beziehungsstatus

  Zeigt den Status der SnapMirror oder SnapVault Beziehung an. Der Staat kann ohne Initialisierung, SnapMirrored oder Abbruch erfolgen. Wenn ein Quell-Volume ausgewählt ist, ist der Beziehungsstatus nicht zutreffend und wird nicht angezeigt.

- Übertragungsstatus

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

  - Wird Abgebrochen

    SnapMirror-Transfers sind aktiviert; ein Vorgang, bei dem der Transfer abgebrochen wird, während das Checkpoint entfernt wird.

  - Prüfen

    Das Zielvolumen wird einer Diagnose-Prüfung unterzogen und es wird keine Übertragung durchgeführt.

  - Abschließen

    SnapMirror Transfers sind aktiviert. Das Volume befindet sich derzeit in der Phase nach dem Transfer für inkrementelle SnapVault Transfers.

  - Leerlauf

    Transfers sind aktiviert, und es wird keine Übertragung durchgeführt.

  - Synchronisiert

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

  - Out-of-Sync

    Die Daten im Ziel-Volume werden nicht mit dem Quell-Volume synchronisiert.

  - Vorbereitung

    SnapMirror Transfers sind aktiviert. Das Volume befindet sich derzeit in der Phase vor der Übertragung für inkrementelle SnapVault Transfers.

  - Warteschlange

    SnapMirror Transfers sind aktiviert. Es werden keine Transfers durchgeführt.

  - Stillgelegt

SnapMirror Transfers sind deaktiviert. Es wird keine Übertragung durchgeführt.

- Wird Stillgelegt

  Ein SnapMirror Transfer läuft. Zusätzliche Transfers sind deaktiviert.

- Übertragung

  SnapMirror Transfers sind aktiviert, und ein Transfer läuft.

- Übergang

  Der asynchrone Datentransfer aus dem Quell- zum Ziel-Volume ist abgeschlossen, und der Übergang zum synchronen Betrieb wurde gestartet.

- Warten

  Ein SnapMirror Transfer wurde initiiert, aber einige zugehörige Aufgaben warten darauf, in die Warteschlange verschoben zu werden.

◦ Max. Übertragungsrate

Zeigt die maximale Übertragungsrate für die Beziehung an. Die maximale Übertragungsrate kann ein numerischer Wert in Kilobyte pro Sekunde (Kbit/s), Megabyte pro Sekunde (Mbit/s), Gigabyte pro Sekunde (Gbit/s) oder Terabyte pro Sekunde (Tbit/s) sein. Wenn kein Limit angezeigt wird, ist die Basistransfer zwischen Beziehungen unbegrenzt.

◦ SnapMirror Richtlinie

Zeigt die Schutzrichtlinie für das Volume an. DPStandard gibt die standardmäßige Richtlinie für den Schutz der asynchronen Spiegelung an, und XDPStandard gibt die standardmäßige asynchrone Vault-Richtlinie an. StrictSync gibt die standardmäßige Richtlinie für den synchronen strengen Schutz an, und Sync gibt die standardmäßige synchrone Richtlinie an. Sie können auf den Richtliniennamen klicken, um die mit dieser Richtlinie verknüpften Details anzuzeigen, einschließlich der folgenden Informationen:

- Übertragungspriorität
- Einstellung der Zugriffszeit ignorieren
- Limit für Versuche
- Kommentare
- SnapMirror-Labels
- Aufbewahrungseinstellungen
- Tatsächliche Snapshot Kopien
- Bewahren Sie Snapshot Kopien auf
- Schwellenwert für Warnung bei Aufbewahrung
- Snapshot-Kopien ohne Aufbewahrungseinstellungen in einer kaskadierenden SnapVault-Beziehung, wobei die Quelle ein Datensicherungs-Volume (DP) ist, gilt nur die Regel „`sm_created`“.

◦ Zeitplan Aktualisieren

Zeigt den SnapMirror Zeitplan an, der der Beziehung zugewiesen ist. Wenn Sie den Cursor über das

Informationssymbol positionieren, werden die Terminplandetails angezeigt.

- Lokale Snapshot-Richtlinie

  Zeigt die Snapshot Kopie-Richtlinie für das Volume an. Die Richtlinie ist Standard, Keine oder ein beliebiger Name, der einer benutzerdefinierten Richtlinie zugewiesen wurde.

- **Ausblick**

  Zeigt die Schutztopologie des ausgewählten Volumes an. Die Topologie enthält grafische Darstellungen aller Volumes, die sich auf das ausgewählte Volume beziehen. Das ausgewählte Volumen wird durch einen dunkelgrauen Rahmen angezeigt, und Linien zwischen Volumes in der Topologie geben den Schutzbeziehungstyp an. Die Richtung der Beziehungen in der Topologie wird von links nach rechts angezeigt, wobei die Quelle jeder Beziehung auf der linken Seite und das Ziel auf der rechten Seite.

  Doppelte Fett gedruckte Zeilen geben eine asynchrone Spiegelbeziehung an, eine einzelne, fettgedruckte Zeile gibt eine asynchrone Vault-Beziehung an, und eine fettgedruckte Zeile und eine nicht-bold-Zeile gibt eine synchrone Beziehung an. Die folgende Tabelle gibt an, ob die Beziehung StrictSync oder Sync ist.

  Durch Klicken mit der rechten Maustaste auf ein Volume wird ein Menü angezeigt, aus dem Sie entweder das Volume schützen oder Daten darauf wiederherstellen können. Mit der rechten Maustaste auf eine Beziehung klicken wird ein Menü angezeigt, aus dem Sie entweder bearbeiten, abbrechen, stilllegen, brechen, entfernen, Oder nehmen Sie eine Beziehung wieder auf.

  Die Menüs werden in den folgenden Fällen nicht angezeigt:

  - Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
  - Wenn es sich um ein FlexGroup Volume handelt
  - Wenn sich das Volume in einer synchronen Schutzbeziehung befindet
  - Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung vorliegt und das Ziel-Cluster noch nicht erkannt wurde, wird durch Klicken auf ein anderes Volume in der Topologie Informationen für das entsprechende Volume ausgewählt und angezeigt. Ein Fragezeichen ( ) In der linken oberen Ecke eines Volumens gibt an, dass entweder das Volumen fehlt oder es noch nicht entdeckt wurde. Sie können außerdem angeben, dass Kapazitätsinformationen nicht vorhanden sind. Wenn Sie den Mauszeiger über das Fragezeichen positionieren, werden weitere Informationen angezeigt, einschließlich Vorschläge für Korrekturmaßnahmen.

    In der Topologie werden Informationen zur Volume-Kapazität, Verzögerung, Snapshot-Kopien und zum letzten erfolgreichen Datentransfer angezeigt, wenn sie einer von mehreren gängigen Topologievorlagen entspricht. Wenn eine Topologie keiner dieser Vorlagen entspricht, werden Informationen zur Volume-Verzögerung und zum letzten erfolgreichen Datentransfer in einer Beziehungstabelle unter der Topologie angezeigt. In diesem Fall gibt die markierte Zeile in der Tabelle das ausgewählte Volume an, und in der Topologieansicht zeigen fettgedruckte Linien mit einem blauen Punkt die Beziehung zwischen dem ausgewählten Volume und seinem Quellvolumen an.

  Topologieansichten umfassen folgende Informationen:

  - Kapazität

    Zeigt die Gesamtkapazität des Volumes an. Wenn Sie den Cursor auf ein Volumen in der Topologie positionieren, werden im Dialogfeld Aktuelle Schwellenwerteinstellungen die aktuellen Warn- und kritischen Schwellwerte für dieses Volume angezeigt. Sie können die Schwellenwerteinstellungen auch bearbeiten, indem Sie im Dialogfeld Aktuelle Schwellenwerteinstellungen auf den Link

Schwellenwerte bearbeiten klicken. Wenn Sie das Kontrollkästchen **Kapazität** deaktivieren, werden alle Kapazitätsinformationen für alle Volumes in der Topologie ausgeblendet.

- Verzögerung

  Zeigt die Verzögerungsdauer und den Verzögerungsstatus der eingehenden Schutzbeziehungen an. Wenn Sie das Kontrollkästchen **lag** deaktivieren, werden alle lag-Informationen für alle Volumes in der Topologie ausgeblendet. Wenn das Kontrollkästchen **lag** gedimmt ist, werden die Verzögerungsinformationen für das ausgewählte Volume in der Beziehungstabelle unter der Topologie sowie die lag-Informationen für alle zugehörigen Volumes angezeigt.

- Snapshot

  Zeigt die Anzahl der für ein Volume verfügbaren Snapshot Kopien an. Wenn Sie das Kontrollkästchen **Snapshot** deaktivieren, werden alle Snapshot Kopie-Informationen für alle Volumes in der Topologie ausgeblendet. Klicken auf das Symbol für die Snapshot Kopie ( ) Zeigt die Liste der Snapshot Kopien für ein Volume an. Die Anzahl der Snapshot Kopien neben dem Symbol wird ungefähr jede Stunde aktualisiert. Die Liste der Snapshot-Kopien wird jedoch beim Klicken auf das Symbol aktualisiert. Dies kann zu einem Unterschied zwischen der in der Topologie angezeigten Anzahl der Snapshot Kopien und der Anzahl der aufgelisteten Snapshot Kopien führen, wenn Sie auf das Symbol klicken.

- Letzte Erfolgreiche Übertragung

  Zeigt den Betrag, die Dauer, die Zeit und das Datum der letzten erfolgreichen Datenübertragung an. Wenn das Kontrollkästchen **Letzter erfolgreicher Transfer** abgeblendet ist, werden die letzten erfolgreichen Übertragungsinformationen für das ausgewählte Volume in der Beziehungstabelle unter der Topologie sowie die letzten erfolgreichen Übertragungsinformationen für alle zugehörigen Volumes angezeigt.

- **Geschichte**

  Zeigt die Historie der eingehenden SnapMirror- und SnapVault-Sicherungsbeziehungen für das ausgewählte Volume in einem Diagramm an. Es sind drei Verlaufsdiagramme verfügbar: Die Dauer des eingehenden Beziehungsverzögerungsablaufs, die Dauer der eingehenden Beziehungstransfers und die Größe der eingehenden Beziehung, die übertragen wurde. Die Verlaufsdaten werden nur angezeigt, wenn Sie ein Zielvolume auswählen. Wenn Sie ein primäres Volume auswählen, sind die Diagramme leer und die Meldung `No data found` Wird angezeigt.

  Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Historische Grafiken können Ihnen bei der Identifizierung von Trends helfen: Wenn zum Beispiel große Datenmengen zur gleichen Zeit des Tages oder der Woche übertragen werden oder wenn der lag-Warn- oder lag-Fehlerschwellenwert konsistent verletzt wird, können Sie geeignete Maßnahmen ergreifen. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

  Sicherungsverlauf-Diagramme zeigen die folgenden Informationen an:

  - **Beziehungsdauer**

    Anzeige von Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Anzeige von Tagen, Monaten oder Jahren auf der horizontalen Achse (x), abhängig vom ausgewählten Zeitraum. Der obere Wert auf der Y-Achse gibt die maximale Verzögerungsdauer an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. In der orangefarbenen Linie im Diagramm wird der lag-

Fehlerschwellenwert angezeigt, während die horizontale gelbe Linie den lag-Warnungsschwellenwert darstellt. Wenn Sie den Mauszeiger über diese Zeilen positionieren, wird die Schwellenwerteinstellung angezeigt. Die waagerechte blaue Linie zeigt die Verzögerungsdauer an. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen interessanten Bereich positionieren.

- **Dauer Der Beziehungsübertragung**

  Anzeige von Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Anzeige von Tagen, Monaten oder Jahren auf der horizontalen Achse (x), abhängig vom ausgewählten Zeitraum. Der obere Wert auf der Y-Achse gibt die maximale Übertragungsdauer an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den Bereich von Interesse positionieren.

  Dieses Diagramm ist nicht für Volumes verfügbar, die sich in synchronen Sicherungsbeziehungen befinden.

- **Beziehung Übertragen Größe**

  Zeigt Bytes, Kilobyte, Megabyte usw. auf der vertikalen Achse (y) je nach Übertragungsgröße an und zeigt Tage, Monate oder Jahre auf der horizontalen Achse (x) je nach ausgewähltem Zeitraum an. Der obere Wert auf der Y-Achse gibt die maximale Übertragungsgröße an, die im auf der x-Achse angezeigten Zeitraum erreicht wurde. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen interessanten Bereich positionieren.

Dieses Diagramm ist nicht für Volumes verfügbar, die sich in synchronen Sicherungsbeziehungen befinden.

Historienbereich

Im Bereich Verlauf werden Diagramme angezeigt, die Informationen über die Kapazität und die Platzreservierungen des ausgewählten Volumes enthalten. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

Diagramme sind möglicherweise leer und die Meldung `No data found` Wird angezeigt, wenn die Daten oder der Status des Volumes über einen Zeitraum hinweg unverändert bleiben.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Verlaufsdiagramme können Ihnen dabei helfen, Trends zu erkennen - wenn beispielsweise die Volumennutzung den Schwellenwert „nahezu voll“ konsistent überschreitet, können Sie entsprechende Maßnahmen ergreifen.

Verlaufsdiagramme zeigen folgende Informationen an:

- **Verwendete Volume-Kapazität**

  Zeigt die verwendete Kapazität im Volume und den Trend in der Art und Weise an, wie die Volume-Kapazität basierend auf dem Nutzungsverlauf verwendet wird, als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende zu „Volume Used Capacity“

klicken, wird die Zeile des Diagramms „Volume Used Capacity“ ausgeblendet.

- **Verwendete Volume-Kapazität vs Gesamt**

  Zeigt den Trend der Volume-Kapazität basierend auf dem Nutzungsverlauf sowie der verwendeten Kapazität, der Gesamtkapazität und den Details der Speicherersparnis durch Deduplizierung und Komprimierung an. Dies sind Liniendiagramme in Byte, Kilobyte, Megabyte, Und so weiter, auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „verwendete Trend-Kapazität“ klicken, wird das Diagramm „verwendete Trendkapazität“ ausgeblendet.

- **Verwendete Volume-Kapazität (%)**

  Zeigt die verwendete Kapazität im Volumen und den Trend in der Art und Weise an, wie die Volume-Kapazität basierend auf dem Nutzungsverlauf, als Liniendiagramme, in Prozent, auf der vertikalen (y) Achse verwendet wird. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende zu „Volume Used Capacity“ klicken, wird die Zeile des Diagramms „Volume Used Capacity“ ausgeblendet.

- **Verwendete Snapshot-Kapazität (%)**

  Zeigt den Schwellenwert für die Snapshot-Reserve und die Snapshot-Warnung als Liniendiagramme und die von den Snapshot Kopien verwendete Kapazität als Diagramm in Prozent auf der vertikalen Achse (y) an. Der Snapshot-Überlauf ist mit verschiedenen Farben dargestellt. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende der Snapshot Reserve klicken, wird die Grafik der Snapshot Reserve ausgeblendet.

Ereignisliste

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

- **Severity**

  Zeigt den Schweregrad des Ereignisses an.

- **Veranstaltung**

  Zeigt den Ereignisnamen an.

- **Auslösezeit**

  Zeigt die Zeit an, die seit der Erzeugung des Ereignisses verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, zu dem das Ereignis generiert wurde.

Bereich „Verwandte Anmerkungen“

Im Bereich Verwandte Anmerkungen können Sie Anmerkungsdetails anzeigen, die mit dem ausgewählten Volume verknüpft sind. Die Details umfassen den Anmerkungsnamen und die Anmerkungswerte, die auf das Volumen angewendet werden. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie SVMs, Aggregate, qtrees, LUNs und Snapshot Kopien anzeigen und navigieren, die mit dem Volume zusammenhängen:

- **Storage Virtual Machine**

  Zeigt die Kapazität und den Integritätsstatus der SVM an, die das ausgewählte Volume enthält.

- * Aggregat*

  Zeigt die Kapazität und den Integritätsstatus des Aggregats an, das das ausgewählte Volume enthält. Für FlexGroup Volumes wird die Anzahl der Aggregate aufgelistet, die die FlexGroup umfassen.

- **Volumen im Aggregat**

  Zeigt die Anzahl und Kapazität aller Volumes an, die zum übergeordneten Aggregat des ausgewählten Volumes gehören. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt. Wenn beispielsweise ein Aggregat zehn Volumes enthält, von denen fünf den Warnstatus und die übrigen fünf den kritischen Status anzeigen, ist der angezeigte Status kritisch. Diese Komponente wird für FlexGroup-Volumes nicht angezeigt.

- **Qtrees**

  Zeigt die Anzahl der vom ausgewählten Volume enthaltenen qtrees sowie die Kapazität von qtrees mit Kontingent an, die das ausgewählte Volume enthält. Die Kapazität der qtrees mit Kontingent wird in Bezug auf die Volume-Datenkapazität angezeigt. Auf der Grundlage des höchsten Schweregrades wird auch der Integritätsstatus der qtrees angezeigt. Wenn ein Volume beispielsweise zehn qtrees, fünf mit Warnstatus und die verbleibenden fünf mit kritischem Status aufweist, ist der angezeigte Status kritisch.

- **NFS Exporte**

  Zeigt die Anzahl und den Status der NFS-Exporte an, die dem Volume zugeordnet sind.

- **CIFS-Freigaben**

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

- **LUNs**

  Zeigt die Anzahl und Gesamtgröße aller LUNs im ausgewählten Volume an. Auf der Grundlage des höchsten Schweregrades wird außerdem der Systemzustand der LUNs angezeigt.

- **Benutzer- und Gruppenquoten**

  Zeigt die Anzahl und den Status der Quoten für Benutzer und Benutzergruppen im Zusammenhang mit dem Volume und seinen qtrees an.

- **FlexClone Volumes**

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

- **Parent Volume**

  Zeigt den Namen und die Kapazität des übergeordneten Volume eines ausgewählten FlexClone Volume an. Das übergeordnete Volume wird nur angezeigt, wenn das ausgewählte Volume ein FlexClone Volume ist.

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ können Sie die Liste der Gruppen anzeigen, die dem ausgewählten Volume zugeordnet sind.

Bereich „Verwandte Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnmeldungen anzeigen, die für das ausgewählte Volume erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Dialogfeld „Richtlinien exportieren“

Das Dialogfeld Richtlinien exportieren zeigt Details zu den Exportrichtlinien, Authentifizierungsprotokollen und aktivierten Zugriffsrechten für die Volumes an, die zur Storage Virtual Machine (SVM) gehören. Mit den Filtern können Sie die Anzeige der Informationen in der Liste der Regeln für den Export anpassen. Standardmäßig werden die Informationen anhand der Indexspalte sortiert.

- **Index**

  Zeigt den Index an, der den Regeln für die Exportrichtlinie zugewiesen ist. Es handelt sich um eine eindeutige Nummer.

- **Zugriffsprotokolle**

  Zeigt die Protokolle an, die für die Regeln für die Exportrichtlinie aktiviert sind.

- * Client Match*

  Zeigt die Clients an, die über Berechtigungen zum Zugriff auf Daten auf den Volumes verfügen, die zur SVM gehören.

- **Nur-Lese-Zugriff**

  Zeigt das Authentifizierungsprotokoll an, das zum Lesen von Daten auf den Volumes verwendet wird, die zur SVM gehören.

- **Schreibzugriff Lesen**

  Zeigt das Authentifizierungsprotokoll an, das zum Lesen oder Schreiben von Daten auf den Volumes verwendet wird, die zur SVM gehören.

Snapshot Kopien in einem Dialogfeld „Volume“

Mit den Snapshot Kopien im Dialogfeld Volume können Sie die Liste der Snapshot Kopien anzeigen. Sie können eine Snapshot-Kopie löschen, um Speicherplatz zu sparen oder frei zu halten, oder wenn die Kopie nicht mehr benötigt wird. Sie können auch die Menge an Festplattenspeicher berechnen, die zurückgewonnen werden kann, wenn eine oder mehrere Snapshot-Kopien gelöscht werden.

Listenansicht

Die Listenansicht zeigt Informationen über die Snapshot Kopien auf dem Volume in Tabellenformat an. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen.

- **Snapshot Kopie**

  Zeigt den Namen der Snapshot Kopie an.

- **Verwendeter Raum %**

  Zeigt prozentual den von der Snapshot Kopie im Volume genutzten Gesamtspeicherplatz an.

- **Gesamtgröße**

  Zeigt die Gesamtgröße der Snapshot Kopie an.

- **Erstellte Zeit**

  Zeigt den Zeitstempel der Snapshot Kopie an.

- **Abhängigkeit**

  Zeigt die Applikationen an, die von der Snapshot Kopie abhängig sind. Mögliche Werte sind SnapMirror, SnapVault, SnapLock, Dump, LUNs, Vclone und beschäftigt.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Berechnen**

  Mit können Sie den Speicherplatz berechnen, der zurückgewonnen werden kann, indem eine oder mehrere Snapshot Kopien gelöscht werden.

- **Auswahl Löschen**

  Löscht eine oder mehrere Snapshot Kopien.

- **Schließen**

  Schließt das Dialogfeld Snapshot Kopien in einem Volume.

- * Neu Berechnen*

  Mit können Sie den Speicherplatz berechnen, der zurückgewonnen werden kann, indem Sie die

ausgewählten Snapshot Kopien löschen.

Die Schaltfläche **Neu berechnen** ist aktiviert, wenn Sie Änderungen an der Auswahl der Snapshot-Kopien vornehmen.

Verwalten und Überwachen von MetroCluster Konfigurationen

Die Monitoring-Unterstützung für MetroCluster-Konfigurationen in der Unified Manager Web-Benutzeroberfläche ermöglicht es Ihnen, auf Verbindungsprobleme in Ihrer MetroCluster-Konfiguration zu überprüfen. Durch die frühzeitige Erkennung eines Verbindungsproblem können Sie Ihre MetroCluster-Konfigurationen effektiv verwalten.

Teile einer Fabric-MetroCluster-Konfiguration

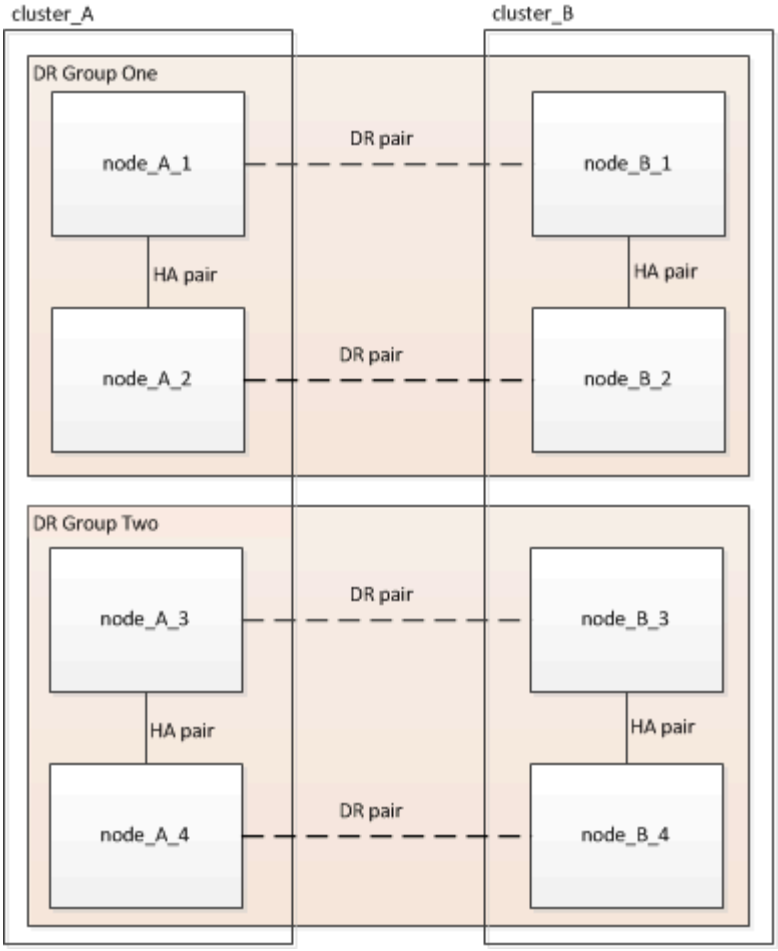
Wenn Sie Ihre MetroCluster Konfiguration planen, sollten Sie sich mit den Hardwarekomponenten und den zugehörigen Interconnects vertraut machen.

Disaster-Recovery-Gruppen (DR)

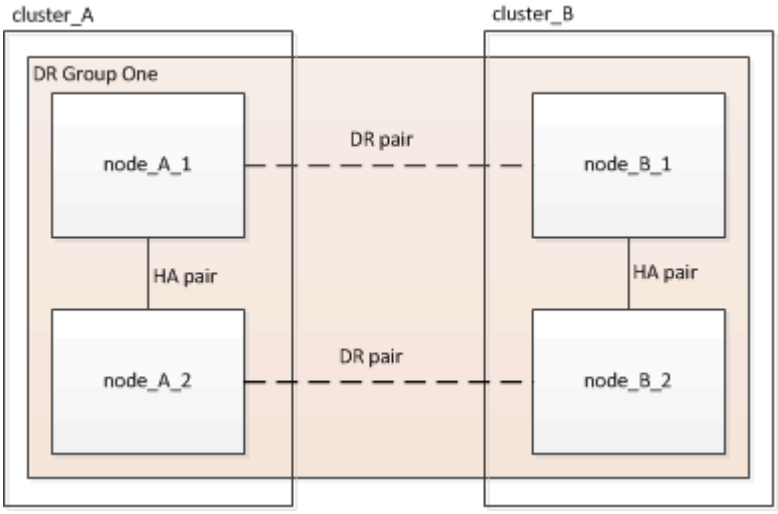
Eine Fabric MetroCluster Konfiguration besteht aus einer oder zwei DR-Gruppen, abhängig von der Anzahl der Nodes in der MetroCluster Konfiguration. Jede DR-Gruppe besteht aus vier Nodes.

- Eine MetroCluster Konfiguration mit acht Nodes besteht aus zwei DR-Gruppen.
- Eine MetroCluster Konfiguration mit vier Nodes besteht aus einer DR-Gruppe.

Die folgende Abbildung zeigt die Organisation der Nodes in einer MetroCluster Konfiguration mit acht Nodes:



Die folgende Abbildung zeigt die Organisation der Nodes in einer MetroCluster Konfiguration mit vier Nodes:



Wichtige Hardwarekomponenten

Eine MetroCluster Konfiguration umfasst die folgenden wichtigen Hardware-Elemente:

- Storage Controller

  Die Storage Controller sind nicht direkt mit dem Storage verbunden, sondern mit zwei redundanten FC Switch Fabrics verbunden.

- FC-to-SAS-Bridges

  Die FC-to-SAS-Bridges verbinden die SAS-Storage-Stacks mit den FC-Switches und geben somit die Möglichkeit, die beiden Protokolle zu überbrücken.

- FC Switches

  Die FC-Switches stellen das Langstrecken-Backbone ISL zwischen den beiden Standorten bereit. Die FC Switches stellen die beiden Storage Fabrics bereit, die die Datenspiegelung zu den Remote Storage Pools ermöglichen.

- Cluster-Peering-Netzwerk

  Das Cluster-Peering-Netzwerk bietet Konnektivität zur Spiegelung der Cluster-Konfiguration, einschließlich der Storage Virtual Machine (SVM)-Konfiguration. Die Konfiguration aller SVMs auf einem Cluster wird dem Partner-Cluster gespiegelt.

Fabric MetroCluster Konfiguration mit acht Nodes

Eine Konfiguration mit acht Nodes besteht aus zwei Clustern, eines an jedem geografisch getrennten Standort. „Cluster_A“ befindet sich am ersten MetroCluster-Standort. „Cluster_B“ befindet sich am zweiten MetroCluster-Standort. Jeder Standort verfügt über ein SAS-Storage-Stack. Zusätzliche Storage-Stacks werden unterstützt, aber nur einer wird an jedem Standort angezeigt. Die HA-Paare sind als Cluster ohne Switch konfiguriert, ohne Cluster Interconnect Switches. Eine geschaltete Konfiguration wird unterstützt, wird aber nicht angezeigt.

Eine Konfiguration mit acht Nodes umfasst folgende Verbindungen:

- FC-Verbindungen von den HBAs jedes Controllers und FC-VI-Adaptern zu jedem der FC-Switches
- Eine FC-Verbindung von jeder FC-zu-SAS-Bridge zu einem FC-Switch
- SAS-Verbindungen zwischen jedem SAS Shelf und von oben und unten auf jedem Stack zu einer FC-to-SAS-Bridge
- Ein HA Interconnect zwischen jedem Controller im lokalen HA-Paar

  Wenn die Controller ein HA-Paar mit einem Gehäuse unterstützen, ist der HA Interconnect intern, was über die Backplane geschieht, sodass ein externer Interconnect nicht erforderlich ist.

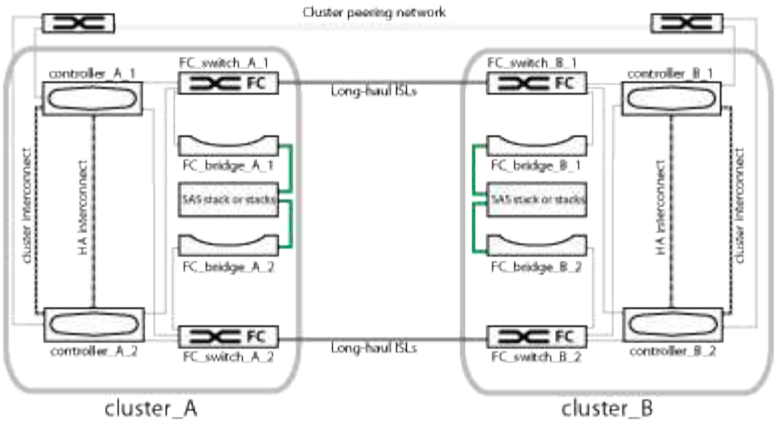
- Ethernet-Verbindungen von den Controllern zu dem vom Kunden bereitgestellten Netzwerk, das für Cluster-Peering verwendet wird

  Die SVM-Konfiguration wird über das Cluster-Peering-Netzwerk repliziert.

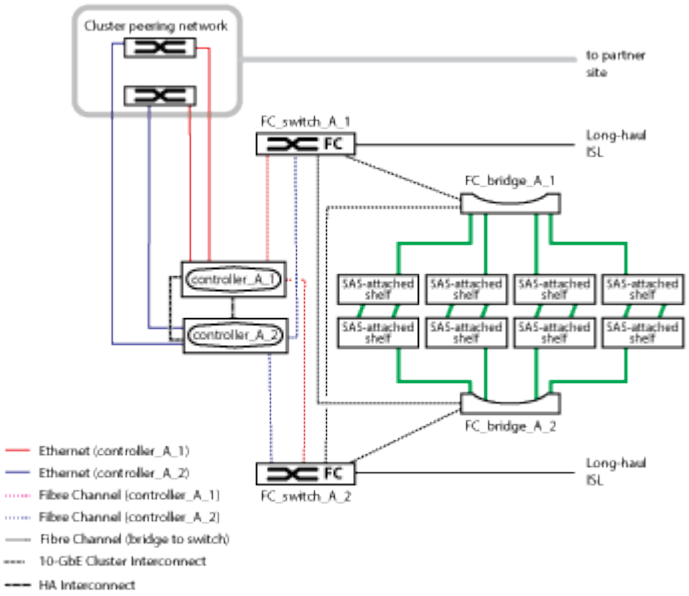
- Ein Cluster-Interconnect zwischen jedem Controller im lokalen Cluster

Fabric MetroCluster Konfiguration mit vier Nodes

Die folgende Abbildung zeigt eine vereinfachte Ansicht einer Fabric MetroCluster Konfiguration mit vier Nodes. Bei einigen Verbindungen stellt eine einzelne Leitung mehrere redundante Verbindungen zwischen den Komponenten dar. Verbindungen zu Daten und Management-Netzwerken werden nicht angezeigt.

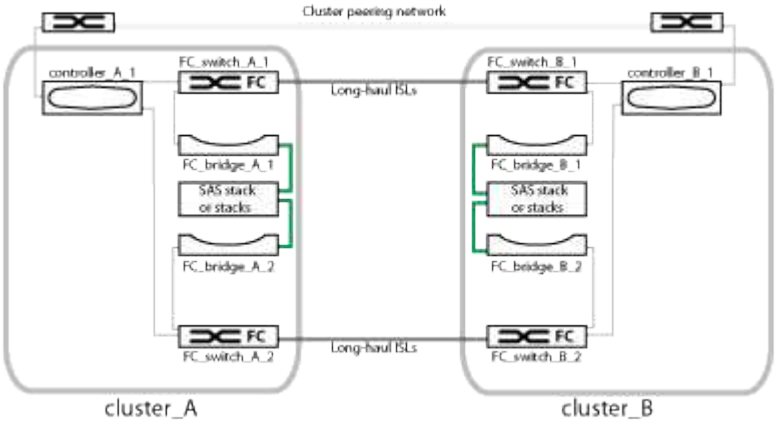


Die folgende Abbildung zeigt eine detailliertere Ansicht der Konnektivität in einem einzelnen MetroCluster Cluster (beide Cluster haben dieselbe Konfiguration):



Fabric MetroCluster Konfiguration mit zwei Nodes

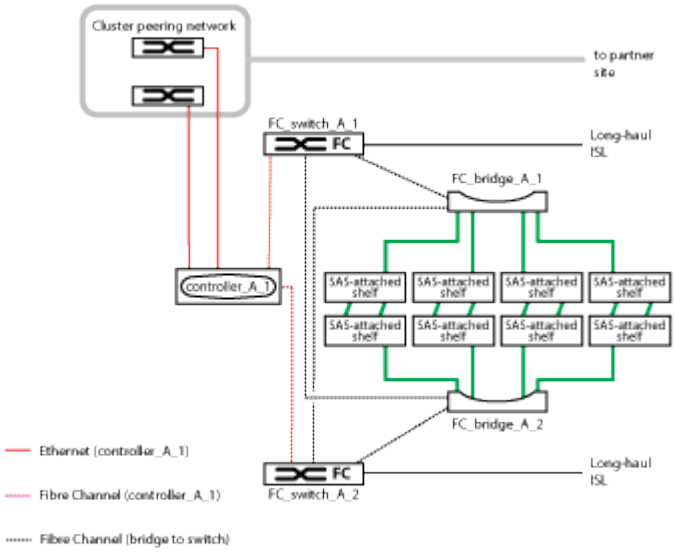
Die folgende Abbildung zeigt eine vereinfachte Ansicht einer Fabric MetroCluster Konfiguration mit zwei Nodes. Bei einigen Verbindungen stellt eine einzelne Leitung mehrere redundante Verbindungen zwischen den Komponenten dar. Verbindungen zu Daten und Management-Netzwerken werden nicht angezeigt.



Eine Konfiguration mit zwei Nodes besteht aus zwei Clustern, eines an jedem geografisch getrennten Standort. „Cluster_A“ befindet sich am ersten MetroCluster-Standort. „Cluster_B“ befindet sich am zweiten MetroCluster-Standort. Jeder Standort verfügt über ein SAS-Storage-Stack. Zusätzliche Storage-Stacks werden unterstützt, aber nur einer wird an jedem Standort angezeigt.

In einer Konfiguration mit zwei Nodes sind die Nodes nicht als HA-Paar konfiguriert.

Die folgende Abbildung zeigt eine detailliertere Ansicht der Konnektivität in einem einzelnen MetroCluster Cluster (beide Cluster haben dieselbe Konfiguration):



Eine Konfiguration mit zwei Nodes umfasst folgende Verbindungen:

- FC-Verbindungen zwischen dem FC-VI-Adapter auf jedem Controller-Modul
- FC-Verbindungen von den HBAs jedes Controller-Moduls mit der FC-to-SAS Bridge für jeden SAS-Shelf-Stack
- SAS-Verbindungen zwischen jedem SAS Shelf und von oben und unten auf jedem Stack zu einer FC-to-SAS-Bridge
- Ethernet-Verbindungen von den Controllern zu dem vom Kunden bereitgestellten Netzwerk, das für Cluster-Peering verwendet wird

  Die SVM-Konfiguration wird über das Cluster-Peering-Netzwerk repliziert.

Teile einer Stretch MetroCluster Konfiguration mit zwei Nodes über SAS

Die MetroCluster SAS-Attached-Konfiguration mit zwei Nodes erfordert mehrere Teile. Dazu gehören zwei Single-Node-Cluster, in denen die Storage-Controller über SAS-Kabel direkt mit dem Storage verbunden sind.

Die MetroCluster Konfiguration umfasst die folgenden wichtigen Hardware-Elemente:

- Storage Controller

  Die Storage-Controller sind über SAS-Kabel direkt mit dem Storage verbunden.

  Jeder Storage Controller ist als DR-Partner für einen Storage Controller am Standort des Partners

konfiguriert.

- Kupfer-SAS-Kabel können für kürzere Entfernungen verwendet werden.
- Optische SAS-Kabel können über größere Entfernungen verwendet werden.

> Bei Systemen mit E-Series Array-LUNs können die Storage-Controller direkt mit den E-Series Storage-Arrays verbunden werden. Bei anderen Array LUNs sind Verbindungen über FC-Switches erforderlich.

"NetApp Interoperabilitäts-Matrix-Tool"

Im IMT können Sie im Feld Storage-Lösung die Auswahl Ihrer MetroCluster Lösung verwenden. Sie verwenden den **Komponenten-Explorer**, um die Komponenten und die ONTAP-Version auszuwählen, um Ihre Suche zu verfeinern. Klicken Sie auf **Ergebnisse anzeigen**, um die Liste der unterstützten Konfigurationen anzuzeigen, die den Kriterien entsprechen.

- Cluster-Peering-Netzwerk

  Das Cluster-Peering-Netzwerk bietet Konnektivität zur Spiegelung der SVM-Konfiguration (Storage Virtual Machine). Die Konfiguration aller SVMs auf einem Cluster wird dem Partner-Cluster gespiegelt.

Teile einer Stretch MetroCluster Konfiguration mit zwei Nodes über eine Bridge

Bei der Planung der MetroCluster Konfiguration sollten Sie sich mit den einzelnen Komponenten der Konfiguration und deren Zusammenspiel vertraut machen.

Die MetroCluster Konfiguration umfasst die folgenden wichtigen Hardware-Elemente:

- Storage Controller

  Die Storage Controller sind nicht direkt mit dem Storage verbunden, sondern mit FC-to-SAS-Bridges verbunden. Die Storage-Controller sind über FC-Kabel zwischen den FC-VI-Adaptern der einzelnen Controller miteinander verbunden.

  Jeder Storage Controller ist als DR-Partner für einen Storage Controller am Standort des Partners konfiguriert.

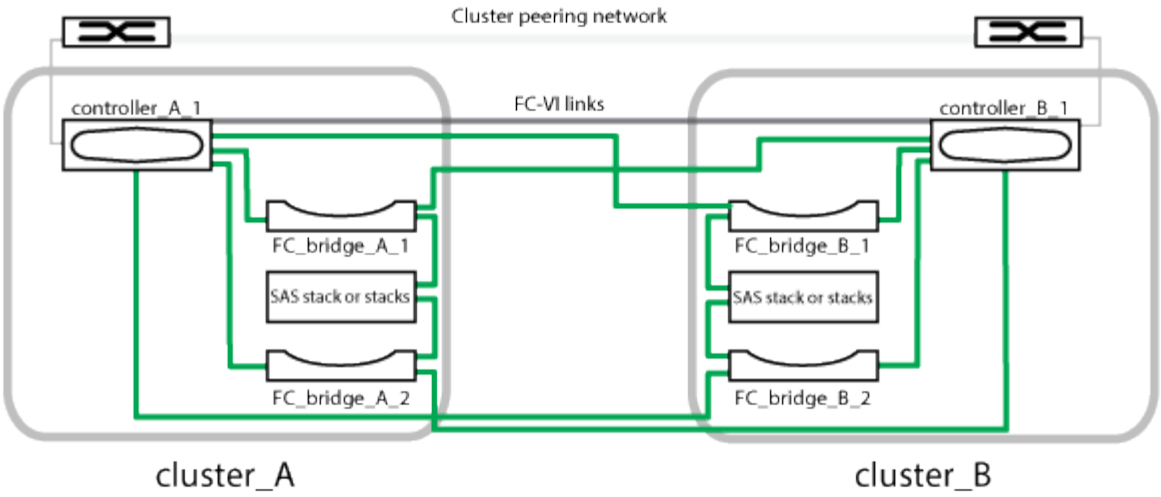
- FC-to-SAS-Bridges

  Die FC-to-SAS-Bridges verbinden die SAS-Storage-Stacks mit den FC-Initiator-Ports auf den Controllern und sorgen somit für den Überbrückung zwischen den beiden Protokollen.

- Cluster-Peering-Netzwerk

  Das Cluster-Peering-Netzwerk bietet Konnektivität zur Spiegelung der SVM-Konfiguration (Storage Virtual Machine). Die Konfiguration aller SVMs auf einem Cluster wird dem Partner-Cluster gespiegelt.

Die folgende Abbildung zeigt eine vereinfachte Ansicht der MetroCluster Konfiguration. Bei einigen Verbindungen stellt eine einzelne Leitung mehrere redundante Verbindungen zwischen den Komponenten dar. Verbindungen zu Daten und Management-Netzwerken werden nicht angezeigt.



- Die Konfiguration besteht aus zwei Single-Node-Clustern.
- Jeder Standort verfügt über einen oder mehrere SAS-Storage-Stacks.

> SAS-Shelves in MetroCluster-Konfigurationen werden mit ACP-Verkabelung nicht unterstützt.

Zusätzliche Storage-Stacks werden unterstützt, aber nur einer wird an jedem Standort angezeigt.

Statusdefinitionen für Cluster-Konnektivität

Die Konnektivität zwischen den Clustern in einer MetroCluster-Konfiguration kann einen der folgenden Status aufweisen: Optimal, beeinträchtigt oder ausgefallen. Wenn Sie über den Konnektivitätsstatus verfügen, können Sie Ihre MetroCluster Konfigurationen effizient managen.

Konnektivitätsstatus	Beschreibung	Wird angezeigt
Optimal	Die Konnektivität zwischen den Clustern in der MetroCluster Konfiguration ist normal.	
Beeinträchtigt	Mindestens ein Fehler beeinträchtigt den Status der Failover-Verfügbarkeit. In der MetroCluster Konfiguration sind jedoch noch beide Cluster aktiv. Beispiel: Wenn die ISL-Verbindung ausgefallen ist, wenn die Intercluster-IP-Verbindung ausgefallen ist oder das Partner-Cluster nicht erreichbar ist.	

Konnektivitätsstatus	Beschreibung	Wird angezeigt
Runter	Die Konnektivität zwischen den Clustern in der MetroCluster Konfiguration ist ausgefallen, da ein oder beide Cluster ausgefallen sind oder sich die Cluster im Failover-Modus befinden. Wenn das Partner-Cluster beispielsweise aufgrund eines Ausfalls oder bei einem geplanten Switchover zu Testzwecken ausfällt,	Umschaltung mit Fehlern: Umschaltung erfolgreich:

Statusdefinitionen zur Datenspiegelung

MetroCluster Konfigurationen ermöglichen Datenspiegelung und zusätzlich die Möglichkeit, einen Failover zu initiieren, wenn der gesamte Standort nicht mehr verfügbar ist. Der Status der Datenspiegelung zwischen den Clustern in einer MetroCluster Konfiguration kann entweder „Normal“ oder „Spiegelung nicht verfügbar“ lauten. Wenn Sie diese Informationen kennen, können Sie Ihre MetroCluster Konfigurationen effektiv managen.

Status Datenspiegelung	Beschreibung	Wird angezeigt
Normal	Die Datenspiegelung zwischen den Clustern in der MetroCluster Konfiguration ist normal.	
Spiegelung Nicht Verfügbar	Das Daten-Mirroring zwischen den Clustern in der MetroCluster Konfiguration ist aufgrund der Umschaltung nicht verfügbar. Wenn das Partner-Cluster beispielsweise aufgrund eines Ausfalls oder bei einem geplanten Switchover zu Testzwecken ausfällt,	Umschaltung mit Fehlern: Umschaltung erfolgreich:

Monitoring der MetroCluster Konfigurationen

Sie können Konnektivitätsprobleme in Ihrer MetroCluster-Konfiguration überwachen. Die Details umfassen den Status der Komponenten und die Konnektivität innerhalb eines Clusters und den Konnektivitätsstatus zwischen den Clustern in der MetroCluster

Konfiguration.

Bevor Sie beginnen

- Die lokalen und die Remote-Cluster in der MetroCluster Konfiguration müssen dem OnCommand Unified Manager hinzugefügt werden.
- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Sie können die auf der Seite „Systemzustand/Cluster-Details“ angezeigten Informationen verwenden, um Verbindungsprobleme zu beheben. Wenn z. B. die Verbindung zwischen dem Node und dem Switch in einem Cluster ausgefallen ist, wird das folgende Symbol angezeigt:

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

Unified Manager überwacht mit Systemzustandsmeldungen den Status der Komponenten und die Konnektivität in der MetroCluster-Konfiguration.

Die Registerkarte MetroCluster-Konnektivität wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

Schritte

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

   Eine Liste aller überwachten Cluster wird angezeigt.

2. Klicken Sie auf der Seite **Systemzustand/Cluster** Inventar auf den Namen des Clusters, für den Sie MetroCluster Konfigurationsdetails anzeigen möchten.
3. Klicken Sie auf der Detailseite **Systemzustand/Cluster** auf die Registerkarte **MetroCluster Konnektivität**.

   Die Topologie der MetroCluster-Konfiguration wird im entsprechenden Cluster-Objektbereich angezeigt.

Nachdem Sie fertig sind

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

Monitoring der MetroCluster Replizierung

Sie können den allgemeinen Zustand der logischen Verbindungen überwachen und diagnostizieren, während Sie gleichzeitig die Daten spiegeln. Sie können die Probleme oder Risiken identifizieren, die die Spiegelung von Cluster-Komponenten wie Aggregaten, Nodes und Storage Virtual Machines unterbrechen.

Bevor Sie beginnen

Der lokale und der Remote-Cluster in der MetroCluster Konfiguration müssen Unified Manager hinzugefügt werden

Über diese Aufgabe

Sie können die auf der Seite „Systemzustand/Cluster-Details“ angezeigten Informationen verwenden, um alle Replikationsprobleme zu beheben.

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

Unified Manager überwacht mit Systemzustandsmeldungen den Status der Komponenten und die Konnektivität in der MetroCluster-Konfiguration.

Schritte

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

   Eine Liste der überwachten Cluster wird angezeigt.

2. Klicken Sie auf der Seite **Systemzustand/Cluster** Inventory auf den Namen des Clusters, für den Sie MetroCluster-Replikationsdetails anzeigen möchten, und klicken Sie dann 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.

Nachdem Sie fertig sind

Wenn Sie Spiegelungsprobleme in Ihrer MetroCluster Konfiguration feststellen, müssen Sie sich bei System Manager einloggen oder auf die ONTAP CLI zugreifen, um die Probleme zu beheben.

Verwalten von Anmerkungen für Speicherobjekte

In Unified Manager können Sie Anmerkungen erstellen, um Storage-Objekte zu beschriften. Mit Annotationen können Sie kritische Ressourcen leicht identifizieren und geeignete Aktionen durchführen, z. B. wichtige Ressourcen einer Gruppe hinzufügen, eine Gruppenaktion zuweisen oder einen Bericht mit kommentierten Ressourcen erstellen.

Welche Anmerkungen sind

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

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

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

Funktionieren von Anmerkungsregeln in Unified Manager

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

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

Bestimmten Bedingungen

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

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

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

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

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

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

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

Beispiel einer Anmerkungsregel mit Bedingungen

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

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

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

Bedingungsgruppen

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

Beispiel einer Anmerkungsregel mit Bedingungsgruppen

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

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

◦ Der Anmerkungswert der Datenpriorität lautet „kritisch“. Diese Bedingungsgruppe bezeichnet alle Volumes, die „vol“ in ihren Namen enthalten und die mit dem Wert für die datenprioritäre Annotation mit „kritisch“ beschriftet werden.

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

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

Beschreibung der vordefinierten Anmerkungswerte

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

- **Datenpriorität:unternehmenskritisch**

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

- **Datenpriorität:hoch**

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

- **Datenpriorität:Niedrig**

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

Anzeigen der Anmerkungsliste und der Details

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungen** auf den Anmerkungsnamen, um die zugehörigen Details anzuzeigen.

Anmerkungen werden dynamisch hinzugefügt

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Klicken Sie auf der Seite **Anmerkungen** auf **Anmerkung hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkung hinzufügen** einen Namen und eine Beschreibung für die Anmerkung ein.

   Sie können beim Erstellen von Anmerkungen auch Werte zu Anmerkungen hinzufügen.
4. Optional: Klicken Sie im Abschnitt **Anmerkungswerte** auf **Hinzufügen**, um der Anmerkung Werte hinzuzufügen.
5. Klicken Sie auf **Speichern und Schließen**.

Anmerkungen manuell zu einzelnen Speicherobjekten hinzufügen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

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

So fügen Sie Kommentare hinzu:	Tun Sie das…
Cluster	a. Klicken Sie Auf **Gesundheit** > **Cluster**. b. Wählen Sie ein oder mehrere Cluster aus.
Volumes	a. Klicken Sie Auf **Gesundheit** > **Volumen**. b. Wählen Sie ein oder mehrere Volumes aus.

So fügen Sie Kommentare hinzu:	Tun Sie das…
SVMs	a. Klicken Sie auf **Health** > **SVMs**. b. Wählen Sie eine oder mehrere SVMs aus.

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

Hinzufügen von Werten zu Beschriftungen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können vordefinierten Anmerkungen keine Werte hinzufügen.

Schritte

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

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

4. Klicken Sie Auf **Hinzufügen**.

Anmerkungsregeln werden erstellt

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungsregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkungsregel hinzufügen** einen Namen für die Anmerkungsregel an.
4. Wählen Sie im Feld **Zielobjekttyp** den Typ des Speicherobjekts aus, das Sie mit Anmerkungen versehen möchten.
5. Wählen Sie in den Feldern **Anmerkung anwenden** den Anmerkungs- und Anmerkungswert aus, den Sie verwenden möchten.
6. Führen Sie im Abschnitt **Bedingungen** die entsprechende Aktion aus, um eine Bedingung, eine Bedingungsgruppe oder beide zu erstellen:

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

7. Klicken Sie Auf **Hinzufügen**.

Beispiel für das Erstellen einer Anmerkungsregel

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

1. Geben Sie einen Namen für die Anmerkungsregel an.
2. Wählen Sie den Zielobjekttyp als Storage Virtual Machine (SVM) aus.
3. Wählen Sie eine Anmerkung aus der Liste der Anmerkungen aus, und geben Sie einen Wert an.
4. Wählen Sie im Abschnitt Bedingungen als Operand **Objektname** aus.

5. Wählen Sie als Operator * enthält* aus.
6. Geben Sie den Wert als ein `svm_data`.
7. Klicken Sie auf **Bedingungsgruppe hinzufügen**.
8. Wählen Sie als Operand **Objektname** aus.
9. Wählen Sie als Operator * enthält* aus.
10. Geben Sie den Wert als ein `vol`.
11. Klicken Sie auf **Bedingung hinzufügen**.
12. Wiederholen Sie die Schritte 8 bis 10, indem Sie **Datenpriorität** als Operand in Schritt 8, **ist** als Operator in Schritt 9 und **unternehmenskritisch** als Wert in Schritt 10 auswählen.
13. Klicken Sie Auf **Hinzufügen**.

Konfigurieren von Bedingungen für Anmerkungsregeln

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

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

Beispiel für die Konfiguration einer Bedingung für eine Anmerkungsregel

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

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

1. Geben Sie einen Namen für die Anmerkungsregel ein.
2. Wählen Sie den Zielobjekttyp als SVM aus.
3. Wählen Sie eine Anmerkung aus der Liste der Anmerkungen und einen Wert aus.

4. Wählen Sie im Feld **Bedingungen** als Operand **Objektname** aus.
5. Wählen Sie als Operator * enthält* aus.
6. Geben Sie den Wert als ein `svm_data`.
7. Klicken Sie Auf **Hinzufügen**.

Anmerkungsregeln werden bearbeitet

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

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

   Sie können den Zielobjekttyp für eine Anmerkungsregel nicht ändern.

4. Klicken Sie Auf **Speichern**.

Anmerkungsregeln neu anordnen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungsregeln** auf **Neuordnung**.
3. Ziehen Sie im Dialogfeld **Anmerkungsregel neu anordnen** einzelne oder mehrere Zeilen per Drag-and-Drop, um die Reihenfolge der Anmerkungsregeln neu anzuordnen.
4. Klicken Sie Auf **Speichern**.

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

Anmerkungen werden gelöscht

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

Bevor Sie beginnen

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungen** die zu löschende Anmerkung aus.

   Die Details der ausgewählten Anmerkung werden angezeigt.

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

Ergebnisse

Die ausgewählte Beschriftung und ihr Wert werden gelöscht.

Löschen von Werten aus Anmerkungen

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

Bevor Sie beginnen

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

Über diese Aufgabe

Werte können nicht aus vordefinierten Anmerkungen gelöscht werden.

Schritte

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

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

Anmerkungsregeln werden gelöscht

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungsregeln** die Anmerkungsregel aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie im Dialogfeld **Warnung** auf **Ja**, um den Löschvorgang zu bestätigen.

Beschreibung der Fenster und Dialogfelder Anmerkungen

Sie können alle Anmerkungen auf der Seite Management/Anmerkungen anzeigen und verwalten. Über die Registerkarte „Anmerkungsregeln“ können Sie auch Anmerkungsregeln für Ihre Speicherobjekte konfigurieren.

Management-/Annotationsseite

Auf der Seite „Management/Annotationen“ können Sie Anmerkungen in Unified Manager erstellen, mit denen Storage-Objekte beschriftet werden können, oder Sie können Anmerkungen bearbeiten oder löschen. Sie können Storage-Objekte entweder manuell mit einem annotation=value-Paar beschriften oder Anmerkungsregeln konfigurieren. Storage-Objekte werden basierend auf den verwendeten Annotationen dynamisch beschriftet.

Wenn Sie sich als Operator anmelden, haben Sie nur Lesezugriff auf die Seite. Sie können auf den Schaltflächen Hinzufügen, Bearbeiten oder Löschen auf jeder Registerkarte zugreifen, wenn Sie sich als Speicheradministrator oder Unified Manager-Administrator anmelden.

Registerkarte „Anmerkungen“

Auf der Registerkarte Anmerkungen können Sie Anmerkungen in Unified Manager anzeigen, erstellen, bearbeiten oder löschen.

- **Anmerkungsliste**

  Zeigt die Namen der vordefinierten und benutzerdefinierten Anmerkungen an. Die Anzahl der Anmerkungswerte, die mit jeder Anmerkung verknüpft sind, wird ebenfalls angezeigt. Sie können auf den Anmerkungsnamen klicken, um die Details der Anmerkung anzuzeigen.

Zusammenfassungsbereich

Sie können die folgenden Details der ausgewählten Anmerkung anzeigen:

- **Beschreibung**

  Zeigt die Beschreibung für die Anmerkung an.

- * Erstellt von*

  Zeigt den Namen des Benutzers an, der die Anmerkung erstellt hat.

- **Erstellungsdatum**

  Zeigt das Datum an, an dem die Anmerkung erstellt wurde.

Anmerkung=Werte Paare

Zeigt die Liste der Anmerkungswertpaare und der zugehörigen Speicherobjekte an, die für die ausgewählte Anmerkung verfügbar sind.

- **Wert**

  Zeigt den Namen des annotation=value-Paars an.

- **Anwendbare Cluster**

  Zeigt die Anzahl der Cluster an, die mit einem bestimmten Anmerkungs=Wert-Paar beschriftet sind. Sie können auf die Nummer klicken, um die Seite Cluster anzuzeigen, auf der eine gefilterte Liste der Cluster angezeigt wird, die einem bestimmten Wert zugeordnet sind.

- **Anwendbare Storage Virtual Machines (SVMs)**

  Zeigt die Anzahl der Storage Virtual Machines (SVMs) an, die mit einem bestimmten Annotation=Wertpaar versehen sind. Sie können auf die Nummer klicken, um die Seite Storage Virtual Machines (SVMs) anzuzeigen. In dieser Seite wird eine gefilterte Liste von Storage Virtual Machines (SVMs) angezeigt, die einem bestimmten Wert zugeordnet sind.

- **Geltende Volumen**

Zeigt die Anzahl der Volumes an, die mit einem bestimmten Anmerkungspaar=Wert versehen sind. Sie können auf die Nummer klicken, um die Seite Volumes anzuzeigen, auf der eine gefilterte Liste der Volumes angezeigt wird, die einem bestimmten Wert zugeordnet sind.

Objektzuweisungen über Regeln

Zeigt die Liste der Anmerkungsregeln und die zugehörigen Speicherobjekte für die ausgewählte Anmerkung an.

- * Rang*

  Zeigt die Reihenfolge der Anmerkungsregeln an, die auf die Speicherobjekte angewendet werden sollen.

- **Regeln**

  Zeigt den Namen der Anmerkungsregel an.

- **Zielobjekttyp**

  Zeigt den Typ des Speicherobjekts an, auf das die Anmerkungsregel angewendet wird.

- **Zugehörige Anmerkung**

  Zeigt das auf das Speicherobjekt angewendete annotation=value-Paar an.

- **Anwendbare Objekte**

  Zeigt die Anzahl der Storage-Objekte an, die basierend auf der Anmerkungsregel mit Anmerkungen versehen werden.

Manuelle Objektzuordnungen

Zeigt die Liste der Anmerkungen an, die Sie manuell konfiguriert und mit Speicherobjekten verknüpft haben.

- **Anmerkung=Wertpaar**

  Zeigt den Namen der manuellen Anmerkung und den Wert an.

- **Anwendbare Cluster**

  Zeigt die Anzahl der Cluster an, die mit einem bestimmten manuellen Anmerkungswert versehen sind. Sie können auf die Nummer klicken, um die Seite Cluster anzuzeigen, auf der eine gefilterte Liste der Cluster angezeigt wird, die einem bestimmten Wert zugeordnet sind.

- **Anwendbare Storage Virtual Machines (SVMs)**

  Zeigt die Anzahl der Storage Virtual Machines (SVMs) an, die mit einem bestimmten manuellen Anmerkungswert versehen werden. Sie können auf die Nummer klicken, um die Seite Storage Virtual Machines (SVMs) anzuzeigen. In dieser Seite wird eine gefilterte Liste von Storage Virtual Machines (SVMs) angezeigt, die einem bestimmten Wert zugeordnet sind.

- **Geltende Volumen**

  Zeigt die Anzahl der Volumes an, die mit einem bestimmten manuellen Anmerkungswert versehen werden. Sie können auf die Nummer klicken, um die Seite Volumes anzuzeigen, auf der eine gefilterte Liste der

Volumes angezeigt wird, die einem bestimmten Wert zugeordnet sind.

Befehlsschaltflächen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen. Für vordefinierte Anmerkungen können Sie keine Werte hinzufügen oder löschen.

- **Anmerkung Hinzufügen**

  Öffnet das Dialogfeld Anmerkung hinzufügen, in dem Sie neue benutzerdefinierte Anmerkungen erstellen und der Anmerkung Werte zuweisen können.

- **Aktionen**

  Ermöglicht das Bearbeiten oder Löschen der ausgewählten Beschreibung der Anmerkung.

- **Bearbeiten**

  Öffnet das Dialogfeld Anmerkung bearbeiten, in dem Sie den Anmerkungsnamen und die Beschreibung ändern können.

- **Löschen**

  Ermöglicht das Löschen des Anmerkungswerts. Sie können den Wert nur löschen, wenn er nicht mit Anmerkungsregeln oder Gruppenregeln verknüpft ist.

Registerkarte „Anmerkungsregeln“

Auf der Registerkarte Annotationsregeln werden die Anmerkungsregeln angezeigt, die Sie zum Kommentieren von Speicherobjekten erstellt haben. Sie können Aufgaben wie Hinzufügen, Bearbeiten, Löschen oder Neuanordnen einer Anmerkungsregel durchführen. Sie können auch die Anzahl der Speicherobjekte anzeigen, die der Anmerkungsregel entsprechen.

Befehlsschaltflächen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Hinzufügen**

  Zeigt das Dialogfeld Anmerkungsregel hinzufügen an, in dem Sie Anmerkungsregeln für Speicherobjekte erstellen können.

- **Bearbeiten**

  Zeigt das Dialogfeld Anmerkungsregel bearbeiten an, in dem Sie zuvor konfigurierte Anmerkungsregeln neu konfigurieren können.

- **Löschen**

  Löscht die ausgewählten Anmerkungsregeln.

- **Neuordnung**

  Zeigt das Dialogfeld Anmerkungsregel neu anordnen an, mit dem Sie die Reihenfolge der Anmerkungsregeln neu anordnen können.

Listenansicht

In der Listenansicht werden die Anmerkungsregeln angezeigt, die Sie auf dem Unified Manager-Server erstellt haben. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen. Die Listenansicht der Registerkarte Anmerkungsregeln und die Listenansicht des Abschnitts zugewiesene Regeln auf der Registerkarte Anmerkung enthält die folgenden Spalten:

- Rang
- Name
- Zielobjekttyp
- Zugeordneten Anmerkungswert
- Anwendbare Objekte

Für die Registerkarte Anmerkungsregeln, Associated Annotation, wird eine zusätzliche Spalte angezeigt, in der der Name der auf das Speicherobjekt angewendeten Anmerkung angezeigt wird.

Dialogfeld Anmerkung hinzufügen

Im Dialogfeld Anmerkung hinzufügen können Sie benutzerdefinierte Annotationen erstellen, die Sie über Annotationsregeln mit Clustern, Volumes und Storage Virtual Machines (SVMs) verknüpfen können.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Anmerkungsname**

  Gibt den Namen der Anmerkung an. Sie müssen einen eindeutigen Namen für die Anmerkung eingeben.

- **Beschreibung**

  Gibt eine aussagekräftige Beschreibung der Anmerkung an.

Anmerkungswerte

- **Hinzufügen**

  Fügt der ausgewählten Anmerkung einen neuen Wert hinzu.

- **Löschen**

  Löscht den ausgewählten Wert für eine Anmerkung.

Befehlsschaltflächen

- **Speichern und Schließen**

  Speichert die neue Anmerkung und schließt das Dialogfeld Anmerkung hinzufügen.

- **Abbrechen**

  Schließt das Dialogfeld Anmerkung hinzufügen, ohne Ihre Änderungen zu speichern.

Dialogfeld Anmerkung bearbeiten

Im Dialogfeld Anmerkung bearbeiten können Sie die Beschreibung einer vorhandenen Anmerkung ändern.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Anmerkungsname**

  Zeigt den Namen der Anmerkung an. Dieses Feld kann nicht bearbeitet werden.

- **Beschreibung**

  Enthält eine aussagekräftige Beschreibung der Anmerkung. Sie können dieses Feld bearbeiten, wenn Sie die aktuelle Beschreibung der Anmerkung ändern möchten.

Befehlsschaltflächen

- **Speichern und Schließen**

  Speichert die Änderungen der Anmerkungsbeschreibung und schließt das Dialogfeld.

- **Abbrechen**

  Schließt das Dialogfeld Anmerkung bearbeiten, ohne die Änderungen zu speichern.

Dialogfeld Anmerkungsregel hinzufügen

Im Dialogfeld Anmerkungsregel hinzufügen können Sie in Unified Manager Anmerkungsregeln erstellen, mit denen Storage-Objekte dynamisch beschriftet werden können.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Name**

  Gibt den Namen der Anmerkungsregel an.

- **Zielobjekttyp**

  Gibt den Typ der Storage-Objekte (Storage Virtual Machines (SVMs), Volumes oder Cluster) an, die Anmerkungen enthalten sollen.

- **Anmerkung Anwenden**

  Gibt die Anmerkung und den Wert an, mit dem Speicherobjekte beschriftet werden können, wenn alle Bedingungen erfüllt sind.

- **Bedingungen**

  Gibt Bedingungen an, die bestimmen, welche Speicherobjekte Sie kommentieren können.

Befehlsschaltflächen

- **Speichern und Hinzufügen**

  Fügt die von Ihnen erstellte Anmerkungsregel hinzu. Sie können eine weitere Anmerkungsregel hinzufügen, ohne das Dialogfeld zu schließen.

- **Hinzufügen**

  Fügt die Anmerkungsregel hinzu und schließt das Dialogfeld Anmerkungsregel hinzufügen.

- **Abbrechen**

  Bricht die Änderungen ab und schließt das Dialogfeld Anmerkungsregel hinzufügen.

- **Bedingung Hinzufügen**

  Fügt eine Bedingung hinzu, um die Anmerkungsregel zu definieren.

- **Bedingungsgruppe Hinzufügen**

  Fügt eine Bedingungsgruppe hinzu, um Bedingungen für die Anmerkungsregel zu definieren.

Dialogfeld Anmerkungsregel bearbeiten

Sie können die von Ihnen erstellten Anmerkungsregeln bearbeiten, um Anmerkungen zu Speicherobjekten hinzuzufügen oder zu entfernen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Name**

  Zeigt den Namen der Anmerkungsregel an.

- **Zielobjekttyp**

  Zeigt den Typ des Speicherobjekts an, das mit Anmerkungen versehen werden soll. Sie können den Objekttyp nicht ändern.

- **Anmerkung Anwenden**

  Zeigt die Anmerkung und den Wert an, mit dem Speicherobjekte beschriftet werden können, wenn alle Bedingungen erfüllt sind.

- **Bedingungen**

  Zeigt die Liste der Bedingungen für die Anmerkungsregel an. Sie können die Bedingungen bearbeiten, um die Anmerkung zu Speicherobjekten hinzuzufügen oder zu entfernen.

Befehlsschaltflächen

- **Speichern**

  Speichert die Änderungen, die Sie vorgenommen haben, und schließt das Dialogfeld Anmerkungsregel bearbeiten.

- **Abbrechen**

  Schließt das Dialogfeld Anmerkungsregel bearbeiten, ohne Ihre Änderungen zu speichern.

Dialogfeld Anmerkungsregel neu anordnen

Über das Dialogfeld Anmerkungsregel neu anordnen können Sie die Reihenfolge angeben, in der Anmerkungsregeln auf Speicherobjekte angewendet werden sollen.

Befehlsschaltflächen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Speichern**

  Speichert die Änderungen, die Sie an den Anmerkungsregeln vorgenommen haben, und schließt das Dialogfeld Anmerkungsregel neu anordnen.

- **Abbrechen**

  Schließt das Dialogfeld Anmerkungsregel neu anordnen, ohne die vorgenommenen Änderungen zu speichern.

Listenansicht

- * Rang*

  Zeigt die Reihenfolge an, in der die Anmerkungsregeln auf die Speicherobjekte angewendet werden.

- **Name**

  Zeigt den Namen der Anmerkungsregel an.

- **Zielobjekttyp**

  Zeigt den Typ des Speicherobjekts an, auf das die Anmerkungsregel angewendet wird.

- **Zugehörige Anmerkung**

  Zeigt den Namen der Anmerkung an, die auf das Speicherobjekt angewendet wird.

- **Zugehörige Anmerkung**

  Zeigt den Anmerkungswert für das Speicherobjekt an.

Dialogfeld „Cluster mit Anmerkungen versehen“

Im Dialogfeld „Cluster anfügen“ können Sie Speicherobjekte manuell annotieren. Sie können entweder ein einzelnes Cluster oder mehrere Cluster auswählen und in der vorhandenen Liste mit Anmerkungen mit einem bestimmten Wertpaar versehen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Anmerkung=Wertpaare**

  Hiermit können Sie die erforderliche Annotation für das ausgewählte Cluster auswählen.

- **Anwenden**

  Wendet die ausgewählte Annotation auf das Cluster an.

- **Abbrechen**

  Schließt das Dialogfeld Cluster annotieren, ohne Ihre Änderungen zu speichern.

Dialogfeld „SVM mit Anmerkungen versehen“

Im Dialogfeld „Annotate SVM“ können Sie Storage-Objekte manuell kommentieren. Sie können entweder eine einzelne SVM oder mehrere SVMs auswählen und in der vorhandenen Liste mit Annotationen ein bestimmtes Wertpaar mit einem bestimmten Wert versehen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Anmerkung=Wertpaare**

  Hiermit können Sie die erforderliche Beschriftung für die ausgewählte SVM auswählen.

- **Anwenden**

  Wendet die ausgewählte Anmerkung auf die SVM an.

- **Abbrechen**

  Schließt das Dialogfeld „Annotate SVM“, ohne Ihre Änderungen zu speichern.

Dialogfeld „Volume mit Anmerkungen versehen“

Im Dialogfeld „Ausgabe annotieren“ können Sie Speicherobjekte manuell annotieren. Sie können entweder ein einzelnes Volume oder mehrere Volumes auswählen und in der vorhandenen Liste der Anmerkungen mit einem bestimmten Wertpaar Anmerkungen versehen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Anmerkung=Wertpaare**

  Ermöglicht die Auswahl der erforderlichen Beschriftung für das ausgewählte Volumen.

- **Anwenden**

  Wendet die ausgewählte Beschriftung auf das Volumen an.

- **Abbrechen**

  Schließt das Dialogfeld „Ausgabe annotieren“, ohne Ihre Änderungen zu speichern.

Verwalten und Überwachen von Gruppen

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

Allgemeines zu Gruppen

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

Was eine Gruppe ist

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

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

Funktionsweise von Gruppenregeln für Gruppen

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

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

Bestimmten Bedingungen

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

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

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

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

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

- Operand

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

- Operator

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

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

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

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

  Das Wertfeld ändert sich basierend auf dem ausgewählten Operand.

Beispiel einer Gruppenregel mit Bedingungen

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

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

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

Bedingungsgruppen

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

Beispiel einer Gruppenregel mit Bedingungsgruppen

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

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

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

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

Funktionsweise von Gruppenaktionen auf Speicherobjekten

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

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

Beispiel für Aktionen eindeutiger Gruppen

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

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

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

Verwalten von Gruppen von Storage-Objekten

Sie können Storage-Objekte in Ihrer Umgebung managen, indem Sie Gruppen von Storage-Objekten erstellen. Diese Speicherobjekte müssen die Gruppenregeln erfüllen, die der Gruppe zugeordnet sind.

Hinzufügen von Gruppen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Gruppen**.

2. Klicken Sie auf der Registerkarte **Gruppen** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Gruppe hinzufügen** einen Namen und eine Beschreibung für die Gruppe ein.

   Der Gruppenname muss eindeutig sein.

4. Klicken Sie Auf **Hinzufügen****.

Gruppen werden gelöscht

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

Bevor Sie beginnen

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

Schritte

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

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

Gruppen werden bearbeitet

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppen** die Gruppe aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Gruppe bearbeiten** den Namen, die Beschreibung oder beides für die Gruppe.
4. Klicken Sie Auf **Speichern**.

Gruppenregeln werden hinzugefügt

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Gruppenregel hinzufügen** einen Namen für die Gruppenregel an.
4. Wählen Sie im Feld **Zielobjekttyp** den Typ des Speicherobjekts aus, das Sie gruppieren möchten.
5. Wählen Sie im Feld **Gruppe** die gewünschte Gruppe aus, für die Sie Gruppenregeln erstellen möchten.
6. Führen Sie im Abschnitt **Bedingungen** die folgenden Schritte aus, um eine Bedingung, eine Bedingungsgruppe oder beide zu erstellen:

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

7. Klicken Sie Auf **Hinzufügen**.

Beispiel für das Erstellen einer Gruppenregel

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

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

Gruppenregeln werden bearbeitet

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

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

   Sie können den Zielobjekttyp für eine Gruppenregel nicht ändern.

4. Klicken Sie Auf **Speichern**.

Gruppenregeln werden gelöscht

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

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

Konfigurieren von Bedingungen für Gruppenregeln

Sie können eine oder mehrere Bedingungen zum Erstellen von Gruppenregeln in Unified Manager konfigurieren, die auf die Speicherobjekte angewendet werden. Die Speicherobjekte, die die Gruppenregel erfüllen, werden zu einer Gruppe zusammengefasst.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Gruppen**.
2. Klicken Sie Auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld **Gruppenregel hinzufügen** einen Operand aus der Liste der Operanden aus.
4. Wählen Sie einen Operator für die Bedingung aus.
5. Geben Sie einen erforderlichen Wert ein, oder wählen Sie einen aus der Liste verfügbar aus.
6. Klicken Sie Auf **Hinzufügen**.

Beispiel für das Konfigurieren einer Bedingung für eine Gruppenregel

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

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

1. Geben Sie einen Namen für die Gruppenregel ein.
2. Wählen Sie den Objekttyp als SVM aus.

3. Wählen Sie eine Gruppe aus der Gruppenliste aus.
4. Wählen Sie im Feld **Bedingungen** als Operand **Objektname** aus.
5. Wählen Sie als Operator * enthält* aus.
6. Geben Sie den Wert als ein `svm_data`.
7. Klicken Sie Auf **Hinzufügen**.

Gruppenaktionen werden hinzugefügt

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

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

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

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

Gruppenaktionen werden bearbeitet

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

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

4. Klicken Sie Auf **Speichern**.

Konfigurieren von Schwellenwerten für den Zustand von Volumes für Gruppen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

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

Gruppenaktionen werden gelöscht

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

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

Gruppenaktionen neu anordnen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenaktionen** auf **Neuordnung**.
3. Ziehen Sie im Dialogfeld **Gruppenaktionen neu anordnen** die Zeilen per Drag-and-Drop, um die Reihenfolge der Gruppenaktionen nach Bedarf neu anzuordnen.
4. Klicken Sie Auf **Speichern**.

Beschreibung der Gruppenfenster und Dialogfelder

Sie können die Seite Verwaltung/Gruppen verwenden, um alle Ihre Gruppen anzuzeigen und zu verwalten. Sie können auch Gruppenregeln und Aktionen für Ihre Speicherobjekte auf der Registerkarte Gruppenregeln und Gruppenaktionen konfigurieren.

Management-/Gruppenseite

Die Seite „Management/Groups“ ermöglicht das Erstellen von Gruppen in Unified Manager zur einfachen Verwaltung von Storage-Objekten. Eine Gruppe ist eine dynamische Sammlung von Storage-Objekten (Cluster, Volumes und SVMs). Diese werden durch die für die Gruppe erstellten Gruppenregeln definiert.

Die Seite Verwaltung/Gruppen enthält Registerkarten, auf denen Sie eine Gruppe, Gruppenregeln und Gruppenaktionen hinzufügen, löschen oder bearbeiten können. Wenn Sie sich als Operator anmelden, haben Sie nur Lesezugriff auf die Seite. Sie können auf den Schaltflächen Hinzufügen, Bearbeiten oder Löschen auf jeder Registerkarte zugreifen, wenn Sie sich als Speicheradministrator oder Unified Manager-Administrator anmelden.

Registerkarte „Gruppen“

Auf der Registerkarte Gruppen werden der Name und die Beschreibung der von Ihnen erstellten Gruppen angezeigt. Sie können Aufgaben wie das Hinzufügen, Bearbeiten oder Löschen einer Gruppe ausführen. Auf der Registerkarte wird außerdem die Anzahl der Gruppenregeln und Gruppenaktionen angezeigt, die einer Gruppe, der Anzahl der Cluster, SVMs und Volumes in der Gruppe zugeordnet sind.

Befehlsschaltflächen

- **Hinzufügen**

  Zeigt das Dialogfeld Gruppe hinzufügen an, in dem Sie eine Gruppe hinzufügen und einen Namen und eine Beschreibung für die Gruppe angeben können.

  Sie können auch Gruppenregeln später auf die Gruppe anwenden, um Speicherobjekte aufzunehmen.

- **Bearbeiten**

  Zeigt das Dialogfeld Gruppe bearbeiten an, in dem Sie den Namen und die Beschreibung der ausgewählten Gruppe bearbeiten können.

- **Löschen**

  Löscht die ausgewählte Gruppe.

Listenansicht

In der Listenansicht werden die Gruppen angezeigt, die Sie in Unified Manager erstellt haben. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen. Standardmäßig ist die Liste nach Gruppennamen sortiert.

- **Name**

  Zeigt den Namen der Gruppe an.

- **Beschreibung**

  Zeigt die Beschreibung der Gruppe an.

- **Verbundene Regeln**

  Zeigt die Anzahl der Regeln an, die der Gruppe hinzugefügt wurden.

- **Verbundene Aktionen**

  Zeigt die Anzahl der Gruppenaktionen an, die der Gruppe hinzugefügt wurden.

- **Anwendbare Cluster**

  Zeigt die Anzahl der Cluster an, die in der Gruppe enthalten sind.

- **Anwendbare SVMs**

  Zeigt die Anzahl der in der Gruppe enthaltenen SVMs an.

- **Geltende Volumen**

  Zeigt die Anzahl der Volumes an, die in der Gruppe enthalten sind.

Registerkarte Gruppenregeln

Auf der Registerkarte Gruppenregeln werden die Gruppenregeln angezeigt, die Sie für Gruppen erstellt haben,

um Speicherobjekte zu enthalten. Sie können Aufgaben wie das Hinzufügen, Bearbeiten oder Löschen einer Gruppenregel ausführen. Auf der Registerkarte wird auch der Gruppenname angezeigt, für den die Gruppenregel erstellt wurde, und das Speicherobjekt, für das die Regel angewendet wird. Sie können auch die Anzahl der Speicherobjekte anzeigen, die die Gruppenregel erfüllen.

Befehlsschaltflächen

- **Hinzufügen**

  Zeigt das Dialogfeld Gruppenregel hinzufügen an, in dem Sie Gruppenregeln für Speicherobjekte erstellen können.

- **Bearbeiten**

  Zeigt das Dialogfeld Gruppenregel bearbeiten an, mit dem Sie zuvor konfigurierte Gruppenregeln neu konfigurieren können.

- **Löschen**

  Löscht die ausgewählte Gruppenregel.

Listenansicht

In der Listenansicht werden die Gruppenregeln angezeigt, die Sie für ein bestimmtes Speicherobjekt (Cluster, Volumes oder SVMs) erstellt haben, und die Anzahl der Speicherobjekte, die der definierten Gruppenregel entsprechen.

- **Name**

  Zeigt den Namen der Regel an.

- * Assoziierte Gruppe*

  Zeigt den Namen der Gruppe an, für die die Gruppenregel definiert ist.

- **Zielobjekttyp**

  Zeigt den Typ des Speicherobjekts an, auf das die Gruppenregel angewendet wird.

- **Anwendbare Objekte**

  Zeigt die Anzahl der in der Gruppe enthaltenen Speicherobjekte basierend auf der Gruppenregel an.

Registerkarte Gruppenaktionen

Auf der Registerkarte Gruppenaktionen werden Name und Typ der Gruppenaktionen angezeigt, die Sie für Gruppen definieren. Sie können Aufgaben wie das Hinzufügen, Bearbeiten, Löschen oder Neuanordnen der Gruppenaktionen ausführen. Auf der Registerkarte wird auch der Name der Gruppe angezeigt, auf die die Gruppenaktion angewendet wird.

Befehlsschaltflächen

- **Hinzufügen**

  Zeigt das Dialogfeld Aktion hinzufügen an, in dem Sie Gruppenaktionen für eine Gruppe von

Speicherobjekten erstellen können. Sie können beispielsweise die Schwellenwertstufen von Storage-Objekten in einer Gruppe festlegen.

- **Bearbeiten**

  Zeigt das Dialogfeld „Aktion bearbeiten“ an, in dem Sie bereits konfigurierte Gruppenaktionen neu konfigurieren können.

- **Löschen**

  Löscht die ausgewählte Gruppenaktion.

- **Neuordnung**

  Zeigt das Dialogfeld Gruppenaktionen neu anordnen an, um die Reihenfolge der Gruppenaktionen neu anzuordnen.

Listenansicht

In der Listenansicht werden die Gruppenaktionen angezeigt, die Sie für die Gruppen im Unified Manager-Server erstellt haben. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen.

- * Rang*

  Zeigt die Reihenfolge der Gruppenaktionen an, die auf die Speicherobjekte in einer Gruppe angewendet werden sollen.

- **Name**

  Zeigt den Namen der Gruppenaktion an.

- * Assoziierte Gruppe*

  Zeigt den Namen der Gruppe an, für die die Gruppenaktion definiert ist.

- **Aktionstyp**

  Zeigt den Typ der Gruppenaktion an, die Sie auf den Speicherobjekten einer Gruppe durchführen können.

  Sie können nicht mehrere Gruppenaktionen desselben Aktionstyps für eine Gruppe erstellen. Sie können beispielsweise eine Gruppenaktion zum Festlegen von Volume-Schwellenwerten für eine Gruppe erstellen. Sie können jedoch keine weitere Gruppenaktion für dieselbe Gruppe erstellen, um Volume-Schwellenwerte zu ändern.

- **Beschreibung**

  Zeigt die Beschreibung der Gruppenaktion an.

Dialogfeld Gruppe hinzufügen

Im Dialogfeld Gruppe hinzufügen können Sie anhand der Gruppenregeln Gruppen erstellen, in denen Cluster, Volumes und SVMs eingeschlossen werden können.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Name**

  Gibt den Namen der Gruppe an. Sie müssen einen eindeutigen Namen für die Gruppe eingeben.

- **Beschreibung**

  Gibt eine aussagekräftige Beschreibung der Gruppe an.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die Erstellung einer neuen Gruppe hinzufügen oder abbrechen.

- **Hinzufügen**

  Erstellt die neue Gruppe.

- **Abbrechen**

  Schließt das Dialogfeld Gruppe hinzufügen, ohne Ihre Änderungen zu speichern.

Dialogfeld „Gruppe bearbeiten“

Im Dialogfeld Gruppe bearbeiten können Sie den Namen und die Beschreibung einer Gruppe ändern.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Gruppenname**

  Zeigt den Namen der Gruppe an. Wenn Sie den Gruppennamen ändern, dürfen Sie keinen vorhandenen Gruppennamen verwenden.

- **Beschreibung**

  Gibt eine aussagekräftige Beschreibung der Gruppe an. Sie können dieses Feld bearbeiten, wenn Sie die aktuelle Beschreibung der Gruppe ändern möchten.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die an der Gruppe vorgenommene Änderung speichern oder abbrechen.

- **Speichern**

  Speichert die vorgenommenen Änderungen und schließt das Dialogfeld.

- **Abbrechen**

  Schließt das Dialogfeld Gruppe bearbeiten, ohne Ihre Änderungen zu speichern.

Detailseite Gruppen

Auf der Seite Gruppen-Details können Sie die Details einer ausgewählten Gruppe

anzeigen. Sie können auch zusätzliche Informationen wie Gruppenregeln und Gruppenaktionen anzeigen, die der ausgewählten Gruppe zugeordnet sind.

Befehlsschaltflächen

- **Gruppen Anzeigen**

  Ermöglicht die Navigation zur Seite Gruppen.

- **Aktionen**

  Ermöglicht Ihnen, die Gruppe entsprechend Ihrer Rolle zu bearbeiten oder zu löschen. Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Gruppenregeln Verwalten**

  Hier können Sie zur Seite Gruppenregeln navigieren, auf der Regeln für diese Gruppe angezeigt werden.

- **Gruppenaktionen Verwalten**

  Hier können Sie zur Seite Gruppenaktionen navigieren, auf der Aktionen für diese Gruppe angezeigt werden.

Zusammenfassungsbereich

Sie können die folgenden Gruppendetails anzeigen:

- **Beschreibung**

  Zeigt die für die Gruppe bereitgestellte Beschreibung an.

- * Erstellt von*

  Zeigt den Namen des Benutzers an, der die Gruppe erstellt hat.

- * Erstellungsdatum*

  Zeigt das Datum an, an dem die Gruppe erstellt wurde.

- **Verbundene Regeln**

  Zeigt alle Gruppenregeln an, die für eine Gruppe erstellt wurden, im Tabellenformat. Sie können die Details jeder Gruppenregel anzeigen, z. B. den Regelnamen, den zugeordneten Objekttyp und die Anzahl der Speicherobjekte des zugehörigen Objekttyps.

- **Verbundene Aktionen**

  Zeigt alle Gruppenaktionen an, die für eine Gruppe konfiguriert sind, im Tabellenformat. Sie können die Details jeder Gruppenaktion anzeigen, z. B. Rang, Name, Aktionstyp und Beschreibung.

Dialogfeld Gruppenregel hinzufügen

Im Dialogfeld Gruppenregel hinzufügen können Sie in Unified Manager Gruppenregeln erstellen, um Speicherobjekte dynamisch zu gruppieren. Sie können später

Gruppenaktionen für die Gruppe konfigurieren und anwenden.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Name**

  Gibt den Namen der Gruppenregel an.

- **Zielobjekttyp**

  Gibt den Typ der Speicherobjekte an, die in die Gruppe aufgenommen werden sollen.

- **Gruppe**

  Gibt den Namen der Gruppe an, für die die Gruppenregel erstellt wird.

- **Bedingungen**

  Gibt Bedingungen an, die bestimmen, welche Speicherobjekte in eine Gruppe aufgenommen werden können.

- **Bedingungsgruppe**

  Gibt Bedingungsgruppen an, die eine oder mehrere Bedingungen für die Einbeziehung von Speicherobjekten in eine Gruppe definiert haben.

Befehlsschaltflächen

- **Speichern und Hinzufügen**

  Fügt die Gruppenregel hinzu und ermöglicht das Hinzufügen einer weiteren Gruppenregel, ohne das Dialogfeld zu schließen.

- **Hinzufügen**

  Fügt die Gruppenregel hinzu und schließt das Dialogfeld Gruppenregel hinzufügen.

- **Abbrechen**

  Bricht die Änderungen ab und schließt das Dialogfeld Gruppenregel hinzufügen.

- **Bedingung Hinzufügen**

  Fügt eine Bedingung hinzu, um die Gruppenregel zu definieren.

- **Bedingungsgruppe Hinzufügen**

  Fügt eine Bedingungsgruppe hinzu, um Bedingungen für die Gruppenregel zu definieren.

Dialogfeld Gruppenregel bearbeiten

Sie können die von Ihnen erstellten Gruppenregeln bearbeiten, um die maximale Anzahl von Speicherobjekten in einer Gruppe aufzunehmen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Regelname**

  Zeigt den Namen der Regel an.

- **Zielobjekttyp**

  Zeigt das Speicherobjekt an, das einer ausgewählten Gruppe hinzugefügt werden soll. Sie können den Objekttyp nicht ändern.

- * Assoziierte Gruppe*

  Zeigt die zugeordnete Gruppe an. Sie können eine andere Gruppe für die Gruppenregel auswählen.

- **Zustand**

  Zeigt die Liste der Bedingungen für eine ausgewählte Gruppe an. Sie können die Bedingungen bearbeiten. Die Speicherobjekte werden auf Basis der Änderungen entweder entfernt oder einer ausgewählten Gruppe hinzugefügt.

Befehlsschaltflächen

- **Speichern**

  Speichert die vorgenommenen Änderungen und schließt das Dialogfeld.

- **Abbrechen**

  Schließt das Dialogfeld Gruppenregel bearbeiten, ohne Ihre Änderungen zu speichern.

Dialogfeld Gruppenaktion hinzufügen

Im Dialogfeld Gruppenaktion hinzufügen können Sie Gruppenaktionen konfigurieren, die auf Speicherobjekte einer ausgewählten Gruppe angewendet werden können.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Name**

  Gibt den Namen der Aktion an.

- **Beschreibung**

  Gibt die Beschreibung der Aktion an.

- **Gruppe**

  Gibt die Gruppe an, für die die Aktion konfiguriert ist.

- **Aktionstyp**

  Gibt den Typ der konfigurierten Aktion an. Auf der Grundlage des ausgewählten Aktionstyps wird das Dialogfeld Gruppenaktion hinzufügen erweitert, sodass Sie eine Gruppenaktion durch die Bereitstellung der erforderlichen Werte konfigurieren können.

Unified Manager unterstützt derzeit nur den Aktionstyp für Volume-Schwellenwerte.

Befehlsschaltflächen

- **Hinzufügen**

  Fügt die neue Aktion hinzu und schließt das Dialogfeld.

- **Abbrechen**

  Schließt das Dialogfeld Gruppenaktion hinzufügen, ohne Ihre Änderungen zu speichern.

Abschnitt „Schwellenwerte für Aktionsvolumen gruppieren“

Im Abschnitt Schwellenwerte für Gruppenaktionen-Volume können Sie für Volumes Integritätsschwellenwerte auf Gruppenebene konfigurieren. Diese Schwellenwerte werden auf alle Volumes in einer Gruppe angewendet. Wenn die Schwellenwerte für den Zustand des Volumes auf Gruppenebene konfiguriert sind, sind die globalen Schwellenwerte für den Systemzustand nicht betroffen.

Sie können die Schwellenwerte für den Zustand von Volumes für Folgendes konfigurieren, um eine Gruppenaktion zu konfigurieren:

- Kapazität
- Wachstum
- Qtree Kontingent
- Snapshots
- Inodes

Globale Standardwerte werden verwendet, wenn für eine dieser Kategorien keine Volume-Integritätsschwellenwerte konfiguriert wurden. Sie können Systemzustandsschwellenwerte für folgende festlegen:

- Kapazität
- Wachstum
- Qtree Kontingent
- Snapshots
- Inodes

Abschnitt „Kapazität“

Sie können Bedingungen für die folgenden Statusschwellenwerte für die Volume-Kapazität festlegen:

- **Raum Fast Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als fast voll betrachtet wird:

  - Standardwert: 80 Prozent

    Der Wert für diesen Schwellenwert muss niedriger sein als der Wert für den Schwellenwert „Volume

Full“, damit der Verwaltungsserver ein Ereignis generieren kann.

  - Event generiert: Volumen fast voll
  - Ereignis Schweregrad: Warnung

- **Raum Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als voll betrachtet wird:

  - Standardwert: 90 Prozent
  - Event generiert: Volumen voll
  - Ereignis Schweregrad: Fehler

- **Überengagiert**

  Gibt den Prozentsatz an, bei dem ein Volume als überfordert betrachtet wird:

  - Standardwert: 100 Prozent
  - Event generiert: Volumen überfordert
  - Ereignis Schweregrad: Fehler

Abschnitt „Wachstum“

Sie können die folgenden Integritätsschwellenwerte für das Volume-Wachstum festlegen:

- **Wachstumsrate**

  Gibt den Prozentsatz an, bei dem die Wachstumsrate eines Volumes als normal angesehen wird, bevor das System ein ungewöhnliches Ereignis der Volumenwachstumsrate generiert:

  - Standardwert: 1 Prozent
  - Generiertes Ereignis: Volumenwachstumsrate anormal
  - Ereignis Schweregrad: Warnung

- **Empfindlichkeit Der Wachstumsrate**

  Gibt den Faktor an, der auf die Standardabweichung der Wachstumsrate eines Volumens angewendet wird. Wenn die Wachstumsrate die faktorierte Standardabweichung überschreitet, wird ein ungewöhnliches Ereignis der Volumenwachstumsrate generiert.

  Ein niedrigerer Wert für die Wachstumsrate zeigt an, dass das Aggregat sehr empfindlich auf Veränderungen der Wachstumsrate reagiert. Der Bereich für die Empfindlichkeit der Wachstumsrate liegt zwischen 1 und 5.

  - Standardwert: 2

Abschnitt qtree Kontingente

Sie können die folgenden Statusschwellenwerte für Volume-Quoten festlegen:

- **Fast Überengagiert**

  Gibt den Prozentsatz an, mit dem ein Volume als beinahe durch qtree Kontingente überengagiert werden soll:

- Standardwert: 95 Prozent
- Event erzeugt: Volumen Qtree Kontingent fast überengagiert
- Ereignis Schweregrad: Warnung

- **Überengagiert**

  Gibt den Prozentsatz an, mit dem ein Volume als durch qtree Kontingente überengagiert werden soll:

  - Standardwert: 100 Prozent
  - Event erstellt: Volumen Qtree Kontingent überfordert
  - Ereignis Schweregrad: Fehler

Abschnitt „Snapshot Kopien“

Sie können die folgenden Integritätsschwellenwerte für die Snapshot Kopien in dem Volume festlegen:

- **Snapshot Reserve Voll**

  Gibt den Prozentsatz an, an dem der für Snapshot Kopien reservierte Speicherplatz voll berücksichtigt wird:

  - Standardwert: 90 Prozent
  - Event generiert: Volume Snapshot Reserve voll
  - Ereignis Schweregrad: Fehler

- **Tage Bis Voll**

  Gibt die Anzahl der Tage an, die noch verbleiben, bevor der für Snapshot Kopien reservierte Speicherplatz mit der vollen Kapazität erreicht wird:

  - Standardwert: 7
  - Event generiert: Volume Snapshot Reserve Days bis Kapazitätsreserve
  - Ereignis Schweregrad: Fehler

- * Anzahl*

  Gibt die Anzahl der Snapshot Kopien auf einem Volume an, die als zu viele Kopien gelten:

  - Standardwert: 250
  - Generiertes Ereignis: Zu viele Snapshot Kopien
  - Ereignis Schweregrad: Fehler

Inodes-Abschnitt

Sie können die folgenden Integritätsschwellenwerte für Inodes festlegen:

- **Fast Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als den Großteil seiner Inodes verbraucht wurde:

  - Standardwert: 80 Prozent
  - Event generiert: Inodes fast voll

- Ereignis Schweregrad: Warnung

- **Voll**

  Gibt den Prozentsatz an, bei dem ein Volume als „alle Inodes verbraucht“ betrachtet wird:

  - Standardwert: 90 Prozent
  - Event generiert: Inodes voll
  - Ereignis Schweregrad: Fehler

Dialogfeld Gruppenaktion bearbeiten

Sie können die Gruppenaktion bearbeiten, die Sie für Gruppen erstellt haben, indem Sie das Dialogfeld Gruppenaktion bearbeiten verwenden.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- **Aktionsname**

  Zeigt den Namen der Gruppenaktion an.

- **Beschreibung**

  Zeigt die Beschreibung der Gruppenaktion an.

- **Gruppe**

  Zeigt den Namen der ausgewählten Gruppe an.

- **Aktionstyp**

  Zeigt den Typ der Gruppenaktion an. Sie können den Aktionstyp nicht ändern. Sie können jedoch die Parameter ändern, mit denen Sie die Gruppenaktion konfigurieren.

Befehlsschaltflächen

- **Speichern**

  Speichert die Änderungen, die Sie an der Gruppenaktion vorgenommen haben.

- **Abbrechen**

  Schließt das Dialogfeld Gruppenaktion bearbeiten, ohne Ihre Änderungen zu speichern.

Dialogfeld Gruppenaktionen neu anordnen

Sie können das Dialogfeld Gruppenaktionen neu anordnen verwenden, um die Reihen einer oder mehrerer Gruppenaktionen zu ändern. Die Position einer Gruppenaktion in der Tabelle bestimmt den Rang für die Gruppenaktion.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

- * Rang*

Gibt die Reihenfolge der Gruppenaktion an, die auf Speicherobjekte in einer Gruppe angewendet werden soll.

- **Name**

  Gibt den Namen der Gruppenaktion an.

- **Aktionstyp**

  Gibt den Aktionstyp an, den Sie auf den Speicherobjekten einer Gruppe ausführen können.

- * Assoziierte Gruppe*

  Gibt den Namen der Gruppe an, für die die Gruppenaktionen definiert sind.

Managen und Überwachen von Sicherungsbeziehungen

Mit OnCommand Unified Manager können Sicherungsbeziehungen erstellt, SnapMirror und SnapVault Beziehungen auf gemanagten Clustern überwacht und Fehler behoben werden und Daten können wiederhergestellt werden, sobald sie überschrieben oder verloren sind.

Für SnapMirror Vorgänge gibt es zwei Replizierungstypen:

- Asynchron

  Die Replizierung vom primären zum sekundären Volume wird durch einen Zeitplan festgelegt.

- Synchron

  Die Replizierung wird gleichzeitig auf dem primären und sekundären Volume durchgeführt.

Sie können bis zu 10 Sicherungsjobs gleichzeitig ausführen, ohne die Leistung zu beeinträchtigen. Möglicherweise haben Sie Auswirkungen auf die Leistung, wenn Sie zwischen 11 und 30 Jobs gleichzeitig ausführen. Es wird nicht empfohlen, mehr als 30 Jobs gleichzeitig auszuführen.

Was sind Ressourcen-Pools

Ressourcen-Pools sind Gruppen von Aggregaten, die von einem Storage-Administrator mithilfe von Unified Manager erstellt werden, um Partnerapplikationen für das Backup-Management bereitzustellen.

Ressourcen werden eventuell anhand von Attributen wie Performance, Kosten, physischer Standort oder Verfügbarkeit in einem Pool genutzt. Durch Gruppierung zugehöriger Ressourcen in einem Pool können Sie den Pool als eine Einheit für Monitoring und Bereitstellung behandeln. Dies vereinfacht das Management dieser Ressourcen und ermöglicht eine flexiblere und effizientere Nutzung des Storage.

Während der sekundären Storage-Provisionierung bestimmt Unified Manager das am besten geeignete Aggregat im Ressourcen-Pool zum Schutz anhand folgender Kriterien:

- Das Aggregat ist ein Daten-Aggregat (kein Root-Aggregat) und es ist ONLINE.

- Das Aggregat ist auf einem Ziel-Cluster Knoten, dessen ONTAP Version die gleiche oder größer ist als die Hauptversion des Quell-Clusters.
- Das Aggregat verfügt über den größten verfügbaren Platz aller Aggregate im Ressourcenpool.
- Nach dem Bereitstellen des Ziel-Volume liegt der Aggregatspeicherplatz innerhalb des für das Aggregat definierten Schwellwerts (globaler oder lokaler Schwellenwert, je nachdem, welcher davon zutreffend ist), der für das Aggregat festgelegt wurde.
- Die Anzahl der FlexVol-Volumes auf dem Ziel-Node darf die Plattformgrenze nicht überschreiten.

Arten der SnapMirror Sicherung

Je nach Implementierung Ihrer Topologie des Storage können Sie mit Unified Manager mehrere Arten von SnapMirror Sicherungsbeziehungen konfigurieren. Alle Varianten des SnapMirror Schutzes bieten Failover Disaster Recovery-Schutz, bieten jedoch unterschiedliche Funktionen in Bezug auf Performance, Versionsflexibilität und Sicherung mehrerer Backup-Kopien.

Herkömmliche asynchrone Datensicherungsbeziehungen von SnapMirror

Herkömmlicher SnapMirror asynchroner Schutz bietet Sicherung der Blockreplizierung zwischen Quell- und Ziel-Volumes.

In herkömmlichen SnapMirror Beziehungen werden Spiegelvorgänge schneller ausgeführt als in alternativen SnapMirror Beziehungen, da der Spiegelvorgang auf der Blockreplizierung basiert. Beim herkömmlichen SnapMirror Schutz muss das Ziel-Volume jedoch unter derselben oder einer höheren kleineren Version der ONTAP Software wie das Quell-Volume innerhalb derselben größeren Version (z. B. Version 8.x zu 8.x oder 9.x zu 9.x) ausgeführt werden.

SnapMirror Asynchronous Protection mit versionsflexibler Replizierung

SnapMirror asynchrone Sicherung mit versionsflexibler Replizierung bietet einen logischen Spiegelschutz der Replizierungszwischen Quell- und Ziel-Volumes, selbst wenn diese Volumes unter verschiedenen Versionen von ONTAP 8.3 oder höher ausgeführt werden (z. B. Version 8.3 zu 8.3, oder 8.3 zu 9.1 oder 9.0 zu 8.3).

In SnapMirror Beziehungen mit versionsflexibler Replizierung werden Spiegelvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror Beziehungen.

Aufgrund der langsameren Ausführung eignet sich SnapMirror mit versionsflexibler Replizierungssicherung nicht für den Einsatz unter folgenden Umständen:

- Das Quellobjekt enthält mehr als 10 Millionen Dateien, die gesichert werden müssen.
- Die Recovery-Zeitvorgabe für die geschützten Daten beträgt maximal zwei Stunden. (Das heißt, das Ziel muss immer gespiegelte, wiederherstellbare Daten enthalten, die nicht mehr als zwei Stunden älter sind als die Daten der Quelle.)

In einem der aufgeführten Situationen ist die schnellere blockbasierte Ausführung der SnapMirror Standardsicherung erforderlich.

SnapMirror Asynchronous Protection mit versionsflexibler Replizierung und Option für Backups

SnapMirror Asynchronous Protection mit der versionsflexiblen Replizierungs- und Backup-Option bietet Spiegelschutz zwischen Quell- und Ziel-Volumes und die Möglichkeit, mehrere Kopien der gespiegelten Daten

am Zielspeicherort zu speichern.

Der Storage-Administrator kann festlegen, welche Snapshot Kopien vom Quell- zum Zielsystem gespiegelt werden, und er kann auch angeben, wie lange diese Kopien am Ziel aufbewahrt werden sollen, selbst wenn sie an der Quelle gelöscht werden.

In SnapMirror Beziehungen mit versionsflexibler Replizierung und Backup-Option werden Spiegelvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror Beziehungen.

SnapMirror synchroner Schutz mit strenger Synchronisierung

SnapMirror Synchronous Schutz mit „`strict`“-Synchronisierung sorgt dafür, dass das primäre und sekundäre Volume immer eine echte Kopie voneinander sind. Falls beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replizierungsfehler auftritt, wird der Client-I/O auf das primäre Volume unterbrochen.

SnapMirror synchroner Schutz mit regelmäßiger Synchronisierung

SnapMirror Synchronous Schutz mit „`regular`“-Synchronisierung erfordert nicht, dass das primäre und sekundäre Volume immer eine echte Kopie voneinander sind, wodurch die Verfügbarkeit des primären Volumes gewährleistet wird. Wenn beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replizierungsfehler auftritt, werden die primären und sekundären Volumes nicht mehr synchronisiert und die Client-I/O-Vorgänge werden weiter zum primären Volume fortgesetzt.

> Die Schaltfläche „Wiederherstellen“ und die Schaltflächen zum Beziehungsvorgang sind nicht verfügbar, wenn synchrone Schutzbeziehungen auf der Seite „Gesundheits-/Volume-Bestand“ oder auf der Seite „Angaben zum Zustand/Volumen“ überwacht werden.

Anzeigen von Volume-Sicherungsbeziehungen

Auf der Seite „Schutz/Volume-Beziehungen“ können Sie den Status vorhandener Volume SnapMirror und SnapVault Beziehungen einsehen. Sie können auch Details zu Sicherungsbeziehungen unter anderem hinsichtlich Transfer- und lag-Status, Quell- und Zieldetails, Zeitplan- und Richtlinieninformationen usw. prüfen.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können auch Beziehungsbefehle von dieser Seite aus initiieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Volume Relationships**.

   Die Seite „Schutz/Volume-Beziehungen“ wird angezeigt.

2. Es gibt folgende Möglichkeiten, die Details zur Volume-Sicherung anzuzeigen:

   - Um aktuelle Informationen über alle Volume-Beziehungen anzuzeigen, bleiben Sie auf der Standard **Alle Volume-Beziehungen**-Seite.

- Um detaillierte Informationen zu den Trends der Volume-Übertragung über einen bestimmten Zeitraum anzuzeigen, wählen Sie im Menü Ansicht die Option **Volume Transfer Status (Historisch)**.
- Um detaillierte Informationen über die Volume Transfer-Aktivität auf Tagesbasis anzuzeigen, wählen Sie im Menü Ansicht die Option **Volume Transfer Rate (Historisch)** aus.

Die Volume-Transferansichten zeigen Informationen zu Volumes nur in asynchronen Beziehungen an - Volumes in synchronen Beziehungen werden nicht angezeigt.

Erstellen einer SnapVault-Schutzbeziehung über die Seite „Systemzustand/Volumen-Inventar“

Auf der Seite „Systemzustand“/„Volumes-Bestandsaufnahme“ können Sie SnapVault-Beziehungen für ein oder mehrere Volumes auf derselben Storage Virtual Machine (SVM) erstellen, um Daten-Backups zu Sicherungszwecken zu ermöglichen.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Das Menü * Protect* wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
- Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung vorhanden ist und der Ziel-Cluster noch nicht erkannt wurde

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **Volumes**.
2. Klicken Sie auf der Seite **Health/Volumes** Inventory mit der rechten Maustaste auf ein Volume, das Sie schützen möchten, und wählen Sie **Protect** aus.

   Wenn Sie mehrere Sicherungsbeziehungen auf derselben virtuellen Speichermaschine (SVM) erstellen möchten, wählen Sie auf der Seite Health/Volumes Inventory ein oder mehrere Volumes aus, und klicken Sie in der Symbolleiste auf **Protect**.

3. Wählen Sie im Menü * SnapVault* aus.

   Das Dialogfeld Schutz konfigurieren wird gestartet.

4. Klicken Sie auf **SnapVault**, um die Registerkarte **SnapVault** anzuzeigen und die Informationen zum sekundären Volume zu konfigurieren.
5. Klicken Sie auf **Erweitert**, um Deduplizierung, Komprimierung, Autogrow und Platzgarantie nach Bedarf festzulegen und klicken Sie dann auf **Apply**.
6. Füllen Sie auf der Registerkarte **SnapVault** den Bereich **Zielinformationen** und den Bereich **Beziehungseinstellungen** aus.
7. Klicken Sie Auf **Anwenden**.

Sie gelangen wieder zur Seite „Health/Volumes Inventory“.

8. Klicken Sie oben auf der Seite **Health/Volumes** Inventory auf den Link für die Schutzkonfiguration.

   Wenn Sie nur eine Schutzbeziehung erstellen, wird die Seite Schutz-/Jobdetails angezeigt. Wenn Sie jedoch mehr als eine Schutzbeziehung erstellen, wird eine gefilterte Liste aller Jobs angezeigt, die mit dem Schutzvorgang verknüpft sind.

9. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie nur einen Job haben, klicken Sie auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist.
   - Wenn Sie mehr als einen Job haben:
     i. Klicken Sie in der Liste Jobs auf einen Job.
     ii. Klicken Sie auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist.
     iii. Verwenden Sie die Schaltfläche **Zurück**, um zur gefilterten Liste zurückzukehren und einen anderen Job anzuzeigen.

Erstellen einer SnapVault-Schutzbeziehung auf der Seite „Health/Volume Details“

Sie können eine SnapVault-Beziehung auf der Seite „Systemzustand/Volume-Details“ erstellen, sodass Daten-Backups für Sicherungszwecke auf Volumes aktiviert sind.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten, um diese Aufgabe auszuführen.

Über diese Aufgabe

Das Menü * Protect* wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
- Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung vorhanden ist und der Ziel-Cluster noch nicht erkannt wurde

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Gesundheit/Volumen** mit der rechten Maustaste auf ein Volume in der Topologieansicht, die Sie schützen möchten.
2. Wählen Sie im Menü * Protect* > **SnapVault** aus.

   Das Dialogfeld Schutz konfigurieren wird gestartet.

3. Klicken Sie auf **SnapVault**, um die Registerkarte **SnapVault** anzuzeigen und die Informationen zur sekundären Ressource zu konfigurieren.
4. Klicken Sie auf **Erweitert**, um Deduplizierung, Komprimierung, Autogrow und Platzgarantie nach Bedarf

festzulegen und klicken Sie dann auf **Apply**.

5. Füllen Sie im Dialogfeld **Schutz konfigurieren** den Bereich **Zielinformationen** und den Bereich **Beziehungseinstellungen** aus.
6. Klicken Sie Auf **Anwenden**.

   Sie gelangen zurück zur Seite „Health/Volume Details“.

7. Klicken Sie oben auf der Seite **Health/Volume** Details auf den Link für die Schutzkonfiguration.

   Die Seite Schutz-/Jobdetails wird angezeigt.

8. Klicken Sie auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist.

   Wenn die Aufgabenstellungen abgeschlossen sind, werden die neuen Beziehungen auf der Topologieansicht „Systemzustand/Volume-Details“ angezeigt.

Erstellen einer SnapMirror Sicherungsbeziehung auf der Seite „Systemzustand“/„Volumes-Inventar“

Mithilfe der Seite „Systemzustand“/„Volumes Inventar“ können Sie mehrere SnapMirror Sicherungsbeziehungen gleichzeitig erstellen, indem Sie mehrere Volumes auf derselben SVM auswählen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Über diese Aufgabe

Das Menü * Protect* wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
- Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung vorhanden ist und der Ziel-Cluster noch nicht erkannt wurde

Schritte

1. Klicken Sie auf der Seite **Health/Volumes** Inventory mit der rechten Maustaste auf ein Volume, das Sie schützen möchten.

   Wenn Sie mehrere Sicherungsbeziehungen auf derselben SVM erstellen möchten, wählen Sie auf der Seite Health/Volumes Inventory ein oder mehrere Volumes aus, und klicken Sie in der Symbolleiste auf **Protect** > **SnapMirror**.

   Das Dialogfeld Schutz konfigurieren wird angezeigt.

2. Klicken Sie auf **SnapMirror**, um die Registerkarte **SnapMirror** anzuzeigen und die Zielinformationen zu konfigurieren.

3. Klicken Sie auf **Erweitert**, um die Platzgarantie nach Bedarf festzulegen, und klicken Sie dann auf **Anwenden**.
4. Füllen Sie auf der Registerkarte **SnapMirror** den Bereich **Zielinformationen** und den Bereich **Beziehungseinstellungen** aus.
5. Klicken Sie Auf **Anwenden**.

   Sie gelangen wieder zur Seite „Health/Volumes Inventory“.

6. Klicken Sie oben auf der Seite **Health/Volumes** Inventory auf den Link für die Schutzkonfiguration.

   Wenn Sie nur eine Schutzbeziehung erstellen, wird die Seite Schutz-/Jobdetails angezeigt. Wenn Sie jedoch mehr als eine Schutzbeziehung erstellen, wird eine Liste aller mit dem Schutzvorgang verknüpften Jobs angezeigt.

7. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie nur einen Job haben, klicken Sie auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist.
   - Wenn Sie mehr als einen Job haben:
     i. Klicken Sie in der Liste Jobs auf einen Job.
     ii. Klicken Sie auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist.
     iii. Verwenden Sie die Schaltfläche **Zurück**, um zur gefilterten Liste zurückzukehren und einen anderen Job anzuzeigen.

Ergebnisse

Je nachdem, welche Ziel-SVM Sie während der Konfiguration oder in den Optionen angegeben haben, die Sie in den erweiterten Einstellungen aktiviert haben, kann die SnapMirror Beziehung eine oder mehrere mögliche Varianten sein:

- Falls Sie eine Ziel-SVM angegeben haben, die unter derselben oder einer neueren Version von ONTAP im Vergleich zur des Quell-Volume ausgeführt wird, ist eine auf Replizierung basierende SnapMirror Beziehung das Standardergebnis.
- Wenn Sie eine Ziel-SVM angegeben haben, die im Vergleich zum Quell-Volume unter derselben oder einer neueren Version von ONTAP (8.3 oder höher) ausgeführt wird, aber Sie in den erweiterten Einstellungen eine versionsflexible Replizierung aktiviert haben, ist das Ergebnis eine SnapMirror Beziehung mit versionsflexibler Replizierung.
- Wenn Sie eine Ziel-SVM angegeben haben, die unter einer früheren Version von ONTAP 8.3 oder einer höheren Version als die des Quell-Volume ausgeführt wird, und die frühere Version unterstützt eine versionsflexible Replizierung. Das automatische Ergebnis ist eine SnapMirror Beziehung mit versionsflexibler Replizierung.

Erstellen einer SnapMirror Schutzbeziehung auf der Seite „Systemzustand“/„Volume-Details“

Auf der Seite „Systemzustand“/„Volume-Details“ können Sie eine SnapMirror Beziehung erstellen, sodass die Datenreplizierung zu Sicherungszwecken aktiviert ist. Die

SnapMirror Replizierung ermöglicht Ihnen die Wiederherstellung von Daten vom Ziel-Volume im Falle eines Datenverlusts auf dem Quellsystem.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Über diese Aufgabe

Das Menü * Protect* wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
- Wenn es sich um ein FlexGroup Volume handelt
- Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung besteht und der Ziel-Cluster noch nicht erkannt wurde

Sie können bis zu 10 Sicherungsjobs gleichzeitig ausführen, ohne die Leistung zu beeinträchtigen. Möglicherweise haben Sie Auswirkungen auf die Leistung, wenn Sie zwischen 11 und 30 Jobs gleichzeitig ausführen. Es wird nicht empfohlen, mehr als 30 Jobs gleichzeitig auszuführen.

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Gesundheit/Volumen** mit der rechten Maustaste in die Topologieansicht auf den Namen eines Volumes, das Sie schützen möchten.
2. Wählen Sie aus dem Menü * Protect* > **SnapMirror** aus.

   Das Dialogfeld Schutz konfigurieren wird angezeigt.

3. Klicken Sie auf **SnapMirror**, um die Registerkarte **SnapMirror** anzuzeigen und die Zielinformationen zu konfigurieren.
4. Klicken Sie auf **Erweitert**, um die Platzgarantie nach Bedarf festzulegen, und klicken Sie dann auf **Anwenden**.
5. Füllen Sie im Dialogfeld **Schutz konfigurieren** den Bereich **Zielinformationen** und den Bereich **Beziehungseinstellungen** aus.
6. Klicken Sie Auf **Anwenden**.

   Sie gelangen zurück zur Seite „Health/Volume Details“.

7. Klicken Sie oben auf der Seite **Health/Volume** Details auf den Link für die Schutzkonfiguration.

   Die Aufgaben und Details des Jobs werden auf der Seite „Schutz/Job-Details“ angezeigt.

8. Klicken Sie auf der Seite **Schutz/Job** Details auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist.
9. Wenn die Aufgaben abgeschlossen sind, klicken Sie auf **Zurück** in Ihrem Browser, um zur Detailseite **Gesundheit/Volumen** zurückzukehren.

   Die neue Beziehung wird auf der Topologieansicht „Systemzustand/Volume-Details“ angezeigt.

Ergebnisse

Je nachdem, welche Ziel-SVM Sie während der Konfiguration oder in den Optionen angegeben haben, die Sie in den erweiterten Einstellungen aktiviert haben, kann die SnapMirror Beziehung eine oder mehrere mögliche Varianten sein:

- Falls Sie eine Ziel-SVM angegeben haben, die unter derselben oder einer neueren Version von ONTAP im Vergleich zur des Quell-Volume ausgeführt wird, ist eine auf Replizierung basierende SnapMirror Beziehung das Standardergebnis.
- Wenn Sie eine Ziel-SVM angegeben haben, die im Vergleich zum Quell-Volume unter derselben oder einer neueren Version von ONTAP (Version 8.3 oder höher) ausgeführt wird, aber Sie in den erweiterten Einstellungen eine versionsflexible Replizierung aktiviert haben, ist das Ergebnis eine SnapMirror Beziehung mit versionsflexibler Replizierung.
- Wenn Sie eine Ziel-SVM angegeben haben, die unter einer früheren Version von ONTAP 8.3 ausgeführt wird, oder eine Version, die höher ist als die des Quell-Volume, und die frühere Version unterstützt versionsflexible Replizierung. Das automatische Ergebnis ist eine SnapMirror Beziehung mit versionsflexibler Replizierung.

Erstellen einer SnapMirror Beziehung mit versionsflexibler Replizierung

Sie können eine SnapMirror Beziehung mit versionsflexibler Replizierung erstellen. Die versionsflexible Replizierung ermöglicht Ihnen die Implementierung der SnapMirror Sicherung, selbst wenn Quell- und Ziel-Volumes unter verschiedenen Versionen von ONTAP ausgeführt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.
- Die Quell- und Ziel-SVMs müssen jeweils eine SnapMirror Lizenz aktiviert haben.
- Die Quell- und Ziel-SVMs müssen jeweils unter einer Version von ONTAP ausgeführt werden, die eine versionsflexible Replizierung unterstützt.

Über diese Aufgabe

SnapMirror mit versionsflexibler Replizierung ermöglicht Ihnen die Implementierung von SnapMirror Sicherung auch in heterogenen Storage-Umgebungen, in denen nicht der gesamte Storage unter einer Version von ONTAP läuft. Allerdings werden Spiegelvorgänge, die unter SnapMirror mit versionsflexibler Replizierung durchgeführt werden, nicht so schnell ausgeführt wie in herkömmlichen Blockreplizierung SnapMirror.

Schritte

1. Öffnen Sie das Dialogfeld **Schutz konfigurieren** für das zu schützenden Volume.
    - Wenn Sie die Registerkarte Schutz auf der Seite Health/Volume Details anzeigen, klicken Sie mit der rechten Maustaste in die Topologieansicht, die den Namen eines Volumes hat, das Sie schützen möchten, und wählen Sie aus dem Menü **Protect** > **SnapMirror** aus.
    - Wenn Sie die Seite „Health/Volumes Inventory“ aufrufen, suchen Sie ein Volume, das Sie schützen möchten, und klicken Sie mit der rechten Maustaste darauf. Wählen Sie dann aus dem Menü die Option **Protect** > **SnapMirror** aus. Das Dialogfeld Schutz konfigurieren wird angezeigt.

2. Klicken Sie auf **SnapMirror**, um die Registerkarte **SnapMirror** anzuzeigen.
3. Füllen Sie im Dialogfeld **Schutz konfigurieren** den Bereich **Zielinformationen** und den Bereich **Beziehungseinstellungen** aus.

   Falls Sie eine Ziel-SVM angeben, die unter einer früheren Version von ONTAP ausgeführt wird als das zu schützende Quell-Volume. Falls diese frühere Version die versionsflexible Replizierung unterstützt, konfiguriert diese Aufgabe SnapMirror automatisch mit versionsflexibler Replizierung.

4. Wenn Sie eine Ziel-SVM angeben, die unter derselben Version von ONTAP ausgeführt wird wie die des Quell-Volume, aber Sie dennoch SnapMirror mit versionsflexibler Replikation konfigurieren möchten, klicken Sie auf **Erweitert**, um die versionsflexible Replikation zu aktivieren und dann auf **Apply** zu klicken.
5. Klicken Sie Auf **Anwenden**.

   Sie gelangen zurück zur Seite „Health/Volume Details“.

6. Klicken Sie oben auf der Seite **Health/Volume** Details auf den Link für die Schutzkonfiguration.

   Die Aufgaben und Details der Aufträge werden auf der Seite „Schutz/Job-Details“ angezeigt.

7. Klicken Sie auf der Seite **Schutz/Job** Details auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist.
8. Wenn die Aufgaben abgeschlossen sind, klicken Sie auf **Zurück** in Ihrem Browser, um zur Detailseite **Gesundheit/Volumen** zurückzukehren.

   Die neue Beziehung wird auf der Topologieansicht „Systemzustand/Volume-Details“ angezeigt.

Erstellung von SnapMirror Beziehungen mit versionsflexibler Replizierung mit Backup-Option

Sie können eine SnapMirror Beziehung mit versionsflexiblen Replizierungs- und Backup-Funktionen erstellen. Die Funktion für Backup-Optionen ermöglicht die Implementierung der SnapMirror Sicherung und enthält zudem mehrere Versionen von Backup-Kopien am Zielspeicherort.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.
- Die Quell- und Ziel-SVMs müssen jeweils eine SnapMirror Lizenz aktiviert haben.
- Die Quell- und Ziel-SVMs müssen jeweils eine SnapVault Lizenz aktiviert haben.
- Die Quell- und Ziel-SVMs müssen jeweils unter einer Version der Software von ONTAP (8.3 oder höher) ausgeführt werden, die eine versionsflexible Replizierung unterstützt.

Über diese Aufgabe

Wenn Sie SnapMirror mit Backup-Optionsfunktion konfigurieren, können Sie Ihre Daten mit SnapMirror Disaster Recovery-Funktionen schützen, beispielsweise mit Volume Failover-Fähigkeit und gleichzeitig SnapVault Funktionen bereitstellen, beispielsweise die Sicherung mehrerer Backup-Kopien.

Schritte

1. Öffnen Sie das Dialogfeld **Schutz konfigurieren** für das zu schützenden Volume.
   - Wenn Sie die Registerkarte Schutz auf der Seite Health/Volume Details anzeigen, klicken Sie mit der rechten Maustaste in die Topologieansicht auf den Namen eines Volumes, das Sie schützen möchten, und wählen Sie aus dem Menü **Protect** > **SnapMirror** aus.
   - Wenn Sie die Seite „Health/Volumes Inventory“ aufrufen, suchen Sie ein zu schützende Volume und klicken Sie mit der rechten Maustaste darauf. Wählen Sie dann im Menü * Protect* > **SnapMirror** aus. Das Dialogfeld Schutz konfigurieren wird angezeigt.
2. Klicken Sie auf **SnapMirror**, um die Registerkarte **SnapMirror** anzuzeigen.
3. Füllen Sie im Dialogfeld **Schutz konfigurieren** den Bereich **Zielinformationen** und den Bereich **Beziehungseinstellungen** aus.
4. Klicken Sie auf **Erweitert**, um das Dialogfeld **Erweiterte Zieleinstellungen** anzuzeigen.
5. Wenn das Kontrollkästchen **Versionsflexible Replikation** nicht bereits aktiviert ist, wählen Sie es jetzt aus.
6. Aktivieren Sie das Kontrollkästchen **mit Backup Option**, um die Funktion der Backup-Option zu aktivieren. Klicken Sie dann auf **Apply**.
7. Klicken Sie Auf **Anwenden**.

   Sie gelangen zurück zur Seite „Health/Volume Details“.

8. Klicken Sie oben auf der Seite **Health/Volume** Details auf den Link für die Schutzkonfiguration.

   Die Aufgaben und Details der Aufträge werden auf der Seite „Schutz/Job-Details“ angezeigt.

9. Klicken Sie auf der Seite **Schutz/Job** Details auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist.
10. Wenn die Aufgaben abgeschlossen sind, klicken Sie auf **Zurück** in Ihrem Browser, um zur Detailseite **Gesundheit/Volumen** zurückzukehren.

    Die neue Beziehung wird auf der Topologieansicht „Systemzustand/Volume-Details“ angezeigt.

Konfigurieren von Ziel-Effizienzeinstellungen

Mithilfe des Dialogfelds „Advanced Destination Settings“ können Sie die Effizienzeinstellungen des Ziels, wie Deduplizierung, Komprimierung, Autogrow und Speicherplatzzusage für ein Schutzziel, konfigurieren. Sie verwenden diese Einstellungen, um die Speicherauslastung auf einem Ziel oder einem sekundären Volume zu maximieren.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Standardmäßig stimmen die Effizienzeinstellungen mit denen des Quell-Volume überein. Ausgenommen sind Komprimierungseinstellungen in einer SnapVault-Beziehung, die standardmäßig deaktiviert sind.

Schritte

1. Klicken Sie je nach Art der zu konfigurierende Beziehung entweder auf die Registerkarte **SnapMirror** oder auf die Registerkarte **SnapVault** im Dialogfeld **Schutz konfigurieren**.
2. Klicken Sie im Bereich **Zielinformationen** auf **Erweitert**.

   Das Dialogfeld Erweiterte Zieleinstellungen wird geöffnet.
3. Aktivierung oder Deaktivierung der Effizienzeinstellungen für Deduplizierung, Komprimierung, Autogrow und Speicherplatzzusagen nach Bedarf
4. Klicken Sie auf **Anwenden**, um Ihre Auswahl zu speichern und zum Dialogfeld **Schutz konfigurieren** zurückzukehren.

Erstellen von Zeitplänen für SnapMirror und SnapVault

Sie können grundlegende oder erweiterte Zeitpläne für SnapMirror und SnapVault erstellen, um automatische Datensicherheitstransfers auf einem Quell- oder primären Volume zu ermöglichen. Dadurch werden diese je nach Häufigkeit der Datenänderungen auf Ihren Volumes häufiger oder weniger häufiger durchgeführt.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen den Bereich Zielinformationen im Dialogfeld Schutz konfigurieren bereits ausgefüllt haben.
- Sie müssen Workflow Automation einrichten, um diese Aufgabe auszuführen.

Schritte

1. Klicken Sie im Dialogfeld **Schutz konfigurieren** auf der Registerkarte **SnapMirror** oder auf der Registerkarte **SnapVault** im Bereich **Beziehungseinstellungen** auf den Link **Zeitplan erstellen**.

   Das Dialogfeld Zeitplan erstellen wird angezeigt.
2. Geben Sie im Feld **Terminplanname** den Namen ein, den Sie dem Zeitplan geben möchten.
3. Wählen Sie eine der folgenden Optionen:
   - **Einfach**

     Wählen Sie aus, wenn Sie einen grundlegenden Intervall-Stil-Zeitplan erstellen möchten.
   - **Erweitert**

     Wählen Sie aus, wenn Sie einen Zeitplan im Cron-Stil erstellen möchten.
4. Klicken Sie Auf **Erstellen**.

   Der neue Zeitplan wird in der Dropdown-Liste „SnapMirror Schedule“ oder „SnapVault Schedule“ angezeigt.

Erstellen von Kaskadierungs- oder Fanout-Beziehungen, um den Schutz vor einer bestehenden Schutzbeziehung zu erweitern

Sie können den Schutz vor einer bestehenden Beziehung erweitern, indem Sie entweder einen Fanout vom Quell-Volume oder eine Kaskade vom Zielvolumen einer bestehenden Beziehung erstellen. Dies kann der Fall sein, wenn Sie Daten von einem Standort auf mehrere Standorte kopieren oder durch das Erstellen weiterer Backups zusätzlichen Schutz bieten müssen.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie Auf **Schutz** > **Volume Relationships**.
2. Wählen Sie auf der Seite **Schutz/Volume Beziehungen** die SnapMirror Beziehung aus, aus der Sie den Schutz erweitern möchten.
3. Klicken Sie in der Aktionsleiste auf **Schutz erweitern**.
4. Wählen Sie im Menü entweder **aus Quelle** oder **aus Ziel** aus, je nachdem, ob Sie eine Fanout-Beziehung aus der Quelle oder eine Kaskadenbeziehung aus dem Ziel erstellen.
5. Wählen Sie entweder **mit SnapMirror** oder **mit SnapVault** aus, je nach Art der von Ihnen erstellten Schutzbeziehung.

   Das Dialogfeld Schutz konfigurieren wird angezeigt.
6. Füllen Sie die Informationen aus, wie im Dialogfeld **Schutz konfigurieren** angegeben.

Bearbeiten von Schutzbeziehungen auf der Seite „Schutz/Volume-Beziehungen“

Sie können vorhandene Schutzbeziehungen bearbeiten, um die maximale Übertragungsrate, die Schutzrichtlinie oder den Schutzzeitplan zu ändern. Sie können eine Beziehung bearbeiten, um die für Datentransfers verwendete Bandbreite zu verringern oder die Häufigkeit geplanter Transfers zu erhöhen, da sich Daten oft ändern.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die ausgewählten Volumes müssen Schutzbeziehungsziele sein. Sie können Beziehungen nicht bearbeiten, wenn Quell-Volumes, Volumes für die Lastverteilung oder Volumes ausgewählt werden, die nicht Ziel einer SnapMirror oder SnapVault Beziehung sind.

Schritte

1. Wählen Sie auf der Seite **Schutz/Volume-Beziehungen** in der Liste Volumes ein oder mehrere Volumes in derselben SVM aus, für die Sie die Beziehungseinstellungen bearbeiten möchten, und wählen Sie dann in der Symbolleiste **Bearbeiten** aus.

Das Dialogfeld Beziehung bearbeiten wird angezeigt.

2. Bearbeiten Sie im Dialogfeld „Beziehungen bearbeiten*“ die maximale Übertragungsrate, die Schutzrichtlinie oder den Schutzzeitplan nach Bedarf.
3. Klicken Sie Auf **Anwenden**.

   Die Änderungen werden auf die ausgewählten Beziehungen angewendet.

Bearbeiten von Schutzbeziehungen auf der Seite „Angaben zum Zustand/Volumen“

Sie können vorhandene Schutzbeziehungen bearbeiten, um die aktuelle maximale Übertragungsrate, Schutzrichtlinie oder den Schutzzeitplan zu ändern. Sie können eine Beziehung bearbeiten, um die für Datentransfers verwendete Bandbreite zu verringern oder die Häufigkeit geplanter Transfers zu erhöhen, da sich Daten oft ändern.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Workflow Automation muss installiert und konfiguriert sein.

Über diese Aufgabe

Die ausgewählten Volumes müssen Schutzbeziehungsziele sein. Sie können Beziehungen nicht bearbeiten, wenn Quell-Volumes, Volumes für die Lastverteilung oder Volumes ausgewählt werden, die nicht Ziel einer SnapMirror oder SnapVault Beziehung sind.

Schritte

1. Suchen Sie auf der Seite **Schutz** der **Gesundheit/Volumen**-Details in der Topologie die Schutzbeziehung, die Sie bearbeiten möchten, und klicken Sie mit der rechten Maustaste darauf.
2. Wählen Sie im Menü * Bearbeiten* aus.

   Alternativ können Sie im Menü **Aktionen** die Option **Beziehung** > **Bearbeiten** wählen, um die Beziehung zu bearbeiten, für die Sie die Details anzeigen.

   Das Dialogfeld Beziehung bearbeiten wird angezeigt.

3. Bearbeiten Sie im Dialogfeld „Beziehungen bearbeiten*“ die maximale Übertragungsrate, die Schutzrichtlinie oder den Schutzzeitplan nach Bedarf.
4. Klicken Sie Auf **Anwenden**.

   Die Änderungen werden auf die ausgewählten Beziehungen angewendet.

Erstellen einer SnapMirror-Richtlinie zur Maximierung der Übertragungseffizienz

Sie können eine SnapMirror-Richtlinie erstellen, um die SnapMirror Übertragungspriorität für Sicherungsbeziehungen festzulegen. Mithilfe der SnapMirror Richtlinien lässt sich die Übertragungseffizienz von der Quelle zum Ziel maximieren, indem Prioritäten zugewiesen werden, sodass Transfers mit niedriger Priorität nach Transfers mit normaler Priorität

geplant werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.
- Bei dieser Aufgabe wird davon ausgegangen, dass Sie den Bereich Zielinformationen im Dialogfeld Schutz konfigurieren bereits abgeschlossen haben.

Schritte

1. Klicken Sie im Dialogfeld **Schutz konfigurieren** auf der Registerkarte **SnapMirror** im Bereich **Beziehungseinstellungen** auf den Link **Richtlinien erstellen**.

   Das Dialogfeld SnapMirror-Richtlinie erstellen wird angezeigt.

2. Geben Sie im Feld **Policy Name** einen Namen ein, den Sie der Richtlinie geben möchten.
3. Wählen Sie im Feld * Priorität übertragen* die Übertragungspriorität aus, die Sie der Richtlinie zuweisen möchten.
4. Geben Sie im Feld **Kommentar** einen optionalen Kommentar für die Richtlinie ein.
5. Klicken Sie Auf **Erstellen**.

   Die neue Richtlinie wird in der Dropdown-Liste SnapMirror-Richtlinie angezeigt.

Erstellen einer SnapVault-Richtlinie zur Maximierung der Übertragungseffizienz

Sie können eine neue SnapVault-Richtlinie erstellen, um die Priorität für eine SnapVault-Übertragung festzulegen. Anhand von Richtlinien wird die Effizienz der Übertragungen in einer Sicherungsbeziehung vom primären zum sekundären Volume maximiert.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.
- Sie müssen bereits den Bereich Zielinformationen im Dialogfeld Schutz konfigurieren ausgefüllt haben.

Schritte

1. Klicken Sie im Dialogfeld **Schutz konfigurieren** auf der Registerkarte **SnapVault** im Bereich **Beziehungseinstellungen** auf den Link **Richtlinien erstellen**.

   Die Registerkarte SnapVault wird angezeigt.

2. Geben Sie im Feld **Policy Name** den Namen ein, den Sie der Richtlinie geben möchten.
3. Wählen Sie im Feld **Priorität übertragen** die Übertragungspriorität aus, die Sie der Richtlinie zuweisen möchten.
4. Geben Sie im Feld **Kommentar** einen Kommentar für die Richtlinie ein.
5. Fügen Sie im Bereich **Replication Label** eine Replikationbeschriftung bei Bedarf hinzu oder bearbeiten Sie sie.

6. Klicken Sie Auf **Erstellen**.

   Die neue Richtlinie wird in der Dropdown-Liste Richtlinie erstellen angezeigt.

Aktive Datensicherungstransfers wird auf der Seite „Protection/Volume Relationships“ abgebrochen

Sie können eine aktive Datensicherung abbrechen, wenn Sie eine SnapMirror Replikation anhalten möchten, die gerade ausgeführt wird. Sie können auch den Checkpoint beim Neustart für Transfers nach dem Basistransfer löschen. Sie können eine Übertragung abbrechen, wenn sie mit einem anderen Vorgang, z. B. einer Volume-Verschiebung, kollidieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Über diese Aufgabe

Die Abbruchaktion wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
- Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung besteht und der Ziel-Cluster noch nicht erkannt wurde

Sie können den Kontrollpunkt für den Neustart für einen Basistransfer nicht löschen.

Schritte

1. Um Übertragungen für eine oder mehrere Schutzbeziehungen abzubrechen, wählen Sie auf der Seite **Schutz/Volume-Beziehungen** ein oder mehrere Volumes aus und klicken Sie in der Symbolleiste auf **Abbrechen**.

   Das Dialogfeld Übertragung abbrechen wird angezeigt.

2. Wenn Sie den Kontrollpunkt für den Neustart für einen Transfer löschen möchten, der kein Basistransfer ist, wählen Sie **Checkpoints löschen** aus.
3. Klicken Sie Auf **Weiter**.

   Das Dialogfeld Übertragung abbrechen wird geschlossen, und der Status des Jobs abbrechen wird oben auf der Seite Schutz-/Volume-Beziehungen angezeigt, zusammen mit einem Link zu den Jobdetails.

4. Klicken Sie auf den Link **Details anzeigen**, um weitere Details zur Seite **Schutz/Job** anzuzeigen und den Job-Fortschritt anzuzeigen.

Die aktive Datensicherung wird von der Seite „Gesundheits-/Volume-Details“ abgebrochen

Sie können eine aktive Datensicherung abbrechen, wenn Sie eine SnapMirror Replikation

anhalten möchten, die gerade ausgeführt wird. Sie können auch den Checkpoint für den Neustart eines Transfers löschen, wenn es sich nicht um einen Basistransfer handelt. Sie können eine Übertragung abbrechen, wenn sie mit einem anderen Vorgang, z. B. einer Volume-Verschiebung, kollidieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Über diese Aufgabe

Die Abbruchaktion wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
- Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung besteht und der Ziel-Cluster noch nicht erkannt wurde

Sie können den Kontrollpunkt für den Neustart für einen Basistransfer nicht löschen.

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Gesundheit/Volumen** mit der rechten Maustaste auf die Beziehung in der Topologieansicht für die Datenübertragung, die Sie abbrechen möchten, und wählen Sie **Abbrechen** aus.

   Das Dialogfeld Übertragung abbrechen wird angezeigt.

2. Wenn Sie den Kontrollpunkt für den Neustart für einen Transfer löschen möchten, der kein Basistransfer ist, wählen Sie **Checkpoints löschen** aus.
3. Klicken Sie Auf **Weiter**.

   Das Dialogfeld Übertragung abbrechen wird geschlossen, und der Status des Abbruchvorgangs wird oben auf der Seite Health/Volume Details sowie ein Link zu den Jobdetails angezeigt.

4. Klicken Sie auf den Link **Details anzeigen**, um weitere Details zur Seite **Schutz/Job** anzuzeigen und den Job-Fortschritt anzuzeigen.
5. Klicken Sie auf jeden Job, um seine Details anzuzeigen.
6. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Detailseite **Gesundheit/Volumen** zurückzukehren.

   Der Abbruchvorgang ist abgeschlossen, wenn alle Aufgabenstellungen erfolgreich abgeschlossen wurden.

Eine Schutzbeziehung wird auf der Seite „Schutz/Volume-Beziehungen“ stillgelegt

Auf der Seite „Schutz/Volume-Beziehungen“ können Sie eine Schutzbeziehung stilllegen, um vorübergehend Datenübertragungen zu verhindern. Sie könnten eine Beziehung stilllegen, wenn Sie eine Snapshot Kopie eines SnapMirror Ziel-Volumes erstellen möchten, das eine Datenbank enthält, und Sie wollen sicherstellen, dass der Inhalt

während des Snapshot Kopiervorgangs stabil ist.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Über diese Aufgabe

Die Aktion quiesce wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
- Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung vorhanden ist und der Ziel-Cluster noch nicht erkannt wurde
- Wenn Workflow Automation und Unified Manager noch nicht in Kombination Paar liegen

Schritte

1. Um Transfers für eine oder mehrere Schutzbeziehungen stillzulegen, wählen Sie auf der Seite **Schutz/Volume-Beziehungen** ein oder mehrere Volumes aus und klicken Sie in der Symbolleiste auf **Quiesce**.

   Das Dialogfeld Quiesce wird angezeigt.

2. Klicken Sie Auf **Weiter**.

   Der Status des Jobs quiesce wird oben auf der Seite Health/Volume Details angezeigt, zusammen mit einem Link zu den Jobdetails.

3. Klicken Sie auf den Link **Details anzeigen**, um zur Detailseite **Schutz/Job** weitere Details und den Job-Fortschritt aufzurufen.
4. Klicken Sie auf den Pfeil **Zurück** in Ihrem Browser, um zur Seite **Schutz/Volume-Beziehungen** zurückzukehren.

   Der quiesce-Job ist abgeschlossen, wenn alle Arbeitsaufgaben erfolgreich abgeschlossen wurden.

Eine Schutzbeziehung wird auf der Seite „Health/Volume Details“ stillgelegt

Sie können eine Schutzbeziehung stilllegen, um einen vorübergehenden Ausfall von Datentransfers zu verhindern. Sie könnten eine Beziehung stilllegen, wenn Sie eine Snapshot Kopie eines SnapMirror Ziel-Volumes erstellen möchten, das eine Datenbank enthält, und Sie wollen sicherstellen, dass der Inhalt während der Snapshot Kopie stabil ist.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Über diese Aufgabe

Die Aktion quiesce wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
- Wenn die Volume-ID unbekannt ist, z. B. wenn Sie über eine Cluster-übergreifende Beziehung verfügen und das Ziel-Cluster noch nicht erkannt wurde
- Wenn Workflow Automation und Unified Manager noch nicht in Kombination Paar liegen

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Gesundheit/Volumen** mit der rechten Maustaste auf die Beziehung in der Topologieansicht für die Schutzbeziehung, die Sie stilllegen möchten.
2. Wählen Sie im Menü * Quiesce* aus.
3. Klicken Sie auf **Ja**, um fortzufahren.

   Der Status des Jobs quiesce wird oben auf der Seite Health/Volume Details angezeigt, zusammen mit einem Link zu den Jobdetails.

4. Klicken Sie auf den Link **Details anzeigen**, um zur Detailseite **Schutz/Job** weitere Details und den Job-Fortschritt aufzurufen.
5. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Detailseite **Gesundheit/Volumen** zurückzukehren.

   Der quiesce-Job ist abgeschlossen, wenn alle Arbeitsaufgaben erfolgreich abgeschlossen wurden.

Brechen einer SnapMirror Beziehung von der Seite „Schutz/Volume-Beziehungen“

Sie können eine Sicherungsbeziehung unterbrechen, um die Datenübertragung zwischen einem Quell-Volume und einem Ziel-Volume in einer SnapMirror Beziehung zu unterbrechen. Wenn Sie Daten migrieren, für Disaster Recovery-Zwecke oder zum Testen von Applikationen nutzen möchten, können Sie eine Beziehung unterbrechen. Das Zielvolume wird auf ein Lese-/Schreib-Volume geändert. Man kann keine SnapVault Beziehung durchbrechen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Seite **Schutz/Volume Relationships** ein oder mehrere Volumes mit Schutzbeziehungen aus, für die Sie die Datenübertragung beenden möchten und klicken Sie in der Symbolleiste auf **break**.

   Das Dialogfeld Beziehung unterbrechen wird angezeigt.

2. Klicken Sie auf **Weiter**, um die Beziehung zu brechen.

3. Überprüfen Sie auf der Seite **Schutz/Volume Relationships** in der Spalte **Relationship State**, ob die Beziehung unterbrochen ist.

   Die Spalte „Beziehungsstatus“ ist standardmäßig ausgeblendet, sodass Sie sie in der Spaltenliste „ein-/ausblenden“ auswählen müssen .

Die SnapMirror-Beziehung von der Seite „Systemzustand/Volume-Details“ abbricht

Sie können eine Sicherungsbeziehung auf der Seite Systemzustand/Volume-Details unterbrechen und die Datentransfers zwischen einem Quell- und Ziel-Volume in einer SnapMirror Beziehung stoppen. Wenn Sie Daten migrieren, für Disaster Recovery-Zwecke oder zum Testen von Applikationen nutzen möchten, können Sie eine Beziehung unterbrechen. Das Zielvolume wird in ein Lese- und Schreib-Volume geändert. Man kann keine SnapVault Beziehung durchbrechen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Registerkarte **Schutz** der Seite **Gesundheit/Volume** Details aus der Topologie die SnapMirror Beziehung aus, die Sie brechen möchten.
2. Klicken Sie mit der rechten Maustaste auf das Ziel und wählen Sie im Menü die Option **Pause** aus.

   Das Dialogfeld Beziehung unterbrechen wird angezeigt.

3. Klicken Sie auf **Weiter**, um die Beziehung zu brechen.
4. Stellen Sie in der Topologie sicher, dass die Beziehung unterbrochen ist.

Entfernen einer Schutzbeziehung von der Seite „Schutz/Volume-Beziehungen“

Auf der Seite „Schutz/Volume-Beziehungen“ können Sie eine Schutzbeziehung entfernen, um eine bestehende Beziehung zwischen der ausgewählten Quelle und dem ausgewählten Ziel dauerhaft zu löschen: Zum Beispiel, wenn Sie eine Beziehung unter Verwendung eines anderen Ziels erstellen möchten. Durch diesen Vorgang werden alle Metadaten entfernt und können nicht rückgängig gemacht werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Seite **Schutz/Volume-Beziehungen** ein oder mehrere Volumes mit Schutzbeziehungen aus, die Sie entfernen möchten, und klicken Sie in der Symbolleiste auf **Entfernen**.

Das Dialogfeld Beziehung entfernen wird angezeigt.

2. Klicken Sie auf **Weiter**, um die Beziehung zu entfernen.

   Die Beziehung wird von der Seite „Schutz/Volume-Beziehungen“ entfernt.

Entfernen einer Schutzbeziehung von der Seite „Gesundheits-/Volume-Details“

Sie können eine Schutzbeziehung entfernen, um eine vorhandene Beziehung zwischen der ausgewählten Quelle und dem ausgewählten Ziel dauerhaft zu löschen, z. B. wenn Sie eine Beziehung unter Verwendung eines anderen Ziels erstellen möchten. Durch diesen Vorgang werden alle Metadaten entfernt und können nicht rückgängig gemacht werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Registerkarte **Protection** der Seite **Health/Volume** Details aus der Topologie die SnapMirror Beziehung aus, die Sie entfernen möchten.
2. Klicken Sie mit der rechten Maustaste auf den Namen des Ziels und wählen Sie im Menü die Option **Entfernen**.

   Das Dialogfeld Beziehung entfernen wird angezeigt.

3. Klicken Sie auf **Weiter**, um die Beziehung zu entfernen.

   Die Beziehung wird von der Seite „Health/Volume Details“ entfernt.

Wiederaufnahme geplanter Transfers für eine stillgelegte Beziehung auf der Seite „Schutz/Volume-Beziehungen“

Nachdem Sie eine Beziehung stillgelegt haben, um geplante Transfers zu stoppen, können Sie **Resume** verwenden, um geplante Transfers erneut zu aktivieren, damit Daten auf dem Quell- oder Primärvolume geschützt sind. Transfers werden im nächsten geplanten Transferintervall von einem Kontrollpunkt fortgesetzt, falls vorhanden.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Über diese Aufgabe

Sie können maximal 10 stillgelegene Beziehungen auswählen, auf denen die Übertragung fortgesetzt werden soll.

Schritte

1. Wählen Sie auf der Seite **Schutz/Volume-Beziehungen** ein oder mehrere Volumes mit stillgelegten Beziehungen aus, und klicken Sie in der Symbolleiste auf **Wiederaufnehmen**.
2. Klicken Sie im Dialogfeld **Fortsetzen** auf **Weiter**.

   Sie gelangen wieder zur Seite „Schutz/Volume-Beziehungen“.

3. Um die zugehörigen Aufgaben anzuzeigen und deren Fortschritt zu verfolgen, klicken Sie auf den Job-Link, der oben auf der Seite **Schutz/Volume-Beziehungen** angezeigt wird.
4. Führen Sie einen der folgenden Schritte aus:
   - Wenn nur ein Job angezeigt wird, klicken Sie auf der Seite Schutz-/Jobdetails auf **Aktualisieren**, um die Aufgabenliste und die mit dem Konfigurationsauftrag verbundenen Aufgabendetails zu aktualisieren und zu bestimmen, wann der Job abgeschlossen ist.
   - Wenn mehrere Jobs angezeigt werden,
     i. Klicken Sie auf der Seite Schutz/Jobs auf den Job, für den Sie die Details anzeigen möchten.
     ii. Klicken Sie auf der Seite Schutz-/Jobdetails auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist. Nach Abschluss der Jobs werden die Datenübertragungen im nächsten geplanten Übertragungsintervall fortgesetzt.

Wiederaufnahme geplanter Transfers für eine stillgelegte Beziehung von der Seite „Systemzustand/Volume-Details“ aus

Nachdem Sie eine Beziehung stillgelegt haben, um geplante Transfers zu stoppen, können Sie **Resume** auf der Seite Health/Volume Details verwenden, um geplante Transfers erneut zu aktivieren, so dass Daten auf dem Quell- oder Primärvolume geschützt sind. Transfers werden im nächsten geplanten Transferintervall von einem Kontrollpunkt fortgesetzt, falls vorhanden.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Gesundheit/Volumen** mit der rechten Maustaste in die Topologieansicht auf eine stillgelegene Beziehung, die Sie fortsetzen möchten.

   Alternativ können Sie im Menü **Aktionen** > **Beziehung Fortsetzen** die Option **Fortsetzen** wählen.

2. Klicken Sie im Dialogfeld **Fortsetzen** auf **Weiter**.

   Sie gelangen zurück zur Seite „Health/Volume Details“.

3. Um die zugehörigen Aufgaben anzuzeigen und deren Fortschritt zu verfolgen, klicken Sie auf den Job-Link, der oben auf der Seite **Health/Volume** Details angezeigt wird.
4. Klicken Sie auf der Seite **Schutz/Job** Details auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um

festzustellen, wann der Job abgeschlossen ist.

Nach Abschluss der Jobs werden die Datenübertragungen im nächsten geplanten Übertragungsintervall fortgesetzt.

Schutzbeziehungen werden auf der Seite „Schutz/Volume-Beziehungen“ initialisiert oder aktualisiert

Auf der Seite „Schutz/Volume-Beziehungen“ können Sie eine erste Basistransfer für eine neue Schutzbeziehung durchführen oder eine Beziehung aktualisieren, wenn sie bereits initialisiert ist und Sie eine manuelle, außerplanmäßige inkrementelle Aktualisierung durchführen möchten, um sie sofort zu übertragen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Klicken Sie auf der Seite **Schutz/Volume Relationships** mit der rechten Maustaste auf ein Volume und wählen Sie ein oder mehrere Volumes mit Beziehungen aus, die Sie aktualisieren oder initialisieren möchten, und klicken Sie dann in der Symbolleiste auf **Initialisieren/Aktualisieren**.

   Das Dialogfeld Initialisieren/Aktualisieren wird angezeigt.

2. Wählen Sie auf der Registerkarte **Übertragungsoptionen** eine Übertragungspriorität und die maximale Übertragungsrate aus.
3. Klicken Sie auf **Quelle Snapshot Kopien** und dann in der Spalte **Snapshot Kopie** auf **Standard**.

   Das Dialogfeld Quell-Snapshot-Kopie auswählen wird angezeigt.

4. Wenn Sie eine vorhandene Snapshot Kopie angeben möchten, anstatt die Standard-Snapshot Kopie zu übertragen, klicken Sie auf **vorhandene Snapshot Kopie** und wählen Sie eine Snapshot Kopie aus der Liste aus.
5. Klicken Sie Auf **Absenden**.

   Sie gelangen wieder zum Dialogfeld Initialisieren/Aktualisieren.

6. Wenn Sie mehr als eine Quelle zum Initialisieren oder Aktualisieren ausgewählt haben, klicken Sie auf **Standard** für die nächste Quelle, für die Sie eine vorhandene Snapshot Kopie angeben möchten.
7. Klicken Sie auf **Senden**, um die Initialisierung oder Aktualisierung des Jobs zu starten.

   Der Initialisierungs- oder Aktualisierungsauftrag wird gestartet, Sie gelangen wieder zur Seite Beziehungen zu Schutz/Volume und oben auf der Seite wird ein Link Jobs angezeigt.

8. Klicken Sie auf der Seite **Health/Volumes** Inventory auf **Jobs anzeigen**, um den Status jedes Initialisierungs- oder Aktualisierungs-Jobs zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.

9. Klicken Sie auf die einzelnen Jobs, um die entsprechenden Details anzuzeigen.
10. Klicken Sie auf den Pfeil **Zurück** in Ihrem Browser, um zur Seite **Schutz/Volume-Beziehungen** zurückzukehren.

    Der Initialisierungs- oder Aktualisierungsvorgang ist abgeschlossen, wenn alle Aufgaben erfolgreich abgeschlossen wurden.

Initialisierung oder Aktualisierung von Schutzbeziehungen auf der Seite „Health/Volume Details“

Sie können eine erste Basistransfer für eine neue Schutzbeziehung durchführen oder eine Beziehung aktualisieren, wenn sie bereits initialisiert ist und Sie eine manuelle, außerplanmäßige inkrementelle Aktualisierung durchführen möchten, um Daten sofort zu übertragen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Suchen Sie auf der Registerkarte **Schutz** der Seite **Gesundheit/Volumen** Details in der Topologie die Schutzbeziehung, die Sie initialisieren oder aktualisieren möchten, und klicken Sie dann mit der rechten Maustaste darauf.
2. Wählen Sie im Menü die Option **Initialisieren/aktualisieren**.

   Alternativ können Sie im Menü **Aktionen** die Option **Beziehung** > **Initialisieren/Aktualisieren** wählen, um die Beziehung zu initialisieren oder zu aktualisieren, für die Sie die Details anzeigen.

   Das Dialogfeld Initialisieren/Aktualisieren wird angezeigt.

3. Wählen Sie auf der Registerkarte **Übertragungsoptionen** eine Übertragungspriorität und die maximale Übertragungsrate aus.
4. Klicken Sie auf **Quelle Snapshot Kopien** und dann in der Spalte **Snapshot Kopie** auf **Standard**.

   Das Dialogfeld Quell-Snapshot-Kopie auswählen wird angezeigt.

5. Wenn Sie eine vorhandene Snapshot Kopie angeben möchten, anstatt die Standard-Snapshot Kopie zu übertragen, klicken Sie auf **vorhandene Snapshot Kopie** und wählen Sie eine Snapshot Kopie aus der Liste aus.
6. Klicken Sie Auf **Absenden**.

   Sie gelangen wieder zum Dialogfeld Initialisieren/Aktualisieren.

7. Wenn Sie mehr als eine Quelle zum Initialisieren oder Aktualisieren ausgewählt haben, klicken Sie auf **Standard** für die nächste Lese-/Schreibquelle, für die Sie eine vorhandene Snapshot Kopie angeben möchten.

   Sie können keine andere Snapshot Kopie für Volumes für die Datensicherung auswählen.

8. Klicken Sie auf **Senden**, um die Initialisierung oder Aktualisierung des Jobs zu starten.

   Der Initialisierungs- oder Aktualisierungsauftrag wird gestartet, Sie gelangen wieder zur Seite Health/Volume Details und oben auf der Seite wird ein Link Jobs angezeigt.

9. Klicken Sie auf der Seite **Health/Volume** Details auf **Jobs anzeigen**, um den Status jedes Initialisierungs- oder Aktualisierungs-Jobs zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.

10. Klicken Sie auf die einzelnen Jobs, um die entsprechenden Details anzuzeigen.
11. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Detailseite **Gesundheit/Volumen** zurückzukehren.

    Der Initialisierungs- oder Aktualisierungsvorgang ist abgeschlossen, wenn alle Aufgabenstellungen erfolgreich abgeschlossen wurden.

Erneutes Synchronisieren von Schutzbeziehungen auf der Seite „Schutz/Volume-Beziehungen“

Auf der Seite „Schutz/Volume-Beziehungen“ können Sie eine Beziehung neu synchronisieren, um sie von einem Ereignis wiederherzustellen, bei dem das Quell-Volume deaktiviert wurde, oder wenn Sie die aktuelle Quelle auf ein anderes Volume ändern möchten.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Seite **Schutz/Volume Relationships** ein oder mehrere Volumes mit stillgelegten Beziehungen aus und klicken Sie in der Symbolleiste auf **resynchronisieren**.

   Das Dialogfeld „Resynchronisieren“ wird angezeigt.

2. Wählen Sie auf der Registerkarte **Resynchronisierung Optionen** eine Übertragungs-Priorität und die maximale Übertragungsrate aus.
3. Klicken Sie auf **Quelle Snapshot Kopien** und dann in der Spalte **Snapshot Kopie** auf **Standard**.

   Das Dialogfeld Quell-Snapshot-Kopie auswählen wird angezeigt.

4. Wenn Sie eine vorhandene Snapshot Kopie angeben möchten, anstatt die Standard-Snapshot Kopie zu übertragen, klicken Sie auf **vorhandene Snapshot Kopie** und wählen Sie eine Snapshot Kopie aus der Liste aus.
5. Klicken Sie Auf **Absenden**.

   Sie werden wieder zum Dialogfeld „erneut synchronisieren“ angezeigt.

6. Wenn Sie mehrere Quellen zum erneuten Synchronisieren ausgewählt haben, klicken Sie für die nächste Quelle, für die Sie eine vorhandene Snapshot Kopie angeben möchten, auf **Standard**.

7. Klicken Sie auf **Senden**, um die Neusynchronisierung zu beginnen.

   Der Resynchronisierung-Job wird gestartet, Sie werden auf die Seite Beziehungen zu Schutz/Volumes zurückgegeben und oben auf der Seite wird ein Link zu Jobs angezeigt.

8. Klicken Sie auf der Seite **Schutz/Volume-Beziehungen** auf **Jobs anzeigen**, um den Status der einzelnen Neusynchronisierung zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.

9. Klicken Sie auf den Pfeil **Zurück** in Ihrem Browser, um zur Seite **Schutz/Volume-Beziehungen** zurückzukehren.

   Die Neusynchronisierung ist nach erfolgreichem Abschluss aller Aufgabenstellungen abgeschlossen.

Erneutes Synchronisieren von Schutzbeziehungen auf der Seite „Systemzustand/Volume-Details“

Sie können Daten auf einer SnapMirror oder SnapVault-Beziehung neu synchronisieren, die unterbrochen wurde, und dann wurde das Ziel gelesen/geschrieben, sodass die Daten auf der Quelle mit den Daten auf dem Ziel übereinstimmen. Sie können auch neu synchronisieren, wenn eine erforderliche gemeinsame Snapshot Kopie auf dem Quell-Volume gelöscht wird, sodass SnapMirror oder SnapVault Updates fehlschlagen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Suchen Sie auf der Registerkarte **Schutz** der Detailseite **Gesundheit/Volumen** in der Topologie die Schutzbeziehung, die Sie neu synchronisieren möchten, und klicken Sie mit der rechten Maustaste darauf.
2. Wählen Sie im Menü * resynchronisieren* aus.

   Alternativ können Sie im Menü **Aktionen** die Option **Beziehung** > **Resynchronisieren** wählen, um die Beziehung, für die Sie die Details anzeigen, neu zu synchronisieren.

   Das Dialogfeld „Resynchronisieren“ wird angezeigt.

3. Wählen Sie auf der Registerkarte **Resynchronisierung Optionen** eine Übertragungs-Priorität und die maximale Übertragungsrate aus.
4. Klicken Sie auf **Quelle Snapshot Kopien** und dann in der Spalte **Snapshot Kopie** auf **Standard**.

   Das Dialogfeld Quell-Snapshot-Kopie auswählen wird angezeigt.

5. Wenn Sie eine vorhandene Snapshot Kopie angeben möchten, anstatt die Standard-Snapshot Kopie zu übertragen, klicken Sie auf **vorhandene Snapshot Kopie** und wählen Sie eine Snapshot Kopie aus der Liste aus.
6. Klicken Sie Auf **Absenden**.

Sie werden wieder zum Dialogfeld „erneut synchronisieren“ angezeigt.

7. Wenn Sie mehrere Quellen zum erneuten Synchronisieren ausgewählt haben, klicken Sie für die nächste Quelle, für die Sie eine vorhandene Snapshot Kopie angeben möchten, auf **Standard**.
8. Klicken Sie auf **Senden**, um die Neusynchronisierung zu beginnen.

   Der Resynchronisierung-Job wurde gestartet, Sie werden wieder zur Seite „Details zu Funktionszustand/Volumen“ und oben auf der Seite wird ein Link zu Jobs angezeigt.

9. Klicken Sie auf der Seite **Health/Volume** Details auf **Jobs anzeigen**, um den Status der einzelnen Neusynchronisierung zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.

10. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Detailseite **Gesundheit/Volumen** zurückzukehren.

    Die Neusynchronisierung ist abgeschlossen, nachdem alle Aufgabenstellungen erfolgreich abgeschlossen wurden.

Umkehrung von Schutzbeziehungen auf der Seite „Schutz/Volume-Beziehungen“

Wenn ein Notfall das Quellvolume in Ihrer Schutzbeziehung deaktiviert, können Sie das Zielvolume für die Bereitstellung von Daten verwenden, indem Sie es in ein Lese-/Schreibvolume konvertieren, während Sie die Quelle reparieren oder ersetzen. Wenn die Quelle für den Empfang von Daten erneut verfügbar ist, können Sie mithilfe der Resynchronisierung auf umgekehrter Richtung die Beziehung herstellen und die Daten auf der Quelle mit den Daten auf dem Ziel für Lesen/Schreiben synchronisieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.
- Die Beziehung darf keine SnapVault Beziehung sein.
- Eine Schutzbeziehung muss bereits vorhanden sein.
- Die Schutzbeziehung muss gebrochen werden.
- Sowohl die Quelle als auch das Ziel müssen online sein.
- Die Quelle darf nicht Ziel eines anderen Datensicherungs-Volumes sein.

Über diese Aufgabe

- Wenn Sie diese Aufgabe ausführen, werden Daten in der Quelle, die neuer als die Daten in der gemeinsamen Snapshot Kopie ist, gelöscht.
- Bei der erneuten Synchronisierung erstellte Richtlinien und Zeitpläne sind dieselben wie in der ursprünglichen Sicherungsbeziehung.

  Wenn Richtlinien und Zeitpläne nicht vorhanden sind, werden sie erstellt.

Schritte

1. Wählen Sie auf der Seite **Schutz/Volume Relationships** ein oder mehrere Volumes mit Beziehungen aus, die Sie umkehren möchten, und klicken Sie in der Symbolleiste auf **Resync umkehren**.

   Das Dialogfeld Resync umkehren wird angezeigt.

2. Stellen Sie sicher, dass die Beziehungen im Dialogfeld **Resync** umkehren angezeigt werden, für die Sie die Neusynchronisierung rückgängig machen möchten, und klicken Sie dann auf **Senden**.

   Die umgekehrte Resynchronisierung wird gestartet, Sie gelangen wieder zur Seite Beziehungen zu Schutz/Volume und oben auf der Seite wird ein Link zu Jobs angezeigt.

3. Klicken Sie auf der Seite **Schutz/Volume-Beziehungen** auf **Jobs anzeigen**, um den Status jedes umgekehrten Neusynchronisierung zu verfolgen.

   Eine gefilterte Liste der Jobs, die mit diesem Vorgang in Verbindung stehen, wird angezeigt.

4. Klicken Sie auf den Pfeil **Zurück** in Ihrem Browser, um zur Seite **Schutz/Volume-Beziehungen** zurückzukehren.

   Nach erfolgreichem Abschluss aller Jobaufgaben ist die Neusynchronisierung bei umgekehrter Neusynchronisierung abgeschlossen.

Rückkehrung von Schutzbeziehungen auf der Seite „Gesundheits-/Volume-Details“

Wenn ein Notfall das Quellvolume in Ihrer Schutzbeziehung deaktiviert, können Sie das Zielvolume für die Bereitstellung von Daten verwenden, indem Sie es in Lese-/Schreibzugriff konvertieren, während Sie die Quelle reparieren oder ersetzen. Wenn die Quelle für den Empfang von Daten erneut verfügbar ist, können Sie mithilfe der Resynchronisierung auf umgekehrter Richtung die Beziehung herstellen und die Daten auf der Quelle mit den Daten auf dem Ziel für Lesen/Schreiben synchronisieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.
- Die Beziehung darf keine SnapVault Beziehung sein.
- Eine Schutzbeziehung muss bereits vorhanden sein.
- Die Schutzbeziehung muss gebrochen werden.
- Sowohl die Quelle als auch das Ziel müssen online sein.
- Die Quelle darf nicht Ziel eines anderen Datensicherungs-Volumes sein.

Über diese Aufgabe

- Wenn Sie diese Aufgabe ausführen, werden Daten in der Quelle, die neuer als die Daten in der gemeinsamen Snapshot Kopie ist, gelöscht.
- Die für die umgekehrte Resynchronisierung erstellten Richtlinien und Zeitpläne sind mit denen in der ursprünglichen Schutzbeziehung identisch.

Wenn Richtlinien und Zeitpläne nicht vorhanden sind, werden sie erstellt.

Schritte

1. Suchen Sie auf der **Schutz**-Registerkarte der **Gesundheit/Volumen**-Detailseite in der Topologie die SnapMirror-Beziehung, auf der Sie Quelle und Ziel umkehren möchten, und klicken Sie mit der rechten Maustaste darauf.
2. Wählen Sie aus dem Menü die Option **Resync rückwärts**.

   Das Dialogfeld Resync umkehren wird angezeigt.

3. Stellen Sie sicher, dass die Beziehung, die im Dialogfeld **Resync** umkehren angezeigt wird, die Beziehung ist, für die Sie die Neusynchronisierung rückgängig machen möchten, und klicken Sie dann auf **Absenden**.

   Das Dialogfeld „Resync umkehren“ wird geschlossen und oben auf der Seite „Health/Volume Details“ wird ein Job-Link angezeigt.

4. Klicken Sie auf der Seite **Health/Volume** Details auf **Jobs anzeigen**, um den Status jedes umgekehrten Neusynchronisierung zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.

5. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Detailseite **Gesundheit/Volumen** zurückzukehren.

   Nach erfolgreichem Abschluss aller Jobaufgaben ist die Neusynchronisierung bei umgekehrter Neusynchronisierung abgeschlossen.

Wiederherstellen von Daten mithilfe der Seite „Health/Volumes Inventory“

Sie können überschreibende oder gelöschte Dateien, Verzeichnisse oder ein gesamtes Volume anhand einer Snapshot Kopie wiederherstellen. Dazu verwenden Sie die Wiederherstellungsfunktion auf der Seite „Systemzustand“/„Volumes-Inventar“.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

NTFS-Dateiströme können nicht wiederhergestellt werden.

Die Wiederherstellungsoption ist nicht verfügbar, wenn:

- Die Volume-ID ist unbekannt, z. B. wenn Sie eine Intercluster-Beziehung haben und der Ziel-Cluster noch nicht erkannt wurde.
- Das Volume ist ein FlexGroup Volume.
- Das Volume ist für die synchrone SnapMirror Replizierung konfiguriert.

Schritte

1. Wählen Sie auf der Seite **Health/Volumes** Inventory ein Volume aus, aus dem Sie Daten wiederherstellen möchten.
2. Klicken Sie in der Symbolleiste auf **Wiederherstellen**.

   Das Dialogfeld Wiederherstellen wird angezeigt.

3. Wählen Sie das Volume und die Snapshot Kopie aus, von dem Sie Daten wiederherstellen möchten, falls sie sich von dem Standard unterscheiden.
4. Wählen Sie die Elemente aus, die Sie wiederherstellen möchten.

   Sie können das gesamte Volume wiederherstellen oder Ordner und Dateien angeben, die wiederhergestellt werden sollen.

5. Wählen Sie den Speicherort aus, an dem die ausgewählten Elemente wiederhergestellt werden sollen; entweder **Originalstandort** oder **alternativer Standort**.
6. Klicken Sie Auf **Wiederherstellen**.

   Der Wiederherstellungsprozess beginnt.

Wiederherstellen von Daten über die Seite „Health/Volume Details“

Sie können überschreibte oder gelöschte Dateien, Verzeichnisse oder ein gesamtes Volume anhand einer Snapshot Kopie wiederherstellen. Dazu verwenden Sie die Wiederherstellungsfunktion auf der Seite „Systemzustand“/„Volume-Details“.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

NTFS-Dateiströme können nicht wiederhergestellt werden.

Die Wiederherstellungsoption ist nicht verfügbar, wenn:

- Die Volume-ID ist unbekannt, z. B. wenn Sie eine Intercluster-Beziehung haben und der Ziel-Cluster noch nicht erkannt wurde.
- Das Volume ist ein FlexGroup Volume.
- Das Volume ist für die synchrone SnapMirror Replizierung konfiguriert.

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Gesundheit/Volumen** mit der rechten Maustaste in die Topologieansicht auf den Namen des Volumes, das wiederhergestellt werden soll.
2. Wählen Sie im Menü * Wiederherstellen* aus.

   Alternativ können Sie im Menü **Aktionen Restore** die aktuelle Lautstärke, für die Sie die Details anzeigen, schützen.

Das Dialogfeld Wiederherstellen wird angezeigt.

3. Wählen Sie das Volume und die Snapshot Kopie aus, von dem Sie Daten wiederherstellen möchten, falls sie sich von dem Standard unterscheiden.
4. Wählen Sie die Elemente aus, die Sie wiederherstellen möchten.

   Sie können das gesamte Volume wiederherstellen oder Ordner und Dateien angeben, die wiederhergestellt werden sollen.

5. Wählen Sie den Speicherort aus, an dem die ausgewählten Elemente wiederhergestellt werden sollen: Entweder **Originalstandort** oder **alternativer bestehender Standort**.
6. Wenn Sie einen alternativen vorhandenen Standort auswählen, führen Sie einen der folgenden Schritte aus:
   - Geben Sie im Textfeld Pfad wiederherstellen den Pfad des Speicherorts ein, zu dem die Daten wiederhergestellt werden sollen, und klicken Sie dann auf **Verzeichnis auswählen**.
   - Klicken Sie auf **Durchsuchen**, um das Dialogfeld Verzeichnisse durchsuchen zu starten und führen Sie die folgenden Schritte aus:
     i. Wählen Sie das Cluster, die SVM und das Volume aus, das Sie wiederherstellen möchten.
     ii. Wählen Sie in der Tabelle Name einen Verzeichnisnamen aus.
     iii. Klicken Sie Auf **Verzeichnis Auswählen**.
7. Klicken Sie Auf **Wiederherstellen**.

   Der Wiederherstellungsprozess beginnt.

> Wenn eine Wiederherstellung zwischen Cloud Volumes ONTAP HA Clustern mit einem NDMP-Fehler fehlschlägt, müssen Sie möglicherweise eine explizite AWS Route im Ziel-Cluster hinzufügen, damit das Ziel mit der Cluster-Management-LIF des Quellsystems kommunizieren kann. Sie führen diesen Konfigurationsschritt mithilfe von OnCommand Cloud Manager aus.

Erstellen von Ressourcenpools

Sie können das Dialogfeld Ressourcen-Pool erstellen verwenden, um Aggregate für Bereitstellungszwecke zu gruppieren.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Ressourcen-Pools können Aggregate von verschiedenen Clustern enthalten, aber das gleiche Aggregat kann nicht zu verschiedenen Ressourcen-Pools gehören.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcen-Pools**.
2. Klicken Sie auf der Seite **Schutz/Ressourcen-Pools** auf **Erstellen**.

3. Befolgen Sie die Anweisungen im Dialogfeld **Ressourcen-Pool erstellen**, um einen Namen und eine Beschreibung anzugeben und um dem Ressourcenpool, den Sie erstellen möchten, Aggregate als Mitglieder hinzuzufügen.

Bearbeiten von Ressourcenpools

Sie können einen vorhandenen Ressourcenpool bearbeiten, wenn Sie den Namen des Ressourcenpool und die Beschreibung ändern möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die Schaltfläche **Bearbeiten** ist nur aktiviert, wenn ein Ressourcenpool ausgewählt ist. Wenn mehrere Ressourcen-Pools ausgewählt sind, ist die Schaltfläche **Bearbeiten** deaktiviert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcen-Pools**.
2. Wählen Sie einen Ressourcenpool aus der Liste aus.
3. Klicken Sie Auf **Bearbeiten**.

   Das Fenster „Ressourcen-Pool bearbeiten“ wird angezeigt.

4. Bearbeiten Sie den Namen und die Beschreibung des Ressourcenpool nach Bedarf.
5. Klicken Sie Auf **Speichern**.

   Der neue Name und eine neue Beschreibung werden in der Liste Ressourcen-Pool angezeigt.

Anzeigen des Ressourcenpools-Inventars

Auf der Seite „Protection/Resource Pools“ können Sie den Ressourcenpoolbestand anzeigen und die verbleibende Kapazität für jeden Ressourcenpool überwachen.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcen-Pools**.

   Der Ressourcenpoolbestand wird angezeigt.

Hinzufügen von Mitgliedern des Ressourcenpool

Ein Ressourcen-Pool besteht aus einer Reihe von Mitglied-Aggregaten. Sie können zu vorhandenen Ressourcen-Pools Aggregate hinzufügen, um den für die Provisionierung

des sekundären Volumes verfügbaren Speicherplatz zu erhöhen.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können nicht mehr als 200 Aggregate gleichzeitig einem Ressourcen-Pool hinzufügen. Aggregate, die im Dialogfeld Aggregate angezeigt werden, gehören keiner anderen Ressource-Pool an.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcen-Pools**.
2. Wählen Sie aus der Liste **Ressourcen-Pools** einen Ressourcen-Pool aus.

   Die Mitglieder des Ressourcenpool werden im Bereich unterhalb der Ressourcenpoolliste angezeigt.
3. Klicken Sie im Bereich Resource Pool Member auf **Add**.

   Das Dialogfeld Aggregate wird angezeigt.
4. Wählen Sie ein oder mehrere Aggregate aus.
5. Klicken Sie Auf **Hinzufügen**.

   Das Dialogfeld wird geschlossen, und die Aggregate werden in der Mitgliederliste für den ausgewählten Ressourcenpool angezeigt.

Entfernen von Aggregaten aus Ressourcen-Pools

Sie können Aggregate aus einem vorhandenen Ressourcen-Pool entfernen, wenn Sie beispielsweise ein Aggregat für einen anderen Zweck verwenden möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Ressourcen-Pool-Mitglieder werden nur angezeigt, wenn ein Ressourcen-Pool ausgewählt ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcen-Pools**.
2. Wählen Sie den Ressourcen-Pool aus, aus dem Sie Mitgliederaggregate entfernen möchten.

   Die Liste der Mitgliederaggregate wird im Mitgliederbereich angezeigt.
3. Wählen Sie ein oder mehrere Aggregate aus.

   Die Schaltfläche **Entfernen** ist aktiviert.

4. Klicken Sie Auf **Entfernen.**

   Ein Warndialogfeld wird angezeigt.

5. Klicken Sie auf **Ja**, um fortzufahren.

   Die ausgewählten Aggregate werden aus dem Bereich Mitglieder entfernt.

Löschen von Ressourcenpools

Sie können Ressourcenpools löschen, wenn sie nicht mehr benötigt werden. Beispielsweise möchten Sie die Mitgliedslegierung von einem Ressourcenpool auf mehrere andere Ressourcenpools verteilen, sodass der ursprüngliche Ressourcenpool überflüssig wird.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die Schaltfläche **Löschen** ist nur aktiviert, wenn mindestens ein Ressourcen-Pool ausgewählt ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcen-Pools**.
2. Wählen Sie den Ressourcenpool aus, den Sie löschen möchten.
3. Klicken Sie Auf **Löschen**.

   Der Ressourcen-Pool wird aus der Ressourcen-Pool-Liste entfernt und seine Aggregate werden aus der Mitgliederliste entfernt.

Allgemeines zu SVM-Zuordnungen

Storage Virtual Machine (SVM)-Zuordnungen werden von einer Quell-SVM zu einer Ziel-SVM zugeordnet, die von Partnerapplikationen zur Ressourcenauswahl und zur Bereitstellung von sekundären Volumes verwendet werden.

Zwischen einer Quell-SVM und einer Ziel-SVM werden immer Zuordnungen erstellt, unabhängig davon, ob die Ziel-SVM ein sekundäres oder tertiäres Ziel ist. Zum Erstellen einer Zuordnung zu einer tertiären Ziel-SVM kann eine sekundäre Ziel-SVM nicht als Quelle verwendet werden.

SVMs können auf drei Arten zugeordnet werden:

- Zuordnen einer beliebigen SVM

  Sie können eine Zuordnung zwischen jeder beliebigen primären Quell-SVM und einer oder mehreren Ziel-SVMs erstellen. Das bedeutet, dass alle bestehenden SVMs, die derzeit Schutz benötigen, sowie alle zukünftig erstellten SVMs mit den angegebenen Ziel-SVMs verknüpft sind. Beispielsweise könnte es sinnvoll sein, dass Applikationen aus verschiedenen Quellen an verschiedenen Standorten auf einer oder mehreren Ziel-SVMs an einem Standort gesichert werden.

- Eine bestimmte SVM zuordnen

  Sie können eine Zuordnung zwischen einer bestimmten Quell-SVM und einer oder mehreren spezifischen Ziel-SVMs erstellen. Wenn Sie beispielsweise vielen Clients Storage-Services bereitstellen, deren Daten voneinander getrennt sein müssen, können Sie diese Option auswählen, um eine bestimmte Quell-SVM einer bestimmten Ziel-SVM zu zuordnen, die nur diesem Client zugewiesen ist.

- Zuordnung zu einer externen SVM

  Sie können eine Verknüpfung zwischen einer Quell-SVM und einem externen, flexiblen Volume einer Ziel-SVM erstellen.

Anforderungen an SVM und Ressourcen-Pool zur Unterstützung von Storage-Services

Die Konformität in Partnerapplikationen kann besser gewährleistet werden, wenn einige für Storage-Services spezifische SVM-Zuordnungs- und Ressourcen-Pool-Anforderungen eingehalten werden: Wenn Sie beispielsweise SVM zuweisen und in Unified Manager Ressourcen-Pools erstellen, um eine Sicherungstopologie in einem Storage-Service zu unterstützen, der von einer Partner-Applikation bereitgestellt wird.

Einige Applikationen arbeiten mit dem Unified Manager Server zusammen, um Services bereitzustellen, die SnapMirror oder SnapVault Backups zwischen Quell-Volumes und Sicherungs-Volumes an sekundären oder tertiären Standorten automatisch konfigurieren und ausführen. Um diese Sicherungs-Storage-Services zu unterstützen, müssen Sie mit Unified Manager die erforderlichen SVM-Zuordnungen und Ressourcenpools konfigurieren.

Um den Storage-Service mit Single-Hop- oder kaskadierter Sicherung zu unterstützen, einschließlich der Replizierung von einem primären SnapMirror Quell- oder SnapVault Volume auf Ziel-SnapMirror oder zu SnapVault Backup-Volumes an sekundären oder tertiären Standorten, sind die folgenden Anforderungen zu erfüllen:

- SVM-Zuordnungen müssen zwischen der SVM, die die SnapMirror Quelle oder das primäre SnapVault Volume enthält, und einer beliebigen SVM konfiguriert werden, auf der sich entweder ein sekundäres Volume oder ein tertiäres Volume befinden.
  - Beispielsweise zur Unterstützung einer Schutztopologie, in der sich das Quell-Volume Vol_A auf der SVM_1 befindet, und zum sekundären SnapMirror Ziel-Volume Vol_B auf der SVM_2, Das tertiäre SnapVault Backup Volume Vol_ C befindet sich auf SVM_3. Sie müssen die Unified Manager Web-UI verwenden, um eine SnapMirror Verknüpfung zwischen SVM_1 und SVM_2 und einer SnapVault Backup-Verbindung zwischen SVM_1 und SVM_3 zu konfigurieren.

    In diesem Beispiel ist eine SnapMirror Zuordnung oder eine SnapVault-Backup-Zuordnung zwischen SVM_2 und SVM_3 nicht erforderlich und wird nicht verwendet.

  - Um eine Schutztopologie zu unterstützen, in der sich sowohl das Quell-Volume Vol_A als auch das SnapMirror Ziel-Volume Vol_B auf SVM_1 befinden, müssen Sie eine SnapMirror Verknüpfung zwischen SVM_1 und SVM_1 konfigurieren.
- Die Ressourcenpools müssen Cluster-Aggregatressourcen enthalten, die den zugehörigen SVMs zur Verfügung stehen.

  Sie konfigurieren Ressourcen-Pools über die Unified Manager Web-UI und weisen dann über die Partnerapplikation das sekundäre Storage Service-Ziel und die tertiären Ziel-Nodes zu.

SVM-Zuordnungen werden erstellt

Mit dem Assistenten „Create Storage Virtual Machine Associations“ können Partnerapplikationen eine Quell-Storage Virtual Machine (SVM) einer Ziel-SVM zuweisen, um sie mit SnapMirror- und SnapVault-Beziehungen zu verwenden. Partnerapplikationen verwenden diese Verknüpfungen zum Zeitpunkt der Erstbereitstellung der Ziel-Volumes, um zu ermitteln, welche Ressourcen ausgewählt werden sollen.

Bevor Sie beginnen

- Die von Ihnen verknüpfen, muss bereits vorhanden sein.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Für jede Quell-SVM und jeden Beziehungstyp können Sie nur eine Ziel-SVM auf jedem Ziel-Cluster auswählen.

Das Ändern von Zuordnungen mithilfe der Funktionen Löschen und Erstellen wirkt sich nur auf zukünftige Bereitstellungsvorgänge aus. Es verschiebt keine vorhandenen Ziel-Volumes.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **SVM-Zuordnungen**.
2. Klicken Sie auf der Seite **Protection/Storage Virtual Machine Associations** auf **Create**.

   Der Assistent Create Storage Virtual Machine Associations wird gestartet.

3. Wählen Sie eine der folgenden Quellen aus:
   - * Any*

     Wählen Sie diese Option, wenn Sie eine Zuordnung zwischen einer beliebigen primären SVM-Quelle zu einer oder mehreren Ziel-SVM erstellen möchten. Das bedeutet, dass alle vorhandenen SVMs, die derzeit Schutz benötigen, sowie alle zukünftig erstellten SVMs der angegebenen Ziel-SVM zugeordnet sind. Beispielsweise könnte es sinnvoll sein, dass Applikationen aus verschiedenen Quellen an verschiedenen Standorten an einem Standort auf einer oder mehreren Ziel-SVM an einem Standort gesichert werden.

   - **Single**

     Wählen Sie diese Option, wenn Sie eine bestimmte Quell-SVM auswählen möchten, die einer oder mehreren Ziel-SVMs zugeordnet ist. Wenn Sie beispielsweise vielen Clients Storage-Services bereitstellen, deren Daten voneinander getrennt sein müssen, wählen Sie diese Option, um eine bestimmte SVM-Quelle einem bestimmten SVM-Ziel zu zuordnen, das nur diesem Client zugewiesen ist.

   - **Keine (Extern)**

     Wählen Sie diese Option, wenn Sie eine Zuordnung zwischen einer Quell-SVM und einem externen flexiblen Volume einer Ziel-SVM erstellen möchten.

4. Wählen Sie einen oder beide Arten von Schutzbeziehungen aus, die Sie erstellen möchten:

- **SnapMirror**
- **SnapVault**

5. Klicken Sie Auf **Weiter**.
6. Wählen Sie ein oder mehrere SVM-Schutzziele aus.
7. Klicken Sie Auf **Fertig Stellen**.

Anzeigen von SVM-Zuordnungen

Über die Seite Verknüpfungen zu Protection-/Storage Virtual Machines können Sie vorhandene SVM-Zuordnungen und ihre Eigenschaften anzeigen und feststellen, ob zusätzliche SVM-Verknüpfungen erforderlich sind.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **SVM-Zuordnungen**.

   Die Liste der SVM-Zuordnungen und ihrer Eigenschaften wird angezeigt.

SVM-Zuordnungen werden gelöscht

Sie können SVM-Zuordnungen für Partnerapplikationen löschen, um die sekundäre Bereitstellungsbeziehung zwischen Quell- und Ziel-SVMs zu entfernen. Dies kann beispielsweise geschehen, wenn die Ziel-SVM voll ist und Sie eine neue SVM-Sicherungszuordnung erstellen möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die Schaltfläche **Löschen** ist deaktiviert, bis mindestens eine SVM-Zuordnung ausgewählt ist. Das Ändern von Zuordnungen mithilfe der Funktionen „Löschen und Erstellen“ wirkt sich nur auf zukünftige Bereitstellungsvorgänge aus. Vorhandene Ziel-Volumes werden nicht verschoben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **SVM-Zuordnungen**.
2. Wählen Sie mindestens eine SVM-Zuordnung aus.

   Die Schaltfläche **Löschen** ist aktiviert.

3. Klicken Sie Auf **Löschen.**

   Ein Warndialogfeld wird angezeigt.

4. Klicken Sie auf **Ja**, um fortzufahren.

   Die ausgewählte SVM-Zuordnung wird aus der Liste entfernt.

Was sind Jobs

Ein Job besteht aus einer Reihe von Aufgaben, die Sie mit Unified Manager überwachen können. Durch das Anzeigen von Jobs und den zugehörigen Aufgaben können Sie feststellen, ob ein Job erfolgreich abgeschlossen wurde.

Jobs werden gestartet, wenn Sie SnapMirror- und SnapVault-Beziehungen erstellen, wenn Sie eine Beziehungsoperation ausführen (Break, edit, quiesce, remove, resume, Werden neu synchronisiert und umgekehrt neu synchronisiert), wenn Sie Wiederherstellungsaufgaben ausführen, wenn Sie sich bei einem Cluster anmelden usw.

Wenn Sie einen Job initiieren, können Sie den Job und den Fortschritt der zugehörigen Job-Aufgaben über die Seite „Schutz/Jobs“ und die Seite „Schutz/Job-Details“ überwachen.

Überwachen von Jobs

Mithilfe der Seite Schutz/Jobs können Sie den Job-Status überwachen und Jobeigenschaften wie Speicherdiensttyp, Status, Abgesendete Zeit und Abgeschlossene Zeit anzeigen, um festzustellen, ob ein Job erfolgreich abgeschlossen wurde oder nicht.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Jobs**.

   Die Seite Schutz/Jobs wird angezeigt.

2. Zeigen Sie die Spalte **Status** an, um den Status der aktuell ausgeführten Jobs zu bestimmen.
3. Klicken Sie auf einen Jobnamen, um Details zu diesem Job anzuzeigen.

   Die Seite Schutz-/Jobdetails wird angezeigt.

Anzeigen von Jobdetails

Nachdem Sie einen Job gestartet haben, können Sie den Fortschritt auf der Seite Schutz-/Jobdetails verfolgen und die zugehörigen Aufgaben auf mögliche Fehler überwachen.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Jobs**.
2. Klicken Sie auf der Seite **Schutz/Jobs** in der Spalte **Name** auf einen Jobnamen, um die Liste der Aufgaben anzuzeigen, die mit dem Job verknüpft sind.
3. Klicken Sie auf eine Aufgabe, um zusätzliche Informationen im Bereich **Aufgabendetails** und im Bereich **Aufgabenmeldungen** rechts neben der Aufgabenliste anzuzeigen.

Abbrechen von Jobs

Sie können die Seite Schutz/Jobs verwenden, um einen Job abzubrechen, wenn der Vorgang zu lang dauert, zu viele Fehler auftritt oder nicht mehr benötigt wird. Sie können einen Job nur dann abbrechen, wenn ihm Status und Typ erlauben. Sie können jeden laufenden Job abbrechen.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Jobs**.
2. Wählen Sie in der Liste der Jobs einen Job aus, und klicken Sie dann auf **Abbrechen**.
3. Klicken Sie in der Bestätigungsaufforderung auf **Ja**, um den ausgewählten Job abzubrechen.

Erneutes Versuch eines fehlgeschlagenen Schutzjobs

Nachdem Sie Maßnahmen ergriffen haben, um einen fehlgeschlagenen Schutzauftrag zu beheben, können Sie den Job mit **Retry** erneut ausführen. Durch Wiederversuchen eines Jobs wird mithilfe der ursprünglichen Job-ID ein neuer Job erstellt.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können nur einen fehlgeschlagenen Job gleichzeitig erneut versuchen. Wenn Sie mehrere Jobs auswählen, wird die Schaltfläche **Wiederholen** deaktiviert. Es können nur Jobs vom Typ Protection Configuration and Protection Relationship Operation wiederholt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Jobs**.
2. Wählen Sie aus der Liste der Aufträge einen einzelnen Auftrag vom Typ fehlgeschlagener Schutzkonfiguration oder Schutzbeziehung aus.

   Die Schaltfläche **Wiederholen** ist aktiviert.

3. Klicken Sie Auf **Wiederholen**.

Der Job wird neu gestartet.

Beschreibung der Fenster und Dialogfelder zu Sicherungsbeziehungen

Sie können Sicherungsdetails wie Ressourcen-Pools, SVM-Zuordnungen und Sicherungsjobs anzeigen und managen. Sie können die entsprechende Seite mit den Konfigurations-/Integritätsschwellenwerten verwenden, um globale Schwellenwerte für den Systemzustand für Aggregate, Volumes und Beziehungen zu konfigurieren.

Sicherungs-/Ressourcen-Pools

Auf der Seite „Protection/Resource Pools“ werden vorhandene Ressourcen-Pools und deren Mitglieder angezeigt. Hier können Sie Ressourcen-Pools für Bereitstellungszwecke erstellen, überwachen und verwalten.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Erstellen**

  Öffnet das Dialogfeld „Ressourcen-Pool erstellen“, das Sie zum Erstellen von Ressourcenpools verwenden können.

- **Bearbeiten**

  Hier können Sie den Namen und die Beschreibung der von Ihnen erstellten Ressourcenpools bearbeiten.

- **Löschen**

  Ermöglicht Ihnen das Löschen eines oder mehrerer Ressourcenpools.

Liste der Ressourcenpools

Die Liste „Ressourcen-Pools“ zeigt (tabellarisch) die Eigenschaften vorhandener Ressourcen-Pools an.

- **Ressourcen-Pool**

  Zeigt den Namen des Ressourcen-Pools an.

- **Beschreibung**

  Beschreibt den Ressourcenpool.

- **SnapLock Typ**

  Zeigt den SnapLock-Typ an, der von den Aggregaten im Ressourcenpool verwendet wird. Gültige Werte für den SnapLock-Typ sind Compliance, Unternehmen und nicht-SnapLock. Ein Ressourcen-Pool kann Aggregate von nur einem SnapLock-Typ enthalten.

- **Gesamtkapazität**

  Zeigt die Gesamtkapazität (in MB, GB usw.) des Ressourcen-Pools an.

- * Genutzte Kapazität*

  Zeigt den Speicherplatz an (in MB, GB usw.), der im Ressourcenpool verwendet wird.

- **Verfügbare Kapazität**

  Zeigt den Speicherplatz an (in MB, GB usw.), der im Ressourcen-Pool verfügbar ist.

- **%** Genutzt

  Zeigt den Prozentsatz des Speicherplatzes an, der im Ressourcenpool verwendet wird.

Schaltflächen der Mitgliederliste

Mit den Schaltflächen der Mitgliederliste können Sie die folgenden Aufgaben ausführen:

- **Hinzufügen**

  Ermöglicht Ihnen das Hinzufügen von Mitgliedern zum Ressourcenpool.

- **Löschen**

  Ermöglicht Ihnen, einen oder mehrere Mitglieder aus dem Ressourcenpool zu löschen.

Mitgliederliste

Die Mitgliederliste zeigt (tabellarisch) die Mitglieder des Ressourcenpool und ihre Eigenschaften an, wenn ein Ressourcenpool ausgewählt ist.

- **Status**

  Zeigt den aktuellen Status des Mitgliedaggregats an. Der Status kann kritisch sein (), Fehler (), Warnung (Oder normal ().

- **Aggregatname**

  Zeigt den Namen des Mitgliedaggregats an.

- **Bundesland**

  Zeigt den aktuellen Status des Aggregats an. Dieser kann einer der folgenden Werte sein:

  - Offline

    Lese- oder Schreibzugriff ist nicht zulässig.

  - Online

    Lese- und Schreibzugriff auf die Volumes, die in diesem Aggregat gehostet werden, ist zulässig.

  - Eingeschränkt

    Begrenzte Operationen (wie etwa die Paritätsrekonstruktion) sind zulässig, der Datenzugriff ist jedoch nicht zulässig.

- Wird Erstellt

  Das Aggregat wird erstellt.

- Zerstören

  Das Aggregat wird zerstört.

- Fehlgeschlagen

  Das Aggregat kann nicht online gebracht werden.

- Eingefroren

  Das Aggregat bedient (vorübergehend) keine Anforderungen.

- Uneinheitlich

  Das Aggregat wurde als beschädigt markiert; Sie sollten sich an den technischen Support wenden.

- Eisenbeschränkungen

  Diagnosetools können nicht auf dem Aggregat ausgeführt werden.

- Montage

  Das Aggregat wird gerade montiert.

- Teilweise

  Mindestens eine Festplatte für das Aggregat gefunden wurde, aber zwei oder mehr Disketten fehlen.

- Wird Stillgelegt

  Das Aggregat wird stillgelegt.

- Stillgelegt

  Das Aggregat wird stillgelegt.

- Umgekehrt

  Die Umrüstung eines Aggregats ist abgeschlossen.

- Nicht Abgehängt

  Das Aggregat wurde abgehängt.

- Entmounten

  Das Aggregat wird offline geschaltet.

- Unbekannt

  Das Aggregat wird erkannt, die Aggregat-Informationen werden noch nicht vom Unified Manager Server abgerufen.

Standardmäßig ist diese Spalte ausgeblendet.

- * Cluster*

  Zeigt den Namen des Clusters an, zu dem das Aggregat gehört.

- **Knoten**

  Zeigt den Namen des Node an, auf dem sich das Aggregat befindet.

- **Gesamtkapazität**

  Zeigt die Gesamtkapazität (in MB, GB usw.) des Aggregats an.

- * Genutzte Kapazität*

  Zeigt die Menge an Speicherplatz (in MB, GB usw.) an, die im Aggregat verwendet wird.

- **Verfügbare Kapazität**

  Zeigt die Menge an Speicherplatz (in MB, GB usw.) an, die im Aggregat verfügbar ist.

- **%** Genutzt

  Zeigt den Prozentsatz des Speicherplatzes an, der im Aggregat verwendet wird.

- **Festplattentyp**

  Zeigt den RAID-Konfigurationstyp an. Dieser kann einer der folgenden sein:

  - RAID0: Alle RAID-Gruppen sind vom Typ RAID0.
  - RAID4: Alle RAID-Gruppen sind vom Typ RAID4.
  - RAID-DP: Alle RAID-Gruppen vom Typ RAID-DP.
  - RAID-TEC: Alle RAID Gruppen sind vom Typ RAID-TEC.
  - Gemischtes RAID: Das Aggregat enthält RAID-Gruppen unterschiedlicher RAID-Typen (RAID0, RAID4, RAID-DP und RAID-TEC). Standardmäßig ist diese Spalte ausgeblendet.

Dialogfeld „Ressourcen-Pool erstellen“

Sie können im Dialogfeld Ressourcen-Pool erstellen einen neuen Ressourcen-Pool benennen und beschreiben sowie Aggregate zu diesem Ressourcenpool hinzufügen und aus diesem Ressourcenpool löschen.

Name Des Ressourcenpool

Mit den Textfeldern können Sie die folgenden Informationen hinzufügen, um einen Ressourcenpool zu erstellen:

Ermöglicht die Angabe eines Ressourcenpoolnamens.

Beschreibung

Ermöglicht Ihnen, einen Ressourcenpool zu beschreiben.

Mitglieder

Zeigt die Mitglieder des Ressourcen-Pools an. Sie können auch Mitglieder hinzufügen und löschen.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Hinzufügen**

  Öffnet das Dialogfeld Aggregate, damit Sie dem Ressourcen-Pool Aggregate von einem bestimmten Cluster hinzufügen können. Sie können Aggregate von verschiedenen Clustern hinzufügen. Dasselbe Aggregat kann jedoch nicht mehr als einem Ressourcen-Pool hinzugefügt werden.

- **Entfernen**

  Hiermit können Sie ausgewählte Aggregate aus dem Ressourcen-Pool entfernen.

- **Erstellen**

  Erstellt den Ressourcenpool. Diese Schaltfläche ist erst aktiviert, wenn die Informationen in die Felder „Ressourcenpoolname“ oder „Beschreibung“ eingegeben wurden.

- **Abbrechen**

  Die Änderungen werden nicht mehr gespeichert, und das Dialogfeld „Create Resource Pool“ wird geschlossen.

Dialogfeld „Ressourcen-Pool bearbeiten“

Über das Dialogfeld „Ressourcen-Pool bearbeiten“ können Sie den Namen und die Beschreibung eines vorhandenen Ressourcen-Pools ändern. Wenn beispielsweise der ursprüngliche Name und die Beschreibung ungenau oder falsch sind, können Sie sie ändern, damit sie genauer sind.

Textfelder

Mit den Textfeldern können Sie die folgenden Informationen für den ausgewählten Ressourcenpool ändern:

- **Name Des Ressourcen-Pools**

  Ermöglicht die Eingabe eines neuen Namens.

- **Beschreibung**

  Ermöglicht die Eingabe einer neuen Beschreibung.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Speichern**

  Speichert die Änderungen am Namen und der Beschreibung des Ressourcenpool.

- **Abbrechen**

  Sperrt die Änderungen und schließt das Dialogfeld „Ressourcen-Pool bearbeiten“.

Dialogfeld „Aggregate“

Im Dialogfeld Aggregate können Sie die Aggregate auswählen, die Sie Ihrem Ressourcen-Pool hinzufügen möchten.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Hinzufügen**

  Fügt die ausgewählten Aggregate dem Ressourcenpool hinzu. Die Schaltfläche Hinzufügen ist erst aktiviert, wenn mindestens ein Aggregat ausgewählt wurde.

- **Abbrechen**

  Sperrt die Änderungen und schließt das Dialogfeld Aggregate.

Aggregatliste

In der Liste Aggregate werden die Namen und Eigenschaften der überwachten Aggregate (tabellarisch) angezeigt.

- **Status**

  Zeigt den aktuellen Status eines Volumes an. Der Status kann kritisch sein (), Fehler (), Warnung (Oder normal ().

  Sie können den Zeiger über den Status verschieben, um weitere Informationen zu dem für das Volume generierten Ereignis oder Ereignissen anzuzeigen.

- **Aggregatname**

  Zeigt den Namen des Aggregats an.

- **Bundesland**

  Zeigt den aktuellen Status des Aggregats an. Dieser kann einer der folgenden Werte sein:

  - Offline

    Lese- oder Schreibzugriff ist nicht zulässig.

  - Eingeschränkt

    Begrenzte Operationen (wie etwa die Paritätsrekonstruktion) sind zulässig, der Datenzugriff ist jedoch nicht zulässig.

  - Online

Lese- und Schreibzugriff auf die Volumes, die in diesem Aggregat gehostet werden, ist zulässig.

- Wird Erstellt

  Das Aggregat wird erstellt.

- Zerstören

  Das Aggregat wird zerstört.

- Fehlgeschlagen

  Das Aggregat kann nicht online gebracht werden.

- Eingefroren

  Das Aggregat bedient (vorübergehend) keine Anforderungen.

- Uneinheitlich

  Das Aggregat wurde als beschädigt markiert; Sie sollten sich an den technischen Support wenden.

- Eisenbeschränkungen

  Diagnosetools können nicht auf dem Aggregat ausgeführt werden.

- Montage

  Das Aggregat wird gerade montiert.

- Teilweise

  Mindestens eine Festplatte für das Aggregat gefunden wurde, aber zwei oder mehr Disketten fehlen.

- Wird Stillgelegt

  Das Aggregat wird stillgelegt.

- Stillgelegt

  Das Aggregat wird stillgelegt.

- Umgekehrt

  Die Umrüstung eines Aggregats ist abgeschlossen.

- Nicht Abgehängt

  Das Aggregat ist offline.

- Entmounten

  Das Aggregat wird offline geschaltet.

- Unbekannt

  Das Aggregat wird erkannt, die Aggregat-Informationen werden noch nicht vom Unified Manager

Server abgerufen.

- * Cluster*

  Zeigt den Namen des Clusters an, auf dem sich das Aggregat befindet.

- **Knoten**

  Zeigt den Namen des Storage-Controllers an, der das Aggregat enthält.

- **Gesamtkapazität**

  Zeigt die Gesamtdatengröße (in MB, GB usw.) des Aggregats an. Standardmäßig ist diese Spalte ausgeblendet.

- * Engagierte Kapazität*

  Zeigt den gesamten Speicherplatz an (in MB, GB usw.), der für alle Volumes im Aggregat festgelegt ist. Standardmäßig ist diese Spalte ausgeblendet.

- * Genutzte Kapazität*

  Zeigt die Menge an Speicherplatz (in MB, GB usw.) an, die im Aggregat verwendet wird.

- **Verfügbare Kapazität**

  Zeigt die Menge an Speicherplatz (in MB, GB usw.) an, die für Daten im Aggregat verfügbar ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Verfügbar %**

  Zeigt den Prozentsatz des Speicherplatzes an, der für Daten im Aggregat verfügbar ist. Standardmäßig ist diese Spalte ausgeblendet.

- **%** Genutzt

  Zeigt den Prozentsatz des Speicherplatzes an, der von Daten im Aggregat verwendet wird.

- **RAID-Typ**

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

Seite „Verknüpfungen zu Sicherungs-/Storage Virtual Machines“

Auf der Seite Verknüpfungen zu Protection/Storage Virtual Machines können vorhandene SVM Verknüpfungen zwischen Quell- und Ziel-SVMs angezeigt werden. Außerdem können Sie neue SVM-Verknüpfungen erstellen, die von Partnerapplikationen zum Erstellen von SnapMirror und SnapVault Beziehungen verwendet werden.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Erstellen**

  Öffnet den Assistenten zum Erstellen von Storage Virtual Machine-Zuordnungen.

- **Löschen**

  Hiermit können Sie die ausgewählten SVM-Zuordnungen löschen.

Liste der Storage Virtual Machine (SVM)-Verknüpfungen

Die Liste Storage Virtual Machine Associations wird in einer Tabelle die erstellten Quell- und Ziel-SVM-Zuordnungen sowie die Art der für jede Zuordnung zugelassenen Sicherungsbeziehung angezeigt.

- * Source Storage Virtual Machine*

  Zeigt den Namen der Quell-SVM an.

- * Quellcluster*

  Zeigt den Namen des Quell-Clusters an.

- **Zielspeicher Virtual Machine**

  Zeigt den Namen der Ziel-SVM an.

- **Zielcluster**

  Zeigt den Namen des Ziel-Clusters an.

- **Typ**

  Zeigt die Art der Schutzbeziehung an. Beziehungstypen sind entweder SnapMirror oder SnapVault.

Assistent zum Erstellen von Storage Virtual Machine-Zuordnungen

Mit dem Assistenten „Create Storage Virtual Machine Associations“ können Sie Storage Virtual Machines (SVMs) aus Quell- und Ziel-Storage zur Verwendung in SnapMirror und SnapVault Sicherungsbeziehungen zuordnen.

Wählen Sie Quell-SVM aus

Im Fenster Quell-Storage-Virtual Machine auswählen können Sie die SVM in der SVM-Zuordnung als Quelle oder primäre SVM auswählen.

- * Any*

  Ermöglicht Ihnen, eine Zuordnung zwischen einer beliebigen SVM-Quelle zu einem oder mehreren Ziel oder einer sekundären SVM zu erstellen. Das bedeutet, dass alle vorhandenen SVMs, die derzeit Schutz benötigen, sowie alle zukünftig erstellten SVMs der angegebenen Ziel-SVM zugeordnet sind. Beispielsweise könnte es sinnvoll sein, dass Applikationen aus verschiedenen Quellen an verschiedenen Standorten an einem Standort auf einer oder mehreren Ziel-SVM an einem Standort gesichert werden.

- **Single**

Hiermit können Sie eine bestimmte Quell-SVM mit einer oder mehreren Ziel-SVMs verknüpfen. Wenn Sie beispielsweise vielen Clients Storage-Services bereitstellen, deren Daten voneinander getrennt sein müssen, wählen Sie diese Option, um eine bestimmte SVM-Quelle einem bestimmten SVM-Ziel zu zuordnen, das nur diesem Client zugewiesen ist.

- **Keine (Extern)**

  Damit lässt sich eine Verknüpfung zwischen einer Quell-SVM und einem externen, flexiblen Volume einer Ziel-SVM erstellen.

  - Storage Virtual Machine

    Führt die Namen der verfügbaren Quell-SVMs auf

  - Cluster

    Listet die Cluster auf, auf denen sich die SVM befindet

- **Erlauben Sie solche Beziehungen**

  Ermöglicht Ihnen die Auswahl des Beziehungstyps für die Zuordnung:

  - SnapMirror

    Gibt eine SnapMirror-Beziehung als Zuordnungstyp an. Wenn Sie diese Option auswählen, wird die Datenreplikation von den ausgewählten Quellen zu den ausgewählten Zielen aktiviert.

  - SnapVault

    Gibt eine SnapVault-Beziehung als Zuordnungstyp an. Wenn Sie diese Option auswählen, werden Backups von den ausgewählten primären Standorten zu den ausgewählten sekundären Standorten aktiviert.

Wählen Sie Schutzziele

Im Fenster Schutzziele auswählen des Assistenten zum Erstellen von Storage-VM-Zuordnungen können Sie auswählen, wo die Daten kopiert oder repliziert werden sollen. Sie können eine Zuordnung nur auf einer Ziel-SVM pro Cluster erstellen.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Weiter**

  Sie gelangen zur nächsten Seite des Assistenten.

- **Zurück**

  Kehrt zur vorherigen Seite des Assistenten zurück.

- **Fertig**

  Wendet Ihre Auswahl an und erstellt die Verknüpfung.

- **Abbrechen**

  Schließt die Auswahl aus und schließt den Assistenten zum Erstellen von Storage-VM-Zuordnungen.

Schutz-/Jobseite

Auf der Seite „Schutz/Jobs“ können Sie den aktuellen Status und weitere Informationen zu allen aktuell ausgeführten Partnerbewerbungs-Sicherungsaufgaben sowie zu abgeschlossenen Jobs anzeigen. Anhand dieser Informationen können Sie feststellen, welche Jobs noch ausgeführt werden und ob ein Job erfolgreich oder fehlgeschlagen ist.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Abbrechen**

  Bricht den ausgewählten Job ab. Diese Option ist nur verfügbar, wenn der ausgewählte Job ausgeführt wird.

- **Retry**

  Startet einen fehlgeschlagenen Job vom Typ Schutzkonfiguration oder Schutzbeziehung neu. Sie können nur einen fehlgeschlagenen Job gleichzeitig erneut versuchen. Wenn mehrere fehlgeschlagene Jobs ausgewählt wurden, ist die Schaltfläche **Wiederholen** deaktiviert. Fehlgeschlagene Speicherserviceaufträge können nicht erneut ausgeführt werden.

- **Aktualisieren**

  Aktualisiert die Liste der Jobs und die ihnen zugeordneten Informationen.

Auftragsliste

Die Liste Jobs zeigt im Tabellenformat eine Liste der laufenden Jobs an. Standardmäßig werden in der Liste nur die Jobs angezeigt, die innerhalb der letzten Woche generiert wurden. Sie können die Spaltensortierung und -Filterung verwenden, um die angezeigten Jobs anzupassen.

- **Status**

  Zeigt den aktuellen Status eines Jobs an. Der Status kann „Fehler“ sein (❗) Oder normal (✅).

- **Job-Id**

  Zeigt die Identifikationsnummer des Jobs an. Standardmäßig ist diese Spalte ausgeblendet.

  Die Job-ID-Nummer ist eindeutig und wird vom Server beim Start des Jobs zugewiesen. Sie können nach einem bestimmten Job suchen, indem Sie die Job-ID-Nummer in das Textfeld eingeben, das vom Spaltenfilter bereitgestellt wird.

- **Name**

  Zeigt den Namen des Jobs an.

- **Typ**

  Zeigt den Jobtyp an. Die Jobtypen sind wie folgt:

  - **Cluster Acquisition**

    Ein Workflow Automation Job findet gerade ein Cluster neu statt.

  - **Schutzkonfiguration**

    Ein Sicherungsauftrag initiiert Workflow Automation Workflows wie beispielsweise cron-Zeitpläne, die Erstellung von SnapMirror Richtlinien usw.

  - **Schutz Beziehung Betrieb**

    Ein Schutzauftrag führt SnapMirror Vorgänge aus.

  - **Protection Workflow Chain**

    Ein Workflow Automation Job führt mehrere Workflows aus.

  - **Wiederherstellen**

    Ein Wiederherstellungsauftrag wird ausgeführt.

  - **Cleanup**

    Der Job reinigt Artefakte von Storage-Servicemitgliedern, die für Wiederherstellungen nicht mehr benötigt werden.

  - **Konform**

    Der Job überprüft die Konfiguration der Storage Service-Mitglieder, um sicherzustellen, dass sie den Anforderungen entsprechen.

  - * Zerstöre*

    Der Job zerstört einen Speicherdienst.

  - **Import**

    Der Job importiert nicht verwaltete Speicherobjekte in einen vorhandenen Speicherdienst.

  - **Ändern**

    Der Job ändert die Attribute eines vorhandenen Storage-Service.

  - **Anmeldung**

    Der Job abonnieren Mitglieder zu einem Storage-Service.

  - **Abmelden**

    Der Job hebt Mitglieder von einem Storage-Service ab.

  - **Aktualisierung**

Ein Update-Auftrag für den Schutz wird ausgeführt.

- **WFA Konfiguration**

  Ein Workflow Automation Job führt zur Übermittlung von Cluster-Anmeldedaten und zur Synchronisierung von Datenbank-Caches.

- **Bundesland**

  Zeigt den laufenden Status des Jobs an. Folgende Statusoptionen stehen zur Verfügung:

  - **Abgebrochen**

    Der Job wurde abgebrochen.

  - **Aborting**

    Der Job wird abgebrochen.

  - **Abgeschlossen**

    Der Job ist abgeschlossen.

  - **Laufen**

    Der Job wird ausgeführt.

- **Einreichungszeit**

  Zeigt die Zeit an, zu der der Job gesendet wurde.

- **Dauer**

  Zeigt die Zeit an, die der Job zum Abschluss benötigt hat. Diese Spalte wird standardmäßig angezeigt.

- **Abgeschlossene Zeit**

  Zeigt die Zeit an, zu der der Job beendet wurde. Standardmäßig ist diese Spalte ausgeblendet.

Einzelheiten zu Sicherung/Auftrag

Auf der Seite „Schutz-/Jobdetails“ können Sie den Status und weitere Informationen zu laufenden, in der Warteschlange befindlichen oder abgeschlossenen Sicherungsaufgaben anzeigen. Diese Informationen können Sie zur Überwachung des Arbeitsfortschritts des Schutzjobs und zur Behebung von Fehlern bei Jobs verwenden.

Jobzusammenfassung

In der Jobübersicht werden die folgenden Informationen angezeigt:

- Job-ID
- Typ
- Bundesland

- Einreichungszeit
- „Ende“
- Dauer

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Aktualisieren**

  Aktualisiert die Aufgabenliste und die Eigenschaften, die jeder Aufgabe zugeordnet sind.

- **Jobs Anzeigen**

  Kehrt zur Seite „Schutz/Jobs“ zurück.

Aufgabenliste

Die Aufgabenliste zeigt in einer Tabelle alle Aufgaben an, die mit einem bestimmten Job verknüpft sind, und die Eigenschaften, die mit jeder Aufgabe verknüpft sind.

- **Startzeit**

  Zeigt den Tag und die Uhrzeit an, zu der die Aufgabe gestartet wurde. Standardmäßig werden die letzten Aufgaben oben in der Spalte angezeigt, und ältere Aufgaben werden unten angezeigt.

- **Typ**

  Zeigt den Aufgabentyp an.

- **Bundesland**

  Der Status einer bestimmten Aufgabe:

  - **Abgeschlossen**

    Die Aufgabe ist abgeschlossen.

  - **Queued**

    Die Aufgabe wird ausgeführt.

  - **Laufen**

    Die Aufgabe wird ausgeführt.

  - **Warten**

    Ein Job wurde gesendet, und einige zugeordnete Aufgaben warten darauf, in die Warteschlange gestellt und ausgeführt zu werden.

- **Status**

  Zeigt den Aufgabenstatus an:

- **Fehler (⚠️)**

  Die Aufgabe ist fehlgeschlagen.

- **Normal (✅)**

  Die Aufgabe war erfolgreich.

- **Übersprungen (↷)**

  Eine Aufgabe ist fehlgeschlagen, sodass nachfolgende Aufgaben übersprungen werden.

- **Dauer**

  Zeigt die verstrichene Zeit seit Beginn der Aufgabe an.

- **Abgeschlossene Zeit**

  Zeigt die Zeit an, zu der die Aufgabe abgeschlossen ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Task-ID**

  Zeigt die GUID an, die eine einzelne Aufgabe für einen Job identifiziert. Die Spalte kann sortiert und gefiltert werden. Standardmäßig ist diese Spalte ausgeblendet.

- **Abhängigkeitsreihenfolge**

  Zeigt eine Ganzzahl an, die die Tasksequenz in einem Diagramm darstellt, wobei der ersten Aufgabe Null zugewiesen wird. Standardmäßig ist diese Spalte ausgeblendet.

- **Fenster mit den Aufgabendetails**

  Zeigt zusätzliche Informationen zu jeder Aufgabe an, einschließlich des Aufgabennamens, der Aufgabenbeschreibung und, falls die Aufgabe fehlgeschlagen ist, einen Grund für den Fehler.

- **Aufgabenbereich Messages**

  Zeigt Meldungen an, die für die ausgewählte Aufgabe spezifisch sind. Meldungen können einen Grund für den Fehler und Vorschläge zur Behebung enthalten. Nicht alle Aufgaben zeigen Aufgabenmeldungen an.

Dialogfeld „Erweiterte sekundäre Einstellungen“

Im Dialogfeld Erweiterte sekundäre Einstellungen können Sie die versionsflexible Replikation, das Backup mehrerer Kopien und speicherbezogene Einstellungen auf einem sekundären Volume aktivieren. Sie können das Dialogfeld Erweiterte sekundäre Einstellungen verwenden, wenn Sie die aktuellen Einstellungen aktivieren oder deaktivieren möchten.

Platzsparende Einstellungen maximieren die Menge der gespeicherten Daten, einschließlich folgender: Deduplizierung, Datenkomprimierung, Autogrow und Speicherplatzgarantie.

Das Dialogfeld enthält die folgenden Felder:

- **Versionsflexible Replikation Aktivieren**

SnapMirror mit versionsflexibler Replizierung Die versionsflexible Replizierung ermöglicht den SnapMirror Schutz eines Quell-Volume, selbst wenn das Ziel-Volume unter einer früheren Version von ONTAP als jenem des Quell-Volume ausgeführt wird, solange sowohl das Quell- als auch das Ziel-Volume ONTAP 8.3 oder höher ausgeführt werden.

  - Aktivieren Sie Backup

    Wenn die versionsflexible Replizierung aktiviert ist, können auch mehrere Snapshot Kopien der SnapMirror Quelldaten an die SnapMirror Zieladresse übertragen und dort aufbewahrt werden.

- **Deduplizierung Aktivieren**

  Aktiviert in einer SnapVault Beziehung Deduplizierung auf dem sekundären Volume, sodass keine doppelten Datenblöcke mehr vorhanden sind und somit Platzeinsparungen erzielt werden können. Möglicherweise verwenden Sie die Deduplizierung, wenn die Platzeinsparungen mindestens 10 % betragen und wenn die Überschreibungsrate nicht schnell ist. Die Deduplizierung wird häufig in virtualisierten Umgebungen, in File Shares und für Backup-Daten eingesetzt. Diese Einstellung ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, wird dieser Vorgang nach jedem Transfer initiiert.

  - Aktivieren Sie Die Komprimierung

    Ermöglicht transparente Datenkomprimierung. Möglicherweise verwenden Sie die Komprimierung, wenn die Speicherersparnis mindestens 10 % beträgt, wenn der potenzielle Overhead akzeptabel ist und es genügend Systemressourcen gibt, um die Komprimierung während nicht-Spitzenzeiten durchzuführen. In einer SnapVault-Beziehung ist diese Einstellung standardmäßig deaktiviert. Die Komprimierung ist nur bei Auswahl der Deduplizierung verfügbar.

  - Inline-Komprimierung

    Ermöglicht sofortige Platzeinsparungen durch Datenkomprimierung vor dem Schreiben der Daten auf die Festplatte. Möglicherweise wird die Inline-Komprimierung verwendet, wenn Ihr System während der Spitzenzeiten nicht mehr als 50 % Auslastung erreicht, und wenn das System neue Schreibvorgänge und zusätzliche CPUs in Spitzenzeiten bewältigen kann. Diese Einstellung ist nur verfügbar, wenn „`Komprimierung aktivieren`“ ausgewählt ist.

- **Autogrow Aktivieren**

  Ermöglicht es Ihnen, das Zielvolume automatisch zu erhöhen, wenn der Prozentsatz des freien Speicherplatzes unter dem angegebenen Schwellenwert liegt, solange der Speicherplatz auf dem zugehörigen Aggregat verfügbar ist.

- **Maximale Größe**

  Legt den maximalen Prozentsatz fest, zu dem ein Volume wachsen kann. Der Standardwert ist 20 Prozent größer als die Größe des Quell-Volumes. Ein Volume wächst nicht automatisch, wenn die aktuelle Größe größer oder gleich dem maximalen Autogrow Prozentsatz ist. Dieses Feld ist nur aktiviert, wenn die Autogrow-Einstellung aktiviert ist.

- **Größe Erhöhen**

  Gibt die prozentuale Erhöhung an, mit der das Volumen automatisch wächst, bevor der maximale Prozentsatz des Quell-Volumes erreicht wird.

- * Raumgarantie*

Stellt sicher, dass auf dem sekundären Volume genügend Speicherplatz zugewiesen wird, damit Datentransfers immer erfolgreich durchgeführt werden. Die Einstellung für die Speicherplatzgarantie kann eine der folgenden sein:

- Datei
- Datenmenge
- Kein Beispiel: Sie können ein 200 GB-Volume haben, das Dateien mit einer Gesamtmenge von 50 GB enthält; diese Dateien enthalten jedoch nur 10 GB Daten. Volume-Garantie weist dem Ziel-Volume unabhängig vom Inhalt der Quelle 200 GB zu. Dateigarantie weist 50 GB zu, um sicherzustellen, dass genügend Speicherplatz für Dateien auf der Quelle reserviert ist. Wenn Sie in diesem Szenario „Keine“ auswählen, wird nur 10 GB auf dem Ziel für den tatsächlich genutzten Speicherplatz der Dateidaten auf der Quelle zugewiesen.

Die Speicherplatzzusage ist standardmäßig auf das Volume festgelegt.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Anwenden**

  Speichert die ausgewählten Effizienzeinstellungen und wendet diese an, wenn Sie im Dialogfeld Schutz konfigurieren auf **Anwenden** klicken.

- **Abbrechen**

  Legt die Auswahl auf und schließt das Dialogfeld Erweiterte Zieleinstellungen.

Verwandte Informationen

"Technischer Bericht 3966 von NetApp: Leitfaden zur NetApp Datenkomprimierung und Deduplizierung sowie Implementierungsleitfaden (Clustered Data ONTAP)"

Dialogfeld „Erweiterte Zieleinstellungen“

Sie können das Dialogfeld Erweiterte Zieleinstellungen verwenden, um die Einstellungen für die Speicherplatzgarantien auf einem Zielvolume zu aktivieren. Möglicherweise wählen Sie erweiterte Einstellungen aus, wenn die Speicherplatzgarantie auf der Quelle deaktiviert ist, sie jedoch auf dem Ziel aktiviert sein soll. Die Einstellungen für Deduplizierung, Komprimierung und Autogrow in einer SnapMirror Beziehung setzen sich vom Quell-Volume fort und können nicht geändert werden.

Speicherplatzgarantie

Stellt sicher, dass auf dem Ziel-Volume genügend Speicherplatz zugewiesen wird, damit Datentransfers immer erfolgreich durchgeführt werden. Die Einstellung für die Speicherplatzgarantie kann eine der folgenden sein:

- Datei

  Die Speicherplatzgarantie für Dateien steht in ONTAP 8.3 nicht zur Verfügung.

- Datenmenge

- Keine

Sie können z. B. ein 200-GB-Volume mit Dateien mit einer Gesamtmenge von 50 GB haben, diese Dateien enthalten jedoch nur 10 GB Daten. Volume-Garantie weist dem Ziel-Volume unabhängig vom Inhalt der Quelle 200 GB zu. Dateigarantie weist 50 GB zu, um sicherzustellen, dass genügend Speicherplatz für Quelldateien auf dem Ziel reserviert ist. Wenn Sie in diesem Szenario **Keine** auswählen, werden nur 10 GB auf dem Ziel für den tatsächlichen Speicherplatz zugewiesen, der von Dateidaten auf der Quelle verwendet wird.

Die Speicherplatzzusage ist standardmäßig auf das Volume festgelegt.

Dialogfeld „Wiederherstellen“

Im Dialogfeld Wiederherstellen können Sie Daten aus einer bestimmten Snapshot Kopie in einem Volume wiederherstellen.

Wiederherstellen von

Im Bereich Wiederherstellen von können Sie angeben, von wo aus Sie Daten wiederherstellen möchten.

- **Lautstärke**

  Gibt das Volume an, von dem Sie Daten wiederherstellen möchten. Standardmäßig wird das Volume ausgewählt, auf dem Sie die Wiederherstellungsaktion gestartet haben. Sie können aus der Dropdown-Liste ein anderes Volume auswählen, das alle Volumes mit Sicherungsbeziehungen zum Volume enthält, auf dem Sie die Wiederherstellungsaktion gestartet haben.

- **Snapshot Kopie**

  Gibt an, welche Snapshot Kopie zum Wiederherstellen von Daten verwendet werden soll. Standardmäßig wird die aktuellste Snapshot Kopie ausgewählt. Sie können auch eine andere Snapshot Kopie aus der Dropdown-Liste auswählen. Die Liste der Snapshot Kopien ändert sich, je nachdem, welches Volume ausgewählt wurde.

- **Liste von maximal 995 Dateien und Verzeichnissen**

  In der Liste werden standardmäßig maximal 995 Objekte angezeigt. Sie können dieses Kontrollkästchen deaktivieren, wenn alle Objekte innerhalb des ausgewählten Volumes angezeigt werden sollen. Dieser Vorgang kann einige Zeit dauern, wenn die Anzahl der Elemente sehr groß ist.

Elemente zum Wiederherstellen auswählen

Im Bereich Elemente auswählen, die wiederhergestellt werden sollen, können Sie entweder das gesamte Volume oder bestimmte Dateien und Ordner auswählen, die wiederhergestellt werden sollen. Sie können maximal 10 Dateien, Ordner oder eine Kombination aus beiden Dateien auswählen. Wenn die maximale Anzahl von Elementen ausgewählt ist, werden die Kontrollkästchen Elementauswahl deaktiviert.

- **Pfad-Feld**

  Zeigt den Pfad zu den Daten an, die wiederhergestellt werden sollen. Sie können entweder zu dem Ordner und den Dateien navigieren, die Sie wiederherstellen möchten, oder Sie können den Pfad eingeben.

  Dieses Feld ist leer, bis Sie einen Pfad auswählen oder eingeben. Klicken Sie Auf Nachdem Sie einen Pfad ausgewählt haben, werden Sie in der Verzeichnisstruktur eine Ebene nach oben verschoben.

- **Ordner- und Dateiliste**

Zeigt den Inhalt des eingegebenen Pfads an. Standardmäßig wird der Stammordner angezeigt. Durch Klicken auf einen Ordnernamen wird der Inhalt des Ordners angezeigt.

Sie können Elemente auswählen, die wiederhergestellt werden sollen:

- Wenn Sie den Pfad mit einem bestimmten Dateinamen eingeben, der im Feld Pfad angegeben ist, wird die angegebene Datei in den Ordnern und Dateien angezeigt.
- Wenn Sie einen Pfad eingeben, ohne eine bestimmte Datei anzugeben, wird der Inhalt des Ordners in der Liste Ordner und Dateien angezeigt. Sie können bis zu 10 Dateien, Ordner oder eine Kombination aus beiden Dateien für die Wiederherstellung auswählen.

  Wenn ein Ordner mehr als 995 Elemente enthält, wird eine Meldung angezeigt, die angibt, dass zu viele Elemente angezeigt werden müssen. Wenn Sie mit dem Vorgang fortfahren, werden alle Elemente im angegebenen Ordner wiederhergestellt. Sie können das Kontrollkästchen „`List maximum of 995 files and Directories`“ deaktivieren, wenn Sie alle Objekte innerhalb des ausgewählten Volumes anzeigen möchten.

NTFS-Dateiströme können nicht wiederhergestellt werden.

Wiederherstellen auf

Im Bereich Wiederherstellen können Sie angeben, wo Sie die Daten wiederherstellen möchten.

- **Originalstandort in `Volume_Name`**

  Stellt die ausgewählten Daten in das Verzeichnis auf der Quelle wieder her, von der die Daten ursprünglich gesichert wurden.

- **Alternativer Standort**

  Stellt die ausgewählten Daten an einem neuen Speicherort wieder her:

  - Pfad Wiederherstellen

    Gibt einen alternativen Pfad für die Wiederherstellung der ausgewählten Daten an. Der Pfad muss bereits vorhanden sein. Mit der Schaltfläche **Browse** navigieren Sie zum Speicherort, an dem die Daten wiederhergestellt werden sollen, oder Sie können den Pfad manuell mit dem Format Cluster://svm/Volume/path eingeben.

  - Verzeichnishierarchie beibehalten

    Wenn diese Option aktiviert ist, wird die Struktur der ursprünglichen Datei oder des ursprünglichen Verzeichnisses beibehalten. Wenn die Quelle beispielsweise /A/B/C/myfile.txt ist und das Ziel /X/Y/Z ist, stellt Unified Manager die Daten unter Verwendung der folgenden Verzeichnisstruktur auf dem Ziel wieder her: /X/Y/Z/A/B/C/myfile.txt.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Abbrechen**

  Wird Ihre Auswahl nicht mehr dargestellt und das Dialogfeld Wiederherstellen wird geschlossen.

- **Wiederherstellen**

  Wendet Ihre Auswahl an und beginnt den Wiederherstellungsprozess.

Dialogfeld „Verzeichnisse durchsuchen“

Sie können das Dialogfeld Verzeichnisse durchsuchen verwenden, wenn Sie Daten in einem Verzeichnis eines Clusters und einer SVM wiederherstellen möchten, die sich von der ursprünglichen Quelle unterscheidet. Das ursprüngliche Quell-Cluster und das ursprüngliche Volume werden standardmäßig ausgewählt.

Im Dialogfeld Verzeichnisse durchsuchen können Sie den Cluster, SVM, Volume und Verzeichnispfad auswählen, zu dem Daten wiederhergestellt werden sollen.

- * Cluster*

  Zeigt die verfügbaren Cluster-Ziele an, zu denen Sie wiederherstellen können. Standardmäßig wird der Cluster des ursprünglichen Quell-Volume ausgewählt.

- **SVM-Dropdown-Liste**

  Listet die verfügbare SVM auf, die für das ausgewählte Cluster verfügbar ist. Standardmäßig wird die SVM des ursprünglichen Quell-Volume ausgewählt.

- **Lautstärke**

  Listet alle Lese-/Schreib-Volumes einer ausgewählten SVM auf. Sie können die Volumes nach Namen und nach verfügbaren Speicherplatz filtern. Das Volumen mit dem meisten Raum wird zuerst aufgelistet, und so weiter, in absteigender Reihenfolge. Standardmäßig ist das ursprüngliche Quell-Volume ausgewählt.

- **Dateipfad Textfeld**

  Hier können Sie den Dateipfad eingeben, in den Sie Daten wiederherstellen möchten. Der von Ihnen eingegebenen Pfad muss bereits vorhanden sein.

- **Name**

  Zeigt die Namen der verfügbaren Ordner für das ausgewählte Volume an. Wenn Sie auf einen Ordner in der Liste Name klicken, werden die Unterordner angezeigt, sofern vorhanden. Die in den Ordnern enthaltenen Dateien werden nicht angezeigt. Klicken Sie Auf Nachdem Sie einen Ordner ausgewählt haben, werden Sie in der Verzeichnisstruktur eine Ebene nach oben verschoben.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Wählen Sie Das Verzeichnis** Aus

  Wendet Ihre Auswahl an und schließt das Dialogfeld Verzeichnisse durchsuchen. Wenn kein Verzeichnis ausgewählt ist, ist diese Schaltfläche deaktiviert.

- **Abbrechen**

Legt die Auswahl auf und schließt das Dialogfeld Verzeichnisse durchsuchen.

Dialogfeld „Schutz konfigurieren“

Im Dialogfeld „Sicherung konfigurieren“ können Sie SnapMirror und SnapVault Beziehungen für alle Volumes mit Lese-, Schreib- und Datensicherung auf den Clustern erstellen. So stellen Sie sicher, dass die Daten auf einem Quell-Volume oder dem primären Volume repliziert werden.

Registerkarte „Quelle“

- **Topologieansicht**

  Zeigt eine visuelle Darstellung der Beziehung an, die Sie erstellen. Die Quelle in der Topologie ist standardmäßig hervorgehoben.

- **Quellinformationen**

  Zeigt Details zu den ausgewählten Quell-Volumes an, einschließlich der folgenden Informationen:

  - Quell-Cluster-Name
  - Quell-SVM-Name
  - Kumulierte Volume-Gesamtgröße

    Zeigt die Gesamtgröße aller ausgewählten Quell-Volumes an.

  - Genutzte Gesamtgröße für das verwendete Volume

    Zeigt die verwendete Größe des kumulativen Volumens für alle ausgewählten Quell-Volumes an.

  - Quell-Volume

    Zeigt die folgenden Informationen in einer Tabelle an:

    - Quell-Volume

      Zeigt die Namen der ausgewählten Quell-Volumes an.

    - Typ

      Zeigt den Volume-Typ an.

    - SnapLock-Typ

      Zeigt den SnapLock-Typ des Volumes an. Die Optionen sind Compliance, Enterprise und nicht-SnapLock.

    - Snapshot Kopie

      Zeigt die Snapshot Kopie an, die für den Basistransfer verwendet wird. Wenn das Quell-Volume gelesen/geschrieben wird, bedeutet der Wert „Standard“ in der Spalte „Snapshot Kopie“, dass standardmäßig eine neue Snapshot Kopie erstellt wird und für den Basistransfer verwendet wird. Wenn es sich bei dem Quell-Volume um ein Datensicherungs-Volume handelt, bedeutet der Wert

„Standard“ in der Spalte Snapshot Kopie, dass keine neue Snapshot Kopie erstellt und alle vorhandenen Snapshot-Kopien an das Zielsystem übertragen werden. Wenn Sie auf den Wert der Snapshot Kopie klicken, wird eine Liste der Snapshot Kopien angezeigt, aus denen Sie eine vorhandene Snapshot Kopie auswählen können, die für den Basistransfer verwendet werden soll. Sie können keine andere Snapshot Standardkopie auswählen, wenn der Quelltyp Datensicherung ist.

Registerkarte „SnapMirror“

Ermöglicht Ihnen die Angabe eines Ziel-Clusters, einer Storage Virtual Machine (SVM) und eines Aggregats für eine Sicherungsbeziehung sowie eine Namenskonvention für Ziele bei der Erstellung einer SnapMirror Beziehung. Sie können auch eine SnapMirror-Richtlinie und einen Zeitplan angeben.

- **Topologieansicht**

  Zeigt eine visuelle Darstellung der Beziehung an, die Sie erstellen. Die SnapMirror Zielressource in der Topologie ist standardmäßig hervorgehoben.

- **Zielinformationen**

  Ermöglicht Ihnen die Auswahl der Zielressourcen für eine Schutzbeziehung:

  - Erweiterter Link

    Startet das Dialogfeld „Erweiterte Zieleinstellungen“, wenn Sie eine SnapMirror-Beziehung erstellen.

  - Cluster

    Führt die Cluster auf, die als Schutzziel-Hosts verfügbar sind. Dies ist ein erforderliches Feld.

  - Storage Virtual Machine (SVM)

    Führt die SVMs auf, die im ausgewählten Cluster verfügbar sind. Bevor die SVM-Liste gefüllt wird, muss ein Cluster ausgewählt werden. Dies ist ein erforderliches Feld.

  - Aggregat

    Führt die Aggregate auf der ausgewählten SVM auf. Bevor die Aggregatliste gefüllt wird, muss ein Cluster ausgewählt werden. Dies ist ein erforderliches Feld. In der Aggregatliste werden die folgenden Informationen angezeigt:

    - Rang

      Wenn mehrere Aggregate alle Anforderungen an ein Ziel erfüllen, gibt die Platzierung der Priorität an, in der das Aggregat aufgeführt ist, entsprechend den folgenden Bedingungen:

      A. Ein Aggregat, das sich auf einem anderen Knoten als dem Quell-Volume-Knoten befindet, wird bevorzugt, um die Fault Domain-Trennung zu ermöglichen.
      B. Ein Aggregat auf einem Node mit weniger Volumes ist vorzuziehen, um den Lastausgleich über Nodes in einem Cluster hinweg zu ermöglichen.
      C. Ein Aggregat mit mehr freiem Speicherplatz als andere Aggregate wird bevorzugt zum Kapazitätsausgleich verwendet. Ein Rang von 1 bedeutet, dass das Aggregat nach den drei Kriterien am meisten bevorzugt wird.

    - Aggregatname

Der Name des Aggregats

- Verfügbare Kapazität
- Menge an Speicherplatz, der im Aggregat für Daten verfügbar ist
- Ressourcen-Pool

  Der Name des Ressourcen-Pools, zu dem das Aggregat gehört

◦ Benennungskonvention

Gibt die standardmäßige Namenskonvention an, die auf das Ziel-Volume angewendet wird. Sie können die angegebene Namenskonvention akzeptieren oder eine benutzerdefinierte erstellen. Die Namenskonvention kann die folgenden Attribute haben: %C, %M, %V und %N, wobei %C der Clustername ist, %M der SVM-Name, %V das Quell-Volume und %N der Name des Zielknotennamens der Topologie ist.

Das Namensgebungsfeld ist rot markiert, wenn Ihr Eintrag ungültig ist. Wenn Sie auf den Link „`Preview Name`“ klicken, wird eine Vorschau der von Ihnen eingegebenen Namenskonvention angezeigt, und der Vorschautext wird dynamisch aktualisiert, wenn Sie eine Namenskonvention in das Textfeld eingeben. Ein Suffix zwischen 001 und 999 wird dem Zielnamen angehängt, wenn die Beziehung erstellt wird und ersetzt das `nnn` Dies wird im Vorschaufentext angezeigt, wobei 001 zuerst zugewiesen wird, 002 Sekunden zugewiesen werden usw.

- **Beziehungseinstellungen**

  Hier können Sie die maximale Übertragungsrate, die SnapMirror-Richtlinie und die Planung der Sicherungsbeziehung festlegen:

  ◦ Max. Übertragungsrate

  Gibt die maximale Rate an, mit der Daten zwischen Clustern über das Netzwerk übertragen werden. Wenn Sie keine maximale Übertragungsrate verwenden möchten, ist der Basistransfer zwischen den Beziehungen unbegrenzt. Wenn jedoch ONTAP 8.2 ausgeführt wird und das primäre Cluster und das sekundäre Cluster die gleiche sind, wird diese Einstellung ignoriert.

  ◦ SnapMirror Richtlinie

  Gibt die ONTAP SnapMirror-Richtlinie für die Beziehung an. Der Standardwert ist DPDefault.

  ◦ Erstellen Sie Die Policy

  Startet das Dialogfeld SnapMirror-Richtlinie erstellen, mit dem Sie eine neue SnapMirror-Richtlinie erstellen und verwenden können.

  ◦ SnapMirror Zeitplan

  Gibt die ONTAP SnapMirror-Richtlinie für die Beziehung an. Verfügbare Zeitpläne umfassen Keine, 5min, 8hour, täglich, stündlich, Und wöchentlich. Der Standardwert ist Keine. Er gibt an, dass kein Zeitplan mit der Beziehung verknüpft ist. Beziehungen ohne Zeitpläne haben keine Verzögerungswerte, wenn sie nicht zu einem Storage-Service gehören.

  ◦ Zeitplan Erstellen

  Startet das Dialogfeld „Zeitplan erstellen“, in dem Sie einen neuen SnapMirror Zeitplan erstellen

können.

Registerkarte „SnapVault“

Ermöglicht Ihnen die Angabe eines sekundären Clusters, einer SVM und eines Aggregats für eine Sicherungsbeziehung sowie eine Namenskonvention für sekundäre Volumes während der Erstellung einer SnapVault-Beziehung. Sie können auch eine SnapVault-Richtlinie und einen Zeitplan angeben.

- **Topologieansicht**

  Zeigt eine visuelle Darstellung der Beziehung an, die Sie erstellen. Die sekundäre SnapVault Ressource in der Topologie ist standardmäßig hervorgehoben.

- **Sekundärinformationen**

  Ermöglicht Ihnen die Auswahl der sekundären Ressourcen für eine Sicherungsbeziehung:

  - Erweiterter Link

    Öffnet das Dialogfeld Erweiterte sekundäre Einstellungen.

  - Cluster

    Führt die Cluster auf, die als sekundäre Schutz-Hosts verfügbar sind. Dies ist ein erforderliches Feld.

  - Storage Virtual Machine (SVM)

    Führt die SVMs auf, die im ausgewählten Cluster verfügbar sind. Bevor die SVM-Liste gefüllt wird, muss ein Cluster ausgewählt werden. Dies ist ein erforderliches Feld.

  - Aggregat

    Führt die Aggregate auf der ausgewählten SVM auf. Bevor die Aggregatliste gefüllt wird, muss ein Cluster ausgewählt werden. Dies ist ein erforderliches Feld. In der Aggregatliste werden die folgenden Informationen angezeigt:

    - Rang

      Wenn mehrere Aggregate alle Anforderungen an ein Ziel erfüllen, gibt die Platzierung der Priorität an, in der das Aggregat aufgeführt ist, entsprechend den folgenden Bedingungen:

      A. Ein Aggregat, das sich auf einem anderen Knoten als dem primären Volume-Knoten befindet, wird bevorzugt, um die Trennung der Fehlerdomäne zu ermöglichen.
      B. Ein Aggregat auf einem Node mit weniger Volumes ist vorzuziehen, um den Lastausgleich über Nodes in einem Cluster hinweg zu ermöglichen.
      C. Ein Aggregat mit mehr freiem Speicherplatz als andere Aggregate wird bevorzugt zum Kapazitätsausgleich verwendet. Ein Rang von 1 bedeutet, dass das Aggregat nach den drei Kriterien am meisten bevorzugt wird.

    - Aggregatname

      Der Name des Aggregats

    - Verfügbare Kapazität

- Menge an Speicherplatz, der im Aggregat für Daten verfügbar ist
- Ressourcen-Pool

  Der Name des Ressourcen-Pools, zu dem das Aggregat gehört

◦ Benennungskonvention

Gibt die standardmäßige Namenskonvention an, die auf das sekundäre Volume angewendet wird. Sie können die angegebene Namenskonvention akzeptieren oder eine benutzerdefinierte erstellen. Die Namenskonvention kann folgende Attribute haben: %C, %M, %V und %N, wobei %C der Clustername ist, %M der SVM-Name, %V das Quell-Volume und %N der Name des sekundären Topologieknoten ist.

Das Namensgebungsfeld ist rot markiert, wenn Ihr Eintrag ungültig ist. Wenn Sie auf den Link „`Preview Name`“ klicken, wird eine Vorschau der von Ihnen eingegebenen Namenskonvention angezeigt, und der Vorschautext wird dynamisch aktualisiert, wenn Sie eine Namenskonvention in das Textfeld eingeben. Wenn Sie einen ungültigen Wert eingeben, werden die ungültigen Informationen als rote Fragezeichen im Vorschaubereich angezeigt. Ein Suffix zwischen 001 und 999 wird dem sekundären Namen angehängt, wenn die Beziehung erstellt wird und ersetzt das `nnn` Dies wird im Vorschaufentext angezeigt, wobei 001 zuerst zugewiesen wird, 002 Sekunden zugewiesen werden usw.

- **Beziehungseinstellungen**

  Ermöglicht Ihnen die Angabe der maximalen Übertragungsrate, der SnapVault-Richtlinie und des SnapVault-Zeitplans, die die Sicherungsbeziehung verwendet:

  ◦ Max. Übertragungsrate

  Gibt die maximale Rate an, mit der Daten zwischen Clustern über das Netzwerk übertragen werden. Wenn Sie keine maximale Übertragungsrate verwenden möchten, ist der Basistransfer zwischen den Beziehungen unbegrenzt. Wenn jedoch ONTAP 8.2 ausgeführt wird und das primäre Cluster und das sekundäre Cluster die gleiche sind, wird diese Einstellung ignoriert.

  ◦ SnapVault-Richtlinie

  Gibt die ONTAP SnapVault-Richtlinie für die Beziehung an. Der Standardwert ist XDPDefault.

  ◦ Erstellen Sie Die Policy

  Öffnet das Dialogfeld SnapVault-Richtlinie erstellen, in dem Sie eine neue SnapVault-Richtlinie erstellen und verwenden können.

  ◦ SnapVault Zeitplan

  Gibt den ONTAP SnapVault-Zeitplan für die Beziehung an. Verfügbare Zeitpläne umfassen Keine, 5min, 8hour, täglich, stündlich, Und wöchentlich. Der Standardwert ist Keine. Er gibt an, dass kein Zeitplan mit der Beziehung verknüpft ist. Beziehungen ohne Zeitpläne haben keine Verzögerungswerte, wenn sie nicht zu einem Storage-Service gehören.

  ◦ Zeitplan Erstellen

  Öffnet das Dialogfeld Zeitplan erstellen, in dem Sie einen SnapVault-Zeitplan erstellen können.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Abbrechen**

  Die Auswahl wird von der Option „Schutz konfigurieren“ entstellt und das Dialogfeld „Schutz konfigurieren“ wird geschlossen.

- **Anwenden**

  Wendet Ihre Auswahl an und beginnt den Schutzprozess.

Dialogfeld „Zeitplan erstellen“

Im Dialogfeld „Zeitplan erstellen“ können Sie einen einfachen oder erweiterten Sicherungsplan für SnapMirror und SnapVault Beziehungsübertragungen erstellen. Möglicherweise erstellen Sie einen neuen Zeitplan, mit dem sich die Häufigkeit der Datentransfers durch häufige Datenaktualisierungen erhöhen lässt. Zudem können Sie bei unregelmäßigen Datenänderungen einen weniger Zeitplan erstellen.

Zeitpläne können nicht für SnapMirror synchrone Beziehungen konfiguriert werden.

- **Zielcluster**

  Der Name des Clusters, den Sie auf der Registerkarte SnapVault oder auf der Registerkarte SnapMirror im Dialogfeld Schutz konfigurieren ausgewählt haben.

- **Terminplanname**

  Den Namen, den Sie für den Zeitplan angeben. Zeitplannamen können aus den Zeichen A bis Z, a bis z, 0 bis 9 sowie einem der folgenden Sonderzeichen bestehen: ! @ # € % ^ & * ( ) _ -. Die Namen des Zeitplans dürfen die folgenden Zeichen nicht enthalten: < >.

- **Basic oder Advanced**

  Der Zeitplanmodus, den Sie verwenden möchten.

  Der Basismodus umfasst die folgenden Elemente:

  - Wiederholen

    Wie oft eine geplante Übertragung erfolgt. Zur Auswahl stehen stündlich, täglich und wöchentlich.

  - Tag

    Wenn eine Wiederholung von wöchentlich ausgewählt wird, wird der Tag der Woche, an dem eine Übertragung stattfindet, angezeigt.

  - Zeit

    Wenn Daily oder Weekly ausgewählt ist, wird die Uhrzeit des Transfers angezeigt.

    Der erweiterte Modus umfasst die folgenden Elemente:

◦ Monaten

Eine kommagetrennte numerische Liste, die die Monate des Jahres darstellt. Gültige Werte betragen 0 bis 11, wobei der Wert 0 im Januar steht usw. Dieses Element ist optional. Wenn Sie das Feld leer lassen, müssen Sie jeden Monat Transfers machen.

◦ Tage

Eine kommagetrennte numerische Liste, die den Tag des Monats darstellt. Gültige Werte sind 1 bis 31. Dieses Element ist optional. Wenn Sie das Feld leer lassen, bedeutet dies, dass ein Transfer jeden Tag des Monats stattfindet.

◦ Wochentage

Eine kommagetrennte numerische Liste, die die Wochentage darstellt. Gültige Werte sind 0 bis 6, wobei 0 für Sonntag usw. gelten. Dieses Element ist optional. Wenn Sie das Feld leer lassen, bedeutet dies, dass ein Transfer jeden Tag der Woche stattfindet. Wenn ein Wochentag, jedoch ein Tag des Monats nicht angegeben wird, erfolgt eine Übertragung nur am angegebenen Wochentag und nicht am Tag.

◦ Stunden

Eine kommagetrennte numerische Liste, die die Anzahl der Stunden pro Tag darstellt. Gültige Werte sind 0 bis 23, wobei 0 für Mitternacht stehen. Dieses Element ist optional.

◦ Minuten

Eine kommagetrennte numerische Liste, die die Minuten in einer Stunde darstellt. Gültige Werte sind 0 bis 59. Dieses Element ist erforderlich.

Dialogfeld SnapMirror-Richtlinie erstellen

Im Dialogfeld Richtlinie erstellen können Sie eine Richtlinie erstellen, mit der Sie die Priorität für SnapMirror Transfers festlegen können. Anhand von Richtlinien wird die Effizienz der Transfers von der Quelle zum Ziel maximiert.

- **Zielcluster**

  Der Name des Clusters, den Sie auf der Registerkarte SnapMirror im Dialogfeld „Schutz konfigurieren“ ausgewählt haben.

- **Ziel-SVM**

  Der Name der SVM, die Sie auf der Registerkarte SnapMirror im Dialogfeld Schutz konfigurieren ausgewählt haben.

- **Policy Name**

  Der Name, den Sie für die neue Richtlinie angeben. Richtliniennamen können aus den Zeichen A bis Z, a bis z, 0 bis 9, Punkt (.), Bindestrich (-), Und Unterstrich (_).

- * Priorität Übertragen*

  Die Priorität, mit der ein Transfer für asynchrone Vorgänge ausgeführt wird. Sie können entweder Normal

oder Niedrig auswählen. Beziehungen mit Richtlinien übertragen, die eine normale Übertragungspriorität festlegen, die vor den Richtlinien ausgeführt wird, die eine niedrige Übertragungspriorität angeben.

- **Kommentar**

  Ein optionales Feld, in dem Sie Kommentare zur Richtlinie hinzufügen können.

- **Neustart Übertragen**

  Gibt an, welche Neustartaktion ausgeführt werden soll, wenn eine Übertragung durch einen Abbruch oder einen beliebigen Ausfall unterbrochen wird, z. B. ein Netzwerkausfall. Sie können eine der folgenden Optionen auswählen:

  - Immer

    Gibt an, dass vor dem Neustart eines Transfers eine neue Snapshot Kopie erstellt wird, wird der Transfer dann, wenn eine vorhanden ist, von einem Checkpoint neu gestartet, gefolgt von einem inkrementellen Transfer aus der neu erstellten Snapshot Kopie.

  - Nie

    Gibt an, dass unterbrochene Transfers nie neu gestartet werden.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Abbrechen**

  Legt die Auswahl auf und schließt das Dialogfeld Schutz konfigurieren.

- **Anwenden**

  Wendet Ihre Auswahl an und beginnt den Schutzprozess.

Dialogfeld SnapVault-Richtlinie erstellen

Im Dialogfeld SnapVault-Richtlinie erstellen können Sie eine Richtlinie erstellen, in der Sie die Priorität für SnapVault-Transfers festlegen können. Sie verwenden Richtlinien, um die Effizienz der Übertragungen vom primären zum sekundären Volume zu maximieren.

- **Zielcluster**

  Der Name des Clusters, den Sie im Dialogfeld Schutz konfigurieren auf der Registerkarte SnapVault ausgewählt haben.

- **Ziel-SVM**

  Der Name der SVM, die Sie im Dialogfeld Schutz konfigurieren auf der Registerkarte SnapVault ausgewählt haben.

- **Policy Name**

  Der Name, den Sie für die neue Richtlinie angeben. Richtliniennamen können aus den Zeichen A bis Z, a

bis z, 0 bis 9, Punkt (.), Bindestrich (-), Und Unterstrich (_).

- * Priorität Übertragen*

  Die Priorität, mit der die Übertragung ausgeführt wird. Sie können entweder Normal oder Niedrig auswählen. Beziehungen mit Richtlinien übertragen, die eine normale Übertragungspriorität festlegen, die vor den Richtlinien ausgeführt wird, die eine niedrige Übertragungspriorität angeben. Die Standardeinstellung ist Normal.

- **Kommentar**

  Ein optionales Feld, in das Sie bis zu 255 Zeichen zur SnapVault-Richtlinie hinzufügen können.

- **Zugriffszeit Ignorieren**

  Gibt an, ob inkrementelle Transfers für Dateien ignoriert werden, für die nur die Zugriffszeit geändert wurde.

- **Replikationbeschriftung**

  Führt in einer Tabelle die Regeln auf, die mit von ONTAP ausgewählten Snapshot Kopien verknüpft sind und über eine bestimmte Replizierungsbeschriftung in einer Richtlinie verfügen. Folgende Informationen und Maßnahmen stehen ebenfalls zur Verfügung:

  - Befehlsschaltflächen

    Mit den Befehlsschaltflächen können Sie die folgenden Aktionen ausführen:

    - Zusatz

      Ermöglicht es Ihnen, ein Etikett und eine Aufbewahrungsanzahl für Snapshot Kopien zu erstellen.

    - Anzahl Der Aufbewahrung Bearbeiten

      Ermöglicht Ihnen, die Anzahl der Aufbewahrung eines vorhandenen Snapshot-Kopieretiketts zu ändern. Der Aufbewahrungszähler muss eine Zahl zwischen 1 und 251 sein. Die Summe aller Aufbewahrungszählungen für alle Regeln darf 251 nicht überschreiten.

    - Löschen

      Ermöglicht Ihnen das Löschen eines vorhandenen Etiketts für Snapshot Kopien.

  - Label Für Snapshot Kopie

    Zeigt den Namen der Snapshot Kopie an. Wenn Sie ein oder mehrere Volumes mit derselben lokalen Snapshot-Kopie-Richtlinie auswählen, wird ein Eintrag für jedes Etikett in der Richtlinie angezeigt. Wenn Sie mehrere Volumes auswählen, die zwei oder mehr lokale Snapshot-Kopie-Richtlinien haben, werden in der Tabelle alle Labels aus allen Richtlinien angezeigt

  - Zeitplan

    Zeigt den Zeitplan an, der mit jedem Etikett der Snapshot Kopie verknüpft ist. Wenn eine Bezeichnung mehr als einen Zeitplan enthält, werden die Zeitpläne für diese Bezeichnung in einer kommagetrennten Liste angezeigt. Wenn Sie mehrere Volumes mit demselben Etikett, jedoch mit unterschiedlichen Zeitplänen auswählen, wird im Zeitplan „`verschiedene`“ angezeigt, um anzugeben, dass mehr als ein Zeitplan den ausgewählten Volumes zugeordnet ist.

◦ Anzahl Der Zielaufbewahrungsziele

Zeigt die Anzahl der Snapshot Kopien mit dem angegebenen Label an, die auf dem sekundären SnapVault aufbewahrt werden. Aufbewahrungszählungen für Etiketten mit mehreren Zeitplänen zeigen die Summe der Aufbewahrungsanzahl für jedes Etikett und jedes Terminplanpaar an. Wenn Sie mehrere Volumes mit zwei oder mehr lokalen Snapshot-Kopie-Richtlinien auswählen, ist die Anzahl der Aufbewahrung leer.

Dialogfeld „Beziehung bearbeiten“

Sie können eine bestehende Schutzbeziehung bearbeiten, um die maximale Übertragungsrate, die Schutzrichtlinie oder den Schutzzeitplan zu ändern.

Zielinformationen

- **Zielcluster**

  Der Name des ausgewählten Ziel-Clusters.

- **Ziel-SVM**

  Der Name der ausgewählten SVM

- **Beziehungseinstellungen**

  Hier können Sie die maximale Übertragungsrate, die SnapMirror-Richtlinie und die Planung der Sicherungsbeziehung festlegen:

  ◦ Max. Übertragungsrate

  Gibt die maximale Geschwindigkeit an, mit der Basisdaten zwischen Clustern über das Netzwerk übertragen werden. Wenn diese Option ausgewählt ist, ist die Netzwerkbandbreite auf den von Ihnen angegebenen Wert beschränkt. Sie können einen numerischen Wert eingeben und dann entweder Kilobyte pro Sekunde (kbps), Megabyte pro Sekunde (MBit/s), Gigabyte pro Sekunde (Gbit/s) oder Terabyte pro Sekunde (Tbit/s) auswählen. Die maximale Übertragungsrate, die Sie angeben, muss größer als 1 kbps und weniger als 4 Tbps sein. Wenn Sie keine maximale Übertragungsrate verwenden möchten, ist der Basistransfer zwischen den Beziehungen unbegrenzt. Wenn das primäre Cluster und das sekundäre Cluster identisch sind, wird diese Einstellung deaktiviert.

  ◦ SnapMirror Richtlinie

  Gibt die ONTAP SnapMirror-Richtlinie für die Beziehung an. Der Standardwert ist DPDefault.

  ◦ Erstellen Sie Die Policy

  Startet das Dialogfeld SnapMirror-Richtlinie erstellen, mit dem Sie eine neue SnapMirror-Richtlinie erstellen und verwenden können.

  ◦ SnapMirror Zeitplan

  Gibt die ONTAP SnapMirror-Richtlinie für die Beziehung an. Verfügbare Zeitpläne umfassen Keine, 5min, 8hour, täglich, stündlich, Und wöchentlich. Der Standardwert ist Keine. Er gibt an, dass kein Zeitplan mit der Beziehung verknüpft ist. Beziehungen ohne Zeitpläne haben keine Verzögerungswerte, wenn sie nicht zu einem Storage-Service gehören.

◦ Zeitplan Erstellen

Startet das Dialogfeld „Zeitplan erstellen“, in dem Sie einen neuen SnapMirror Zeitplan erstellen können.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Abbrechen**

  Legt die Auswahl auf und schließt das Dialogfeld Schutz konfigurieren.

- **Senden**

  Wendet Ihre Auswahl an und schließt das Dialogfeld Beziehung bearbeiten.

Dialogfeld „Initialisierung/Aktualisierung“

Das Dialogfeld Initialisieren/Aktualisieren ermöglicht Ihnen die Durchführung einer ersten Basistransfer für eine neue Schutzbeziehung oder die Aktualisierung einer Beziehung, wenn sie bereits initialisiert ist und Sie ein manuelles, ungeplantes, inkrementelles Update durchführen möchten.

Registerkarte Übertragungsoptionen

Auf der Registerkarte Übertragungsoptionen können Sie die Initialisierungspriorität einer Übertragung ändern und die während der Übertragung verwendete Bandbreite ändern.

- * Priorität Übertragen*

  Die Priorität, mit der die Übertragung ausgeführt wird. Sie können entweder Normal oder Niedrig auswählen. Beziehungen mit Richtlinien, die eine normale Übertragungspriorität festlegen, die vor denen ausgeführt wird, die eine niedrige Übertragungspriorität angeben. Standardmäßig ist „Normal“ ausgewählt.

- **Max. Transferrate**

  Gibt die maximale Rate an, mit der Daten zwischen Clustern über das Netzwerk übertragen werden. Wenn Sie keine maximale Übertragungsrate verwenden möchten, ist der Basistransfer zwischen den Beziehungen unbegrenzt. Wenn jedoch ONTAP 8.2 ausgeführt wird und das primäre Cluster und das sekundäre Cluster die gleiche sind, wird diese Einstellung ignoriert. Wenn Sie mehrere Beziehungen mit unterschiedlichen maximalen Transferraten auswählen, können Sie eine der folgenden maximalen Transferraten festlegen:

  ◦ Verwenden Sie Werte, die bei der Einrichtung oder Bearbeitung einzelner Beziehungen angegeben sind

    Bei Auswahl dieser Option verwenden Initialisierungsvorgänge und Updates die maximale Übertragungsrate, die zum Zeitpunkt der Erstellung oder Bearbeitung der einzelnen Beziehungen festgelegt wurde. Dieses Feld ist nur verfügbar, wenn mehrere Beziehungen mit unterschiedlichen Transferraten initialisiert oder aktualisiert werden.

  ◦ Unbegrenzt

Zeigt an, dass es keine Bandbreitenbeschränkung bei Übertragungen zwischen Beziehungen gibt. Dieses Feld ist nur verfügbar, wenn mehrere Beziehungen mit unterschiedlichen Transferraten initialisiert oder aktualisiert werden.

- Beschränken Sie die Bandbreite auf

  Wenn diese Option ausgewählt ist, ist die Netzwerkbandbreite auf den von Ihnen angegebenen Wert beschränkt. Sie können einen numerischen Wert eingeben und dann entweder Kilobyte pro Sekunde (kbps), Megabyte pro Sekunde (Mbps), Gigabyte pro Sekunde (Gbps) oder Terabyte pro Sekunde (Tbit/s) auswählen. Die maximale Übertragungsrate, die Sie angeben, muss größer als 1 kbps und weniger als 4 Tbps sein.

Registerkarte „Snapshot Kopien der Quelle“

Auf der Registerkarte Snapshot Kopien der Quelle werden die folgenden Informationen über die Snapshot Kopie der Quelle angezeigt, die für den Basistransfer verwendet wird:

- **Quellvolumen**

  Zeigt die Namen der entsprechenden Quell-Volumes an.

- **Zielvolumen**

  Zeigt die Namen der ausgewählten Zielvolumes an.

- **Quelltyp**

  Zeigt den Volume-Typ an. Der Typ kann entweder Lesen/Schreiben oder Datenschutz sein.

- **Snapshot Kopie**

  Zeigt die Snapshot Kopie an, die für den Datentransfer verwendet wird. Wenn Sie auf den Wert der Snapshot Kopie klicken, wird das Dialogfeld Quell-Snapshot Kopie auswählen angezeigt, in dem Sie abhängig von dem Typ der Sicherungsbeziehung und dem Vorgang, den Sie durchführen, eine bestimmte Snapshot Kopie für Ihren Transfer auswählen können. Die Option, eine andere Snapshot Kopie anzugeben, ist nicht für Datensicherungsquellen verfügbar.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Abbrechen**

  Legt die Auswahl auf und schließt das Dialogfeld Initialisieren/Aktualisieren.

- **Senden**

  Speichert Ihre Auswahl und startet den Job initialisieren oder aktualisieren.

Dialogfeld erneut synchronisieren

Das Dialogfeld „Resynchronisieren“ ermöglicht Ihnen die erneuten Synchronisierung von Daten auf einer SnapMirror oder SnapVault-Beziehung, die zuvor beschädigt war, und danach wurde das Ziel zu einem Datenträger mit Lese-/Schreibzugriff hergestellt. Sie

können auch neu synchronisieren, wenn eine erforderliche gemeinsame Snapshot Kopie auf dem Quell-Volume gelöscht wird, sodass SnapMirror oder SnapVault Updates fehlschlagen.

Registerkarte Resynchronisierung Optionen

Auf der Registerkarte „Resynchronisierungsoptionen“ können Sie die Übertragungspriorität und die maximale Übertragungsrate für die Sicherungsbeziehung festlegen, die neu synchronisiert wird.

- * Priorität Übertragen*

  Die Priorität, mit der die Übertragung ausgeführt wird. Sie können entweder Normal oder Niedrig auswählen. Beziehungen zu Richtlinien, die eine normale Übertragungspriorität festlegen, die vor der Ausführung mit Richtlinien ausgeführt wird, die eine niedrige Übertragungspriorität angeben.

- **Max. Transferrate**

  Gibt die maximale Rate an, mit der Daten zwischen Clustern über das Netzwerk übertragen werden. Wenn diese Option ausgewählt ist, ist die Netzwerkbandbreite auf den von Ihnen angegebenen Wert beschränkt. Sie können einen numerischen Wert eingeben und dann entweder Kilobyte pro Sekunde (kbps), Megabyte pro Sekunde (Mbps), Gigabyte pro Sekunde (Gbps) oder Tbps auswählen. Wenn Sie keine maximale Übertragungsrate verwenden möchten, ist der Basistransfer zwischen den Beziehungen unbegrenzt. Wenn Sie jedoch ONTAP 8.2 verwenden und der primäre Cluster und das sekundäre Cluster identisch sind, wird diese Einstellung deaktiviert.

Registerkarte „Snapshot Kopien der Quelle“

Auf der Registerkarte Snapshot Kopien der Quelle werden die folgenden Informationen über die Snapshot Kopie der Quelle angezeigt, die für den Basistransfer verwendet wird:

- **Quellvolumen**

  Zeigt die Namen der entsprechenden Quell-Volumes an.

- **Zielvolumen**

  Zeigt die Namen der ausgewählten Zielvolumes an.

- **Quelltyp**

  Zeigt den Volume-Typ an: Lese-/Schreib- oder Datenschutz.

- **Snapshot Kopie**

  Zeigt die Snapshot Kopie an, die für den Datentransfer verwendet wird. Durch Klicken auf den Wert der Snapshot Kopie wird das Dialogfeld Quell-Snapshot Kopie auswählen angezeigt, in dem abhängig von dem Typ der Sicherungsbeziehung und dem von Ihnen laufenden Vorgang eine bestimmte Snapshot Kopie für Ihren Transfer auswählen kann.

Befehlsschaltflächen

- **Senden**

  Startet die Neusynchronisierung und schließt das Dialogfeld „Resynchronisieren“.

- **Abbrechen**

  Bricht Ihre Auswahl ab und schließt das Dialogfeld „erneut synchronisieren“.

Wählen Sie das Dialogfeld Snapshot-Kopie der Quelle aus

Sie verwenden das Dialogfeld Quell-Snapshot Kopie auswählen, um eine bestimmte Snapshot Kopie zum Übertragen von Daten zwischen Sicherungsbeziehungen auszuwählen, oder Sie wählen das Standardverhalten aus, das je nach Initialisierung, Aktualisierung oder erneuten Synchronisierung einer Beziehung variiert. Außerdem können Sie wählen, ob die Beziehung eine SnapMirror oder SnapVault ist.

Standard

Ermöglicht Ihnen, das Standardverhalten auszuwählen, um zu ermitteln, welche Snapshot Kopie zum Initialisieren, Aktualisieren und erneuten Synchronisieren von Transfers für SnapVault- und SnapMirror-Beziehungen verwendet wird.

Wenn Sie einen SnapVault-Transfer durchführen, lautet das Standardverhalten für jeden Vorgang wie folgt:

Betrieb	Standardmäßiges SnapVault-Verhalten, wenn die Quelle Lese-/Schreibzugriff ist	Standardmäßiges SnapVault-Verhalten, wenn Quelle Datensicherung (DP) ist
Initialisieren	Erstellt eine neue Snapshot Kopie und überträgt sie.	Überträgt die zuletzt exportierte Snapshot Kopie.
Aktualisierung	Überträgt nur gekennzeichnete Snapshot-Kopien, wie in der Richtlinie angegeben	Überträgt die zuletzt exportierte Snapshot Kopie.
Neu Synchronisieren	Überträgt alle gekennzeichneten Snapshot-Kopien, die nach der neuesten gemeinsamen Snapshot-Kopie erstellt wurden.	Überträgt die neueste beschriftete Snapshot Kopie.

Wenn Sie einen SnapMirror Transfer durchführen, verhält sich das Standardverhalten jedes Vorgangs wie folgt:

Betrieb	Standardverhalten von SnapMirror	Standardverhalten von SnapMirror bei einer Beziehung zweiter Hop in einer SnapMirror-zu-SnapMirror-Kaskadierung
Initialisieren	Erstellt eine neue Snapshot Kopie und überträgt sie sowie alle Snapshot Kopien, die vor der neuen Snapshot Kopie erstellt wurden.	Überträgt alle Snapshot Kopien von der Quelle.

Betrieb	Standardverhalten von SnapMirror	Standardverhalten von SnapMirror bei einer Beziehung zweiter Hop in einer SnapMirror-zu-SnapMirror-Kaskadierung
Aktualisierung	Erstellt eine neue Snapshot Kopie und überträgt sie sowie alle Snapshot Kopien, die vor der neuen Snapshot Kopie erstellt wurden.	Überträgt alle Snapshot Kopien.
Neu Synchronisieren	Erstellt eine neue Snapshot Kopie und überträgt anschließend alle Snapshot Kopien vom Quellspeicherort.	Überträgt alle Snapshot Kopien vom sekundären Volume auf das tertiäre Volume und löscht alle Daten, die nach der Erstellung der neuesten allgemeinen Snapshot Kopie hinzugefügt wurden.

Vorhandene Snapshot Kopie

Ermöglicht Ihnen, eine vorhandene Snapshot Kopie aus der Liste auszuwählen, wenn die Auswahl von Snapshot Kopien für diesen Vorgang zulässig ist.

- **Snapshot Kopie**

  Zeigt die vorhandenen Snapshot Kopien an, aus denen Sie für eine Übertragung auswählen können.

- **Erstellungsdatum**

  Zeigt das Datum und die Uhrzeit der Erstellung der Snapshot Kopie an. Snapshot Kopien werden von Neuesten bis zuletzt aufgelistet, wobei sich das neueste an der Spitze der Liste befinden.

Wenn Sie einen SnapVault Transfer durchführen und Sie eine vorhandene Snapshot Kopie auswählen möchten, um sie von einer Quelle auf ein Ziel zu übertragen, sieht das folgende Verhalten für jeden Vorgang aus:

Betrieb	Verhalten von SnapVault beim Angeben einer Snapshot Kopie	Verhalten von SnapVault bei Angabe einer Snapshot Kopie in einer Kaskadierung
Initialisieren	Überträgt die angegebene Snapshot Kopie.	Die Auswahl von Quell-Snapshot Kopien wird für Datensicherungs-Volumes nicht unterstützt.
Aktualisierung	Überträgt die angegebene Snapshot Kopie.	Die Auswahl von Quell-Snapshot Kopien wird für Datensicherungs-Volumes nicht unterstützt.
Neu Synchronisieren	Überträgt die ausgewählte Snapshot Kopie.	Die Auswahl von Quell-Snapshot Kopien wird für Datensicherungs-Volumes nicht unterstützt.

Wenn Sie einen SnapMirror Transfer durchführen und Sie eine vorhandene Snapshot Kopie auswählen möchten, um sie von einer Quelle auf ein Ziel zu übertragen, sieht die Vorgehensweise für jeden Vorgang wie folgt aus:

Betrieb	Verhalten von SnapMirror beim Angeben einer Snapshot Kopie	Verhalten von SnapMirror bei der Angabe einer Snapshot Kopie in einer Kaskadierung
Initialisieren	Überträgt alle Snapshot Kopien auf der Quelle bis zur angegebenen Snapshot Kopie.	Die Auswahl von Quell-Snapshot Kopien wird für Datensicherungs-Volumes nicht unterstützt.
Aktualisierung	Überträgt alle Snapshot Kopien auf der Quelle bis zur angegebenen Snapshot Kopie.	Die Auswahl von Quell-Snapshot Kopien wird für Datensicherungs-Volumes nicht unterstützt.
Neu Synchronisieren	Überträgt alle Snapshot Kopien vom Quell- bis zur ausgewählten Snapshot Kopie. Anschließend werden alle Daten gelöscht, die nach der Erstellung der neuesten allgemeinen Snapshot Kopie hinzugefügt wurden.	Die Auswahl von Quell-Snapshot Kopien wird für Datensicherungs-Volumes nicht unterstützt.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Senden**

  Reicht Ihre Auswahl ein und schließt das Dialogfeld QuellSnapshot Kopie auswählen.

- **Abbrechen**

  Legt die Auswahl auf und schließt das Dialogfeld „Quell-Snapshot-Kopie auswählen“.

Dialogfeld „Resync“ umkehren

Wenn eine Sicherungsbeziehung besteht, die beschädigt ist, da das Quell-Volume deaktiviert wurde und das Ziel ein Lese-/Schreib-Volume erstellt wird, kann durch die umgekehrte Resynchronisierung die Richtung der Beziehung rückgängig gemacht werden, so dass das Ziel zur neuen Quelle wird und das Quell-Volume zum neuen Ziel wird.

Wenn ein Notfall das Quellvolume in Ihrer Schutzbeziehung deaktiviert, können Sie das Zielvolume für die Bereitstellung von Daten verwenden, indem Sie es in Lese-/Schreibzugriff konvertieren, während Sie die Quelle reparieren oder ersetzen, die Quelle aktualisieren und die Beziehung wiederherstellen. Wenn Sie einen umgekehrten Neusynchronisierung durchführen, werden Daten auf der Quelle, die neuer als die Daten auf der gemeinsamen Snapshot Kopie sind, gelöscht.

Vor der Neusynchronisierung

Zeigt die Quelle und das Ziel einer Beziehung an, bevor eine umgekehrte Resynchronisierung durchgeführt wird.

- **Quellvolumen**

  Name und Standort des Quell-Volumes vor einer umgekehrten Resynchronisierung .

- **Zielvolumen**

  Name und Standort des Zielvolumens vor einer umgekehrten Resync-Operation .

Nach umgekehrter Resynchronisierung

Zeigt an, was Quelle und Ziel einer Beziehung nach einer Reserve-Resynchronisierung ist.

- **Quellvolumen**

  Name und Standort des Quell-Volume nach umgekehrter Resynchronisierung

- **Zielvolumen**

  Name und Standort des Ziel-Volumes nach einer umgekehrten Resync-Operation.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aktionen ausführen:

- **Senden**

  Startet die umgekehrte Neusynchronisierung.

- **Abbrechen**

  Schließt das Dialogfeld „Resync umkehren“, ohne einen umgekehrten Resync-Vorgang zu initiieren.

Sicherungs-/Volume-Beziehungen Seite

Auf der Seite „Schutz/Volume-Beziehungen“ werden Informationen zu Sicherungsbeziehungen im Storage-System angezeigt.

Verwenden Sie die Schaltfläche **Exportieren**, um die Details aller Beziehungen in kommagetrennte Werte zu exportieren (`.csv`) Datei.

- **Beziehungsstatus**

  Zeigt den aktuellen Status der Schutzbeziehung an.

  Der Status kann ein Fehler sein (), Warnung (Oder normal ().

- **Lag-Status**

  Zeigt den Verzögerungsstatus für verwaltete Beziehungen und für nicht verwaltete Beziehungen an, die mit

dieser Beziehung verknüpft sind. Der Verzögerungsstatus kann sein:

- Fehler ( )

  Die Verzögerungsdauer ist größer oder gleich dem lag-Fehlerschwellenwert.

- Warnung ( )

  Die Verzögerungsdauer ist größer oder gleich dem lag-Warnungsschwellenwert.

- Normal ( )

  Die Verzögerungsdauer liegt innerhalb der normalen Grenzwerte.

- Keine Angabe

  Der lag-Status gilt nicht für synchrone Beziehungen, da ein Zeitplan nicht konfiguriert werden kann.

- **Transferstatus**

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

  - Wird Abgebrochen

    SnapMirror-Transfers sind aktiviert; ein Vorgang, bei dem der Transfer abgebrochen wird, während das Checkpoint entfernt wird.

  - Prüfen

    Das Zielvolumen wird einer Diagnose-Prüfung unterzogen und es wird keine Übertragung durchgeführt.

  - Abschließen

    SnapMirror Transfers sind aktiviert. Das Volume befindet sich derzeit in der Phase nach dem Transfer für inkrementelle SnapVault Transfers.

  - Leerlauf

    Transfers sind aktiviert, und es wird keine Übertragung durchgeführt.

  - Synchronisiert

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

  - Out-of-Sync

    Die Daten im Ziel-Volume werden nicht mit dem Quell-Volume synchronisiert.

  - Vorbereitung

    SnapMirror Transfers sind aktiviert. Das Volume befindet sich derzeit in der Phase vor der Übertragung für inkrementelle SnapVault Transfers.

  - Warteschlange

SnapMirror Transfers sind aktiviert. Es werden keine Transfers durchgeführt.

- Stillgelegt

  SnapMirror Transfers sind deaktiviert. Es wird keine Übertragung durchgeführt.

- Wird Stillgelegt

  Ein SnapMirror Transfer läuft. Zusätzliche Transfers sind deaktiviert.

- Übertragung

  SnapMirror Transfers sind aktiviert, und ein Transfer läuft.

- Übergang

  Der asynchrone Datentransfer aus dem Quell- zum Ziel-Volume ist abgeschlossen, und der Übergang zum synchronen Betrieb wurde gestartet.

- Warten

  Ein SnapMirror Transfer wurde initiiert, aber einige zugehörige Aufgaben warten darauf, in die Warteschlange verschoben zu werden.

- **Beziehungstyp**

  Zeigt den Beziehungstyp an, mit dem ein Volume repliziert wird. Beziehungstypen:

  - Asynchrones Spiegeln
  - Asynchroner Vault
  - StrictSync
  - Synchron

- **Quell-SVM**

  Zeigt den Namen der Quell-SVM an.

  Wenn die Meldung angezeigt wird `Resource-key not discovered` Angezeigt wird, könnte dies bedeuten, dass die SVM im Cluster vorhanden, jedoch noch nicht zum Unified Manager Inventar hinzugefügt wurde oder dass sie nach der letzten Aktualisierung des Clusters erstellt wurde. Sie müssen sicherstellen, dass die SVM existiert, oder eine erneute Erkennung im Cluster durchführen, um die Liste der Ressourcen zu aktualisieren.

  Sie können den Mauszeiger über die Quell-SVM bewegen, um Informationen wie das Cluster, den Volume-Typ, die zulässigen Protokolle und das verwendete Speichervolumen anzuzeigen. Weitere Details zur SVM können Sie anzeigen, indem Sie auf den Namen der SVM klicken.

- **Quellvolumen**

  Zeigt das zu schützende Quell-Volume an. Weitere Details zum Quell-Volume können Sie anzeigen, indem Sie auf den Namen des Quell-Volumes klicken.

  Wenn die Meldung angezeigt wird `Resource-key not discovered` Angezeigt wird, kann dies bedeuten, dass das Volume im Cluster vorhanden ist, diesem jedoch noch nicht hinzugefügt wurde oder dass das Volume nach der letzten Aktualisierung des Clusters erstellt wurde. Sie müssen sicherstellen,

dass das Volume vorhanden ist, oder eine erneute Erkennung im Cluster durchführen, um die Liste der Ressourcen zu aktualisieren.

- **Ziel-SVM**

  Zeigt den Namen der Ziel-SVM an.

  Sie können den Mauszeiger über die Ziel-SVM verschieben, um Informationen wie den Cluster, den Volume-Typ, die zulässigen Protokolle und den genutzten Speicherplatz zu sehen. Weitere Details zur SVM können Sie anzeigen, indem Sie auf den Namen der SVM klicken.

- **Zielvolumen**

  Zeigt den Namen des Zieldatenträgers an.

  Sie können den Mauszeiger über ein Volume bewegen, um Informationen wie das Aggregat mit dem Volume, dem überbelegten Speicherplatz des qtree, dem Status der letzten Verschiebung des Volume und dem im Volume zugewiesenen Speicherplatz anzuzeigen. Sie können auch Details zu verwandten Objekten wie z.B. die SVM anzeigen, zu der das Volume gehört, das Aggregat, zu dem das Volume gehört, und alle Volumes, die zu diesem Aggregat gehören.

- **Dauer Der Verzögerung**

  Zeigt die Zeitspanne an, die die Daten auf dem Spiegel hinter der Quelle hinkt.

  Die Verzögerungsdauer sollte bei StrictSync Beziehungen nahe oder gleich 0 Sekunden sein.

- **Letzte Erfolgreiche Aktualisierung**

  Zeigt die Zeit des letzten erfolgreichen SnapMirror oder SnapVault Vorgangs an.

  Die letzte erfolgreiche Aktualisierung gilt nicht für synchrone Beziehungen.

- **Letzte Transferdauer**

  Zeigt die Zeit an, die für den letzten Datentransfer benötigt wurde.

  Die Übertragungsdauer ist für StrictSync-Beziehungen nicht anwendbar, da die Übertragung gleichzeitig erfolgen sollte.

- **Letzte Transfergröße**

  Zeigt die Größe der letzten Datenübertragung in Byte an.

  Die Übertragungsgröße ist nicht für StrictSync-Beziehungen anwendbar.

- **Gesundheit Der Beziehung**

  Zeigt den Systemzustand der Beziehung des Clusters an.

- * Beziehungsstatus*

  Zeigt den Mirror-Status der SnapMirror Beziehung an.

- * Ungesunde Gründe*

Der Grund, warum die Beziehung in einem ungesunden Zustand ist.

- * Quellcluster*

  Zeigt den Namen des Quell-Clusters für die SnapMirror Beziehung an.

- **Quellknoten**

  Zeigt den Namen des Quell-Node für die SnapMirror Beziehung an.

- **Zielcluster**

  Zeigt den Namen des Ziel-Clusters für die SnapMirror Beziehung an.

- **Zielknoten**

  Zeigt den Namen des Ziel-Node für die SnapMirror-Beziehung an.

- * Priorität Übertragen*

  Zeigt die Priorität an, mit der eine Übertragung ausgeführt wird. Die Übertragungspriorität ist normal oder niedrig. Transfers mit normaler Priorität werden vor Transfers mit niedriger Priorität geplant.

  Die Übertragungspriorität gilt nicht für synchrone Beziehungen, da alle Transfers mit derselben Priorität behandelt werden.

- **Richtlinien**

  Zeigt die Schutzrichtlinie für das Volume an. Sie können auf den Richtliniennamen klicken, um die mit dieser Richtlinie verknüpften Details anzuzeigen, einschließlich der folgenden Informationen:

  - Übertragungspriorität

    Gibt die Priorität an, mit der ein Transfer für asynchrone Vorgänge ausgeführt wird. Die Übertragungspriorität ist normal oder niedrig. Transfers mit normaler Priorität werden vor Transfers mit niedriger Priorität geplant. Die Standardeinstellung ist „Normal“.

  - Zugriffszeit ignorieren

    Gilt nur für SnapVault Beziehungen. Dadurch wird festgelegt, ob inkrementelle Transfers Dateien ignorieren, deren Zugriffszeit sich geändert hat. Die Werte sind entweder wahr oder falsch. Der Standardwert ist falsch.

  - Wenn die Beziehung nicht synchronisiert ist

    Gibt die Aktion an, die ONTAP ausführt, wenn eine synchrone Beziehung nicht synchronisiert werden kann. StrictSync-Beziehungen beschränken den Zugriff auf das primäre Volume, wenn die Synchronisierung mit dem sekundären Volume nicht möglich ist. Synchronisierungsbeziehungen schränken den Zugriff auf das primäre nicht ein, wenn eine Synchronisierung mit dem sekundären nicht möglich ist.

  - Limit für Versuche

    Gibt die maximale Anzahl der Zeiten an, die zu jedem manuellen oder geplanten Transfer für eine SnapMirror Beziehung versucht werden sollen. Der Standardwert ist 8.

- Kommentare

  Enthält ein Textfeld für Kommentare, die speziell für die ausgewählte Richtlinie festgelegt sind.

- SnapMirror-Etikett

  Gibt das SnapMirror-Label für den ersten Zeitplan an, der der Richtlinie für Snapshot-Kopien zugeordnet ist. Das SnapMirror-Label wird vom SnapVault-Subsystem verwendet, wenn Sie Snapshot Kopien auf einem SnapVault-Ziel sichern.

- Aufbewahrungseinstellungen

  Gibt an, wie lange Backups aufbewahrt werden, basierend auf der Zeit oder der Anzahl der Backups.

- Tatsächliche Snapshot Kopien

  Gibt die Anzahl der Snapshot-Kopien auf diesem Volume an, die mit der angegebenen Beschriftung übereinstimmen.

- Bewahren Sie Snapshot Kopien auf

  Gibt die Anzahl der SnapVault Snapshot Kopien an, die nicht automatisch gelöscht werden, selbst wenn das maximale Limit für die Richtlinie erreicht wird. Die Werte sind entweder wahr oder falsch. Der Standardwert ist falsch.

- Schwellenwert für Warnung bei Aufbewahrung

  Gibt das Limit für die Snapshot Kopie an, bei dem eine Warnung gesendet wird, um anzugeben, dass das maximale Aufbewahrungslimit fast erreicht ist.

- **Zeitplan**

  Zeigt den Namen des Schutzplans an, der der Beziehung zugeordnet ist. Sie können auf den Terminplannamen klicken, um Details zum Zeitplan anzuzeigen.

  Der Zeitplan gilt nicht für synchrone Beziehungen.

- **Version Flexible Replikation**

  Zeigt entweder Ja, Ja mit Sicherungsoption oder Keine an.

Schutz-/Volume-Transferstatus (Historisch)-Seite

Auf der Seite Protection/Volume Transfer Status (Historical) können Sie die Übertragungstrends des Volumes über einen bestimmten Zeitraum analysieren. Auf dieser Seite wird außerdem angezeigt, ob die Volume-Übertragung erfolgreich war oder nicht.

Verwenden Sie die Schaltfläche **Export**, um die Details aller überwachten Volumes in kommagetrennte Werte zu exportieren (`.csv`) Datei.

> Auf dieser Seite werden Informationen für Volumes nur in asynchronen Beziehungen angezeigt – Volumes in synchronen Beziehungen werden nicht angezeigt.

- * Quellcluster*

  Zeigt den Quellcluster-Namen an.

- **Quell-SVM**

  Zeigt den Namen der Storage Virtual Machine (SVM) an.

- **Quellvolumen**

  Zeigt den Namen des Quell-Volumes an.

- **Zielcluster**

  Zeigt den Ziel-Cluster-Namen an.

- **Ziel-SVM**

  Zeigt den Namen der Ziel-SVM an.

- **Zielvolumen**

  Zeigt den Namen des Zieldatenträgers an.

- **Operationsergebnis**

  Zeigt an, ob die Volume-Übertragung erfolgreich war.

- **Startzeit Der Übertragung**

  Zeigt die Startzeit der Volume-Übertragung an.

- **Endzeit Übertragen**

  Zeigt die Endzeit der Volume-Übertragung an.

- **Transferdauer**

  Zeigt die Zeit an, die für die Durchführung der Volume-Übertragung benötigt wurde (in Stunden).

- **Transfergröße**

  Zeigt die Größe (in MB) des übertragenen Volumes an.

- **Operationstyp**

  Zeigt den Typ der Volume-Übertragung an.

Seite „Protection/Volume Transfer Rate“ (Historical)

Auf der Seite Protection/Volume Transfer Rate (Historical) können Sie die Menge des täglich übertragenen Datenvolumens analysieren. Auf dieser Seite finden Sie auch Details zu den täglichen Volume-Transfers und die Zeit, die erforderlich ist, um den Transfervorgang abzuschließen.

Verwenden Sie die Schaltfläche **Export**, um die Details aller überwachten Volumes in kommagetrennte Werte zu exportieren (`.csv`) Datei.

Auf dieser Seite werden Informationen für Volumes nur in asynchronen Beziehungen angezeigt – Volumes in synchronen Beziehungen werden nicht angezeigt.

- **Gesamtübertragungsgröße**

  Zeigt die Gesamtgröße der Volume-Übertragung in Gigabyte an.

- **Tag**

  Zeigt den Tag an, an dem die Volume-Übertragung initiiert wurde.

- **Endzeit**

  Zeigt die Endzeit der Volume-Übertragung mit dem Datum an.

Ausführen von Sicherungs-Workflows mithilfe von OnCommand Workflow Automation

OnCommand Workflow Automation lässt sich in Unified Manager integrieren, um Workflows für Ihre Storage-Klassen auszuführen und SVMs mit Infinite Volume zu überwachen, die keine Storage-Klassen haben.

Konfigurieren einer Verbindung zwischen Workflow Automation und Unified Manager

Es besteht die Möglichkeit, eine sichere Verbindung zwischen OnCommand Workflow Automation (WFA) und Unified Manager zu konfigurieren. Durch die Verbindung zur Workflow-Automatisierung können Unternehmen Sicherungsfunktionen wie SnapMirror und SnapVault Konfigurations-Workflows sowie Befehle zum Management von SnapMirror Beziehungen nutzen.

Bevor Sie beginnen

- Die installierte Version von Workflow Automation muss 4.2 oder höher sein.
- Sie müssen „`WFA Pack zum Management von Clustered Data ONTAP`“ Version 9.5.0 oder neuer auf dem WFA Server installiert haben. Das erforderliche Paket können Sie im NetApp Storage Automation Store herunterladen.

  "WFA Pack zum Management von ONTAP"

- Sie müssen den Namen des in Unified Manager erstellten Datenbankbenutzers haben, um WFA- und Unified Manager-Verbindungen zu unterstützen.

  Diesem Datenbankbenutzer muss die Rolle „Integration Schema“ zugewiesen worden sein.

- In Workflow Automation müssen Sie entweder die Administratorrolle oder die Rolle „Architekt“ zuweisen.

- Sie müssen über die Host-Adresse, die Portnummer 443, den Benutzernamen und das Passwort für die Workflow Automation-Einrichtung verfügen.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Setup-Menü auf **Workflow Automation**.
2. Wählen Sie im Bereich **OnCommand Unified Manager Database User** der Seite **Setup/Workflow Automation** den Namen aus und geben Sie das Kennwort für den Datenbankbenutzer ein, den Sie erstellt haben, um Unified Manager- und Workflow-Automatisierungsverbindungen zu unterstützen.
3. Geben Sie im Bereich **OnCommand Workflow Automation Credentials** der Seite **Setup/Workflow Automation** den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) sowie den Benutzernamen und das Passwort für das Setup der Workflow-Automatisierung ein.

   Sie müssen den Unified Manager Server Port (Port 443) verwenden.

4. Klicken Sie Auf **Speichern**.
5. Wenn Sie ein selbstsigniertes Zertifikat verwenden, klicken Sie auf **Ja**, um das Sicherheitszertifikat zu autorisieren.

   Die Seite Setup/Workflow-Automatisierung wird angezeigt.

6. Klicken Sie auf **Ja**, um die Web-Benutzeroberfläche neu zu laden, und fügen Sie die Workflow-Automation-Funktionen hinzu.

Entfernen des OnCommand Workflow Automation Setup aus Unified Manager

Sie können das OnCommand Workflow Automation Setup aus Unified Manager entfernen, wenn Sie Workflow-Automatisierung nicht mehr verwenden möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Setup-Menü auf **Workflow Automation**.
2. Klicken Sie auf der Seite **Setup/Workflow Automation** auf **Setup entfernen**.

Was passiert, wenn OnCommand Workflow Automation neu installiert oder aktualisiert wird

Bevor Sie OnCommand Workflow Automation neu installieren oder aktualisieren OnCommand Workflow Automation, müssen Sie zuerst die Verbindung zwischen OnCommand Workflow Automation und Unified Manager entfernen und sicherstellen, dass alle aktuell ausgeführten oder geplanten Jobs angehalten werden.

Sie müssen Unified Manager auch manuell aus OnCommand Workflow Automation löschen.

Nachdem Sie OnCommand Workflow Automation neu installiert oder aktualisiert haben, müssen Sie die Verbindung zu Unified Manager erneut einrichten.

Beschreibung der OnCommand Workflow Automation-Setup-Fenster und Dialogfelder

Sie können OnCommand Workflow Automation über die Seite Setup/Workflow-Automatisierung in Unified Manager einrichten.

Seite „Setup/Workflow Automation“

Auf der Seite Setup/Workflow-Automatisierung können Sie die Einstellungen für die Integration von OnCommand Workflow Automation in Unified Manager konfigurieren. Sie können die Einstellungen auch hinzufügen, ändern oder löschen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Unified Manager Datenbankbenutzer

In diesem Bereich können Sie die Anmeldeinformationen eines Datenbankbenutzers eingeben, der für die Verbindung von Unified Manager mit Workflow Automation erforderlich ist:

- **Name**

  Ermöglicht die Angabe des Benutzernamens eines Datenbankbenutzers, der für den Zugriff auf Daten in der Unified Manager-Datenbank verwendet werden kann. Standardmäßig ist kein Datenbankbenutzer ausgewählt. Sie können einen Datenbankbenutzer aus der Dropdown-Liste auswählen.

- **Passwort**

  Ermöglicht Ihnen die Angabe eines Passworts für den angegebenen Benutzernamen.

Belege für den Erfolg von OnCommand Workflow Automation

In diesem Bereich können Sie die Zugangsdaten für ein Workflow Automation Konto eingeben, das für die Verbindung mit Unified Manager erforderlich ist:

- **Hostname oder IP-Adresse**

  Gibt den Namen oder die IP-Adresse des Workflow Automation Host-Servers an, der zum Pairing mit Unified Manager verwendet wird.

- **Port**

  Zeigt die erforderliche Portnummer des Workflow Automation Host-Servers an, der 443 ist.

- **Benutzername**

  Ermöglicht Ihnen, einen Benutzernamen anzugeben, der zur Anmeldung bei Workflow Automation verwendet werden kann.

- **Passwort**

Ermöglicht Ihnen die Angabe eines Passworts für den angegebenen Benutzernamen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die Setup-Optionen entfernen, speichern oder abbrechen:

- **Setup Entfernen**

  Der Workflow Automation Setup wurde aus Unified Manager entfernt.

- **Speichern**

  Speichert die Konfigurationseinstellungen für die ausgewählte Option.

Performance-Management mithilfe von Performance-Kapazität und verfügbaren IOPS-Informationen

Performance Capacity zeigt an, wie viel Durchsatz eine Ressource erhalten kann, ohne die nützliche Performance dieser Ressource zu überschreiten. Wenn Sie die Nutzung vorhandener Performance-Zähler verwenden, ist die Performance-Kapazität der Punkt, an dem Sie die maximale Auslastung eines Node oder Aggregats erhalten, bevor die Latenz zu einem Problem wird.

Unified Manager sammelt Performance-Kapazitätsstatistiken von Nodes und Aggregaten in jedem Cluster. *Performance-Kapazität verwendet* ist der Prozentsatz der derzeit genutzten Performance-Kapazität und *Performance Capacity free* ist der Prozentsatz der noch verfügbaren Performance-Kapazität.

Während die freie Performance-Kapazität einen Prozentsatz der noch verfügbaren Ressource bietet, gibt Ihnen *verfügbare IOPS* die Anzahl an IOPS an, die der Ressource hinzugefügt werden können, bevor sie die maximale Performance-Kapazität erreicht. Mithilfe dieser Kennzahl können Sie sicherstellen, dass Sie Workloads mit einer vorab festgelegten Anzahl von IOPS zu einer Ressource hinzufügen können.

Das Monitoring der Informationen zur Performance-Kapazität bietet folgende Vorteile:

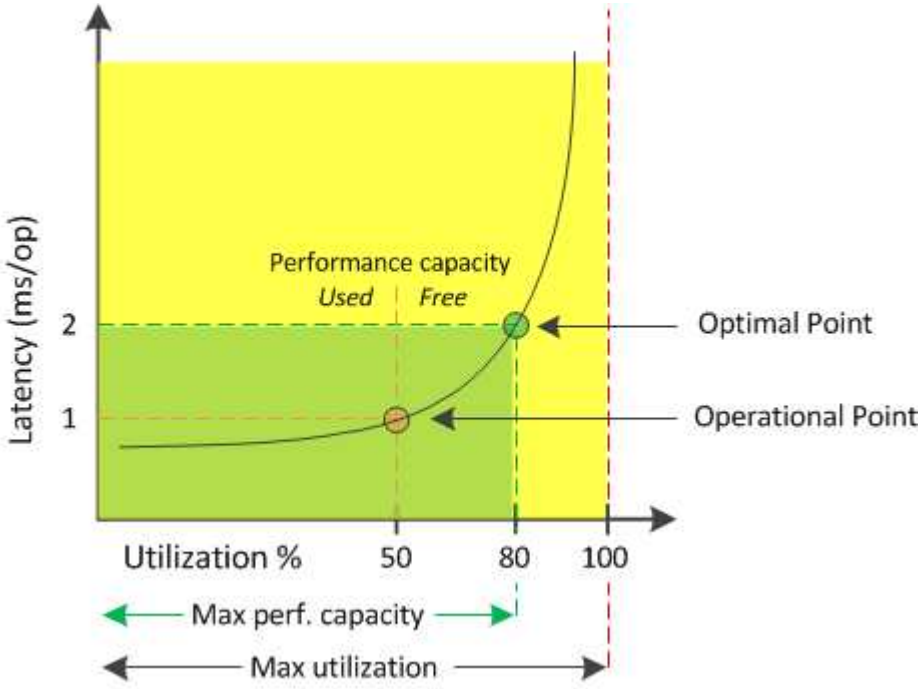
- Hilft bei der Workflow-Bereitstellung und beim Lastausgleich.
- Hilft Ihnen, eine Überlastung eines Knotens zu verhindern oder seine Ressourcen über den optimalen Punkt hinaus zu schieben, wodurch die Fehlerbehebung verringert wird.
- Präzisere Bestimmung, bei denen möglicherweise zusätzliche Storage-Geräte erforderlich sind

Welche Performance-Kapazität wird verwendet

Mit dem verwendeten Zähler für die Performance-Kapazität können Sie ermitteln, ob die Performance eines Node oder Aggregats an einem Punkt anliegt, an dem sich die Performance bei einer Workload-Steigerung verschlechtern kann. Es kann Ihnen auch zeigen, ob ein Node oder Aggregat derzeit zu bestimmten Zeiten überlastet ist. Die Verwendung der Performance-Kapazität ähnelt der Auslastung, allerdings bietet die vorherige Appliance einen besseren Einblick in die verfügbaren Performance-Funktionen in einer physischen Ressource für einen bestimmten Workload.

Daten zur Performance-Kapazität sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.

Die optimale genutzte Performance-Kapazität ist der Punkt, an dem ein Node oder Aggregat optimale Auslastung und Latenz (Reaktionszeit) bietet und effizient eingesetzt wird. In der folgenden Abbildung ist eine Beispiellatenz im Vergleich zur Auslastungskurve gezeigt für ein Aggregat.



In diesem Beispiel weist der_Operationspunkt_ darauf hin, dass das Aggregat derzeit bei einer Auslastung von 50 % und einer Latenz von 1.0 ms/op. Arbeitet Basierend auf den vom Aggregat erfassten Statistiken stellt Unified Manager fest, dass für dieses Aggregat zusätzliche Performance-Kapazität verfügbar ist. In diesem Beispiel wird der *optimale Punkt* als Punkt identifiziert, an dem das Aggregat bei einer Auslastung von 80 % und einer Latenz von 2.0 ms/op. Liegt Somit können Sie diesem Aggregat auch mehr Volumes und LUNs hinzufügen, sodass Ihre Systeme effizienter genutzt werden.

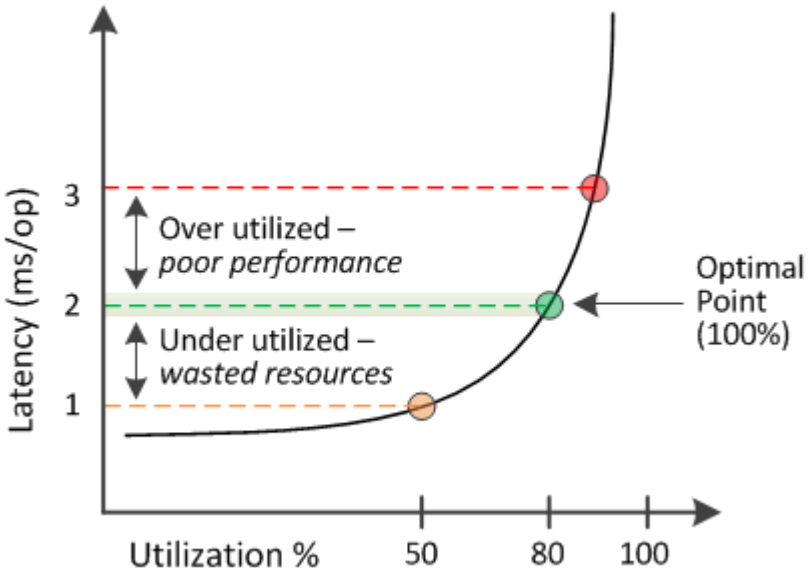
Der verwendete Zähler für die Performance-Kapazität soll eine größere Zahl sein als der Zähler „`Auslastung`“, da die Performance-Kapazität die Auswirkungen auf die Latenz hinzufügt. Wenn beispielsweise ein Node oder Aggregat zu 70 % genutzt wird, kann der Wert für die Performance-Kapazität je nach Latenzwert im Bereich von 80 % bis 100 % liegen.

In einigen Fällen kann der Auslastungszähler jedoch höher auf der Seite Dashboards/Leistung sein. Dies ist normal, da das Dashboard die aktuellen Zählerwerte zu jedem Erfassungszeitraum aktualisiert. Es werden die Durchschnittswerte über einen Zeitraum nicht angezeigt, wie die anderen Seiten in der Benutzeroberfläche von Unified Manager. Der verwendete Zähler für die Performance-Kapazität dient am besten als Indikator für die über einen Zeitraum gemittelte Performance, während der Auslastungszähler am besten zur Ermittlung der unmittelbaren Nutzung einer Ressource genutzt wird.

Was der Wert der verwendeten Performance-Kapazität bedeutet

Der von Performance genutzte Wert hilft Ihnen dabei, die Nodes und Aggregate zu identifizieren, die derzeit zu stark ausgelastet sind oder nicht ausgelastet sind. Auf diese Weise können Sie Workloads neu verteilen, um die Effizienz der Storage-Ressourcen zu steigern.

Die folgende Abbildung zeigt die Latenz im Vergleich zur Auslastungskurve einer Ressource und identifiziert mit farbigen Punkten drei Bereiche, in denen sich der aktuelle betriebliche Punkt befinden könnte.



- Ein Prozentsatz der genutzten Performance-Kapazität gleich 100 ist am optimalen Punkt.

  Die Ressourcen werden jetzt effizient genutzt.

- Ein Prozentsatz an Performance, der höher als 100 ist, bedeutet, dass der Node oder das Aggregat zu stark ausgelastet ist und dass Workloads eine suboptimale Performance erhalten.

  Der Ressource sollten keine neuen Workloads hinzugefügt werden, die bestehende Workloads müssen eventuell neu verteilt werden.

- Ein Prozentsatz an Performance-Kapazität unter 100 zeigt an, dass der Node oder das Aggregat nicht ausgelastet ist und dass die Ressourcen nicht effizient genutzt werden.

  Der Ressource können weitere Workloads hinzugefügt werden.

Im Gegensatz zur Auslastung kann die genutzte Performance-Kapazität über 100 % liegen. Es gibt keinen maximalen Prozentsatz, aber Ressourcen werden in der Regel zwischen 110 % und 140 % liegen, wenn sie überausgelastet sind. Höhere Prozentsätze deuten auf eine Ressource mit schwerwiegenden Problemen hin.

Was verfügbar ist, ist IOPS

Der verfügbare IOPS-Zähler ermittelt die verbleibende Anzahl an IOPS, die einem Node oder Aggregat hinzugefügt werden kann, bevor die Ressource ihr Limit erreicht. Die gesamten IOPS, die ein Node bereitstellen kann, basieren auf den physischen Eigenschaften des Node, beispielsweise auf der Anzahl der CPUs, der CPU-Geschwindigkeit und dem RAM-Umfang. Die gesamten IOPS, die ein Aggregat bereitstellen kann, basieren auf den physischen Eigenschaften der Festplatten, zum Beispiel auf einer SATA-, SAS- oder SSD-Festplatte.

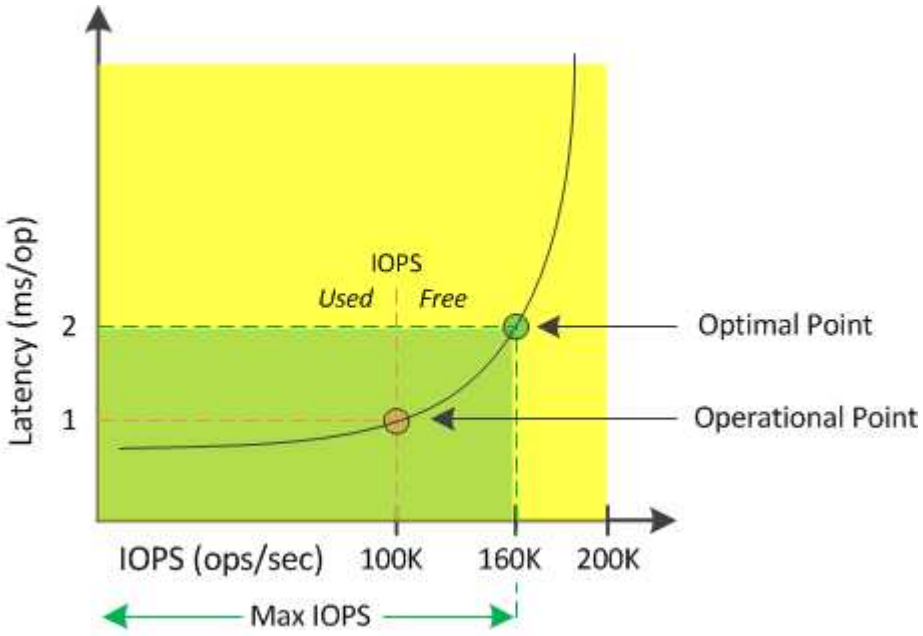
Während der freie Zähler für Performance-Kapazität den Prozentsatz einer noch verfügbaren Ressource

angibt, liefert der verfügbare IOPS-Zähler genau die Anzahl der IOPS (Workloads) für eine Ressource, bevor sie die maximale Performance-Kapazität erreicht.

Wenn Sie beispielsweise zwei Storage-Systeme FAS2520 und FAS8060 nutzen, erhalten Sie bei einem Performance-Kapazitätswert von 30 % auch freie Performance-Kapazität. Dieser Wert bietet jedoch keine Übersicht darüber, wie viele Workloads auf diesen Nodes implementiert werden können. Der verfügbare IOPS-Zähler zeigt möglicherweise, dass bei der FAS8060 500 verfügbare IOPS verfügbar sind, bei der FAS2520 jedoch nur 100 verfügbare IOPS.

Verfügbare IOPS-Daten sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.

Die folgende Abbildung zeigt eine Beispiellatenz im Vergleich zur IOPS-Kurve für einen Node.



Die maximale Anzahl an IOPS, die eine Ressource liefern kann, ist die Anzahl der IOPS, wenn der Zähler für die Performance-Kapazität bei 100 % liegt (der optimale Punkt). Der Betriebspunkt identifiziert, dass der Node derzeit bei 100.000 IOPS mit einer Latenz von 1.0 ms/op arbeitet Auf der Grundlage der vom Node erfassten Statistiken ermittelt Unified Manager, dass die maximalen IOPS für den Node 160.000 beträgt, was bedeutet, dass 60.000 freie oder verfügbare IOPS vorhanden sind. Daher können Sie diesem Node weitere Workloads hinzufügen, sodass die Systeme effizienter genutzt werden.

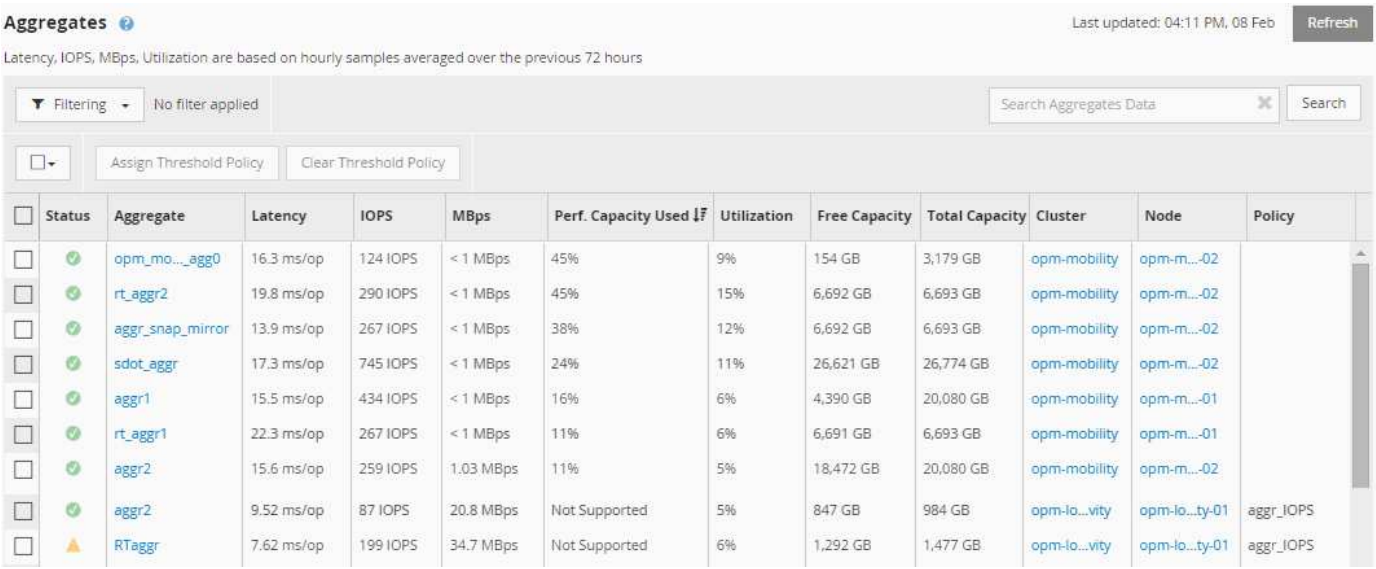
Wenn die Ressource minimale Benutzeraktivitäten hat, wird der verfügbare IOPS-Wert unter Annahme eines allgemeinen Workloads auf Grundlage von etwa 4,500 IOPS pro CPU-Kern berechnet. Das liegt daran, dass Unified Manager nicht über die Daten verfügt, um die Eigenschaften des Workloads, der bereitgestellt werden soll, exakt abzuschätzen.

Anzeigen der verwendeten Werte für die Node- und Aggregat-Performance

Sie können die verwendeten Werte für die Performance-Kapazität für alle Nodes oder für alle Aggregate in einem Cluster überwachen oder Details für einen einzelnen Node oder Aggregat anzeigen.

Die verwendeten Werte für die Performance-Kapazität werden auf der Seite Performance Dashboard, auf den Seiten Performance Inventory, Top Performers, Create Threshold Policy, auf den Seiten Performance Explorer

und in Detaildiagrammen angezeigt. Beispielsweise enthält die Seite „Performance/Aggregate Inventory“ eine Spalte „Perf“. Kapazität zur Anzeige des verwendeten Werts für die Performance-Kapazität aller Aggregate.



Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS
	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS

Der Status „`N/A`“ wird angezeigt, wenn Nodes nicht mit der Software ONTAP 9.0 oder höher installiert wurden.

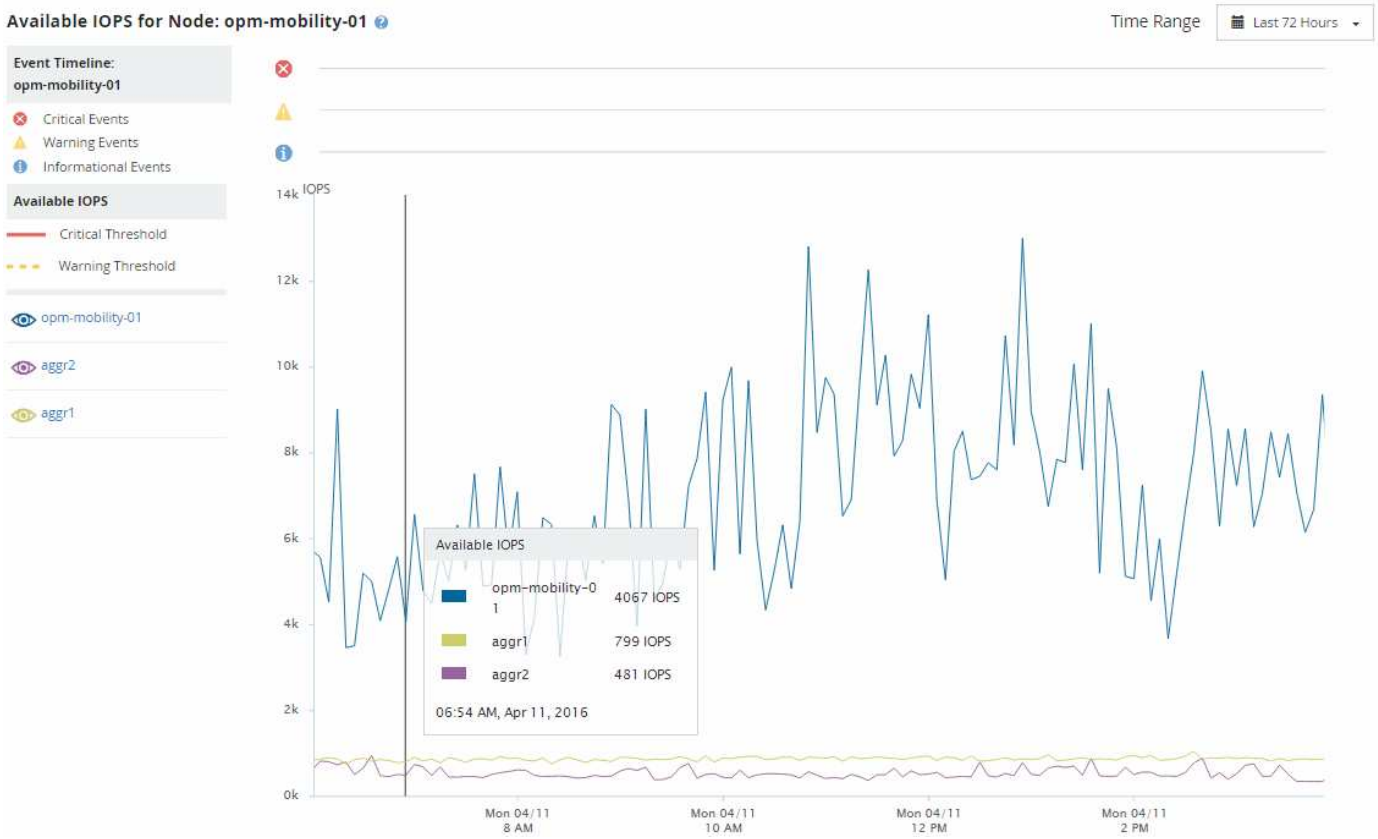
Durch das Monitoring des verwendeten Zählers für die Performance-Kapazität können Sie Folgendes identifizieren:

- Unabhängig davon, ob Nodes oder Aggregate auf jedem Cluster einen hohen Wert an Performance-Kapazität aufweisen
- Gibt an, ob Nodes oder Aggregate auf beliebigen Clustern über Ereignisse mit aktiver Performance-Kapazität verfügen
- Die Nodes und Aggregate verfügen über die in einem Cluster genutzte Kapazität mit der höchsten und niedrigsten Performance
- Zählerwerte im Bereich Latenz und Auslastung in Verbindung mit Nodes oder Aggregaten mit hohen Werten im Bereich der Performance-Kapazität
- Auswirkungen auf die verwendete Performance-Kapazität für Nodes in einem HA-Paar auf einen Node, wenn einer der Nodes ausfällt
- Die am stärksten ausgelasteten Volumes und LUNs auf einem Aggregat mit hoher Performance-Kapazität

Anzeigen der verfügbaren IOPS-Werte für Node und Aggregat

Sie können die verfügbaren IOPS-Werte für alle Nodes und alle Aggregate in einem Cluster überwachen. Alternativ können Sie Details zu einem einzelnen Node oder Aggregat anzeigen.

Verfügbare IOPS-Werte werden in den Performance Explorer-Seitendiagrammen angezeigt. Wenn Sie beispielsweise einen Node auf der Seite „Performance/Node Explorer“ anzeigen, können Sie das Zählerdiagramm „`verfügbare IOPS`“ in der Liste auswählen, damit Sie die verfügbaren IOPS-Werte für mehrere Aggregate auf diesem Node vergleichen können.



Durch das Monitoring des verfügbaren IOPS-Zählers können Sie Folgendes identifizieren:

- Die Nodes oder Aggregate mit den höchsten verfügbaren IOPS-Werten unterstützen Sie bei der Entscheidung, wo zukünftige Workloads implementiert werden können.
- Die Nodes oder Aggregate mit den kleinsten verfügbaren IOPS-Werten, um die zu überwachenden Ressourcen auf potenzielle künftige Performance-Probleme zu identifizieren.
- Die am stärksten ausgelasteten Volumes und LUNs auf einem Aggregat mit kleinem verfügbaren IOPS-Wert.

Anzeigen von Zählerdiagrammen zur Performance-Kapazität zur Erkennung von Problemen

Auf der Seite „Performance Explorer“ können Sie die verwendeten Performance-Kapazitäten für Nodes und Aggregate anzeigen. Damit können Sie detaillierte Performance-Kapazitätsdaten für die ausgewählten Nodes und Aggregate für einen bestimmten Zeitraum anzeigen.

Über diese Aufgabe

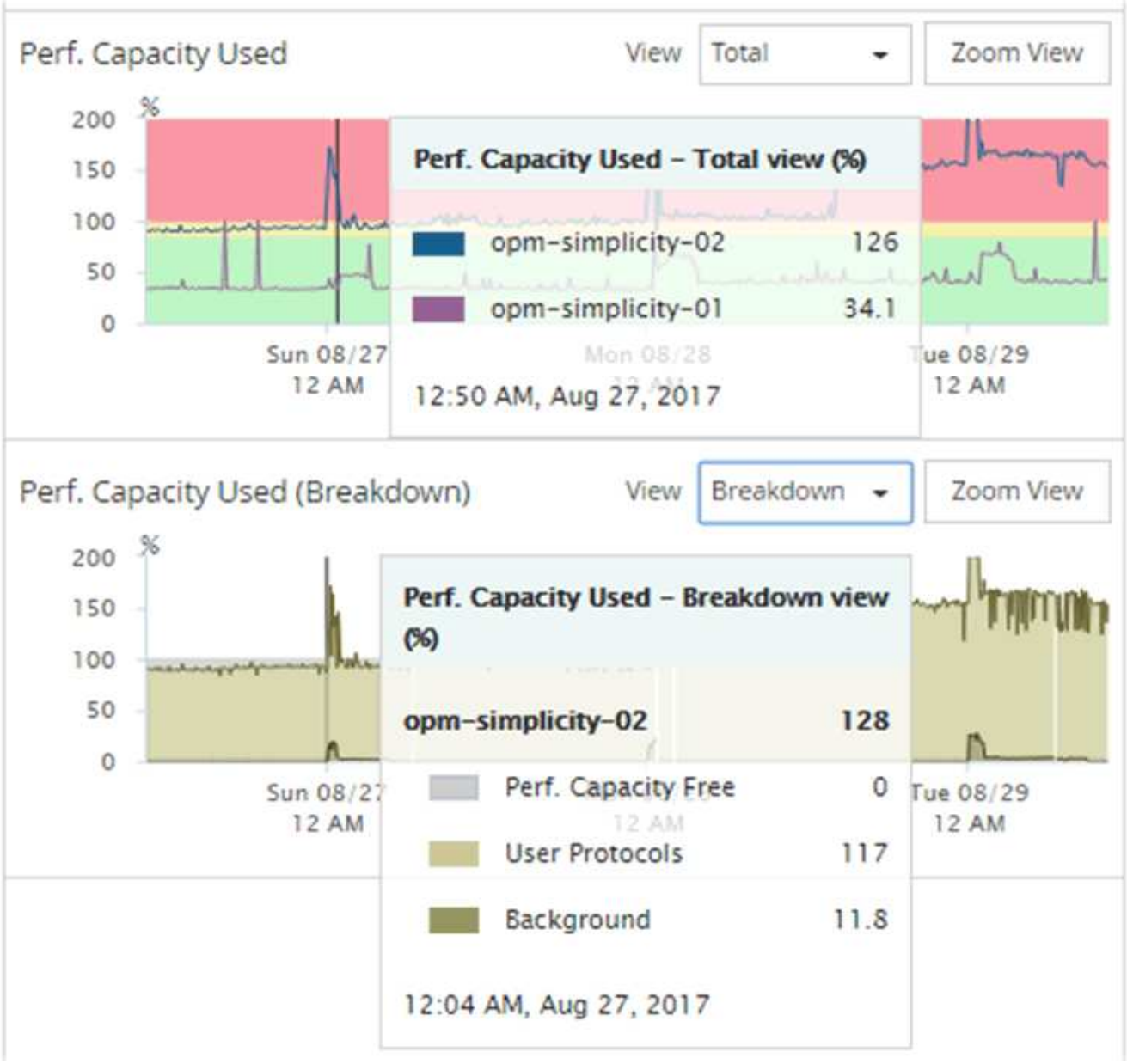
Das Standard-Zählerdiagramm zeigt die Werte der verwendeten Performance-Kapazität für die ausgewählten Nodes oder Aggregate an. Das Counter Chart Breakdown zeigt die Werte für die Gesamtkapazität des Root-Objekts an, das basierend auf Benutzerprotokollen und Hintergrundsystemprozessen in die Nutzung unterteilt ist. Darüber hinaus wird die Menge der freien Performance-Kapazität dargestellt.

Da einige Hintergrundaktivitäten zu System- und Datenmanagement als Benutzer-Workloads identifiziert und als Benutzerprotokolle kategorisiert werden, erscheint der Prozentsatz der Benutzerprotokolle künstlich hoch, wenn diese Prozesse ausgeführt werden. Diese Prozesse laufen normalerweise um Mitternacht, wenn die Cluster-Nutzung gering ist. Wenn bei der Durchführung von Benutzerprotokollen um Mitternacht eine Spitze sichtbar ist, überprüfen Sie, ob Cluster-Backup-Jobs oder andere Hintergrundaktivitäten zu diesem Zeitpunkt konfiguriert wurden.

Schritte

1. Wählen Sie die **Explorer** Registerkarte von einem Knoten oder Aggregat * Landing* Seite.
2. Klicken Sie im Fenster **Counter Charts** auf **Choose Charts** und wählen Sie dann die Option *Perf. Diagramm „verwendete Kapazität“.
3. Blättern Sie nach unten, bis Sie das Diagramm anzeigen können.

   Die Farben des Standarddiagramms zeigen an, wenn sich das Objekt im optimalen Bereich (gelb) befindet, wenn das Objekt nicht ausgelastet ist (grün) und wenn das Objekt überausgelastet ist (rot). Das Diagramm zeigt detaillierte Performance-Kapazitätsdetails nur für das Root-Objekt.



4. Wenn Sie eine Karte in einem vollen Format anzeigen möchten, klicken Sie auf **Zoom View**.

   Auf diese Weise können Sie mehrere Zählerdiagramme in einem separaten Fenster öffnen, um die genutzte Performance-Kapazität mit IOPS- oder MB/s-Werten im gleichen Zeitraum zu vergleichen.

Performance-Kapazität nutzte Schwellenwertbedingungen für die Performance

Sie können benutzerdefinierte Performance-Schwellenwertrichtlinien erstellen, damit Ereignisse ausgelöst werden, wenn der für einen Node oder ein Aggregat genutzte Performance-Wert die festgelegte Einstellung für den verwendeten Schwellenwert für die Performance-Kapazität überschreitet.

Außerdem können Nodes mit einem Schwellenwert von „`Performance Capacity used Takeover`“ konfiguriert werden. Diese Schwellenwertrichtlinie gibt die für beide Nodes verwendeten Performance-Statistiken in einem HA-Paar an und ermittelt, ob einem der beiden Nodes genügend Kapazität fehlen würde, wenn der andere Node ausfällt. Da der Workload während des Failover` Kombination der Workloads der

beiden Partner-Nodes ist, kann die gleiche Performance-Kapazität, die für eine Übernahme verwendet wird, auf beide Nodes angewendet werden.

> Die genutzte Performance-Kapazität entspricht der Leistung im Allgemeinen den Nodes. Ist der Node-übergreifende Datenverkehr jedoch über seinen Failover-Partner für einen der Nodes vorgesehen, kann die Gesamt-Performance, die bei der Ausführung aller Workloads auf einem Partner-Node verwendet wird, auf einem anderen Partner-Node geringfügig anders sein – je nachdem, welcher Node ausgefallen ist.

Die verwendeten Performance-Kapazitäten können auch als sekundäre Performance-Schwellenwerteinstellungen verwendet werden, um bei der Definition von Schwellenwerten für LUNs und Volumes eine kombinierte Schwellenwertrichtlinie zu erstellen. Die verwendete Performance-Kapazität wird auf das Aggregat oder den Node angewendet, auf dem sich das Volume oder die LUN befindet. Sie können beispielsweise anhand der folgenden Kriterien eine kombinierte Schwellenwertrichtlinie erstellen:

Storage Objekt	Performance-Zähler	Warnschwellenwert	Kritischer Schwellenwert	Dauer
Datenmenge	Latenz	15 ms/OP	25 ms/OP	20 Minuten

Aufgrund von Grenzwertrichtlinien wird ein Ereignis nur erzeugt, wenn beide Bedingungen während der gesamten Dauer nicht erfüllt werden.

Verwenden der Performance-Kapazität, die zum Managen der Performance verwendet wird

In der Regel möchten Unternehmen mit einer Performance-Kapazität von unter 100 Prozent betreiben, um die Ressourcen effizient zu nutzen und gleichzeitig zusätzliche Performance-Kapazitäten zu reservieren, um Spitzenlasten zu erzielen. Anhand von Schwellenwertrichtlinien kann angepasst werden, wenn Warnmeldungen gesendet werden, um hohe Werte für die verwendete Kapazität zu erreichen.

Sie können bestimmte Ziele basierend auf Ihren Performance-Anforderungen festlegen. So könnten Finanzdienstleister mehr Performance-Kapazität reservieren, um eine zeitnahe Ausführung von Transaktionen zu gewährleisten. Diese Unternehmen möchten möglicherweise Schwellenwerte für die verwendete Performance-Kapazität im Bereich von 70-80 Prozent festlegen. Produzierende Unternehmen mit geringeren Margen können sich für weniger Performance-Kapazität entscheiden, wenn sie bereit sind, Performance zu riskieren, um DIE IT-Kosten besser zu managen. Diese Unternehmen können Grenzwerte für die verwendete Performance-Kapazität im Bereich von 85-95 Prozent festlegen.

Wenn der verwendete Wert für die Performance-Kapazität den in einer benutzerdefinierten Schwellenwertrichtlinie festgelegten Prozentsatz überschreitet, sendet Unified Manager eine Alarm-E-Mail und fügt das Ereignis zur Seite „Ereignisbestand“ hinzu. Auf diese Weise lassen sich potenzielle Probleme verwalten, bevor sie die Performance beeinträchtigen. Diese Ereignisse können auch als Indikatoren verwendet werden, an denen Sie Workloads und Änderungen innerhalb Ihrer Nodes und Aggregate vornehmen müssen.

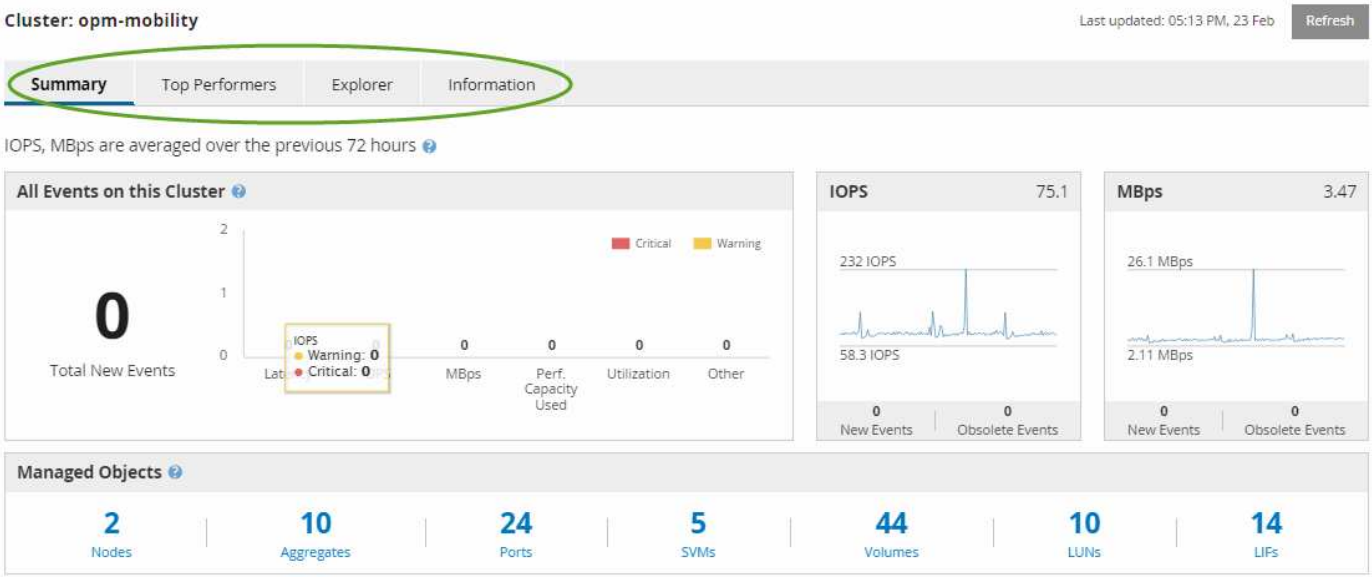
Monitoring der Cluster-Performance über die Startseite des Performance Cluster

Auf der Seite „Performance Cluster Landing“ wird der Performance-Status eines ausgewählten Clusters angezeigt, der von einer Instanz von Unified Manager überwacht wird. Auf dieser Seite können Sie die allgemeine Performance eines bestimmten Clusters bewerten und schnell alle erkannten Cluster-spezifischen Ereignisse bemerken, lokalisieren oder zur Behebung zuweisen.

Informationen zur Landing Page des Performance Cluster

Die Seite „Performance Cluster Landing“ bietet eine grundlegende Performance-Übersicht über ein ausgewähltes Cluster und legt den Performance-Status der 10 wichtigsten Objekte im Cluster fest. Leistungsprobleme werden oben auf der Seite im Bereich „Alle Ereignisse auf diesem Cluster“ angezeigt.

Die Performance Cluster Landing Page bietet eine allgemeine Übersicht über jedes Cluster, das von einer Instanz von Unified Manager gemanagt wird. Auf dieser Seite erhalten Sie Informationen zu Ereignissen und der Performance sowie Informationen zur Überwachung und Fehlerbehebung der Cluster. Das folgende Bild zeigt ein Beispiel der „Performance Cluster Landing Page“ für den Cluster mit dem Namen „opm-Mobility“:



Die Ereignisanzahl auf der Seite „Cluster Summary“ entspricht möglicherweise nicht der Ereignisanzahl auf der Seite „Performance Event Inventory“. Dies liegt daran, dass auf der Seite „Cluster Summary“ jeweils ein Ereignis in den Bars für Latenz und Auslastung angezeigt werden kann, wenn gegen eine Kombinationsrichtlinie ein Schwellenwert überschritten wurde, während auf der Seite „Performance Event Inventory“ nur ein Ereignis angezeigt wird, wenn die Kombinationsrichtlinie nicht eingehalten wurde.

Wenn ein Cluster aus dem Management durch Unified Manager entfernt wurde, wird rechts neben dem Cluster-Namen oben auf der Seite der Status **removed** angezeigt.

Landing Page für Performance Cluster

Auf der Seite „Performance Cluster Landing“ wird der Performance-Status eines ausgewählten Clusters angezeigt. Auf der Seite können Sie alle Details zu jedem Performance-Zähler für die Storage-Objekte im ausgewählten Cluster abrufen.

Klicken Sie auf die Schaltfläche **Favoriten** ( ) Um dieses Objekt zu Ihrer Liste der bevorzugten Speicherobjekte hinzuzufügen. Eine blaue Taste ( ) Zeigt an, dass dieses Objekt bereits ein Favorit ist.

Die Landing Page für Performance Cluster enthält vier Registerkarten, die die Cluster-Details in vier Informationsbereiche trennen:

- Übersichtsseite
  - Bereich Cluster-Ereignisse
  - Bereich „Managed Objects“
- Seite „Top Performers“
- Explorer-Seite
- Informationsseite

Performance Cluster Summary

Die Seite Performance Cluster Summary bietet eine Zusammenfassung der aktiven Ereignisse, IOPS Performance und MB/s für ein Cluster. Diese Seite enthält auch die Gesamtzahl der Storage-Objekte im Cluster.

Teilfenster „Cluster-Performance“-Ereignisse

Im Teilfenster Cluster Performance-Ereignisse werden Performance-Statistiken und alle aktiven Ereignisse für das Cluster angezeigt. Dies ist am hilfreichsten, wenn es um das Monitoring der Cluster und aller Cluster-bezogenen Performance und Ereignisse geht.

Alle Ereignisse in diesem Clusterfenster

Im Teilfenster „Alle Ereignisse“ in diesem Teilfenster „Cluster“ werden alle aktiven Cluster-Performance-Ereignisse der letzten 72 Stunden angezeigt. Die Gesamtzahl der aktiven Ereignisse wird ganz links angezeigt. Diese Zahl stellt die Summe aller neuen und bestätigten Ereignisse für alle Speicherobjekte in diesem Cluster dar. Sie können auf den Link „Aktive Ereignisse insgesamt“ klicken, um zur Seite „Ereignisbestand“ zu navigieren, die gefiltert wird, um diese Ereignisse anzuzeigen.

Im Balkendiagramm für aktive Ereignisse insgesamt für das Cluster wird die Gesamtzahl der aktiven kritischen und Warnereignisse angezeigt:

- Latenz (insgesamt für Nodes, Aggregate, SVMs, Volumes, LUNs, Und Namespaces)
- IOPS (insgesamt für Cluster, Nodes, Aggregate, SVMs, Volumes, LUNs und Namespaces)
- MB/s (insgesamt für Cluster, Nodes, Aggregate, SVMs, Volumes, LUNs, Namespaces, Ports und LIFs)
- Verwendete Performance-Kapazität (insgesamt für Nodes und Aggregate)
- Auslastung (insgesamt für Nodes, Aggregate und Ports)
- Sonstiges (Cache-Miss-Verhältnis für Volumes)

Die Liste enthält aktive Performanceereignisse, die aus benutzerdefinierten Schwellenwertrichtlinien, systemdefinierten Schwellenwertrichtlinien und dynamischen Schwellenwerten ausgelöst werden.

Diagrammdaten (vertikale Zählerbalken) werden rot (angezeigt) Für kritische Ereignisse, und gelb ( ) Für Warnereignisse. Positionieren Sie den Cursor über jede vertikale Zählerleiste, um den tatsächlichen Typ und die Anzahl der Ereignisse anzuzeigen. Sie können auf **Aktualisieren** klicken, um die Daten des Zählerfelds zu aktualisieren.

Sie können kritische Ereignisse und Warnereignisse im Leistungsdiagramm für aktive Ereignisse anzeigen oder ausblenden, indem Sie in der Legende auf die Symbole **kritisch** und **Warnung** klicken. Wenn Sie bestimmte Ereignistypen ausblenden, werden die Legende-Symbole grau angezeigt.

Thekenabdeckungen

Die Zählerfelder zeigen Cluster-Aktivitäten und Performance-Ereignisse der letzten 72 Stunden an und umfassen die folgenden Zähler:

- **IOPS-Zählerpanel**

  IOPS gibt die Betriebsgeschwindigkeit des Clusters in der Anzahl der ein-/Ausgabevorgänge pro Sekunde an. Dieses Zählerfeld bietet eine allgemeine Übersicht über den IOPS-Zustand des Clusters im vorherigen Zeitraum von 72 Stunden. Sie können den Mauszeiger über die Trendkurve positionieren, um den IOPS-Wert für einen bestimmten Zeitpunkt anzuzeigen.

- **MB/s-Zähler-Panel**

  MB/s gibt an, wie viele Daten in Megabyte pro Sekunde an und aus dem Cluster übertragen wurden. Dieses Zählerfeld bietet eine allgemeine Übersicht über den Zustand des Clusters im Vergleich mit dem vorherigen 72-Stunden-Zeitraum. Sie können den Cursor über die Trendlinie des Diagramms positionieren, um den Mbps-Wert für eine bestimmte Zeit anzuzeigen.

Die Zahl oben rechts im Diagramm im grauen Balken ist der Durchschnittswert aus dem letzten 72-Stunden-Zeitraum. Die Zahlen unten und oben im Trendliniendiagramm sind die Mindest- und Höchstwerte der letzten 72 Stunden. Der graue Balken unterhalb des Diagramms enthält die Anzahl der aktiven (neuen und bestätigten) Ereignisse und der veralteten Ereignisse aus dem Zeitraum der letzten 72 Stunden.

Die Zählerfelder enthalten zwei Arten von Ereignissen:

- * Aktiv*

  Zeigt an, dass das Leistungsereignis aktuell aktiv ist (neu oder bestätigt). Das Problem, das das Ereignis verursacht hat, wurde nicht selbst behoben oder wurde nicht behoben. Der Performance-Zähler für das Storage-Objekt bleibt über dem Performance-Schwellenwert.

- **Veraltet**

  Zeigt an, dass das Ereignis nicht mehr aktiv ist. Das Problem, das das Ereignis verursacht hat, hat sich selbst korrigiert oder wurde behoben. Der Performance-Zähler für das Storage-Objekt liegt nicht mehr über dem Performance-Schwellenwert.

Bei **Active Events** können Sie Ihren Cursor über das Ereignissymbol positionieren und auf die Ereignisnummer klicken, um die entsprechende Seite mit den Ereignisdetails zu verlinken. Wenn es mehrere Ereignisse gibt, können Sie auf **Alle Ereignisse anzeigen** klicken, um die Seite „Ereignisbestand“ anzuzeigen, die gefiltert wird, um alle Ereignisse für den ausgewählten Zählertyp des Objekts anzuzeigen.

Bereich „Managed Objects“

Der Fensterbereich verwaltete Objekte auf der Registerkarte Performance-Übersicht bietet eine Übersicht über die Speicherobjekttypen und -Zählungen für das Cluster. In diesem Teilfenster können Sie den Status der Objekte in jedem Cluster verfolgen.

Die Anzahl der verwalteten Objekte ist die Anzahl der Point-in-Time-Daten vom letzten Erfassungszeitraum. Neue Objekte werden in 15-Minuten-Intervallen entdeckt.

Durch Klicken auf die verknüpfte Nummer eines Objekttyps wird die Seite „Objekt-Performance-Bestandsaufnahme“ für diesen Objekttyp angezeigt. Die Seite „Objektbestandsliste“ wird gefiltert, um nur die Objekte auf diesem Cluster anzuzeigen.

Die verwalteten Objekte sind:

- **Knoten**

  Ein physisches System in einem Cluster

- **Aggregate**

  Ein Satz aus mehreren redundanten Array von unabhängigen Festplatten (RAID)-Gruppen, die als eine einzige Einheit zur Sicherung und Bereitstellung gemanagt werden können.

- **Ports**

  Ein physischer Verbindungspunkt auf Knoten, der zur Verbindung mit anderen Geräten im Netzwerk verwendet wird.

- **SVMs**

  Eine virtuelle Maschine, die Netzwerkzugriff über eindeutige Netzwerkadressen ermöglicht. Eine SVM kann Daten aus einem anderen Namespace bereitstellen und kann vom Rest des Clusters getrennt verwaltet werden.

- **Bände**

  Eine logische Einheit, die über ein oder mehrere der unterstützten Zugriffsprotokolle zugängliche Benutzerdaten enthält. Die Zählung umfasst sowohl FlexVol Volumes als auch FlexGroup Volumes. Es umfasst keine FlexGroup Komponenten oder Infinite Volumes.

- **LUNs**

  Der Bezeichner einer logischen Fibre Channel (FC)-Einheit oder einer logischen iSCSI-Einheit. Eine logische Einheit entspricht in der Regel einem Speichervolumen und wird innerhalb eines Computerbetriebssystems als Gerät dargestellt.

- **LIFs**

  Eine logische Netzwerkschnittstelle, die einen Netzwerkzugriffspunkt für einen Node darstellt. Die Anzahl umfasst alle LIF-Typen.

Seite „Top Performers“

Auf der Seite „Top Performers“ werden die Speicherobjekte angezeigt, die je nach dem ausgewählten Performance-Zähler die höchste oder niedrigste Performance haben. Beispielsweise können Sie in der Kategorie SVMs die SVMs mit den höchsten IOPS, mit der höchsten Latenz oder mit den niedrigsten MB/s anzeigen. Diese Seite wird auch angezeigt, wenn einer der Top-Performer aktive Performanceereignisse hat (Neu oder bestätigt).

Auf der Seite Top Performers werden maximal 10 Objekte angezeigt. Das Volume-Objekt umfasst sowohl FlexVol Volumes als auch FlexGroup Volumes. Es umfasst keine FlexGroup Komponenten oder Infinite Volumes.

- **Zeitbereich**

  Sie können einen Zeitbereich für die Anzeige der Top-Performer auswählen. Der ausgewählte Zeitbereich gilt für alle Speicherobjekte. Verfügbare Zeitbereiche:

  - Letzte Stunde
  - Letzte 24 Stunden
  - Letzte 72 Stunden (Standard)
  - Letzte 7 Tage

- **Metrisch**

  Klicken Sie auf das Menü **metrisch**, um einen anderen Zähler auszuwählen. Zähleroptionen sind nur dem Objekttyp zugeordnet. Verfügbare Zähler für das Objekt **Volumes** sind beispielsweise **Latenz**, **IOPS** und **Mbps**. Durch Ändern des Zählers werden die Plattendaten basierend auf dem ausgewählten Zähler mit den Top-Performern neu geladen.

  Verfügbare Zähler:

  - Latenz
  - IOPS
  - MB/Sek.
  - Verwendete Performance-Kapazität (für Nodes und Aggregate)
  - Auslastung (für Nodes und Aggregate)

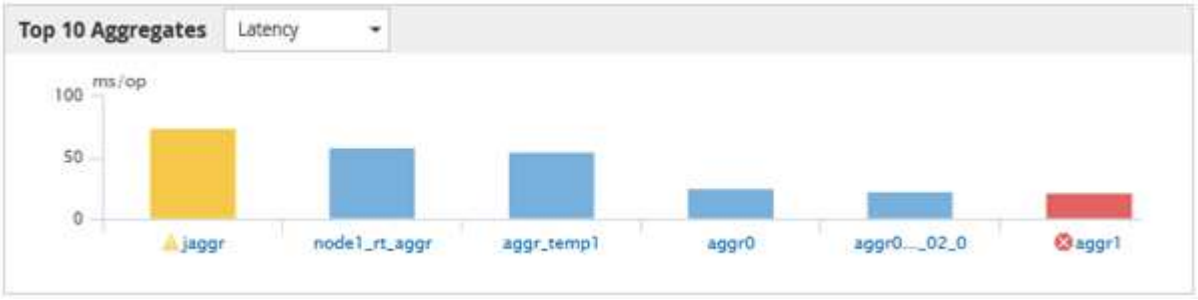
- * Sortieren*

  Klicken Sie auf das Menü **Sortieren**, um eine aufsteigende oder absteigende Sortierung für das ausgewählte Objekt und den ausgewählten Zähler auszuwählen. Die Optionen sind **höchste bis niedrigste** und **niedrigste bis höchste**. Bei diesen Optionen werden die Objekte mit höchster Performance oder mit geringster Performance angezeigt.

- **Counter Bar**

  Der Zählerbalken im Diagramm zeigt die Performance-Statistiken für jedes Objekt an, die als Balken für dieses Objekt dargestellt sind. Die Balkendiagramme sind farbcodiert. Wenn der Zähler keinen Performance-Schwellenwert überschreitet, wird der Zählerbalken in blau angezeigt. Wenn eine Schwellenverletzung aktiv ist (ein neues oder quited Event), wird der Balken in der Farbe für das Ereignis angezeigt: Warnereignisse werden in Gelb (angezeigt), und kritische Ereignisse werden in rot ( ).

Schwellenverletzungen werden zudem durch Symbole für die Schweregrade für Warn- und kritische Ereignisse angezeigt.



Die X-Achse zeigt für jedes Diagramm die besten Interpreten für den ausgewählten Objekttyp an. Die Y-Achse zeigt die Einheiten an, die für den ausgewählten Zähler gelten. Wenn Sie unter jedem vertikalen Balkendiagramm auf den Objektnamen klicken, werden Sie zur Seite Performance Landing für das ausgewählte Objekt navigieren.

- **Severity Ereignisanzeige**

  Das Symbol **Severity Event** wird links neben einem Objektnamen für den aktiven kritischen (angezeigt ⊗) Oder Warnung (⚠) Ereignisse in den Grafiken der Top-Performer. Klicken Sie zum Anzeigen auf das Symbol * Severity Event*:

  - **Ein Event**

    Navigiert zur Seite mit den Veranstaltungsdetails für dieses Ereignis.

  - * Zwei oder mehr Veranstaltungen*

    Navigiert zur Seite „Ereignisbestand“, die gefiltert wird, um alle Ereignisse für das ausgewählte Objekt anzuzeigen.

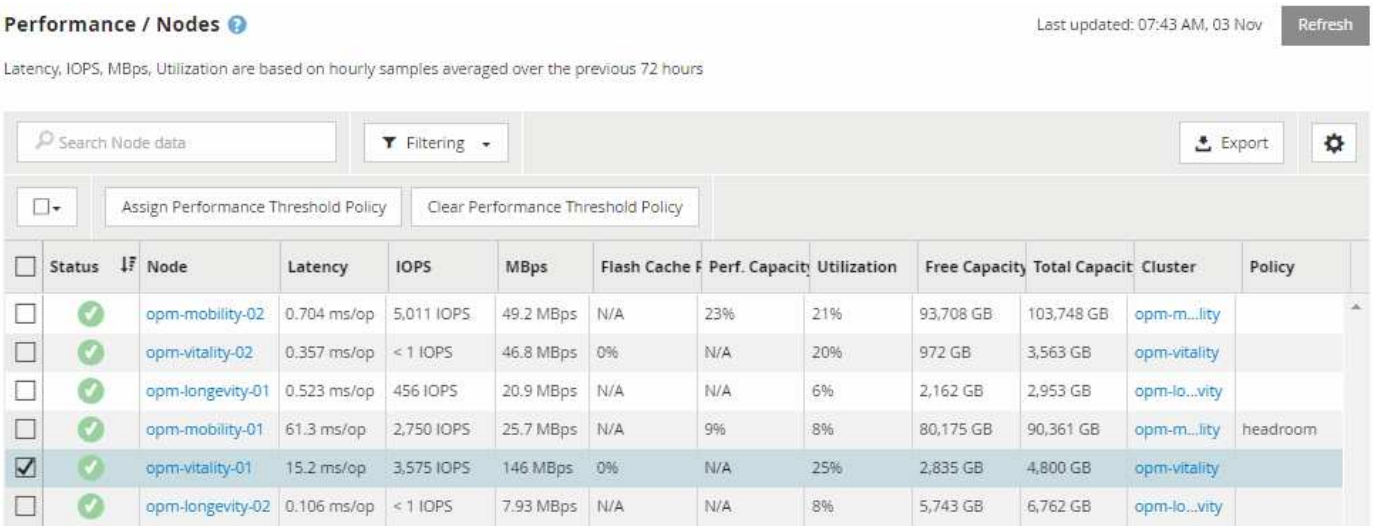
- **Export-Taste**

  Erstellt ein `.csv` Datei, die die in der Zählerleiste angezeigten Daten enthält. Sie können die Datei für das einzelne Cluster erstellen, das Sie anzeigen, oder für alle Cluster im Datacenter.

Überwachung der Performance mithilfe der Seiten „Performance Inventory“ (Performance-Bestandsaufnahme

Auf den Objektbestands-Performance-Seiten werden Performance-Informationen, Performance-Ereignisse und Objektzustand für alle Objekte innerhalb einer Objekttyp-Kategorie angezeigt. Dadurch erhalten Sie einen schnellen Überblick über den Performance-Status jedes Objekts in einem Cluster, beispielsweise für alle Nodes oder alle Volumes.

Die Seiten für die Objektbestandsleistung bieten einen allgemeinen Überblick über den Objektstatus, sodass Sie die Gesamtleistung aller Objekte bewerten und Objektleistungsdaten vergleichen können. Sie können den Inhalt der Objektbestandsseiten durch Suchen, Sortieren und Filtern verfeinern. Dies ist insbesondere beim Monitoring und Management der Objekt-Performance von Vorteil, da Objekte mit Performance-Problemen schnell lokalisiert und der Fehlerbehebungsprozess gestartet werden kann.



Standardmäßig werden Objekte auf den Seiten des Performance-Inventars nach Wichtigkeit der Objektleistung sortiert. Objekte mit neuen kritischen Performance-Ereignissen werden zuerst aufgeführt, Objekte mit Warnmeldungen werden an zweiter Stelle aufgeführt. Dies bietet eine unmittelbare visuelle Darstellung von Problemen, die behoben werden müssen. Alle Performance-Daten basieren auf einem Durchschnitt von 72 Stunden.

Sie können einfach von der Seite „Objektbestandsleistung“ zu einer Seite mit Objektdetails navigieren, indem Sie in der Spalte Objektname auf den Objektnamen klicken. Beispielsweise klicken Sie auf der Seite Performance/Nodes Inventory in der Spalte **Nodes** auf ein Node-Objekt. Die Seite Objektdetails enthält detaillierte Informationen und Details zum ausgewählten Objekt, einschließlich eines Gegenübers aktiver Ereignisse.

Objektüberwachung mithilfe der Bestandsseiten des Performance-Objekts

Über die Seiten zum Performance-Objektbestand können Sie die Objekt-Performance basierend auf den Werten bestimmter Performance-Zähler oder auf der Grundlage von Performance-Ereignissen überwachen. Dies ist vorteilhaft, da durch die Identifizierung von Objekten mit Performance-Ereignissen die Ursache von Cluster-Performance-Problemen untersucht werden kann.

Auf den Seiten des Performance-Objektbestands werden die zugeordneten Zähler, zugeordnete Objekte und Performance-Schwellenwertrichtlinien für alle Objekte in allen Clustern angezeigt. Auf diesen Seiten können Sie außerdem Richtlinien für Leistungsschwellenwerte auf Objekte anwenden. Sie können die Seite anhand einer beliebigen Spalte sortieren und alle Objektnamen oder -Daten durchsuchen.

Sie können Daten von diesen Seiten in kommagetrennte Werte exportieren (`.csv`) Datei mit der Schaltfläche **Exportieren** und dann die exportierten Daten zum Erstellen von Berichten verwenden.

Inhalt der Seite zur Leistungsbestandsliste wird verfeinert

Die Inventarseiten für Performance-Objekte enthalten Tools, mit denen Sie Inhalte aus Objektbeständen verfeinern können, damit Sie bestimmte Daten schnell und einfach auffinden können.

Die Informationen auf den Seiten zum Bestand von Performance-Objekten können umfangreich sein und häufig über mehrere Seiten hinweg erfasst werden. Diese umfassenden Daten eignen sich hervorragend für

das Monitoring, die Nachverfolgung und die Performance. Das Auffinden bestimmter Daten erfordert jedoch Tools, mit denen Sie die gesuchten Daten schnell finden. Daher enthalten die Seiten für den Bestand von Performance-Objekten Funktionen zum Suchen, Sortieren und Filtern. Darüber hinaus können Suchen und Filtern zusammenarbeiten, um Ihre Ergebnisse weiter einzugrenzen.

Suchen auf den Seiten „Objektbestandsleistung“

Sie können Zeichenfolgen auf den Seiten „Objektbestandsleistung“ suchen. Verwenden Sie das Feld **Suche** oben rechts auf der Seite, um Daten anhand des Objektnamens oder des Richtliniennamens schnell zu finden. So lassen sich entweder spezifische Objekte und zugehörige Daten schnell finden oder Richtlinien schnell finden und zugehörige Richtlinienobjektdaten anzeigen.

Schritte

1. Führen Sie je nach Ihren Suchanforderungen eine der folgenden Optionen durch:

So finden Sie das:	Geben Sie dies ein…
Zu einem bestimmten Objekt	Der Objektname in das Feld * Suchen* und klicken Sie auf **Suchen**. Das Objekt, nach dem Sie gesucht haben, und die zugehörigen Daten werden angezeigt.
Eine benutzerdefinierte Richtlinie für Leistungsschwellenwerte	Der Name der Richtlinie ganz oder teilweise in das Feld **Suche** und klicken Sie auf **Suchen**. Die Objekte, die der von Ihnen gesuchten Richtlinie zugeordnet sind, werden angezeigt.

Sortieren auf den Seiten „Objektbestandsleistung“

Sie können alle Daten auf den Seiten „Objektbestandsleistung“ nach jeder Spalte in aufsteigender oder absteigender Reihenfolge sortieren. So können Sie schnell Objektbestandsdaten finden, was bei der Überprüfung der Leistung oder beim Beginn eines Fehlerbehebungsprozesses hilfreich ist.

Über diese Aufgabe

Die ausgewählte Spalte für die Sortierung wird durch einen markierten Spaltenüberschrift und ein Pfeilsymbol angezeigt, das die Sortierrichtung rechts neben dem Namen angibt. Ein nach-oben-Pfeil zeigt eine aufsteigende Reihenfolge an; ein Pfeil nach unten zeigt die absteigende Reihenfolge an. Die Standard-Sortierreihenfolge ist durch **Status** (Ereignis-Kritikalität) in absteigender Reihenfolge, wobei die wichtigsten Performanceereignisse zuerst aufgelistet werden.

Schritte

1. Sie können auf einen Spaltennamen klicken, um die Sortierreihenfolge der Spalte in aufsteigender oder absteigender Reihenfolge zu ändern.

   Der Inhalt der Seite „Objektbestandsleistung“ wird auf der Grundlage der ausgewählten Spalte in aufsteigender oder absteigender Reihenfolge sortiert.

Filtern von Daten auf den Seiten „Objektbestandsleistung“

Sie können Daten auf den Seiten „Objektbestandsleistung“ filtern, um Daten anhand bestimmter Kriterien schnell zu finden. Mithilfe der Filterung können Sie den Inhalt der Seiten „Objektbestandsleistung“ eingrenzen, um nur die von Ihnen angegebenen Ergebnisse anzuzeigen. Dies bietet eine sehr effiziente Methode, nur die Leistungsdaten anzuzeigen, an denen Sie interessiert sind.

Über diese Aufgabe

Über das Filterfeld können Sie die Rasteransicht entsprechend Ihren Einstellungen anpassen. Verfügbare Filteroptionen basieren auf dem in der Tabelle angezeigten korrelierten Objekttyp. Wenn aktuell Filter angewendet werden, wird links neben dem Filtersteuerelement ein Sternchen (*) angezeigt.

Es werden vier Filterparameter unterstützt.

Parameter	Validierung
Zeichenfolge (Text)	Die Operatoren sind **enthält** und **beginnt mit**.
Nummer	Die Betreiber sind **größer als** und **kleiner als**.
Ressource	Die Operatoren sind **Name enthält** und **Name beginnt mit**.
Status	Die Betreiber sind **ist** und **ist nicht**.

Für jeden Filter sind alle drei Felder erforderlich; die verfügbaren Filter spiegeln die filterbaren Spalten auf der aktuellen Seite wider. Es können maximal vier Filter angewendet werden. Gefilterte Ergebnisse basieren auf kombinierten Filterparametern. Gefilterte Ergebnisse gelten für alle Seiten in Ihrer gefilterten Suche und nicht nur für die aktuell angezeigte Seite.

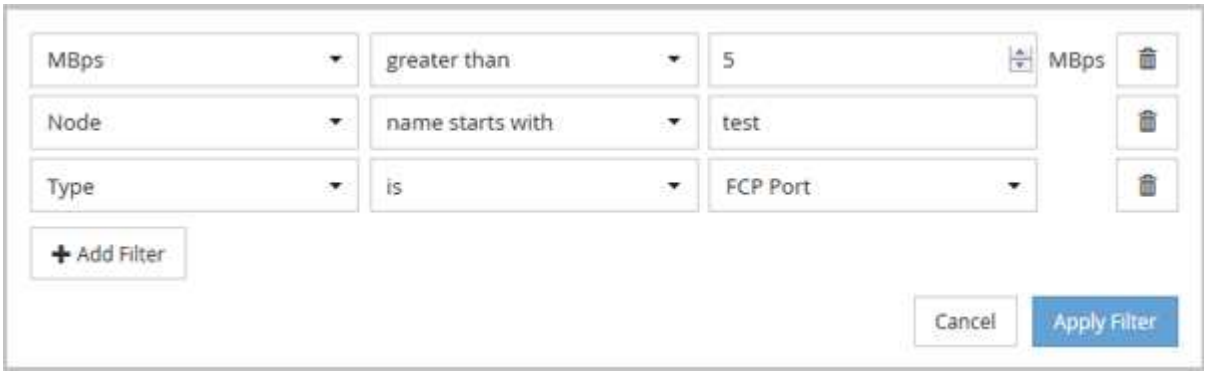
Sie können Filter über das Filterfenster hinzufügen.

1. Klicken Sie oben auf der Seite auf **Filtern**. Das Filterbedienfeld wird angezeigt.
2. Klicken Sie im Filterfenster auf die linke Dropdown-Liste und wählen Sie einen Objektnamen aus, z. B. *Cluster* oder einen Performance-Zähler.
3. Klicken Sie auf die Dropdown-Liste Mitte, und wählen Sie den booleschen Operator **Name enthält** oder **Name beginnt mit** aus, wenn die erste Auswahl ein Objektname war. Wenn es sich bei der ersten Auswahl um einen Leistungszähler handelte, wählen Sie **größer als** oder **kleiner als** aus. Wenn die erste Auswahl **Status** war, wählen Sie **ist** oder **ist nicht**.
4. Wenn für Ihre Suchkriterien ein numerischer Wert erforderlich ist, werden die nach-oben- und nach-unten-Pfeiltasten im Feld rechts angezeigt. Sie können auf die nach-oben- und nach-unten-Pfeiltasten klicken, um den gewünschten numerischen Wert anzuzeigen.
5. Geben Sie bei Bedarf Ihre nicht-numerischen Suchkriterien in das Textfeld rechts ein.
6. Um Filter hinzuzufügen, klicken Sie auf **Filter hinzufügen**. Es wird ein zusätzliches Filterfeld angezeigt. Führen Sie diesen Filter mithilfe des in den vorherigen Schritten beschriebenen Verfahrens aus. Beachten Sie, dass beim Hinzufügen Ihres vierten Filters die Schaltfläche **Filter hinzufügen** nicht mehr angezeigt wird.

7. Klicken Sie Auf **Filter Anwenden**. Die Filteroptionen werden auf das Raster angewendet, und ein Sternchen (*) wird in der Filterschaltfläche angezeigt.
8. Verwenden Sie den Filterbereich, um einzelne Filter zu entfernen, indem Sie auf das Papierkorb-Symbol rechts neben dem zu entfernenden Filter klicken.
9. Um alle Filter zu entfernen, klicken Sie unten im Filterfenster auf **Zurücksetzen**.

Beispiel für die Filterung

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



Nachdem Sie auf **Filter anwenden** geklickt haben, wird das Filterfenster geschlossen und wendet Ihre Filter an.

Analyse der Empfehlungen von Unified Manager für das Tiering von Daten in die Cloud

Auf der Seite „Performance/Volumes Inventory“ werden Informationen zur Größe der auf dem inaktiven (kalten) Volume gespeicherten Benutzerdaten angezeigt. In einigen Fällen erkennt Unified Manager bestimmte Volumes, die durch das Tiering inaktiver Daten auf das Cloud-Tier (Cloud-Provider oder StorageGRID) eines FabricPool-fähigen Aggregats profitieren würden.

FabricPool wurde in ONTAP 9.2 eingeführt. Wenn Sie eine Version der ONTAP Software vor 9.2 verwenden, ist für Unified Manager die Empfehlung für Tiering-Daten ein Upgrade der ONTAP Software erforderlich. Darüber hinaus der `auto` die tiering-Richtlinie wurde in ONTAP 9.4 eingeführt, wenn man also empfiehlt, den zu verwenden `auto` die tiering-Richtlinie muss auf ONTAP 9.4 oder höher aktualisiert werden.

Die folgenden drei Felder zum Inventarbereich von Performance/Volumes enthalten Informationen darüber, ob Sie die Festplattenauslastung Ihres Storage-Systems verbessern und Speicherplatz auf dem Performance-Tier einsparen können, indem Sie inaktive Daten auf die Cloud-Tier verschieben.

- **Tiering-Richtlinie**

  Die Tiering-Richtlinie legt fest, ob die Daten auf dem Volume auf der Performance-Tier verbleiben oder ob

einige der Daten von der Performance-Tier in die Cloud-Tier verschoben werden.

Der Wert in diesem Feld gibt die Tiering-Richtlinie an, die auf das Volume gesetzt ist, auch wenn sich das Volume derzeit nicht auf einem FabricPool Aggregat befindet. Die Tiering-Richtlinie tritt nur in Kraft, wenn das Volume auf einem FabricPool Aggregat ist.

- **Kalte Daten**

  Die kalten Daten zeigen die Größe der auf dem inaktiven (kalten) Volume gespeicherten Benutzerdaten an.

  Ein Wert wird hier nur angezeigt, wenn ONTAP 9.4 oder höher verwendet wird, da es erfordert, dass das Aggregat, auf dem das Volume bereitgestellt wird, über das verfügt `inactive data reporting` Parameter auf gesetzt `enabled`, Und dass die Mindestzahl der Kühltage Schwelle erreicht worden ist (für Volumen, die die verwenden `snapshot-only` Oder `auto` tiering-Richtlinie). Andernfalls wird der Wert als „`N/A`“ aufgeführt.

- * Cloud-Empfehlung*

  Nachdem genügend Informationen über die Datenaktivität auf dem Volume erfasst wurden, kann Unified Manager feststellen, dass keine Aktionen erforderlich sind oder dass Sie Speicherplatz auf der Performance-Tier einsparen können, indem Sie inaktive Daten per Tiering auf das Cloud-Tier verschieben.

> Das Feld „kalte Daten“ wird alle 15 Minuten aktualisiert. Das Feld „Cloud Empfehlung“ wird jedoch alle 7 Tage aktualisiert, wenn die Analyse der kalten Daten auf dem Volume durchgeführt wird. Daher kann die genaue Menge der kalten Daten zwischen den Feldern abweichen. Das Feld Cloud Recommendation zeigt das Datum an, an dem die Analyse ausgeführt wurde.

Wenn die Meldung inaktiver Daten aktiviert ist, zeigt das Feld „kalte Daten“ die genaue Menge inaktiver Daten an. Ohne die Funktion zur Berichterstellung inaktiver Daten bestimmt Unified Manager mithilfe von Performance-Statistiken, ob Daten auf einem Volume inaktiv sind. Die Menge der inaktiven Daten wird in diesem Fall nicht im Feld „kalte Daten“ angezeigt, aber es wird angezeigt, wenn Sie den Mauszeiger über das Wort **Tier** bewegen, um die Cloud-Empfehlung anzuzeigen.

Folgende Cloud-Empfehlungen werden angezeigt:

- **Lernen**. Es wurden nicht genügend Daten gesammelt, um eine Empfehlung zu treffen.
- **Stufe**. Die Analyse hat festgestellt, dass das Volume inaktive (kalte) Daten enthält und dass Sie das Volume so konfigurieren sollten, dass diese Daten in das Cloud-Tier verschoben werden. In einigen Fällen muss hierfür unter Umständen zunächst das Volume in ein FabricPool-fähiges Aggregat verschoben werden. In anderen Fällen, in denen sich das Volume bereits auf einem FabricPool Aggregat befindet, müssen Sie nur die Tiering-Richtlinie ändern.
- **Keine Aktion**. Entweder das Volume verfügt über wenige inaktive Daten. Das Volume ist bereits auf die Tiering-Richtlinie „`Auto`“ für ein FabricPool Aggregat festgelegt, oder das Volume ist ein Datensicherungs-Volume. Dieser Wert wird auch angezeigt, wenn das Volume offline ist oder wenn es in einer MetroCluster-Konfiguration verwendet wird.

Zum Verschieben eines Volumes oder zum Ändern der Tiering-Richtlinie für Volumes oder der Einstellungen für die Berichterstellung für inaktive Daten für das Aggregat verwenden Sie OnCommand System Manager, ONTAP CLI-Befehle oder eine Kombination dieser Tools.

Wenn Sie mit der Rolle „OnCommand Administrator“ oder „Storage Administrator“ bei Unified Manager angemeldet sind, ist der Link „Volume konfigurieren“ in der Cloud-Empfehlung verfügbar, wenn Sie den

Mauszeiger über das Wort „Tier*“ bewegen. Klicken Sie auf diese Schaltfläche, um die Seite Volumes in System Manager zu öffnen, um die empfohlene Änderung vorzunehmen.

Beschreibungen der Seiten zum Leistungsbestand

Mithilfe der Seiten zum Performance-Inventar werden Performance-Informationen über jede der verfügbaren Storage-Objekte wie Cluster, Aggregate, Volumes usw. angezeigt. Sie können mit den Detailseiten für Performance-Objekte verbunden werden, um detaillierte Informationen für ein bestimmtes Objekt anzuzeigen.

Inventarseite für Performance/Cluster

Die Seite „Performance/Cluster Inventory“ zeigt eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jedes Cluster an, das von einer Instanz von Unified Manager überwacht wird. Auf dieser Seite können Sie die Performance des Clusters überwachen sowie Performance-Probleme und Schwellenwertereignisse beheben.

Je nachdem, wie Sie diese Seite aufrufen, wird möglicherweise ein anderer Titel auf der Seite angezeigt, um anzugeben, ob die Liste gefiltert wurde. Wenn beispielsweise alle Cluster angezeigt werden, lautet der Titel „`Cluster`“. Wenn Sie eine Teilmenge von Clustern anzeigen, die von der Seite Schwellenwertrichtlinien zurückgegeben werden, lautet der Titel „`Cluster", auf denen die Richtlinie XYZ angewendet wird`“.

Mit den Schaltflächen oben auf der Seite können Sie Suchen durchführen, um bestimmte Daten zu finden, Filter zu erstellen und anzuwenden, um die Liste der angezeigten Daten einzugrenzen und die Daten auf der Seite in A zu exportieren `.csv` Datei, und fügen Sie Spalten auf der Seite hinzu oder entfernen Sie sie.

Standardmäßig werden Objekte auf den Objektbestandsseiten sortiert, basierend auf dem Kritikereignis der Objektleistung. Objekte mit kritischen Ereignissen werden zuerst aufgeführt und Objekte mit Warnmeldungen werden als zweites aufgeführt. Dies bietet eine unmittelbare visuelle Darstellung von Problemen, die behoben werden müssen. Die Werte der Leistungsindikatoren basieren auf einem Durchschnitt aus den Daten der letzten 72 oder mehr Stunden, wie auf der Seite angegeben. Sie können auf die Schaltfläche „Aktualisieren“ klicken, um die Objektbestandsdaten zu aktualisieren.

Über die Schaltflächen **Performance Threshold Policy** und **Clear PerformanceThreshold Policy** können Sie Schwellenwertrichtlinien für beliebige Objekte auf den Objektbestandsseiten zuweisen oder löschen.

Cluster-Spalten auf der Bestandsseite

Die Seite „Performance/Cluster Inventory“ enthält die folgenden Spalten für jedes Cluster.

- **Status**

  Ein gesundes Objekt ohne aktive Ereignisse zeigt ein grünes Häkchen-Symbol (). Wenn das Objekt über ein aktives Ereignis verfügt, identifiziert das Symbol für die Ereignisanzeige den Schweregrad: Kritische Ereignisse sind rot (Die Fehlerereignisse sind orange (), und Warnereignisse sind gelb ( ).

- * Cluster*

  Der Name des Clusters. Sie können auf den Cluster-Namen klicken, um zur Seite mit den Performance-Details dieses Clusters zu gelangen.

- **IOPS**

  Die ein-/Ausgabevorgänge pro Sekunde auf dem Cluster.

- **Mbps**

  Der Durchsatz auf dem Cluster, gemessen in Megabyte pro Sekunde.

- **Freie Kapazität**

  Die ungenutzte Speicherkapazität für diesen Cluster in Gigabyte

- **Gesamtkapazität**

  Die gesamte Storage-Kapazität für diesen Cluster in Gigabyte

- **Anzahl Knoten**

  Die Anzahl der Nodes im Cluster. Sie können auf die Anzahl der Nodes klicken, um zur Seite „Bestandsaufnahme der Performance/Nodes“ zu navigieren.

- **Hostname oder IP-Adresse**

  Der Host-Name oder die IP-Adresse (IPv4 oder IPv6) der Cluster-Management-LIF.

- **Seriell #**

  Die eindeutige Identifikationsnummer des Clusters.

- **Betriebssystemversion**

  Die Version der ONTAP Software, die auf dem Cluster installiert ist.

  Wenn unterschiedliche Versionen der ONTAP Software auf den Nodes im Cluster installiert werden, wird die niedrigste Versionsnummer aufgeführt. Auf der Seite „Performance/Nodes Inventory“ können Sie die auf jedem Node installierte ONTAP Version anzeigen.

- **Grenzwertrichtlinie**

  Die benutzerdefinierte Performance-Schwellenwertrichtlinie, die für dieses Storage-Objekt aktiv ist, oder Richtlinien. Sie können den Cursor über Richtliniennamen mit Ellipsen (…) positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen **Performance Threshold Policy** und **Clear Performance Threshold Policy** bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Inventarseite für Performance/Nodes

Die Seite Performance/Nodes-Inventar enthält eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jeden Node, der von einer Instanz von Unified Manager überwacht wird. So können Sie die Performance Ihrer Nodes schnell überwachen und Performance-Probleme und Schwellwerte beheben.

Je nachdem, wie Sie zu dieser Seite navigieren, wird oben auf der Seite möglicherweise ein anderer Titel

angezeigt, um anzugeben, ob die Liste gefiltert wurde. Beispiel: Wenn alle Nodes angezeigt werden, lautet der Titel „`Nodes`“. Wenn eine Untergruppe von Nodes angezeigt wird, die von der Seite „Cluster-Inventar“ zurückgegeben wird, lautet der Titel „`Nodes auf Cluster: opm-cluster2`“.

Mit den Schaltflächen oben auf der Seite können Sie Suchen durchführen, um bestimmte Daten zu finden, Filter zu erstellen und anzuwenden, um die Liste der angezeigten Daten einzugrenzen und die Daten auf der Seite in A zu exportieren `.csv` Datei, und fügen Sie Spalten auf der Seite hinzu oder entfernen Sie sie.

Standardmäßig werden Objekte auf den Objektbestandsseiten sortiert, basierend auf dem Kritikereignis der Objektleistung. Objekte mit kritischen Ereignissen werden zuerst aufgeführt und Objekte mit Warnmeldungen werden als zweites aufgeführt. Dies bietet eine unmittelbare visuelle Darstellung von Problemen, die behoben werden müssen. Die Werte der Leistungsindikatoren basieren auf einem Durchschnitt aus den Daten der letzten 72 oder mehr Stunden, wie auf der Seite angegeben. Sie können auf die Schaltfläche „Aktualisieren“ klicken, um die Objektbestandsdaten zu aktualisieren.

Über die Schaltflächen **Performance Threshold Policy** und **Clear PerformanceThreshold Policy** können Sie Schwellenwertrichtlinien für beliebige Objekte auf den Objektbestandsseiten zuweisen oder löschen.

Spalten auf der Seite „Knoten“

Die Seite „Performance/Nodes Inventory“ enthält die folgenden Spalten für jeden Node:

- **Status**

  Ein gesundes Objekt ohne aktive Ereignisse zeigt ein grünes Häkchen-Symbol (). Wenn das Objekt über ein aktives Ereignis verfügt, identifiziert das Symbol für die Ereignisanzeige den Schweregrad: Kritische Ereignisse sind rot (Die Fehlerereignisse sind orange (), und Warnereignisse sind gelb ( ).

- **Knoten**

  Der Name des Node. Sie können auf den Node-Namen klicken, um zur Seite mit den Performance-Details dieses Node zu navigieren.

- **Latenz**

  Die durchschnittliche Antwortzeit für alle I/O-Anfragen auf dem Node in Millisekunden pro Vorgang ausgedrückt.

- **IOPS**

  Die durchschnittlichen ein-/Ausgabevorgänge pro Sekunde auf dem Node.

- **Mbps**

  Der Durchsatz auf dem Node, gemessen in Megabyte pro Sekunde.

- **Flash Cache Liest**

  Der Prozentsatz an Leseoperationen auf dem Node, die mit dem Cache zufrieden sind, anstatt von der Festplatte zurückgegeben zu werden.

  Flash Cache-Daten werden nur für Nodes und nur angezeigt, wenn ein Flash Cache Modul im Node installiert ist.

- **Verwendete Leistungskapazität**

  Der Prozentsatz der Performance-Kapazität, die vom Node verbraucht wird.

  Daten zur Performance-Kapazität sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.

- **Nutzung**

  Gibt an, ob die CPU oder der Arbeitsspeicher auf dem Node überlastet sind.

- **Freie Kapazität**

  Die ungenutzte Speicherkapazität des Nodes in Gigabyte

- **Gesamtkapazität**

  Die gesamte Storage-Kapazität des Node in Gigabyte

- * Cluster*

  Der Cluster, zu dem der Node gehört. Sie können auf den Namen des Clusters klicken, um zur Detailseite des Clusters zu navigieren.

- **Grenzwertrichtlinie**

  Die benutzerdefinierte Performance-Schwellenwertrichtlinie, die für dieses Storage-Objekt aktiv ist, oder Richtlinien. Sie können den Cursor über Richtliniennamen mit Ellipsen (…) positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen **Performance Threshold Policy** und **Clear Performance Threshold Policy** bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Inventarseite für Performance/Aggregate

Die Seite „Performance/Aggregates Inventory“ zeigt eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jedes Aggregat an, das durch eine Instanz von Unified Manager überwacht wird. Auf dieser Seite können Sie die Performance Ihrer Aggregate überwachen und Fehler bei Performance-Problemen und Schwellenwerten beheben.

Je nachdem, wie Sie diese Seite aufrufen, wird möglicherweise ein anderer Titel auf der Seite angezeigt, um anzugeben, ob die Liste gefiltert wurde. Wenn beispielsweise alle Aggregate angezeigt werden, lautet der Titel „`Aggregate`“. Wenn Sie eine Untergruppe von Aggregaten anzeigen, die von der Seite Threshold Policies zurückgegeben werden, lautet der Titel „`Aggregates“, auf die Policy aggr_IOPS angewendet wird`“.

Mit den Schaltflächen oben auf der Seite können Sie Suchen durchführen, um bestimmte Daten zu finden, Filter zu erstellen und anzuwenden, um die Liste der angezeigten Daten einzugrenzen und die Daten auf der Seite in A zu exportieren `.csv` Datei, und fügen Sie Spalten auf der Seite hinzu oder entfernen Sie sie.

Standardmäßig werden Objekte auf den Objektbestandsseiten sortiert, basierend auf dem Kritikereignis der Objektleistung. Objekte mit kritischen Ereignissen werden zuerst aufgeführt und Objekte mit Warnmeldungen

werden als zweites aufgeführt. Dies bietet eine unmittelbare visuelle Darstellung von Problemen, die behoben werden müssen. Die Werte der Leistungsindikatoren basieren auf einem Durchschnitt aus den Daten der letzten 72 oder mehr Stunden, wie auf der Seite angegeben. Sie können auf die Schaltfläche „Aktualisieren“ klicken, um die Objektbestandsdaten zu aktualisieren.

Über die Schaltflächen **Performance Threshold Policy** und **Clear PerformanceThreshold Policy** können Sie Schwellenwertrichtlinien für beliebige Objekte auf den Objektbestandsseiten zuweisen oder löschen.

Root-Aggregate werden auf dieser Seite nicht angezeigt.

Aggregiert Spalten der Inventarseite

Die Seite „Performance/Aggregates Inventory“ enthält die folgenden Spalten für jedes Aggregat.

- **Status**

  Ein gesundes Objekt ohne aktive Ereignisse zeigt ein grünes Häkchen-Symbol ( ). Wenn das Objekt über ein aktives Ereignis verfügt, identifiziert das Symbol für die Ereignisanzeige den Schweregrad: Kritische Ereignisse sind rot (Die Fehlerereignisse sind orange ( ), und Warnereignisse sind gelb ( ).

- * Aggregat*

  Sie können auf den Aggregatnamen klicken, um zur Seite mit den Performance-Details dieses Aggregats zu navigieren.

- **Aggregattyp**

  Der Aggregattyp:

  - HDD
  - Hybrid

    Kombiniert HDDs und SSDs, aber Flash Pool wurde nicht aktiviert.

  - Hybrid (Flash Pool)

    Kombiniert HDDs und SSDs und ermöglicht die Aktivierung von Flash Pool.

  - SSD
  - SSD (FabricPool)

    Kombiniert SSDs mit einer Cloud-Tier

  - VMDisk (SDS)

    Virtuelle Laufwerke innerhalb einer virtuellen Maschine

  - VMDisk (FabricPool)

    Kombiniert virtuelle Festplatten mit einer Cloud-Tier

  - LUN (FlexArray) in dieser Spalte wird „`not available`“ angezeigt, wenn auf dem überwachten Speichersystem eine ONTAP-Version vor 8.3 ausgeführt wird.

- **Latenz**

  Die durchschnittliche Reaktionszeit aller I/O-Anforderungen im Aggregat, ausgedrückt in Millisekunden pro Vorgang

- **IOPS**

  Die ein-/Ausgabevorgänge pro Sekunde auf dem Aggregat.

- **Mbps**

  Der Durchsatz im Aggregat, gemessen in Megabyte pro Sekunde.

- **Verwendete Leistungskapazität**

  Der Prozentsatz der Performance-Kapazität, die vom Aggregat verwendet wird.

  Daten zur Performance-Kapazität sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.

- **Nutzung**

  Der Prozentsatz der aktuell verwendeten Festplatten des Aggregats.

- **Freie Kapazität**

  Die ungenutzte Storage-Kapazität dieses Aggregats sind Gigabyte.

- **Gesamtkapazität**

  Die gesamte Storage-Kapazität dieses Aggregats ist Gigabyte.

- **Inaktive Datenberichterstattung**

  Gibt an, ob die Funktion zur Berichterstellung inaktiver Daten auf diesem Aggregat aktiviert oder deaktiviert ist. Bei Aktivierung zeigen Volumes auf diesem Aggregat auf der Seite „Performance/Volumes Inventory“ den Umfang der „kalten“ Daten an.

  Der Wert in diesem Feld lautet „`N/A`“, wenn die Version von ONTAP keine inaktive Datenberichterstattung unterstützt.

- * Cluster*

  Der Cluster, zu dem das Aggregat gehört. Sie können auf den Cluster-Namen klicken, um zur Detailseite des jeweiligen Clusters zu gelangen.

- **Knoten**

  Der Node, zu dem das Aggregat gehört. Sie können auf den Node-Namen klicken, um zur Detailseite dieses Node zu navigieren.

- **Grenzwertrichtlinie**

  Die benutzerdefinierte Performance-Schwellenwertrichtlinie, die für dieses Storage-Objekt aktiv ist, oder Richtlinien. Sie können den Cursor über Richtliniennamen mit Ellipsen (…) positionieren, um den

vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen **Performance Threshold Policy** und **Clear Performance Threshold Policy** bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Inventarseite für Performance/Volumes

Die Seite „Performance/Volumes Inventory“ zeigt eine Übersicht über die Performance-Ereignisse, Zählerdaten und Konfigurationsinformationen für jedes FlexVol Volume und jedes FlexGroup Volume, die durch eine Instanz von Unified Manager überwacht werden. So können Sie die Performance Ihrer Volumes schnell überwachen und Performance-Probleme sowie Schwellenwertereignisse beheben.

Je nachdem, wie Sie zu dieser Seite navigieren, wird oben auf der Seite möglicherweise ein anderer Titel angezeigt, um anzugeben, ob die Liste gefiltert wurde. Wenn beispielsweise alle Volumes angezeigt werden, lautet der Titel „`Volumes`“. Wenn Sie eine Untergruppe von Volumes anzeigen, die von der Seite Threshold Policies zurückgesendet wird, lautet der Titel „`Volumes, auf denen Policy: vol_IOPS`“ angewendet wird.

Mit den Schaltflächen oben auf der Seite können Sie Suchen durchführen, um bestimmte Daten zu finden, Filter zu erstellen und anzuwenden, um die Liste der angezeigten Daten einzugrenzen und die Daten auf der Seite in A zu exportieren `.csv` Datei, und fügen Sie Spalten auf der Seite hinzu oder entfernen Sie sie.

Standardmäßig werden Objekte auf den Objektbestandsseiten sortiert, basierend auf dem Kritikereignis der Objektleistung. Objekte mit kritischen Ereignissen werden zuerst aufgeführt und Objekte mit Warnmeldungen werden als zweites aufgeführt. Dies bietet eine unmittelbare visuelle Darstellung von Problemen, die behoben werden müssen. Die Werte der Leistungsindikatoren basieren auf einem Durchschnitt aus den Daten der letzten 72 oder mehr Stunden, wie auf der Seite angegeben. Sie können auf die Schaltfläche „Aktualisieren“ klicken, um die Objektbestandsdaten zu aktualisieren.

Für Datensicherungs-Volumes (DP) werden nur Zählerwerte für den benutzergenerierten Datenverkehr angezeigt. Wenn das Cluster mit einer Version der ONTAP Software vor 8.3 installiert ist, werden keine Zählerwerte angezeigt.

Über die Schaltflächen **Performance Threshold Policy** und **Clear PerformanceThreshold Policy** können Sie Schwellenwertrichtlinien für beliebige Objekte auf den Objektbestandsseiten zuweisen oder löschen.

Root-Volumes werden auf dieser Seite nicht angezeigt.

Spalten der Seite „Volumeninventar“

Die Seite „Performance/Volumes Inventory“ enthält die folgenden Spalten für jedes Volume:

- **Status**

  Ein gesundes Objekt ohne aktive Ereignisse zeigt ein grünes Häkchen-Symbol (). Wenn das Objekt über ein aktives Ereignis verfügt, identifiziert das Symbol für die Ereignisanzeige den Schweregrad: Kritische Ereignisse sind rot ()Die Fehlerereignisse sind orange (), und Warnereignisse sind gelb ( ).

- **Lautstärke**

Der Name des Volume. Sie können auf den Volume-Namen klicken, um zur Seite mit den Performance-Details des Volumes zu gelangen.

- **Stil**

  Stil eines Volumes, entweder FlexVol oder FlexGroup.

- **Latenz**

  Bei FlexVol Volumes ist dies die durchschnittliche Antwortzeit des Volumes für alle I/O-Anfragen, die in Millisekunden pro Vorgang ausgedrückt wird. Bei FlexGroup Volumes ist dies die durchschnittliche Latenz aller zusammengehörigen Volumes.

- **IOPS**

  Für FlexVol Volumes ist dies die Anzahl der ein-/Ausgabevorgänge pro Sekunde für das Volume. Bei FlexGroup Volumes ist dies die Summe der IOPS für alle zusammengehörigen Volumes.

- **Mbps**

  Bei FlexVol Volumes ist dies der Durchsatz auf dem Volume, der in Megabyte pro Sekunde gemessen wird. Bei FlexGroup Volumes entspricht dies der Summe der MB/s für alle zusammengehörigen Volumes.

- **Freie Kapazität**

  Die ungenutzte Storage-Kapazität des Volumes, ausgedrückt in Gigabyte

- **Gesamtkapazität**

  Die gesamte Storage-Kapazität des Volumes, ausgedrückt in Gigabyte

- **Tiering-Richtlinie**

  Die Tiering-Richtlinie für das Volume. Die Richtlinie wirkt sich nur dann aus, wenn das Volume auf einem FabricPool Aggregat bereitgestellt wird. Folgende Richtlinien stehen zur Verfügung:

  - Keine. Die Daten für dieses Volume verbleiben immer auf der Performance-Tier.
  - Nur Snapshot. Nur Snapshot Daten werden automatisch in die Cloud-Tier verschoben. Alle anderen Daten verbleiben in der Performance-Tier.
  - Backup: Bei Datensicherungs-Volumes werden alle übertragenen Benutzerdaten in der Cloud-Tier gestartet, aber bei späteren Client-Lesezugriffen kann es dazu kommen, heiße Daten zurück in die Performance-Tier zu verschieben.
  - Automatisch. Daten auf diesem Volume werden automatisch zwischen Performance-Tier und Cloud-Tier verschoben, wenn ONTAP feststellt, dass die Daten „`Hot`“ oder „`Cold`“ sind.

- **Kalte Daten**

  Die Größe der auf dem Volume gespeicherten Benutzerdaten, die inaktiv sind (kalte).

  Der Wert wird in den folgenden Situationen als „`N/A`“ aufgelistet:

  - Wenn „`inaktive Datenberichterstattung`“ auf dem Aggregat deaktiviert ist, auf dem sich das Volume befindet.
  - Wenn „`inaktive Datenberichterstattung`“ aktiviert ist, die Mindestdauer für die

Datenerfassung jedoch nicht erreicht wurde.

  - Wenn Sie die Tiering-Richtlinie „`Backup`“ verwenden oder eine Version von ONTAP vor 9.4 verwenden (wenn keine inaktive Datenberichterstattung verfügbar ist).

- * Cloud-Empfehlung*

  Unified Manager führt für jedes Volume eine Kapazitätsanalyse durch, um zu ermitteln, ob Sie die Festplattenauslastung Ihres Storage-Systems verbessern und Speicherplatz auf der Performance-Tier einsparen können, indem inaktive Daten (kalte) Daten auf die Cloud-Tier verschoben werden. Wenn die Empfehlung “Tier” lautet, bewegen Sie den Cursor über das Wort **Tier**, um die Empfehlung anzuzeigen. Mögliche Empfehlungen sind:

  - Lernen. Es wurden nicht genügend Daten gesammelt, um eine Empfehlung zu treffen.
  - Ebene: Die Analyse hat festgestellt, dass das Volume inaktive (kalte) Daten enthält und dass Sie das Volume so konfigurieren sollten, dass diese Daten in das Cloud-Tier verschoben werden.
  - Keine Aktion. Entweder das Volume verfügt über wenig inaktive Daten oder das Volume wurde bereits auf die Tiering-Richtlinie „`Auto`“ gesetzt oder die ONTAP Version unterstützt FabricPool nicht. Wenn Sie mit der Rolle „OnCommand Administrator“ oder „Speicheradministrator“ bei Unified Manager angemeldet sind, können Sie den Cursor über das Wort **Stufe** bewegen. Der Link „Volume konfigurieren“ steht zum Starten des System Managers zur Verfügung, damit Sie die empfohlene Änderung vornehmen können.

- * Cluster*

  Der Cluster, zu dem das Volume gehört. Sie können auf den Cluster-Namen klicken, um zur Detailseite des jeweiligen Clusters zu gelangen.

- **Knoten**

  Der Name des Node, auf dem sich das FlexVol Volume befindet, oder die Anzahl der Nodes, auf denen sich das FlexGroup Volume befindet.

  Bei FlexVol-Volumes können Sie auf der Seite Node-Details auf den Namen klicken, um Node-Details anzuzeigen. Bei FlexGroup Volumes können Sie auf die Zahl klicken, um die Knoten anzuzeigen, die in der FlexGroup auf der Seite Knotenbestand verwendet werden.

- **SVM**

  Die Storage Virtual Machine (SVM), der das Volume angehört. Sie können auf den SVM-Namen klicken, um zur Detailseite dieser SVM zu navigieren.

- * Aggregat*

  Der Name des Aggregats, auf dem sich das FlexVol Volume befindet, oder die Anzahl der Aggregate, auf denen sich das FlexGroup Volume befindet.

  Bei FlexVol Volumes können Sie auf den Namen klicken, um Details zum Aggregat auf der Detailseite anzuzeigen. Bei FlexGroup Volumes können Sie auf die Zahl klicken, um die Aggregate anzuzeigen, die in der FlexGroup auf der Seite „Aggregates Inventory“ verwendet werden.

- **Grenzwertrichtlinie**

  Die benutzerdefinierte Performance-Schwellenwertrichtlinie, die für dieses Storage-Objekt aktiv ist, oder Richtlinien. Sie können den Cursor über Richtliniennamen mit Ellipsen (…) positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die

Schaltflächen **Performance Threshold Policy** und **Clear Performance Threshold Policy** bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Inventarseite für Performance/Ports

Die Seite „Performance/Ports Inventory“ zeigt eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jeden Port an, der von einer Instanz von Unified Manager überwacht wird. So können Sie die Performance Ihrer Ports schnell überwachen und Performance-Probleme sowie Schwellenwertereignisse beheben.

Die Werte des Performance-Zähler werden nur für physische Ports angezeigt. Zählerwerte werden nicht für VLANs oder Interface Groups angezeigt.

Je nachdem, wie Sie zu dieser Seite navigieren, wird oben auf der Seite möglicherweise ein anderer Titel angezeigt, um anzugeben, ob die Liste gefiltert wurde. Wenn z. B. alle Ports angezeigt werden, lautet der Titel „`Ports`“. Wenn Sie eine Untergruppe von Ports anzeigen, die von der Seite Threshold Policies zurückgegeben werden, lautet der Titel „`Ports, auf denen Policy: Port_IOPS` angewendet wird.

Mit den Schaltflächen oben auf der Seite können Sie Suchen durchführen, um bestimmte Daten zu finden, Filter zu erstellen und anzuwenden, um die Liste der angezeigten Daten einzugrenzen und die Daten auf der Seite in A zu exportieren `.csv` Datei, und fügen Sie Spalten auf der Seite hinzu oder entfernen Sie sie.

Standardmäßig werden Objekte auf den Objektbestandsseiten sortiert, basierend auf dem Kritikereignis der Objektleistung. Objekte mit kritischen Ereignissen werden zuerst aufgeführt und Objekte mit Warnmeldungen werden als zweites aufgeführt. Dies bietet eine unmittelbare visuelle Darstellung von Problemen, die behoben werden müssen. Die Werte der Leistungsindikatoren basieren auf einem Durchschnitt aus den Daten der letzten 72 oder mehr Stunden, wie auf der Seite angegeben. Sie können auf die Schaltfläche „Aktualisieren“ klicken, um die Objektbestandsdaten zu aktualisieren.

Über die Schaltflächen **Performance Threshold Policy** und **Clear PerformanceThreshold Policy** können Sie Schwellenwertrichtlinien für beliebige Objekte auf den Objektbestandsseiten zuweisen oder löschen.

Ports Inventory Page Spalten

Die Seite „Performance/Ports Inventory“ enthält die folgenden Spalten für jeden Port:

- **Status**

  Ein gesundes Objekt ohne aktive Ereignisse zeigt ein grünes Häkchen-Symbol ( ). Wenn das Objekt über ein aktives Ereignis verfügt, identifiziert das Symbol für die Ereignisanzeige den Schweregrad: Kritische Ereignisse sind rot (Die Fehlerereignisse sind orange ( ), und Warnereignisse sind gelb ( ).

- **Port**

  Sie können auf den Portnamen klicken, um zur Seite mit den Leistungsdetails dieses Ports zu navigieren.

- **Typ**

  Der Porttyp ist entweder Netzwerk oder Fibre Channel Protocol (FCP).

- **Mbps**

  Der Durchsatz auf dem Port, gemessen in Megabyte pro Sekunde.

- **Nutzung**

  Der Prozentsatz der verfügbaren Bandbreite des Ports, die derzeit verwendet wird.

- * Cluster*

  Der Cluster, zu dem der Port gehört. Sie können auf den Cluster-Namen klicken, um zur Detailseite des jeweiligen Clusters zu gelangen.

- **Knoten**

  Der Node, zu dem der Port gehört. Sie können auf den Node-Namen klicken, um zur Detailseite dieses Node zu navigieren.

- **Geschwindigkeit**

  Die maximale Datentransferrate für den Port.

- * Rolle*

  Die Netzwerkanschlussfunktion: Entweder Data oder Cluster. FCP-Ports können keine Rolle enthalten, und die Rolle wird als „N/A“ angezeigt

- **Grenzwertrichtlinie**

  Die benutzerdefinierte Performance-Schwellenwertrichtlinie, die für dieses Storage-Objekt aktiv ist, oder Richtlinien. Sie können den Cursor über Richtliniennamen mit Ellipsen (…) positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen **Performance Threshold Policy** und **Clear Performance Threshold Policy** bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Inventarseite für Performance/SVMs

Die Seite „Performance/SVMs Inventory“ bietet einen Überblick über Performance-Ereignisse, Daten und Konfigurationsinformationen für jede Storage Virtual Machine (SVM), die durch eine Instanz von Unified Manager überwacht wird. So können Sie die Performance Ihrer SVMs schnell überwachen und Performance-Probleme sowie Schwellwerte beheben.

Je nachdem, wie Sie zu dieser Seite navigieren, wird oben auf der Seite möglicherweise ein anderer Titel angezeigt, um anzugeben, ob die Liste gefiltert wurde. Wenn Sie beispielsweise alle SVMs anzeigen, lautet der Titel „`SVMs`“. Wenn Sie einen Teilsatz von SVMs anzeigen, der von der Seite Threshold Policies zurückgegeben wird, lautet der Titel „`SVMs auf welcher Richtlinie: SVM_IOPS angewendet wird`“.

Mit den Schaltflächen oben auf der Seite können Sie Suchen durchführen, um bestimmte Daten zu finden, Filter zu erstellen und anzuwenden, um die Liste der angezeigten Daten einzugrenzen und die Daten auf der Seite in A zu exportieren `.csv` Datei, und fügen Sie Spalten auf der Seite hinzu oder entfernen Sie sie.

Standardmäßig werden Objekte auf den Objektbestandsseiten sortiert, basierend auf dem Kritikereignis der

Objektleistung. Objekte mit kritischen Ereignissen werden zuerst aufgeführt und Objekte mit Warnmeldungen werden als zweites aufgeführt. Dies bietet eine unmittelbare visuelle Darstellung von Problemen, die behoben werden müssen. Die Werte der Leistungsindikatoren basieren auf einem Durchschnitt aus den Daten der letzten 72 oder mehr Stunden, wie auf der Seite angegeben. Sie können auf die Schaltfläche „Aktualisieren“ klicken, um die Objektbestandsdaten zu aktualisieren.

Über die Schaltflächen **Performance Threshold Policy** und **Clear PerformanceThreshold Policy** können Sie Schwellenwertrichtlinien für beliebige Objekte auf den Objektbestandsseiten zuweisen oder löschen.

Die SVMs, die auf dieser Seite aufgeführt werden, umfassen nur Data and Cluster SVMs. Unified Manager verwendet bzw. zeigt keine Admin- oder Node-SVMs an.

Spalten der „SVMs Inventory“-Seite

Die Seite „Performance/SVMs Inventory“ enthält die folgenden Spalten für jede SVM:

- **Status**

  Ein gesundes Objekt ohne aktive Ereignisse zeigt ein grünes Häkchen-Symbol ( ). Wenn das Objekt über ein aktives Ereignis verfügt, identifiziert das Symbol für die Ereignisanzeige den Schweregrad: Kritische Ereignisse sind rot (Die Fehlerereignisse sind orange ( ), und Warnereignisse sind gelb ( ).

- **SVM**

  Sie können auf den SVM-Namen klicken, um zur Seite mit den Performance-Details dieser SVM zu gelangen.

- **Latenz**

  Die durchschnittliche Reaktionszeit aller I/O-Anforderungen, ausgedrückt in Millisekunden pro Vorgang

- **IOPS**

  Die ein-/Ausgabevorgänge pro Sekunde für die SVM.

- **Mbps**

  Der Durchsatz der SVM wurde in Megabyte pro Sekunde gemessen.

- **Freie Kapazität**

  Die ungenutzte Storage-Kapazität der SVM in Gigabyte

- **Gesamtkapazität**

  Die gesamte Storage-Kapazität der SVM in Gigabyte

- * Cluster*

  Der Cluster, zu dem die SVM gehört. Sie können auf den Cluster-Namen klicken, um zur Detailseite des jeweiligen Clusters zu gelangen.

- **Grenzwertrichtlinie**

Die benutzerdefinierte Performance-Schwellenwertrichtlinie, die für dieses Storage-Objekt aktiv ist, oder Richtlinien. Sie können den Cursor über Richtliniennamen mit Ellipsen (…) positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen **Performance Threshold Policy** und **Clear Performance Threshold Policy** bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Seite „Performance/LUNs Inventory“ (Inventar

Die Seite „Performance/LUNs Inventory“ zeigt eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jede LUN an, die durch eine Instanz von Unified Manager überwacht wird. So können Sie die Performance Ihrer LUNs schnell überwachen und Performance-Probleme sowie Schwellenwertereignisse beheben.

Je nachdem, wie Sie zu dieser Seite navigieren, wird oben auf der Seite möglicherweise ein anderer Titel angezeigt, um anzugeben, ob die Liste gefiltert wurde. Beispiel: Wenn alle LUNs angezeigt werden, lautet der Titel „`LUNs`“. Wenn Sie eine Untergruppe von LUNs anzeigen, die von der Seite Threshold Policies zurückgegeben wird, lautet der Titel „`LUNs auf denen Policy: LUN_IOPS is appliced`“.

Mit den Schaltflächen oben auf der Seite können Sie Suchen durchführen, um bestimmte Daten zu finden, Filter zu erstellen und anzuwenden, um die Liste der angezeigten Daten einzugrenzen und die Daten auf der Seite in A zu exportieren `.csv` Datei, und fügen Sie Spalten auf der Seite hinzu oder entfernen Sie sie.

Standardmäßig werden Objekte auf den Objektbestandsseiten sortiert, basierend auf dem Kritikereignis der Objektleistung. Objekte mit kritischen Ereignissen werden zuerst aufgeführt und Objekte mit Warnmeldungen werden als zweites aufgeführt. Dies bietet eine unmittelbare visuelle Darstellung von Problemen, die behoben werden müssen. Die Werte der Leistungsindikatoren basieren auf einem Durchschnitt aus den Daten der letzten 72 oder mehr Stunden, wie auf der Seite angegeben. Sie können auf die Schaltfläche „Aktualisieren“ klicken, um die Objektbestandsdaten zu aktualisieren.

Über die Schaltflächen **Performance Threshold Policy** und **Clear PerformanceThreshold Policy** können Sie Schwellenwertrichtlinien für beliebige Objekte auf den Objektbestandsseiten zuweisen oder löschen.

Spalten auf der Seite „LUNs-Inventar“

Die Seite „Performance/LUNs Inventory“ enthält die folgenden Spalten für jede LUN:

- **Status**

  Ein gesundes Objekt ohne aktive Ereignisse zeigt ein grünes Häkchen-Symbol (). Wenn das Objekt über ein aktives Ereignis verfügt, identifiziert das Symbol für die Ereignisanzeige den Schweregrad: Kritische Ereignisse sind rot (Die Fehlerereignisse sind orange (), und Warnereignisse sind gelb ( ).

- **LUN**

  Sie können auf den LUN-Namen klicken, um zur Seite mit den Performance-Details dieser LUN zu gelangen.

- **Latenz**

  Die durchschnittliche Reaktionszeit aller I/O-Anforderungen, ausgedrückt in Millisekunden pro Vorgang

- **IOPS**

  Die ein-/Ausgabevorgänge pro Sekunde für die LUN.

- **Mbps**

  Der Durchsatz auf der LUN, gemessen in Megabyte pro Sekunde.

- **Freie Kapazität**

  Die ungenutzte Speicherkapazität der LUN in Gigabyte

- **Gesamtkapazität**

  Die gesamte Storage-Kapazität der LUN in Gigabyte

- * Cluster*

  Der Cluster, zu dem die LUN gehört. Sie können auf den Cluster-Namen klicken, um zur Detailseite des jeweiligen Clusters zu gelangen.

- **Knoten**

  Der Node, zu dem die LUN gehört. Sie können auf den Node-Namen klicken, um zur Detailseite dieses Node zu navigieren.

- **SVM**

  Die Storage Virtual Machine (SVM), der die LUN angehört. Sie können auf den SVM-Namen klicken, um zur Detailseite dieser SVM zu navigieren.

- * Aggregat*

  Das Aggregat, zu dem die LUN gehört. Sie können auf den Aggregatnamen klicken, um zur Detailseite des jeweiligen Aggregats zu navigieren.

- **Lautstärke**

  Das Volume, zu dem die LUN gehört. Sie können auf den Volume-Namen klicken, um zur Detailseite des betreffenden Volumes zu navigieren.

- **Grenzwertrichtlinie**

  Die benutzerdefinierte Performance-Schwellenwertrichtlinie, die für dieses Storage-Objekt aktiv ist, oder Richtlinien. Sie können den Cursor über Richtliniennamen mit Ellipsen (…) positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen **Performance Threshold Policy** und **Clear Performance Threshold Policy** bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Inventarseite für Namespaces

Die Seite Namesaces Inventory zeigt eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jeden Namespace an, der von einer Instanz von Unified Manager überwacht wird. So können Sie die Performance und den Zustand

Ihrer Namespaces schnell überwachen und Probleme sowie Schwellenwertereignisse beheben.

Je nachdem, wie Sie zu dieser Seite navigieren, wird oben auf der Seite möglicherweise ein anderer Titel angezeigt, um anzugeben, ob die Liste gefiltert wurde. Wenn beispielsweise alle Namespaces angezeigt werden, lautet der Titel „`Namesaces`“. Wenn Sie eine Untermenge von Namespaces anzeigen, die von der Seite Threshold Policies zurückgesendet wird, lautet der Titel „`Namespaces“, auf dem Richtlinie: Namespace_IOPS angewendet wird`“.

Mit den Schaltflächen oben auf der Seite können Sie Suchen durchführen, um bestimmte Daten zu finden, Filter zu erstellen und anzuwenden, um die Liste der angezeigten Daten einzugrenzen und die Daten auf der Seite in A zu exportieren `.csv` Datei, und fügen Sie Spalten auf der Seite hinzu oder entfernen Sie sie.

Standardmäßig werden Objekte auf den Objektbestandsseiten sortiert, basierend auf dem Kritikereignis der Objektleistung. Objekte mit kritischen Ereignissen werden zuerst aufgeführt und Objekte mit Warnmeldungen werden als zweites aufgeführt. Dies bietet eine unmittelbare visuelle Darstellung von Problemen, die behoben werden müssen. Die Werte der Leistungsindikatoren basieren auf einem Durchschnitt aus den Daten der letzten 72 oder mehr Stunden, wie auf der Seite angegeben. Sie können auf die Schaltfläche „Aktualisieren“ klicken, um die Objektbestandsdaten zu aktualisieren.

Über die Schaltflächen **Performance Threshold Policy** und **Clear PerformanceThreshold Policy** können Sie Schwellenwertrichtlinien für beliebige Objekte auf den Objektbestandsseiten zuweisen oder löschen.

Spalten der Inventarseite der Namespaces

Die Seite Namesaces Inventory enthält für jeden Namespace die folgenden Spalten:

- **Subsystem**

  Das Subsystem des Namespace.

- **Status**

  Ein gesundes Objekt ohne aktive Ereignisse zeigt ein grünes Häkchen-Symbol (). Wenn das Objekt über ein aktives Ereignis verfügt, identifiziert das Symbol für die Ereignisanzeige den Schweregrad: Kritische Ereignisse sind rot (Die Fehlerereignisse sind orange (), und Warnereignisse sind gelb ( ).

- **Namespace**

  Sie können auf den Namespace-Namen klicken, um zur Seite mit den Performance-Details dieses Namespaces zu navigieren.

- **Bundesland**

  Der aktuelle Status des Namespaces.

  - Offline - Lese- oder Schreibzugriff auf den Namespace ist nicht zulässig.
  - Online - Lese- und Schreibzugriff auf den Namespace ist erlaubt.
  - NV-Fehler: Der Namespace wurde automatisch aufgrund eines NVRAM-Fehlers in den Offline-Modus versetzt.
  - Speicherfehler - für den Namespace ist nicht mehr genügend Speicherplatz vorhanden.

- **SVM**

Die Storage Virtual Machine (SVM), zu der der Namespace gehört. Sie können auf den SVM-Namen klicken, um zur Detailseite dieser SVM zu navigieren.

- * Cluster*

  Der Cluster, zu dem der Namespace gehört. Sie können auf den Cluster-Namen klicken, um zur Detailseite des jeweiligen Clusters zu gelangen.

- **Lautstärke**

  Das Volume, zu dem der Namespace gehört. Sie können auf den Volume-Namen klicken, um zur Detailseite des betreffenden Volumes zu navigieren.

- **Gesamtkapazität**

  Die gesamte Storage-Kapazität des Namespace in Gigabyte.

- **Freie Kapazität**

  Die ungenutzte Speicherkapazität des Namespace in Gigabyte.

- **IOPS**

  Die ein-/Ausgabevorgänge pro Sekunde für den Namespace.

- **Latenz**

  Die durchschnittliche Reaktionszeit aller I/O-Anforderungen im Namespace, angegeben in Millisekunden pro Vorgang

- **Mbps**

  Der Durchsatz im Namespace gemessen in Megabyte pro Sekunde.

- **Grenzwertrichtlinie**

  Die benutzerdefinierte Performance-Schwellenwertrichtlinie, die für dieses Storage-Objekt aktiv ist, oder Richtlinien. Sie können den Cursor über Richtliniennamen mit Ellipsen (…) positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen **Performance Threshold Policy** und **Clear Performance Threshold Policy** bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Performance/LIFs Inventarseite

Die Seite Performance/LIFs-Bestandsaufnahme zeigt eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jede LIF an, die von dieser Instanz von Unified Manager überwacht wird. Auf dieser Seite können Sie die Performance Ihrer LIFs schnell überwachen und Performance-Probleme sowie Schwellenwertereignisse beheben.

Je nachdem, wie Sie zur Seite „Performance/LIFs Inventar“ navigieren, wird oben auf der Seite möglicherweise ein anderer Titel angezeigt, um anzugeben, ob die Liste gefiltert wurde. Beispielsweise lautet der Titel „`LIFs`“, wenn alle LIFs angezeigt werden. Beim Anzeigen einer Untermenge von LIFs, die von der

Seite Threshold Policies zurückgegeben wird, lautet der Titel „`LIFs", auf denen die Richtlinie: LIF_IOPS angewendet wird`“.

Mit den Schaltflächen oben auf der Seite können Sie Suchen durchführen, um bestimmte Daten zu finden, Filter zu erstellen und anzuwenden, um die Liste der angezeigten Daten einzugrenzen und die Daten auf der Seite in A zu exportieren `.csv` Datei, und fügen Sie Spalten auf der Seite hinzu oder entfernen Sie sie.

Standardmäßig werden Objekte auf den Objektbestandsseiten sortiert, basierend auf dem Kritikereignis der Objektleistung. Objekte mit kritischen Ereignissen werden zuerst aufgeführt und Objekte mit Warnmeldungen werden als zweites aufgeführt. Dies bietet eine unmittelbare visuelle Darstellung von Problemen, die behoben werden müssen. Die Werte der Leistungsindikatoren basieren auf einem Durchschnitt aus den Daten der letzten 72 oder mehr Stunden, wie auf der Seite angegeben. Sie können auf die Schaltfläche „Aktualisieren“ klicken, um die Objektbestandsdaten zu aktualisieren.

Über die Schaltflächen **Performance Threshold Policy** und **Clear PerformanceThreshold Policy** können Sie Schwellenwertrichtlinien für beliebige Objekte auf den Objektbestandsseiten zuweisen oder löschen.

Die auf der Seite „Performance/LIFs Inventory“ aufgeführten LIFs enthalten Daten-LIFs, Cluster-LIFs, Node Management LIFs und Intercluster LIFs. Unified Manager verwendet keine System-LIFs oder zeigt diese an.

Spalten der LIFs-Inventarseite

Die Seite „Performance/LIFs Inventar“ enthält die folgenden Spalten für jede LIF.

- **Status**

  Ein gesundes Objekt ohne aktive Ereignisse zeigt ein grünes Häkchen-Symbol (). Wenn das Objekt über ein aktives Ereignis verfügt, identifiziert das Symbol für die Ereignisanzeige den Schweregrad: Kritische Ereignisse sind rot (Die Fehlerereignisse sind orange (), und Warnereignisse sind gelb ( ).

- **LIF**

  Sie können auf den LIF-Namen klicken, um zur Seite mit den Performance-Details dieser LIF zu gelangen.

- **Typ**

  LIF-Typ: Netzwerk (iSCSI, NFS, CIFS), FCP oder NVMf FCP.

- **Latenz**

  Die durchschnittliche Reaktionszeit aller I/O-Anforderungen, ausgedrückt in Millisekunden pro Vorgang Die Latenz gilt nicht für NFS LIFs und CIFS LIFs und wird für diese Typen als K. A. angezeigt.

- **IOPS**

  Die ein-/Ausgangsvorgänge pro Sekunde. IOPS gelten nicht für NFS LIFs und CIFS LIFs und wird für diese Typen als „k. A.“ angezeigt.

- **Mbps**

  Der Durchsatz auf dem LIF, gemessen in Megabyte pro Sekunde.

- * Cluster*

Der Cluster, zu dem die LIF gehört. Sie können auf den Namen des Clusters klicken, um zur Detailseite des Clusters zu navigieren.

- **SVM**

  Die Storage Virtual Machine, zu der das LIF gehört. Sie können auf den SVM-Namen klicken, um zur Detailseite dieser SVM zu navigieren.

- **Lage Zu Hause**

  Der Home-Speicherort für die LIF, angezeigt als Node-Name und Port-Name, getrennt durch einen Doppelpunkt (:). Wenn die Position mit Ellipsen (…) angezeigt wird, können Sie den Cursor über den Ortsnamen positionieren, um die vollständige Position anzuzeigen.

- **Aktuelle Position**

  Der aktuelle Speicherort für die LIF, angezeigt als Node-Name und Portname, getrennt durch einen Doppelpunkt (:). Wenn die Position mit Ellipsen (…) angezeigt wird, können Sie den Cursor über den Ortsnamen positionieren, um die vollständige Position anzuzeigen.

- * Rolle*

  Die LIF-Rolle: Daten, Cluster, Node Management oder Intercluster.

- **Grenzwertrichtlinie**

  Die benutzerdefinierte Performance-Schwellenwertrichtlinie, die für dieses Storage-Objekt aktiv ist, oder Richtlinien. Sie können den Cursor über Richtliniennamen mit Ellipsen (…) positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen **Performance Threshold Policy** und **Clear Performance Threshold Policy** bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Überwachung der Leistung mit den Seiten des Performance Explorers

Auf den Seiten des Performance-Explorers werden ausführliche Informationen über die Performance jedes Objekts in einem Cluster angezeigt. Die Seite bietet eine detaillierte Ansicht der Performance aller Cluster-Objekte, sodass Sie die Performance-Daten bestimmter Objekte über verschiedene Zeiträume auswählen und vergleichen können.

Sie können auch die Gesamtleistung aller Objekte beurteilen und Objekt-Performance-Daten in einem Side-by-Side-Format vergleichen.

Wird ein Objekt nicht mehr von Unified Manager verwaltet, wird rechts neben dem Objektnamen oben auf der Seite Performance Explorer der Status **entfernt** angezeigt.

Allgemeines zum Root-Objekt

Das Root-Objekt ist die Basis, mit der andere Objektvergleiche erstellt werden. So lassen sich Daten von anderen Objekten mit dem Root-Objekt anzeigen und vergleichen. So wird eine Performance-Datenanalyse bereitgestellt, mit der Fehler behoben und die

Objekt-Performance verbessert werden kann.

Der Name des Stammobjekts wird oben im Fenster „Vergleichen“ angezeigt. Unter dem Root-Objekt werden zusätzliche Objekte angezeigt. Obwohl die Anzahl der zusätzlichen Objekte, die Sie dem Vergleichbereich hinzufügen können, nicht begrenzt ist, ist nur ein Root-Objekt zulässig. Die Daten für das Root-Objekt werden automatisch in den Diagrammen im Bereich Counter Charts angezeigt.

Das Root-Objekt kann nicht geändert werden. Es ist immer auf die Objektseite eingestellt, die Sie anzeigen. Wenn Sie beispielsweise die Seite Volume Performance Explorer von Volume1 öffnen, ist Volume1 das Root-Objekt und kann nicht geändert werden. Wenn Sie einen Vergleich mit einem anderen Root-Objekt durchführen möchten, müssen Sie auf den Link für ein Objekt klicken und seine Landing Page öffnen.

Ereignisse und Schwellenwerte werden nur für Root-Objekte angezeigt.

Filter anwenden, um die Liste der korrelierten Objekte im Raster zu reduzieren

Durch Filtern können Sie eine kleinere, besser definierte Untergruppe von Objekten im Raster anzeigen. Wenn Sie beispielsweise 25 Volumes in der Tabelle haben, können Sie durch Filtern nur die Volumes anzeigen, die einen Durchsatz von weniger als 90 MB/s oder eine Latenz größer als 1 ms/op. Haben

Festlegen eines Zeitbereichs für korrelierte Objekte

Mit der Auswahl für den Zeitbereich auf der Seite Performance Explorer können Sie den Zeitbereich für den Vergleich von Objektdaten festlegen. Wenn Sie einen Zeitbereich angeben, wird der Inhalt der Seiten des Performance Explorers verfeinert, um nur die Objektdaten innerhalb des von Ihnen angegebenen Zeitbereichs anzuzeigen.

Über diese Aufgabe

Durch die Feinjustierung des Zeitbereichs können nur die Leistungsdaten angezeigt werden, für die Sie sich interessieren. Sie können einen vordefinierten Zeitbereich auswählen oder einen benutzerdefinierten Zeitbereich angeben. Der Standardzeitbereich liegt bei den vorangegangenen 72 Stunden.

Auswählen eines vordefinierten Zeitbereichs

Die Auswahl eines vordefinierten Zeitbereichs stellt eine schnelle und effiziente Möglichkeit dar, die Datenausgabe bei der Anzeige von Cluster-Objekt-Performance-Daten anzupassen und zu fokussieren. Bei der Auswahl eines vordefinierten Zeitbereichs stehen Daten für bis zu 13 Monate zur Verfügung.

Schritte

1. Klicken Sie oben rechts auf der Seite **Performance Explorer** auf **Zeitbereich**.
2. Wählen Sie auf der rechten Seite des Bedienfelds **Zeitbereich Auswahl** einen vordefinierten Zeitbereich aus.
3. Klicken Sie Auf **Bereich Anwenden**.

Festlegen eines benutzerdefinierten Zeitbereichs

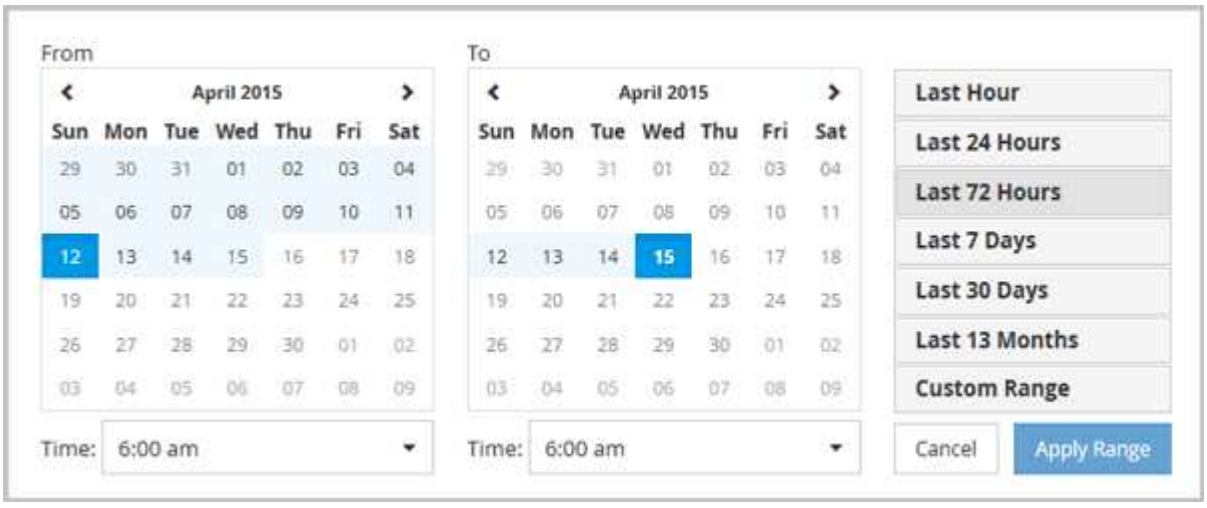
Auf der Seite „Performance Explorer“ können Sie den Datums- und Zeitbereich für Ihre Leistungsdaten angeben. Die Angabe eines benutzerdefinierten Zeitbereichs bietet größere Flexibilität als die Verwendung vordefinierter Zeitbereiche bei der Raffination von Cluster-Objektdaten.

Über diese Aufgabe

Sie können einen Zeitbereich zwischen einer Stunde und 390 Tagen auswählen. 13 Monate sind 390 Tage, weil jeder Monat als 30 Tage gezählt wird. Wenn Sie einen Datums- und Zeitbereich angeben, erhalten Sie weitere Details, mit denen Sie bestimmte Performanceereignisse oder eine Reihe von Ereignissen vergrößern können. Durch das Festlegen eines Zeitbereichs lassen sich auch potenzielle Leistungsprobleme beheben, da durch das Festlegen eines Datums- und Zeitbereichs die Daten des Performance-Ereignisses detaillierter dargestellt werden. Verwenden Sie das Steuerelement **Zeitbereich**, um vordefinierte Datums- und Zeitbereiche auszuwählen, oder geben Sie Ihren eigenen benutzerdefinierten Datums- und Zeitbereich von bis zu 390 Tagen an. Die Schaltflächen für vordefinierte Zeitbereiche variieren von **Letzte Stunde** bis **Letzte 13 Monate**.

Wenn Sie die Option **Letzte 13 Monate** wählen oder einen benutzerdefinierten Datumsbereich größer als 30 Tage angeben, wird ein Dialogfeld angezeigt, in dem Sie darauf hingewiesen werden, dass die Leistungsdaten für einen Zeitraum von mehr als 30 Tagen mit stündlichen Durchschnittswerten und nicht mit einer 5-minütigen Datenabfrage gespeichert werden. Daher kann es zu einem Verlust der visuellen Granularität bei Timeline kommen. Wenn Sie im Dialogfeld auf die Option **nicht wieder anzeigen** klicken, wird die Meldung nicht angezeigt, wenn Sie die Option **Letzte 13 Monate** wählen oder einen benutzerdefinierten Datumsbereich von mehr als 30 Tagen angeben. Die Übersichtsdaten gelten auch für einen kleineren Zeitbereich, wenn der Zeitbereich ein Datum/Uhrzeit enthält, das mehr als 30 Tage von heute entfernt ist.

Bei der Auswahl eines Zeitbereichs (benutzerdefiniert oder vordefiniert) basieren Zeitbereiche von 30 Tagen oder weniger auf 5-Minuten-Intervalldatenproben. Zeitbereiche, die größer als 30 Tage sind, basieren auf einer Stunde Intervalldatenproben.



1. Klicken Sie auf das Dropdown-Feld **Zeitbereich**, und das Fenster Zeitbereich wird angezeigt.
2. Um einen vordefinierten Zeitbereich auszuwählen, klicken Sie rechts neben dem Fenster **Zeitbereich** auf eine der Schaltflächen **Letzte…**. Bei der Auswahl eines vordefinierten Zeitbereichs stehen Daten für bis zu 13 Monate zur Verfügung. Die von Ihnen ausgewählte Schaltfläche für den vordefinierten Zeitbereich wird hervorgehoben, und die entsprechenden Tage und Zeiten werden in den Kalendern und Zeitauswahlschaltern angezeigt.

3. Um einen benutzerdefinierten Datumsbereich auszuwählen, klicken Sie links im Kalender **von** auf das Startdatum. Klicken Sie auf **<** oder **>**, um im Kalender vorwärts oder rückwärts zu navigieren. Um das Enddatum anzugeben, klicken Sie rechts im Kalender **bis** auf ein Datum. Beachten Sie, dass das Standard-Enddatum heute ist, es sei denn, Sie geben ein anderes Enddatum an. Die Schaltfläche **benutzerdefinierter Bereich** rechts neben dem Fenster Zeitbereich wird hervorgehoben, was darauf hinweist, dass Sie einen benutzerdefinierten Datumsbereich ausgewählt haben.
4. Um einen benutzerdefinierten Zeitbereich auszuwählen, klicken Sie unter dem Kalender **von** auf das Steuerelement **Uhrzeit** und wählen die Startzeit aus. Um die Endzeit festzulegen, klicken Sie rechts unter dem **bis**-Kalender auf das Steuerelement **Zeit** und wählen die Endzeit aus. Die Schaltfläche **benutzerdefinierter Bereich** rechts neben dem Fenster Zeitbereich wird hervorgehoben, was darauf hinweist, dass Sie einen benutzerdefinierten Zeitbereich ausgewählt haben.
5. Optional können Sie die Start- und Endzeiten festlegen, wenn Sie einen vordefinierten Datumsbereich auswählen. Wählen Sie den zuvor beschriebenen vordefinierten Datumsbereich aus, und wählen Sie dann die Start- und Endzeiten wie zuvor beschrieben aus. Die ausgewählten Daten werden in den Kalendern markiert, Ihre festgelegten Start- und Endzeiten werden in den Steuerelementen **Zeit** angezeigt und die Schaltfläche **benutzerdefinierter Bereich** ist markiert.
6. Klicken Sie nach Auswahl des Datums- und Zeitbereichs auf **Bereich anwenden**. Die Leistungsstatistiken für diesen Zeitbereich werden in den Diagrammen und in der Zeitleiste „Ereignisse“ angezeigt.

Definieren der Liste der korrelierten Objekte für die Vergleichgrafiken

Im Bereich Zählerdiagramm können Sie eine Liste der korrelierten Objekte für Daten- und Leistungsvergleich definieren. Wenn beispielsweise bei Ihrer Storage Virtual Machine (SVM) ein Performance-Problem auftritt, können Sie alle Volumes in der SVM vergleichen, um das mögliche Problem zu identifizieren.

Über diese Aufgabe

Sie können ein beliebiges Objekt aus dem Raster der korrelierten Objekte den Fenstern „Vergleichen“ und „Zählerdiagramm“ hinzufügen. So können Sie Daten mehrerer Objekte und das Root-Objekt anzeigen und vergleichen. Sie können Objekte in das Raster der korrelierten Objekte hinzufügen und aus diesem entfernen. Das Root-Objekt im Vergleichsfenster kann jedoch nicht entfernt werden.

Das Hinzufügen vieler Objekte zum Vergleichspfenster kann sich negativ auf die Performance auswirken. Um die Leistung zu erhalten, sollten Sie eine begrenzte Anzahl von Diagrammen für den Datenvergleich auswählen.

Schritte

1. Suchen Sie im Objektraster das Objekt, das Sie hinzufügen möchten, und klicken Sie auf die Schaltfläche **Hinzufügen**.

   Die Schaltfläche **Hinzufügen** wird grau, und das Objekt wird der Liste der zusätzlichen Objekte im Fenster Vergleich hinzugefügt. Die Daten des Objekts werden den Diagrammen in den Zähldiagrammen hinzugefügt. Die Farbe des Augensymbols des Objekts ( ) Passt die Farbe der Trend-Zeile des Objekts in den Diagrammen an.

2. Daten für ausgewählte Objekte ausblenden oder anzeigen:

Hier…	Führen Sie diese Aktion durch…
Ausgewähltes Objekt ausblenden	Klicken Sie auf das Augensymbol des ausgewählten Objekts ( ) Im Vergleichfenster. Die Objektdaten sind ausgeblendet, und das Augensymbol für das Objekt wird grau.
Ein ausgeblendtes Objekt anzeigen	Klicken Sie im Vergleichfenster auf das graue Augensymbol des ausgewählten Objekts. Das Augensymbol kehrt in seine ursprüngliche Farbe zurück, und die Objektdaten werden wieder in die Diagramme im Bereich Counter Charts eingefügt.

3. Ausgewählte Objekte aus dem Fensterbereich **Comparing** entfernen:

Hier…	Führen Sie diese Aktion durch…
Ausgewähltes Objekt entfernen	Bewegen Sie den Mauszeiger über den Namen des ausgewählten Objekts im Vergleichenfenster, um die Schaltfläche Objekt entfernen (**X**) anzuzeigen, und klicken Sie dann auf die Schaltfläche. Das Objekt wird aus dem Teilfenster „Vergleichen“ entfernt und seine Daten werden aus den Zählerdiagrammen gelöscht.
Alle ausgewählten Objekte entfernen	Klicken Sie auf die Schaltfläche Alle Objekte entfernen (**X**) oben im Fenster vergleichen. Alle ausgewählten Objekte und ihre Daten werden entfernt, wobei nur das Root-Objekt übrig bleibt.

Allgemeines zu Zählerdiagrammen

Diagramme im Fensterbereich Zählerdiagramme ermöglichen das Anzeigen und Vergleichen von Performancedaten für das Root-Objekt und für Objekte, die Sie aus dem Raster der korrelierten Objekte hinzugefügt haben. Auf diese Weise können Sie Performance-Trends besser verstehen und Performance-Probleme isolieren und lösen.

Standardmäßig werden Zählerdiagramme angezeigt, sind Ereignisse, Latenz, IOPS und MB/s. Optionale Diagramme, die angezeigt werden können, sind Auslastung, verwendete Performance-Kapazität, verfügbare IOPS, IOPS/TB und das Verhältnis „Cache Miss“. Zusätzlich können Sie festlegen, dass sich Gesamtwerte oder Aufbruchwerte für die verwendeten Latenzdiagramme, IOPS, MB/s und Performance-Kapazitäten anzeigen lassen.

Der Performance Explorer zeigt bestimmte Zählerdiagramme standardmäßig an, ob das Speicherobjekt sie alle unterstützt oder nicht. Wenn ein Zähler nicht unterstützt wird, ist das Zählerdiagramm leer und die Meldung `Not applicable for <object>` Wird angezeigt.

Die Diagramme zeigen Leistungstrends für das Root-Objekt und für alle Objekte an, die Sie im Vergleichsanfenster ausgewählt haben. Die Daten in den einzelnen Karten sind wie folgt angeordnet:

- **X-Achse**

  Zeigt den angegebenen Zeitraum an. Wenn Sie keinen Zeitbereich angegeben haben, ist die Standardeinstellung der vorhergehenden 72-Stunden-Periode.

- **Y-Achse**

  Zeigt Zählereinheiten an, die für das ausgewählte Objekt oder Objekte eindeutig sind.

Trendlinienfarben entsprechen der Farbe des Objektnamens, die im vergleichenden Fensterbereich angezeigt wird. Sie können den Cursor auf einer beliebigen Trendlinie über einen Punkt positionieren, um Details zu Zeit und Wert für diesen Punkt anzuzeigen.

Wenn Sie einen bestimmten Zeitraum innerhalb eines Diagramms untersuchen möchten, können Sie eine der folgenden Methoden verwenden:

- Mit der Schaltfläche **<** können Sie den Bereich Counter Charts erweitern, um die Breite der Seite zu erweitern.
- Verwenden Sie den Cursor (wenn er zu einer Lupe übergeht), um einen Teil des Zeitrahmens im Diagramm auszuwählen, um diesen Bereich zu fokussieren und zu vergrößern. Sie können auf „Diagramm zurücksetzen“ klicken, um das Diagramm auf den Standardzeitraum zurückzusetzen.
- Verwenden Sie die Taste **Zoom View**, um ein großes Einzelcounter-Diagramm anzuzeigen, das erweiterte Details und Schwellenwertanzeigen enthält.

Gelegentlich werden Lücken in den Trendlinien angezeigt. Defizite bedeuten, dass entweder Unified Manager Performancedaten aus dem Storage-System sammeln konnte, oder dass Unified Manager möglicherweise nicht verfügbar war.

Arten von Performance-Zählerdiagrammen

Es gibt Standard-Performance-Diagramme, in denen die Zählerwerte für das ausgewählte Speicherobjekt angezeigt werden. In jedem der Counter-Diagramme werden die Gesamtwerte angezeigt, die in Lese-, Schreib- und andere Kategorien unterteilt sind. Darüber hinaus zeigen einige Counter-Diagramme zusätzliche Details an, wenn das Diagramm in der Zoom-Ansicht angezeigt wird.

In der folgenden Tabelle sind die verfügbaren Performance-Zählerdiagramme aufgeführt.

Verfügbare Diagramme	Diagrammbeschreibung
Veranstaltungen	Zeigt kritische, Fehler-, Warn- und Informationsereignisse an, die mit den statistischen Diagrammen für das Root-Objekt korreliert sind. Zusätzlich zu den Performance-Ereignissen werden Systemzustandsereignisse angezeigt, um einen vollständigen Überblick über die Gründe zu geben, warum die Performance beeinträchtigt werden könnte.

Verfügbare Diagramme	Diagrammbeschreibung
Latenz Insgesamt	Anzahl der Millisekunden, die erforderlich sind, um auf Applikationsanforderungen zu reagieren. Beachten Sie, dass die durchschnittlichen Latenzwerte I/O-gewichtet sind.
Latenz - Aufschlüsselung	Dieselben Informationen, die in der Latenzzeit gesamt angezeigt werden, jedoch mit getrennten Performance-Daten in Lese-, Schreib- und sonstige Latenz.die Diagrammoption gilt nur, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume, eine LUN ist. Oder Namespace.
Latenz – Cluster-Komponenten	Dieselben Informationen, die in Latenz-Summe angezeigt werden, jedoch mit den Performance-Daten getrennt nach Cluster-Komponente in Latenz.Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volume ist.
IOPS – gesamt	Anzahl der pro Sekunde verarbeiteten ein-/Ausgabevorgänge.
IOPS – Aufschlüsselung	Die gleichen Informationen, die auf dem IOPS-Wert insgesamt angezeigt werden, jedoch mit getrennten Performance-Daten in Lese-, Schreib- und sonstige IOPS. Bei Anzeige in der Zoom-Ansicht zeigt das Diagramm Volumes die minimalen und maximalen Durchsatzwerte der QoS an, sofern diese in ONTAP konfiguriert sind. Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume, eine LUN, Oder Namespace.
IOPS – Protokolle	Die gleichen Informationen, die unter IOPS insgesamt angezeigt werden, aber die Performance-Daten werden in individuelle Diagramme für den Datenverkehr mit CIFS-, NFS-, FCP-, NVMe- und iSCSI-Protokollen unterteilt. Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt eine SVM ist.

Verfügbare Diagramme	Diagrammbeschreibung
IOPS/TB – gesamt	Anzahl der pro Sekunde verarbeiteten ein-/Ausgabevorgänge, basierend auf dem gesamten Speicherplatz, der vom Workload in Terabyte verbraucht wird. Dieser Zähler, auch I/O-Dichte genannt, misst die Performance mit einer bestimmten Menge an Storage-Kapazität.bei Anzeige in der Zoom-Ansicht zeigt das Diagramm Volumes QoS erwartet und Spitzendurchsatzwerte an, falls es in ONTAP konfiguriert ist. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volume ist.
MB/s – Gesamt	Anzahl der Megabyte an Daten, die in das Objekt und vom Objekt pro Sekunde übertragen werden.
Mbps - Aufschlüsselung	Dieselben Informationen, die im Diagramm MB/s angezeigt werden, jedoch mit Trennung der MB/s-Daten in Festplattenlesevorgänge, Flash Cache Lese-, Schreib- und andere MB/s.bei Anzeige in der Ansicht Zoom zeigt das Volume-Diagramm QoS-Maximaldurchsatz an, sofern es in ONTAP konfiguriert ist. Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume, eine LUN, Oder Namespace. Flash Cache-Daten werden nur für Nodes und nur angezeigt, wenn ein Flash Cache Modul im Node installiert ist.
Genutzte Performance-Kapazität – Insgesamt	Prozentsatz der Performance-Kapazität, die vom Node oder Aggregat verbraucht wird Daten zur Performance-Kapazität sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.
Genutzte Performance-Kapazität – Aufschlüsselung	Die verwendete Performance-Kapazität ist in Benutzerprotokolle und Systembackground-Prozesse unterteilt. Darüber hinaus wird die Menge der freien Performance-Kapazität dargestellt.

Verfügbare Diagramme	Diagrammbeschreibung
Verfügbare IOPS – gesamt	Anzahl der ein-/Ausgabevorgänge pro Sekunde, die derzeit für dieses Objekt verfügbar sind (frei). Diese Zahl ergibt sich aus der Subtraktion der derzeit verwendeten IOPS von den IOPS-Gesamtwerten, die Unified Manager berechnet, die das Objekt ausführen kann. Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt ein Knoten oder Aggregat ist. Verfügbare IOPS-Daten sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.
Auslastung – Gesamt	Verfügbarer Prozentsatz der verfügbaren Ressource des Objekts, das verwendet wird. Die Auslastung zeigt Node-Auslastung für Nodes, Festplattenauslastung für Aggregate und die Bandbreitenauslastung für Ports an. Diese Diagrammoption gilt nur, wenn es sich um ein Node, Aggregat oder Port handelt.
Cache-Miss-Verhältnis - Gesamt	Prozentsatz von Leseanforderungen von Client-Applikationen, die von der Festplatte zurückgegeben werden, anstatt vom Cache zurückgegeben zu werden. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volume ist.

Auswählen der anzuzeigenden Leistungsdiagramme

In der Dropdown-Liste Diagramme auswählen können Sie die Arten von Performance-Zählerdiagrammen auswählen, die im Bereich Counter Charts angezeigt werden sollen. So können Sie basierend auf Ihren Performance-Anforderungen bestimmte Daten und Zähler anzeigen.

Schritte

1. Klicken Sie im Fensterbereich **Counter Charts** auf die Dropdown-Liste **Diagramme auswählen**.
2. Diagramme hinzufügen oder entfernen:

An…	Tun Sie das…
Einzelne Diagramme hinzufügen oder entfernen	Aktivieren Sie die Kontrollkästchen neben den Diagrammen, die Sie anzeigen oder ausblenden möchten
Alle Diagramme hinzufügen	Klicken Sie Auf **Alle Auswählen**

An…	Tun Sie das…
Alle Diagramme entfernen	Klicken Sie Auf **Auswahl Aufheben**

Ihre Diagrammauswahl wird im Bereich Counter Charts angezeigt. Beachten Sie, dass beim Hinzufügen von Diagrammen die neuen Diagramme in den Bereich Counter Charts eingefügt werden, um mit der Reihenfolge der Diagramme zu übereinstimmen, die in der Dropdown-Liste Choose Charts aufgeführt sind. Wenn Sie weitere Diagramme auswählen, muss möglicherweise ein zusätzliches Scrollen durchgeführt werden.

Erweitern des Fensterbereichs Counter Charts

Sie können das Fenster Zählerdiagramme so erweitern, dass die Diagramme größer und lesbarer sind.

Über diese Aufgabe

Nachdem Sie die Vergleichsobjekte und den Zeitbereich für Zähler definiert haben, können Sie einen größeren Counter Charts-Bereich anzeigen. Sie verwenden die **<**-Schaltfläche in der Mitte des Performance Explorer-Fensters, um das Fenster zu erweitern.

Schritte

1. Erweitern oder verkleinern Sie das Fenster **Counter Charts**.

An…	Tun Sie das…
Erweitern Sie das Fenster Counter Charts, um die Breite der Seite anzupassen	Klicken Sie auf die Schaltfläche **<**
Verkleinern Sie das Fenster Counter Charts auf die rechte Hälfte der Seite	Klicken Sie auf die Schaltfläche **>**

Ändern des Fokus der Zählerdiagramme auf einen kürzeren Zeitraum

Mit der Maus können Sie den Zeitbereich reduzieren, um sich auf einen bestimmten Zeitraum im Bereich Zählerdiagramm oder im Fenster Zoomansicht der Zählerdiagramme zu konzentrieren. So sehen Sie eine granularere und mikroskopische Ansicht aller Teile der Zeitachse von Performance-Daten, Ereignissen und Schwellenwerten.

Bevor Sie beginnen

Der Cursor muss in eine Lupe geändert werden, um anzuzeigen, dass diese Funktion aktiv ist.

Bei Verwendung dieser Funktion, die die Zeitleiste so ändert, dass Werte angezeigt werden, die der detaillierteren Anzeige entsprechen, ändert sich der Zeit- und Datumsbereich im Auswahlfeld **Zeitbereich** nicht von den ursprünglichen Werten für das Diagramm.

Schritte

1. Um einen bestimmten Zeitraum anzuzeigen, klicken Sie auf die Lupe und ziehen Sie die Maus, um den Bereich hervorzuheben, den Sie im Detail sehen möchten.

   Die Zählerwerte für den ausgewählten Zeitraum füllen das Zählerdiagramm aus.

2. Um zum ursprünglichen Zeitabschnitt zurückzukehren, der im Auswahlfeld **Zeitbereich** festgelegt wurde, klicken Sie auf die Schaltfläche **Diagrammzoom zurücksetzen**.

   Das Zählerdiagramm wird im Originalzustand angezeigt.

Anzeigen von Ereignisdetails in der Ereigniszeitleiste

Sie können alle Ereignisse und ihre zugehörigen Details im Fenster „Zeitleiste für Ereignisse“ des Performance Explorers anzeigen. Dies ist eine schnelle und effiziente Methode zur Anzeige aller Zustand- und Performance-Ereignisse, die sich während eines bestimmten Zeitbereichs auf dem Root-Objekt auftraten, die bei der Fehlerbehebung von Performance-Problemen hilfreich sein können.

Über diese Aufgabe

Im Bereich Ereigniszeitleiste werden kritische Ereignisse, Fehler, Warnungen und Informationsereignisse angezeigt, die während des ausgewählten Zeitbereichs auf dem Root-Objekt aufgetreten sind. Jeder Schweregrad eines Ereignisses hat seine eigene Zeitachse. Einzelne oder mehrere Ereignisse werden durch einen Ereignispunkt in der Zeitleiste dargestellt. Sie können den Cursor über einen Ereignispunkt positionieren, um die Ereignisdetails anzuzeigen. Um die visuelle Granularität mehrerer Ereignisse zu erhöhen, kann der Zeitbereich verkürzt werden. Dadurch werden mehrere Ereignisse in einzelne Ereignisse verteilt, sodass Sie jedes Ereignis einzeln anzeigen und untersuchen können.

Jeder Punkt des Performance-Ereignisses in der Ereignisleiste wird vertikal mit einer entsprechenden Spitze in den Zählerdiagrammen-Trendlinien, die unter der Ereigniszeitleiste angezeigt werden, angeordnet. Dies bietet eine direkte visuelle Korrelation zwischen Ereignissen und Gesamtleistung. Systemzustandsereignisse werden auch in der Zeitleiste angezeigt, jedoch entsprechen diese Arten von Ereignissen nicht unbedingt einer Spitze in einem der Performance-Diagramme.

Schritte

1. Positionieren Sie den Cursor im Fensterbereich **Ereignisleiste** über einen Ereignispunkt in einer Zeitleiste, um eine Zusammenfassung des Ereignisses oder der Ereignisse an diesem Punkt anzuzeigen.

   In einem Popup-Dialogfeld werden Informationen zu den Ereignistypen, zu Datum und Uhrzeit des Ereignisses, zum Status und zur Dauer des Ereignisses angezeigt.

2. Vollständige Ereignisdetails für ein oder mehrere Ereignisse anzeigen:

Hier…	Klicken Sie hier…
Zeigen Sie Details zu einem einzelnen Event an	**Ereignisdetails anzeigen** im Popup-Dialog.

Hier…	Klicken Sie hier…
Zeigen Sie Details für mehrere Ereignisse an	**Ereignisdetails anzeigen** im Popup-Dialog. Durch Klicken auf ein einzelnes Ereignis im Dialogfeld mehrere Ereignisse wird die entsprechende Seite Ereignisdetails angezeigt.

Zählerdiagramme Ansicht „Zoom“

Die Zählerdiagramme bieten eine Zoom-Ansicht, mit der Sie Leistungsdetails über den angegebenen Zeitraum vergrößern können. So lassen sich Performance-Details und Ereignisse wesentlich granularer anzeigen, was bei der Behebung von Performance-Problemen von Vorteil ist.

Wenn in der Zoom-Ansicht angezeigt wird, bieten einige der Abbruchdiagramme zusätzliche Informationen, die angezeigt werden, wenn sich das Diagramm nicht in der Zoom-Ansicht befindet. So werden beispielsweise im Aufschlüsselung der IOPS, IOPS/TB und MB/s auf den Seiten der Zoom-Ansicht QoS-Richtlinienwerte für Volumes und LUNs angezeigt, wenn sie in ONTAP festgelegt wurden.

Bei systemdefinierten Performance-Schwellenwerten stehen nur die Richtlinien „`Node-Ressourcen überausgelastet`“ und „`QoS Throughput Limit Inered`“ in der Liste **Policies** zur Verfügung. Die anderen systemdefinierten Schwellwertrichtlinien stehen derzeit nicht zur Verfügung.

Anzeigen der Zoom-Ansicht der Zählerdiagramme

Die Zoom-Ansicht der Zählerdiagramme bietet eine feinere Detailebene für das ausgewählte Zählerdiagramm und die zugehörige Zeitleiste. Dadurch werden die Daten der Zählerdiagramme vergrößert, sodass Sie einen schärfereren Überblick über Performanceereignisse und deren zugrunde liegende Ursachen haben können.

Über diese Aufgabe

Sie können die Zoom-Ansicht der Zählerdiagramme für jedes Zählerdiagramm anzeigen.

Schritte

1. Klicken Sie auf **Zoom View**, um das ausgewählte Diagramm zu öffnen ein neues Browser-Fenster.
2. Wenn Sie ein Diagramm anzeigen und dann auf **Zoom View** klicken, wird das Diagramm in Zoom View angezeigt. Wenn Sie die Ansichtsoption ändern möchten, können Sie in der Zoom-Ansicht **Gesamt** auswählen.

Festlegen des Zeitbereichs in der Zoom-Ansicht

Mit dem Steuerelement **Zeitbereich** im Fenster Zähldiagramme Zoom-Ansicht können Sie einen Datums- und Zeitbereich für das ausgewählte Diagramm festlegen. So können Sie bestimmte Daten schnell auf Basis eines voreingestellten Zeitbereichs oder eines

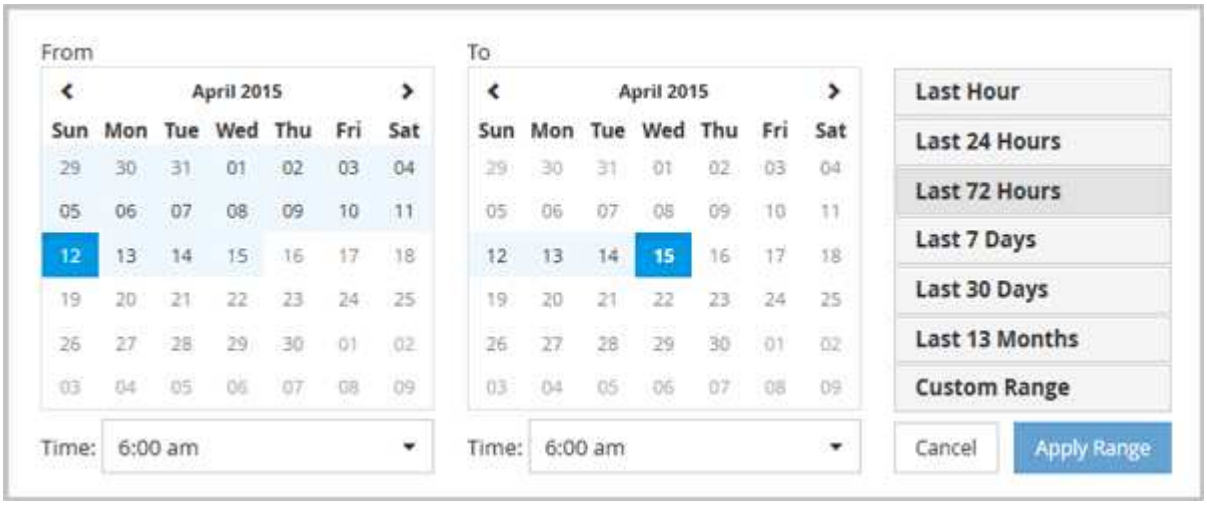
eigenen benutzerdefinierten Zeitbereichs finden.

Über diese Aufgabe

Sie können einen Zeitbereich zwischen einer Stunde und 390 Tagen auswählen. 13 Monate sind 390 Tage, weil jeder Monat als 30 Tage gezählt wird. Wenn Sie einen Datums- und Zeitbereich angeben, erhalten Sie weitere Details, mit denen Sie bestimmte Performanceereignisse oder eine Reihe von Ereignissen vergrößern können. Durch das Festlegen eines Zeitbereichs lassen sich auch potenzielle Leistungsprobleme beheben, da durch das Festlegen eines Datums- und Zeitbereichs die Daten des Performance-Ereignisses detaillierter dargestellt werden. Verwenden Sie das Steuerelement **Zeitbereich**, um vordefinierte Datums- und Zeitbereiche auszuwählen, oder geben Sie Ihren eigenen benutzerdefinierten Datums- und Zeitbereich von bis zu 390 Tagen an. Die Schaltflächen für vordefinierte Zeitbereiche variieren von **Letzte Stunde** bis **Letzte 13 Monate**.

Wenn Sie die Option **Letzte 13 Monate** wählen oder einen benutzerdefinierten Datumsbereich größer als 30 Tage angeben, wird ein Dialogfeld angezeigt, in dem Sie darauf hingewiesen werden, dass die Leistungsdaten für einen Zeitraum von mehr als 30 Tagen mit stündlichen Durchschnittswerten und nicht mit einer 5-minütigen Datenabfrage gespeichert werden. Daher kann es zu einem Verlust der visuellen Granularität bei Timeline kommen. Wenn Sie im Dialogfeld auf die Option **nicht wieder anzeigen** klicken, wird die Meldung nicht angezeigt, wenn Sie die Option **Letzte 13 Monate** wählen oder einen benutzerdefinierten Datumsbereich von mehr als 30 Tagen angeben. Die Übersichtsdaten gelten auch für einen kleineren Zeitbereich, wenn der Zeitbereich ein Datum/Uhrzeit enthält, das mehr als 30 Tage von heute entfernt ist.

Bei der Auswahl eines Zeitbereichs (benutzerdefiniert oder vordefiniert) basieren Zeitbereiche von 30 Tagen oder weniger auf 5-Minuten-Intervalldatenproben. Zeitbereiche, die größer als 30 Tage sind, basieren auf einer Stunde Intervalldatenproben.



1. Klicken Sie auf das Dropdown-Feld **Zeitbereich**, und das Fenster Zeitbereich wird angezeigt.
2. Um einen vordefinierten Zeitbereich auszuwählen, klicken Sie rechts neben dem Fenster **Zeitbereich** auf eine der Schaltflächen **Letzte…**. Bei der Auswahl eines vordefinierten Zeitbereichs stehen Daten für bis zu 13 Monate zur Verfügung. Die von Ihnen ausgewählte Schaltfläche für den vordefinierten Zeitbereich wird hervorgehoben, und die entsprechenden Tage und Zeiten werden in den Kalendern und Zeitauswahlschaltern angezeigt.
3. Um einen benutzerdefinierten Datumsbereich auszuwählen, klicken Sie links im Kalender **von** auf das Startdatum. Klicken Sie auf **<** oder **>**, um im Kalender vorwärts oder rückwärts zu navigieren. Um das Enddatum anzugeben, klicken Sie rechts im Kalender **bis** auf ein Datum. Beachten Sie, dass das Standard-Enddatum heute ist, es sei denn, Sie geben ein anderes Enddatum an. Die Schaltfläche **benutzerdefinierter Bereich** rechts neben dem Fenster Zeitbereich wird hervorgehoben, was darauf

hinweist, dass Sie einen benutzerdefinierten Datumsbereich ausgewählt haben.

4. Um einen benutzerdefinierten Zeitbereich auszuwählen, klicken Sie unter dem Kalender **von** auf das Steuerelement **Uhrzeit** und wählen die Startzeit aus. Um die Endzeit festzulegen, klicken Sie rechts unter dem **bis**-Kalender auf das Steuerelement **Zeit** und wählen die Endzeit aus. Die Schaltfläche **benutzerdefinierter Bereich** rechts neben dem Fenster Zeitbereich wird hervorgehoben, was darauf hinweist, dass Sie einen benutzerdefinierten Zeitbereich ausgewählt haben.
5. Optional können Sie die Start- und Endzeiten festlegen, wenn Sie einen vordefinierten Datumsbereich auswählen. Wählen Sie den zuvor beschriebenen vordefinierten Datumsbereich aus, und wählen Sie dann die Start- und Endzeiten wie zuvor beschrieben aus. Die ausgewählten Daten werden in den Kalendern markiert, Ihre festgelegten Start- und Endzeiten werden in den Steuerelementen **Zeit** angezeigt und die Schaltfläche **benutzerdefinierter Bereich** ist markiert.
6. Klicken Sie nach Auswahl des Datums- und Zeitbereichs auf **Bereich anwenden**. Die Leistungsstatistiken für diesen Zeitbereich werden in den Diagrammen und in der Zeitleiste „Ereignisse“ angezeigt.

Auswählen von Leistungsschwellenwerten in der Zoom-Ansicht der Zählerdiagramme

Das Anwenden von Schwellenwerten in der Zoom-Ansicht von Zählerdiagrammen bietet eine detaillierte Ansicht der Vorkommen von Performance-Schwellenwerten. Auf diese Weise können Sie Schwellenwerte anwenden oder entfernen und die Ergebnisse sofort anzeigen. Dies kann bei der Entscheidung hilfreich sein, ob die Fehlerbehebung Ihr nächster Schritt sein sollte.

Über diese Aufgabe

Durch Auswahl von Schwellenwerten in der Zoom-Ansicht für Zählerdiagramme können Sie präzise Daten zu Ereignissen mit Leistungsschwellenwerten anzeigen. Sie können jeden Schwellenwert anwenden, der im Bereich **Richtlinien** der Zoom-Ansicht der Zählerdiagramme angezeigt wird.

Es kann jeweils nur eine Richtlinie auf das Objekt in der Zoom-Ansicht der Zählerdiagramme angewendet werden.

Schritte

1. Wählen Sie das aus oder heben Sie die Auswahl auf Das ist einer Richtlinie zugeordnet.

   Der ausgewählte Schwellenwert wird auf die Zoom-Ansicht der Zählerdiagramme angewendet. Kritische Schwellenwerte werden als rote Linie angezeigt. Warnschwellenwerte werden als gelbe Linie angezeigt.

Anzeige der minimalen und maximalen Einstellungen für Workload-QoS

In den Performance Explorer-Diagrammen können Sie die durch ONTAP definierten Quality of Service (QoS)-Richtlinieneinstellungen auf einem Volume oder einer LUN anzeigen. Die Einstellung für den maximalen Durchsatz begrenzt die Auswirkungen konkurrierender Workloads auf die Systemressourcen. Eine Einstellung für den Durchsatz stellt sicher, dass ein wichtiger Workload das Mindestdurchsatz erfüllt, unabhängig von der Nachfrage durch konkurrierende Workloads.

Über diese Aufgabe

QoS-Durchsatz „`minimum`“ und „`maximum`“ IOPS- und MB/s-Einstellungen werden in den Zählerdiagrammen

nur angezeigt, wenn sie in ONTAP konfiguriert wurden. Durchsatzminimum-Einstellungen sind nur auf Systemen mit ONTAP 9.2 oder neuer Software, nur auf AFF Systemen verfügbar. Diese Einstellungen lassen sich derzeit nur für IOPS festlegen.

Adaptive QoS-Richtlinien sind ab ONTAP 9.3 verfügbar und werden mit IOPS/TB statt IOPS ausgedrückt. Durch diese Richtlinien wird der QoS-Richtlinienwert automatisch auf Basis der Volume-Größe pro Workload angepasst. Auf diese Weise bleibt das Verhältnis von IOPS zu Terabyte erhalten, wenn sich das Volume ändert. Sie können eine anpassungsfähige QoS-Richtliniengruppe nur auf Volumes anwenden. Die QoS-Terminologie „`erwarted`“ und „`Peak`“ werden für anpassungsfähige QoS-Richtlinien statt der minimalen und maximalen Größe verwendet.

Unified Manager generiert Warnereignisse bei Verletzungen der QoS-Richtlinien, wenn der Workload-Durchsatz die festgelegte Richtlinieneinstellung für QoS während jeder Performance-Einsammlung in der vorherigen Stunde überschritten hat. Der Workload-Durchsatz kann den QoS-Schwellenwert für nur einen kurzen Zeitraum während des jeweiligen Erfassungszeitraums überschreiten. Unified Manager zeigt jedoch den „`average`“-Durchsatz während des Erfassungszeitraums auf dem Diagramm an. Aus diesem Grund werden QoS-Ereignisse angezeigt, während der Durchsatz für einen Workload möglicherweise nicht den in der Tabelle aufgeführten Richtlinienschwellenwert überschritten hat.

Schritte

1. Führen Sie auf der Seite **Performance Explorer** für das ausgewählte Volume oder die ausgewählte LUN die folgenden Aktionen durch, um die QoS-Decken- und Bodeneinstellungen anzuzeigen:

Ihr Ziel ist	Tun Sie das…
IOPS-Obergrenze anzeigen (max. QoS)	Klicken Sie im Diagramm IOPS Total oder Breakdown auf **Zoom View**.
Anzeige der MB/s-Obergrenze (QoS max.)	Klicken Sie im Diagramm MB/s Total oder Breakdown auf **Zoom View**.
IOPS-Bereich anzeigen (QoS-Min.)	Klicken Sie im Diagramm IOPS Total oder Breakdown auf **Zoom View**.
Anzeige der IOPS/TB-Obergrenze (QoS-Spitzenwert)	Klicken Sie bei Volumes im Diagramm IOPS/TB auf **Zoom View**.
Anzeige des IOPS/TB-Bodens (QoS erwartet)	Klicken Sie bei Volumes im Diagramm IOPS/TB auf **Zoom View**.

   Die gestrichelte horizontale Linie gibt den in ONTAP festgelegten maximalen oder minimalen Durchsatzwert an. Sie können auch anzeigen, wann Änderungen an den QoS-Werten implementiert wurden.

2. Um die spezifischen Werte für IOPS und MB/s im Vergleich zur QoS-Einstellung anzuzeigen, bewegen Sie den Cursor in den Diagrammbereich, um das Popup-Fenster anzuzeigen.

Nachdem Sie fertig sind

Wenn bei bestimmten Volumes oder LUNs eine sehr hohe IOPS oder MB/s vorhanden ist und die Systemressourcen besonders stark belastet werden, können Sie mit System Manager oder der ONTAP CLI die

QoS-Einstellungen so anpassen, dass diese Workloads sich nicht auf die Performance anderer Workloads auswirken.

Weitere Informationen zum Anpassen der QoS-Einstellungen finden Sie im Power Guide *ONTAP 9 zur Leistungsüberwachung*.

"ONTAP 9 Leistungsüberwachung – Stromversorgungshandbuch"

Wie verschiedene Arten von QoS-Richtlinien in Unified Manager angezeigt werden

Sie können die von ONTAP definierten Richtlinieneinstellungen für die Quality of Service (QoS) anzeigen, die auf ein Volume oder eine LUN angewendet wurden. Diese Einstellungen finden Sie in den Diagrammen zu IOPS/TB und MB/s im Performance Explorer. Die in den Diagrammen angezeigten Informationen unterscheiden sich je nach QoS-Richtlinie, die auf den Workload angewendet wurde.

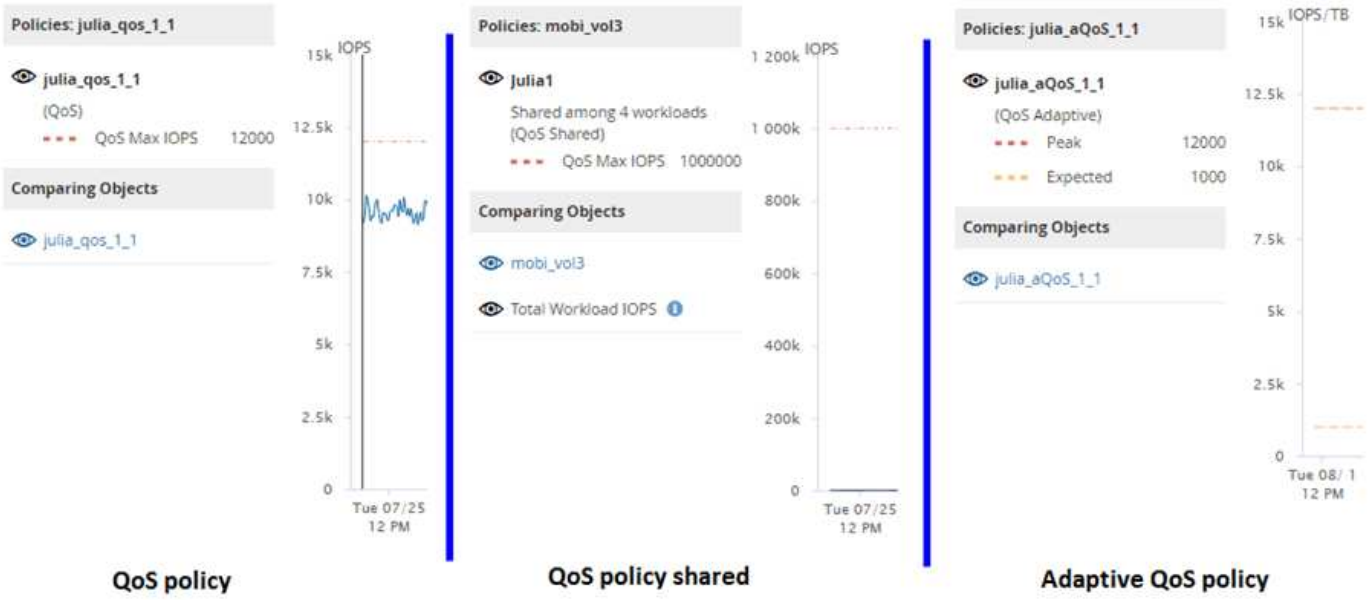
Eine Einstellung für den Durchsatz „`ceiling`“ definiert den maximalen Durchsatz, den der Workload verbrauchen kann, und begrenzt somit die Auswirkungen auf konkurrierende Workloads für Systemressourcen. Durch eine Einstellung für den Durchsatz „`Boden`“ wird der Mindestdurchsatz definiert, der für den Workload verfügbar sein muss, damit ein wichtiger Workload die Mindestdurchsatz-Ziele erfüllt, unabhängig von der Nachfrage durch konkurrierende Workloads.

Gemeinsame und nicht gemeinsam genutzte QoS-Richtlinien für IOPS und MB/s definieren Boden und Decke mit den Begriffen „`minimum`“ und „`maximum`“. Adaptive QoS-Richtlinien für IOPS/TB, die mit ONTAP 9.3 eingeführt wurden, definieren Boden und Obergrenze mit den Begriffen „`erwarted`“ und „`Peak`“.

Mit ONTAP können Sie diese zwei Arten von QoS-Richtlinien erstellen, abhängig davon, wie sie auf Workloads angewendet werden, gibt es in den Performance-Diagrammen drei Arten, die QoS-Richtlinie angezeigt wird.

Art der Richtlinie	Funktionalität	Anzeige in der Unified Manager-Schnittstelle
QoS-Richtlinien für gemeinsame Workloads, die einem einzelnen Workload zugewiesen sind oder QoS-Richtlinien, die nicht gemeinsam genutzt werden, die einem einzelnen Workload oder mehreren Workloads zugewiesen sind	Jeder Workload kann die angegebene Durchsatzeinstellung belegen	Zeigt „`(QoS)`“ an.
QoS-Richtlinien für gemeinsame Nutzung, die mehreren Workloads zugewiesen sind	Alle Workloads teilen sich die angegebene Durchsatzeinstellung	Zeigt „`(QoS Shared)`“ an.
Anpassungsfähige QoS-Richtlinie, die einem einzelnen oder mehreren Workloads zugewiesen ist	Jeder Workload kann die angegebene Durchsatzeinstellung belegen	Zeigt „`(QoS Adaptive)`“ an

Die folgende Abbildung zeigt ein Beispiel dafür, wie die drei Optionen in den Zählerdiagrammen angezeigt werden.



Wenn eine normale QoS-Richtlinie, die in IOPS definiert wurde, im IOPS/TB-Diagramm für einen Workload angezeigt wird, konvertiert ONTAP den IOPS-Wert in einen IOPS/TB-Wert, und Unified Manager zeigt diese Richtlinie im IOPS/TB-Diagramm zusammen mit dem Text „`QoS", definiert in IOPS`“ an.

Wenn eine in IOPS/TB definierte anpassungsfähige QoS-Richtlinie im IOPS-Diagramm für einen Workload angezeigt wird, konvertiert ONTAP den IOPS/TB-Wert in einen IOPS-Wert und Unified Manager zeigt diese Richtlinie im IOPS-Diagramm zusammen mit dem Text „`QoS Adaptive, Definiert in IOPS/Used TB`" oder „`QoS Adaptive, definiert in IOPS/zugewiesenen TB`“, abhängig davon, wie die Einstellung für die IOPS-Spitzenzuweisung konfiguriert ist. Wenn die Zuweisungseinstellung auf „`Alered-space`“ festgelegt ist, wird der IOPS-Spitzenwert basierend auf der Größe des Volumes berechnet. Wenn die Zuweisungseinstellung auf „`used-space`“ festgelegt ist, wird die IOPS-Spitzenauslastung basierend auf der im Volume gespeicherten Datenmenge unter Berücksichtigung der Storage-Effizienz berechnet.

Das IOPS/TB-Diagramm zeigt Performance-Daten nur dann an, wenn die logische Kapazität, die vom Volume verwendet wird, größer als oder gleich 1 TB ist. In der Tabelle werden Lücken angezeigt, wenn die genutzte Kapazität während des ausgewählten Zeitrahmens unter 1 TB fällt.

Anzeigen der Volume-Latenz nach Clusterkomponente

Sie können detaillierte Latenzinformationen zu einem Volume mithilfe der Seite Performance/Volume Explorer anzeigen. Das Zählerdiagramm „Latenz“ zeigt die gesamte Latenz auf dem Volume an, und das Diagramm „Latenz – Aufschlüsselung der Zähler“ ist hilfreich, um die Auswirkungen der Lese- und Schreiblatenz auf das Volume zu ermitteln.

Über diese Aufgabe

Außerdem zeigt das Diagramm Latenz – Cluster-Komponenten einen detaillierten Vergleich der Latenz der einzelnen Cluster-Komponenten an, um zu ermitteln, wie jede Komponente zu der gesamten Latenz auf dem Volume beiträgt. Die folgenden Cluster-Komponenten werden angezeigt:

- Netzwerk
- QoS-Richtlinie

- Netzwerkverarbeitung
- Cluster Interconnect
- Datenverarbeitung
- Aggregatvorgänge
- MetroCluster-Ressourcen
- Cloud-Latenz
- Sync SnapMirror

Schritte

1. Wählen Sie auf der Seite **Performance/Volume Explorer** für Ihr ausgewähltes Volume im Latenzdiagramm im Dropdown-Menü die Option **Cluster Components** aus.

   Das Diagramm Latenz – Cluster-Komponenten wird angezeigt.

2. Um eine größere Version des Diagramms anzuzeigen, wählen Sie **Zoom-Ansicht**.

   Das Vergleichsdiagramm für die Cluster-Komponente wird angezeigt. Sie können den Vergleich einschränken, indem Sie die Auswahl aufheben oder auswählen Der jeder Cluster-Komponente zugeordnet ist.

3. Um die spezifischen Werte anzuzeigen, bewegen Sie den Cursor in den Diagrammbereich, um das Popup-Fenster anzuzeigen.

Anzeigen von SVM-IOPS-Traffic nach Protokoll

Sie können detaillierte IOPS-Informationen für eine SVM über die Seite „Performance/SVM Explorer“ anzeigen. Das Zählerdiagramm „IOPS – Zählerdiagramm“ zeigt die gesamte IOPS-Auslastung auf der SVM. Das Zählerdiagramm „IOPS – Aufschlüsselung Sie dient zur Ermittlung der Auswirkungen von Lese-, Schreib- und anderen IOPS auf die SVM.

Über diese Aufgabe

Außerdem zeigt das Diagramm „IOPS – Protokolle“ einen detaillierten Vergleich des IOPS-Datenverkehrs für jedes auf der SVM zu verwendenden Protokoll. Folgende Protokolle sind verfügbar:

- CIFS
- NFS
- FCP
- ISCSI
- NVMe

Schritte

1. Wählen Sie auf der Seite **Performance/SVM Explorer** für Ihre ausgewählte SVM aus dem IOPS-Diagramm im Dropdown-Menü die Option **Protokolle** aus.

   Das Diagramm IOPS – Protokolle wird angezeigt.

2. Um eine größere Version des Diagramms anzuzeigen, wählen Sie **Zoom-Ansicht**.

   Das erweiterte IOPS-Protokoll-Vergleichstabelle wird angezeigt. Sie können den Vergleich einschränken, indem Sie die Auswahl aufheben oder auswählen Dies ist mit einem Protokoll verbunden.

3. Um die spezifischen Werte anzuzeigen, bewegen Sie den Cursor in den Diagrammbereich eines der beiden Diagramme, um das Popup-Fenster anzuzeigen.

Anzeigen der Latenzdiagramme von Volumes und LUNs zur Überprüfung der Performance-Garantie

Sie können die Volumes und LUNs, die Sie für das Programm „`Performance Guarantee`“ abonniert haben, anzeigen, um zu überprüfen, dass die Latenz den Wert nicht überschritten hat, den Sie garantiert haben.

Über diese Aufgabe

Die Garantie für Latenz-Performance beträgt eine Millisekunde pro Operation, der nicht überschritten werden sollte. Er basiert auf einem stündlichen Durchschnitt und nicht auf dem Standardzeitraum der Performance-Erfassung in fünf Minuten.

Schritte

1. Wählen Sie auf der Seite **Performance Volumes** oder **Performance LUNs** Inventory den gewünschten Datenträger oder LUN aus.
2. Wählen Sie auf der Seite **Performance Explorer** für das ausgewählte Volumen oder die ausgewählte LUN aus dem Auswahlfeld **Statistik in** aus.

   Die horizontale Linie im Latenzdiagramm zeigt eine reibungslosere Linie, da die 5-Minuten-Sammlungen durch den Durchschnitt pro Stunde ersetzt werden.

3. Wenn Sie andere Volumes auf demselben Aggregat haben, die unter der Performance-Garantie liegen, können Sie diese Volumes hinzufügen, um den Latenzwert im gleichen Diagramm anzuzeigen.

Komponenten der ObjektLanding-Pages

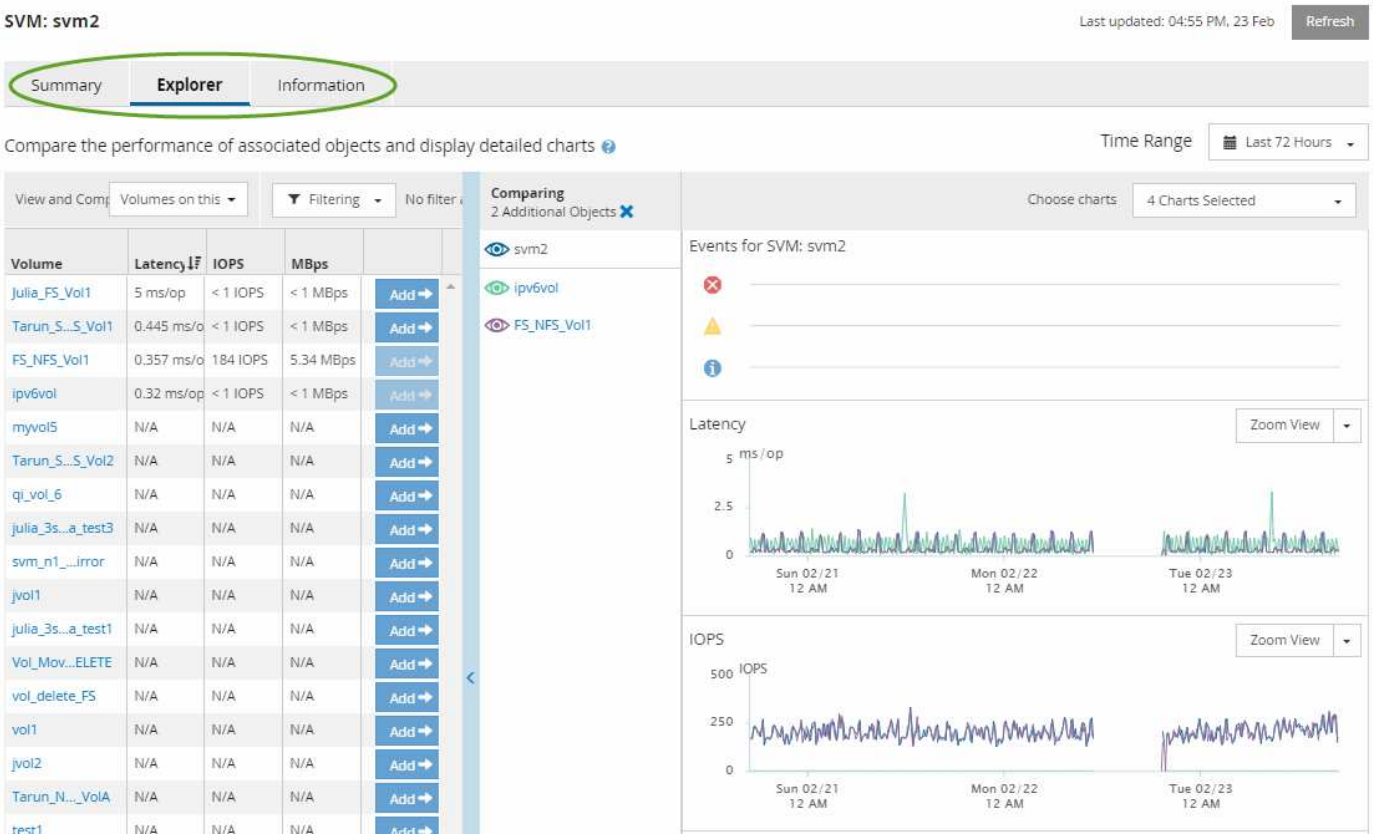
Auf den Seiten „Objekt-Landing“ werden Details zu allen kritischen, Warn- und Informationsereignissen angezeigt. Sie bieten eine detaillierte Ansicht der Performance aller Cluster-Objekte, sodass Sie einzelne Objekte über verschiedene Zeiträume auswählen und vergleichen können.

Auf den Seiten „Objekt-Landing“ können Sie die Gesamtleistung aller Objekte untersuchen und die Performance-Daten des Objekts im nebeneinander liegenden Format vergleichen. Dies ist bei der Leistungsbeurteilung und bei der Fehlersuche von Ereignissen von Vorteil.

> Die Daten, die in den Zusammenfassungsfeldern des Zählers und in den Zählerdiagrammen angezeigt werden, basieren auf einem fünfminütigen Abtastintervall. Die Daten, die im Objektbestandsraster links auf der Seite angezeigt werden, basieren auf einem einstündigen Probenahmeintervall.

Die folgende Abbildung zeigt ein Beispiel für eine Landing Page des Objekts, auf der die Explorer-

Informationen angezeigt werden:



Abhängig vom angezeigten Storage-Objekt kann auf der Objekt-Landing-Page die folgenden Registerkarten enthalten, die Performance-Daten zum Objekt liefern:

- Zusammenfassung

  Zeigt drei oder vier Zählerdiagramme an, die die Ereignisse und die Leistung pro Objekt für den vorangegangenen 72-Stunden-Zeitraum enthalten, einschließlich einer Trendlinie, die die hohen und niedrigen Werte in diesem Zeitraum anzeigt.

- Explorer

  Zeigt ein Raster von Storage-Objekten an, die mit dem aktuellen Objekt verknüpft sind. So können Sie die Performance-Werte des aktuellen Objekts mit den zugehörigen Objekten vergleichen. Diese Registerkarte enthält bis zu elf Zählerdiagramme und eine Zeitbereichauswahl, mit der Sie eine Vielzahl von Vergleichen durchführen können.

- Informationsdaten

  Zeigt Werte für nicht-Performance-Konfigurationsattribute am Storage-Objekt an, einschließlich der installierten Version der ONTAP Software, des HA-Partnernamens und der Anzahl der Ports und LIFs.

- Erstklassige Performance

  Für Cluster: Zeigt die Storage-Objekte an, die basierend auf dem von Ihnen ausgewählten Performance-Zähler die höchste Performance oder die niedrigste Performance haben.

- Failover-Planung

Für Nodes: Zeigt die Schätzung der Performance-Auswirkungen auf einen Node an, wenn der HA-Partner des Node ausfällt.

- Details

  Für Volumes: Zeigt detaillierte Performance-Statistiken für alle I/O-Aktivitäten und Vorgänge für den ausgewählten Volume-Workload an. Diese Registerkarte ist für FlexVol Volumes, FlexGroup Volumes und Komponenten von FlexGroups verfügbar.

Übersichtsseite

Auf der Seite Zusammenfassung werden Zählerdiagramme angezeigt, die Details zu den Ereignissen und der Performance pro Objekt für den vorangegangenen 72-Stunden-Zeitraum enthalten. Diese Daten werden nicht automatisch aktualisiert, sondern sind zum letzten Laden der Seite aktuell. Die Diagramme auf der Übersichtsseite beantworten die Frage *muss ich weiter suchen?*

Diagramme und Zählerstatistiken

Die Übersichtsdiagramme bieten einen schnellen, umfassenden Überblick über die letzten 72 Stunden und helfen Ihnen, mögliche Probleme zu identifizieren, für die weitere Untersuchungen erforderlich sind.

Die Zählerstatistiken der Übersichtsseite werden in Diagrammen angezeigt.

Sie können den Cursor in einem Diagramm über die Trendlinie positionieren, um die Zählerwerte für einen bestimmten Zeitpunkt anzuzeigen. In den Übersichtsdiagrammen wird außerdem die Gesamtzahl der aktiven kritischen und Warnereignisse für die letzten 72 Stunden für die folgenden Zähler angezeigt:

- **Latenz**

  Durchschnittliche Reaktionszeit aller I/O-Anforderungen, in Millisekunden pro Vorgang ausgedrückt

  Wird für alle Objekttypen angezeigt.

- **IOPS**

  Durchschnittliche Betriebsgeschwindigkeit, ausgedrückt in ein-/Ausgabeoperationen pro Sekunde

  Wird für alle Objekttypen angezeigt.

- **Mbps**

  Durchschnittlicher Durchsatz: In Megabyte pro Sekunde ausgedrückt

  Wird für alle Objekttypen angezeigt.

- **Verwendete Leistungskapazität**

  Prozentsatz der Performance-Kapazität, die von einem Node oder Aggregat verbraucht wird

  Nur für Nodes und Aggregate angezeigt Dieses Diagramm wird nur angezeigt, wenn Sie ONTAP 9.0 oder höher verwenden.

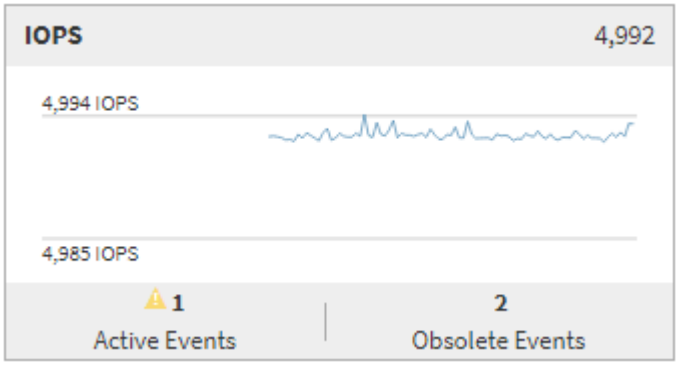
- **Nutzung**

Prozentsatz der Objektauslastung für Nodes und Aggregate oder Bandbreitenauslastung für Ports.

Nur für Nodes, Aggregate und Ports angezeigt

Wenn Sie den Mauszeiger über die Ereignisanzahl für aktive Ereignisse positionieren, werden Typ und Anzahl der Ereignisse angezeigt. Kritische Ereignisse werden rot (), und Warnereignisse werden in gelb ().

Die Zahl oben rechts im Diagramm im grauen Balken ist der Durchschnittswert aus dem letzten 72-Stunden-Zeitraum. Die Zahlen unten und oben im Trendliniendiagramm sind die Mindest- und Höchstwerte der letzten 72 Stunden. Der graue Balken unterhalb des Diagramms enthält die Anzahl der aktiven (neuen und bestätigten) Ereignisse und der veralteten Ereignisse aus dem Zeitraum der letzten 72 Stunden.



- **Latenzzähler-Diagramm**

  Das Latenzzähler-Diagramm bietet einen allgemeinen Überblick über die Objektlatenz für den vorherigen 72-Stunden-Zeitraum. Die Latenz bezeichnet die durchschnittliche Reaktionszeit aller I/O-Anfragen. Sie wird in Millisekunden pro Vorgang ausgedrückt, die Servicezeit, die Wartezeit oder beides, während ein Datenpaket oder ein Block in der betrachten Cluster-Storage-Komponente zu finden ist.

  Oben (Zählerwert): die Zahl in der Kopfzeile zeigt den Durchschnitt für den vorangegangenen 72-Stunden-Zeitraum an.

  Mitte (Performance-Diagramm): die Zahl unten im Diagramm zeigt die niedrigste Latenz an, und die Zahl oben im Diagramm zeigt die höchste Latenz für den letzten 72-Stunden-Zeitraum an. Positionieren Sie den Mauszeiger über die Trendkurve, um den Latenzwert für einen bestimmten Zeitraum anzuzeigen.

  Bottom (Ereignisse): im Pop-up-Fenster werden die Details der Ereignisse angezeigt. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinformationen“ zu navigieren, um vollständige Ereignisdetails anzuzeigen.

- **IOPS-Zählerdiagramm**

  Das IOPS-Zählerdiagramm bietet eine allgemeine Übersicht über den Objekt-IOPS-Zustand des vorherigen Zeitraums von 72 Stunden. IOPS gibt die Geschwindigkeit des Storage-Systems in der Anzahl der ein-/Ausgabe-Vorgänge pro Sekunde an.

  Oben (Zählerwert): die Zahl in der Kopfzeile zeigt den Durchschnitt für den vorangegangenen 72-Stunden-Zeitraum an.

  Mitte (Performance-Diagramm): die Zahl unten im Diagramm zeigt die niedrigsten IOPS an, und die Zahl oben im Diagramm zeigt die höchsten IOPS für den Zeitraum von 72 Stunden an. Positionieren Sie den Mauszeiger über die Trendkurve, um den IOPS-Wert für einen bestimmten Zeitpunkt anzuzeigen.

Bottom (Ereignisse): im Pop-up-Fenster werden die Details der Ereignisse angezeigt. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinformationen“ zu navigieren, um vollständige Ereignisdetails anzuzeigen.

- **MB/s-Zählerdiagramm**

  Das MB/s-Zählerdiagramm zeigt die Performance des Objekts im MB/s an und zeigt an, wie viele Daten in Megabyte pro Sekunde an und vom Objekt übertragen wurden. Das MB/s-Zählerdiagramm bietet eine allgemeine Übersicht über den Zustand des Objekts im Hinblick auf den Zustand der vorherigen 72-Stunden-Periode.

  Oben (Zählerwert): die Zahl in der Kopfzeile zeigt die durchschnittliche Anzahl von Mbps für den vorangegangenen 72-Stunden-Zeitraum an.

  Mitte (Leistungsdiagramm): der Wert unten im Diagramm zeigt die niedrigste Anzahl von Mbit/s an, und der Wert oben im Diagramm zeigt die höchste Anzahl von Mbit/s für den vorangegangenen 72-Stunden-Zeitraum an. Positionieren Sie den Cursor über die Trendlinie des Diagramms, um den Wert für MB/s für eine bestimmte Zeit anzuzeigen.

  Bottom (Ereignisse): im Pop-up-Fenster werden die Details der Ereignisse angezeigt. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinformationen“ zu navigieren, um vollständige Ereignisdetails anzuzeigen.

- **Leistungskapazität verwendetes Zählerdiagramm**

  Das Zählerdiagramm mit der verwendeten Performance-Kapazität zeigt den Prozentsatz der Performance-Kapazität an, die vom Objekt verbraucht wird.

  Oben (Zählerwert): die Zahl im Header zeigt die durchschnittliche Nutzleistung für den vorangegangenen 72-Stunden-Zeitraum an.

  Mittel (Leistungsdiagramm): der Wert unten im Diagramm zeigt den am wenigsten genutzten Prozentsatz der Performance-Kapazität an, und der Wert oben im Diagramm zeigt den am höchsten verwendeten Prozentsatz der Performance-Kapazität für den Zeitraum von 72 Stunden an. Positionieren Sie den Cursor über die Trendkurve, um den für eine bestimmte Zeit verwendeten Performance-Kapazitätswert anzuzeigen.

  Bottom (Ereignisse): im Pop-up-Fenster werden die Details der Ereignisse angezeigt. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinformationen“ zu navigieren, um vollständige Ereignisdetails anzuzeigen.

- **Auslastungszähler-Diagramm**

  Das Zählerdiagramm mit der Auslastung zeigt den Prozentsatz der Objektauslastung an. Das Zählerdiagramm mit der Auslastung bietet einen allgemeinen Überblick über den Prozentsatz der Objekt- oder Bandbreitenauslastung des vorhergehenden Zeitraums von 72 Stunden.

  Oben (Zählerwert): die Zahl in der Kopfzeile zeigt den durchschnittlichen Auslastungsgrad für den vorangegangenen 72-Stunden-Zeitraum an.

  Mitte (Leistungsdiagramm): der Wert unten im Diagramm zeigt den niedrigsten Prozentsatz der Auslastung an, und der Wert oben im Diagramm zeigt den höchsten Auslastungsgrad für den vorangegangenen 72-Stunden-Zeitraum an. Positionieren Sie den Cursor über die Trendkurve, um den Nutzungswert für eine bestimmte Zeit anzuzeigen.

  Bottom (Ereignisse): im Pop-up-Fenster werden die Details der Ereignisse angezeigt. Klicken Sie unter

dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinformationen“ zu navigieren, um vollständige Ereignisdetails anzuzeigen.

Veranstaltungen

In der Ereignishistorie-Tabelle werden, sofern zutreffend, die letzten Ereignisse aufgelistet, die auf diesem Objekt aufgetreten sind. Durch Klicken auf den Ereignisnamen werden Details des Ereignisses auf der Seite Ereignisdetails angezeigt.

Komponenten der Seite Performance Explorer

Auf der Seite „Performance Explorer“ können Sie die Performance ähnlicher Objekte in einem Cluster vergleichen, z. B. aller Volumes in einem Cluster. Dies ist von Vorteil bei der Fehlerbehebung von Performance-Ereignissen und bei der Feinabstimmung der Objekt-Performance. Sie können auch Objekte mit dem Root-Objekt vergleichen, dem Basisobjekt, mit dem andere Objektvergleiche erstellt werden.

Klicken Sie auf die Schaltfläche **Favoriten** ( ) Um dieses Objekt zu Ihrer Liste der bevorzugten Speicherobjekte hinzuzufügen. Eine blaue Taste ( ) Zeigt an, dass dieses Objekt bereits ein Favorit ist.

Klicken Sie auf die Schaltfläche **zur Integritätsansicht wechseln**, um die Seite Integritätsdetails für dieses Objekt anzuzeigen. In einigen Fällen können Sie wichtige Informationen über die Speicherkonfigurationseinstellungen für dieses Objekt erhalten, die bei der Fehlerbehebung hilfreich sein können.

Auf der Seite Performance Explorer werden eine Liste der Cluster-Objekte und ihre Performance-Daten angezeigt. Auf dieser Seite werden alle Clusterobjekte des gleichen Typs (z. B. Volumes und ihre objektspezifischen Performance-Statistiken) in einem tabellarischen Format angezeigt. Diese Ansicht bietet einen effizienten Überblick über die Cluster-Objekt-Performance.

Wenn „N/A“ in einer beliebigen Zelle der Tabelle angezeigt wird, bedeutet dies, dass kein Wert für diesen Zähler verfügbar ist, da zu diesem Zeitpunkt kein I/O für dieses Objekt vorhanden ist.

Die Seite Performance Explorer enthält die folgenden Komponenten:

- **Zeitbereich**

  Ermöglicht die Auswahl eines Zeitbereichs für die Objektdaten.

  Sie können einen vordefinierten Bereich auswählen oder Ihren eigenen benutzerdefinierten Zeitbereich festlegen.

- **Anzeigen und Vergleichen**

  Ermöglicht die Auswahl, welcher Typ des korrelierten Objekts in der Tabelle angezeigt wird.

  Die verfügbaren Optionen hängen vom Root-Objekttyp und dessen verfügbaren Daten ab. Sie können auf die Dropdown-Liste Anzeigen und Vergleichen klicken, um einen Objekttyp auszuwählen. Der ausgewählte Objekttyp wird in der Liste angezeigt.

- **Filterung**

  Hiermit können Sie die Menge der einbezogenen Daten auf der Grundlage Ihrer Präferenzen eingrenzen.

Sie können Filter erstellen, die auf die Objektdaten angewendet werden, z. B. IOPS über 4. Sie können bis zu vier gleichzeitige Filter hinzufügen.

- * Vergleich*

  Zeigt eine Liste der Objekte an, die Sie zum Vergleich mit dem Stammobjekt ausgewählt haben.

  Die Daten für die Objekte im vergleichenden Fensterbereich werden in den Zählerdiagrammen angezeigt.

- **Statistik In** Anzeigen

  Bei Volume und LUNs können Sie auswählen, ob die Statistiken nach jedem Erfassungszyklus angezeigt werden (Standardeinstellung 5 Minuten), oder ob die Statistiken als stündlicher Durchschnitt angezeigt werden. Durch diese Funktionalität können Sie das Latenzdiagramm zur Unterstützung des NetApp „`Performance Guarantee`“-Programms anzeigen.

- **Counter Charts**

  Zeigt graphengraphierte Daten für jede Objektleistungkategorie an.

  Normalerweise werden standardmäßig nur drei oder vier Diagramme angezeigt. Mit der Komponente Diagramm auswählen können Sie zusätzliche Diagramme anzeigen oder bestimmte Diagramme ausblenden. Sie können auch auswählen, ob Sie die Ereigniszeitleiste ein- oder ausblenden möchten.

- **Zeitleiste Für Veranstaltungen**

  Zeigt die Performance- und Integritätsereignisse an, die in der Zeitbereich-Komponente in der von Ihnen ausgewählten Zeitachse auftreten.

Beschreibungen der Seiten des Performance Explorers

Mithilfe der Seiten des Performance Explorer können Sie detaillierte Performance-Informationen über jedes verfügbare Storage-Objekt anzeigen, z. B. Cluster, Aggregate, Volumes usw. Auf diesen Seiten können Sie die Gesamtleistung aller Objekte bewerten und Objektleistendaten im Side-by-Side-Format vergleichen.

Seite „Performance/Cluster Explorer“ beschrieben

Die Seite „Performance/Cluster Explorer“ bietet eine detaillierte Performance-Übersicht über alle Cluster, die von Unified Manager gemanagt werden.

Auf der Seite „Performance/Cluster Explorer“ können Sie die Cluster-Performance nachverfolgen und die Objekte in diesem Cluster während eines bestimmten Zeitraums vergleichen. Dies erleichtert die Fehlerbehebung und Feinanpassung der Performance eines Clusters.

Mithilfe der Funktion „View and Compare“ können Sie die Performance des Clusters mit vergleichen:

- Die Nodes in diesem Cluster
- Die Storage Virtual Machines (SVMs) dieses Clusters
- Die Aggregate auf diesem Cluster

Auf der Seite „Performance/Cluster Explorer“ können Sie:

- Zeigen Sie Probleme mit Schwellenwerten und deren Details an
- Nachverfolgung von Cluster-Performance-Daten
- Untersuchung und Behebung von Problemen mit Schwellenwerten
- Untersuchung und Behebung von Performance-Problemen

Seite „Performance/Node Explorer“

Die Seite Performance/Node Explorer bietet eine detaillierte Performance-Übersicht über alle Nodes innerhalb eines Clusters.

Auf der Seite „Performance/Node Explorer“ können Sie die Node-Performance während eines bestimmten Zeitraums verfolgen und vergleichen. Dies hilft Ihnen bei der Fehlerbehebung und Feinabstimmung der Performance Ihrer Knoten.

Mit der Funktion „Anzeigen und Vergleichen“ können Sie die Performance dieses Knotens mit den folgenden vergleichen:

- Anderen Nodes im selben Cluster
- Die Aggregate auf dem Node
- Die Ports auf dem Node

Auf der Seite Performance/Node Explorer können Sie:

- Zeigen Sie Probleme mit Schwellenwerten und deren Details an
- Verfolgen und Vergleichen von Node-Performance-Daten
- Untersuchung und Behebung von Problemen mit Schwellenwerten
- Untersuchung und Behebung von Performance-Problemen

Explorer-Seite für Performance/Aggregat

Die Seite „Performance/Aggregate Explorer“ bietet eine detaillierte Performance-Übersicht über alle Aggregate in einem Cluster.

Auf der Explorer-Seite „Performance/Aggregate“ können Sie die aggregierte Performance in einem bestimmten Zeitraum nachverfolgen und vergleichen. Dies hilft Ihnen bei der Fehlerbehebung und Feinabstimmung der Performance eines Aggregats.

Root-Aggregate werden auf dieser Seite nicht angezeigt.

Mithilfe der Funktion „Anzeigen und Vergleichen“ können Sie die Performance dieses Aggregats mit folgenden vergleichen:

- Anderer Aggregate auf demselben Node
- Anderen Aggregaten auf demselben Cluster
- Der Node, auf dem sich das Aggregat befindet
- Alle Nodes auf dem Cluster, die dieses Aggregat verwenden
- Die Volumes in diesem Aggregat

Auf der Seite „Performance/Aggregate Explorer“ können Sie:

- Zeigen Sie Probleme mit Schwellenwerten und deren Details an
- Verfolgen und Vergleichen von Aggregat-Performance-Daten
- Untersuchung und Behebung von Problemen mit Schwellenwerten
- Untersuchung und Behebung von Performance-Problemen

Seite „Performance/Volume“ oder „Performance/FlexGroup Explorer“

Diese Seite bietet detaillierte Performance-Informationen für ein Volume in einem Cluster. Der Titel dieser Seite hängt davon ab, ob Sie ein FlexVol-Volume oder ein FlexGroup-Volume anzeigen.

Auf der Seite „Volume“ oder „FlexGroup Explorer“ können Sie die Volume-Performance in einem bestimmten Zeitraum verfolgen und vergleichen. So lassen sich Fehler beheben und die Volume-Performance optimieren.

Root-Volumes werden auf dieser Seite nicht angezeigt.

Verwenden der Funktion „Anzeigen und Vergleichen“:

- Bei FlexVol Volumes können Sie die Performance dieses Volumes mit vergleichen:
  - Andere Volumes auf demselben Aggregat
  - Das Aggregat, auf dem sich dieses Volume befindet
  - Der SVM, auf der sich das Volume befindet
  - Die LUNs, die sich auf diesem Volume befinden
- Bei FlexGroup Volumes können Sie die Performance dieser FlexGroup mit vergleichen:
  - Die Aggregate, auf denen sich die FlexGroup befindet
  - Der SVM, auf der sich die FlexGroup befindet
  - Die zusammengehörigen Volumes der FlexGroup

Die Statistiken in den Diagrammen werden nach jedem Erfassungszeitraum aktualisiert, der standardmäßig alle 5 Minuten beträgt. Die Auswahl von Statistiken zur Ansicht bietet eine Option, um die über die vorherige Stunde gemittelten Statistiken anzuzeigen. Durch diese Funktionalität können Sie das Latenzdiagramm zur Unterstützung des NetApp „`Performance Guarantee`“-Programms anzeigen.

Auf der Seite Performance/Volume Explorer oder Performance/FlexGroup Explorer können Sie:

- Zeigen Sie Probleme mit Schwellenwerten und deren Details an
- Verfolgen und Vergleichen von Volume Performance-Daten
- Untersuchung und Behebung von Problemen mit Schwellenwerten
- Untersuchung und Behebung von Performance-Problemen
- Starten Sie System Manager, um eine Konfigurationsänderung für das Volume vorzunehmen

  Die Schaltfläche **Lautstärke konfigurieren** steht zur Verfügung, wenn Sie sich bei Unified Manager mit der Rolle „OnCommand Administrator“ oder „Speicheradministrator“ und bei Verwendung von ONTAP 9.5 oder höher bei Unified Manager angemeldet haben.

Für Datensicherungs-Volumes (DP) werden nur Zählerwerte für den benutzergenerierten Datenverkehr angezeigt. Wenn das Cluster mit einer Version der ONTAP Software vor 8.3 installiert ist, werden keine Zählerwerte angezeigt.

Seite „Performance/Constituent Volume Explorer“

Die Seite „Performance/Constituent Volume Explorer“ enthält detaillierte Leistungsinformationen für die ausgewählte FlexGroup-Komponente.

Auf der Seite „Performance/Constituent Volume Explorer“ können Sie die Performance eines FlexGroup-Volumes und dessen zusammengehörige Volumes während eines bestimmten Zeitraums verfolgen und vergleichen. Dies hilft bei der Fehlersuche und Feinabstimmung der Performance eines Volume und seiner zusammengehörigen Volumes.

Mithilfe der Funktion „Anzeigen und Vergleichen“ können Sie die Performance dieses zusammengehörigen Volumes mit folgenden Punkten vergleichen:

- Das Aggregat, in dem sich das zusammengehörige Volume befindet
- Der SVM, auf der sich das zusammengehörige Volume befindet
- Das FlexGroup Volume, zu dem das zusammengehörige Volume gehört
- Andere Volumes, die sich auf dem gleichen Aggregat befinden

Auf der Seite „Performance/Constituent Volume Explorer“ können Sie Folgendes ausführen:

- Zeigen Sie Probleme mit Schwellenwerten und deren Details an
- Verfolgen und vergleichen Sie die Performance-Daten der einzelnen Bestandteile
- Untersuchung und Behebung von Problemen mit Schwellenwerten
- Untersuchung und Behebung von Performance-Problemen

Für Datensicherungs-Volumes (DP) werden nur Zählerwerte für den benutzergenerierten Datenverkehr angezeigt. Wenn das Cluster mit einer Version der ONTAP Software vor 8.3 installiert ist, werden keine Zählerwerte angezeigt.

Seite „Performance/Port Explorer“

Die Seite Performance/Port Explorer bietet eine detaillierte Performance-Übersicht über alle Ports in einem Cluster.

Die Werte des Performance-Zähler werden nur für physische Ports angezeigt. Zählerwerte werden nicht für VLANs oder Interface Groups angezeigt.

Auf der Seite „Performance/Port Explorer“ können Sie die Portleistung in einem bestimmten Zeitraum verfolgen und vergleichen. Dies hilft Ihnen bei der Fehlerbehebung und Feinabstimmung der Portleistung.

Mit der Funktion „Ansicht und Vergleich“ können Sie die Leistung dieses Ports mit vergleichen:

- Andere Ports auf demselben Node
- Der Node, auf dem sich der Port befindet

- LIFs am Port

> Nur Cluster und Daten-LIFs werden bei Filterung mit der Option „`LIFs auf diesem Port`“ angezeigt. Es werden keine Intercluster-LIFs angezeigt.

Auf der Seite „Performance/Port Explorer“ können Sie Folgendes ausführen:

- Zeigen Sie Probleme mit Schwellenwerten und deren Details an
- Verfolgen und vergleichen Sie die Port-Performance-Daten
- Untersuchung und Behebung von Problemen mit Schwellenwerten
- Untersuchung und Behebung von Performance-Problemen

Explorer-Seite für Performance/SVM

Der Explorer-Seite „Performance/SVM“ bietet einen detaillierten Performance-Überblick über alle Storage Virtual Machines (SVMs) in einem Cluster.

Auf der Seite „Performance/SVM Explorer“ können Sie die SVM-Performance in einem bestimmten Zeitraum nachverfolgen und vergleichen. Dies erleichtert Ihnen die Fehlerbehebung und Feinanpassung der SVM-Performance.

Mithilfe der Funktion „View and Compare“ können Sie die Performance dieser SVM mit vergleichen:

- Andere SVMs auf demselben Cluster
- Die Volumes auf dieser SVM
- Die LIFs auf dieser SVM

Auf der Seite „Performance/SVM Explorer“ haben Sie die folgenden Möglichkeiten:

- Zeigen Sie Probleme mit Schwellenwerten und deren Details an
- Verfolgen und Vergleichen der SVM-Performance-Daten
- Untersuchung und Behebung von Problemen mit Schwellenwerten
- Untersuchung und Behebung von Performance-Problemen

Seite „Performance/LUN Explorer“

Die Seite „Performance/LUN Explorer“ bietet eine detaillierte Übersicht über die Performance aller LUNs innerhalb eines Clusters.

Auf der Seite „Performance/LUN Explorer“ können Sie die LUN-Performance in einem bestimmten Zeitraum nachverfolgen und vergleichen. Dies hilft Ihnen, Fehler zu finden und die Performance Ihrer LUNs zu optimieren.

Mithilfe der Funktion „Anzeigen und Vergleichen“ können Sie die Performance dieser LUN mit vergleichen:

- Andere LUNs, die sich auf demselben Volume befinden
- Das Volume, auf dem sich die LUN befindet

Die Statistiken in den Diagrammen werden nach jedem Erfassungszeitraum aktualisiert, der standardmäßig

alle 5 Minuten beträgt. Die Auswahl von Statistiken zur Ansicht bietet eine Option, um die über die vorherige Stunde gemittelten Statistiken anzuzeigen. Durch diese Funktionalität können Sie das Latenzdiagramm zur Unterstützung des NetApp „`Performance Guarantee`“-Programms anzeigen.

Auf der Seite „Performance/LUN Explorer“ können Sie:

- Zeigen Sie Probleme mit Schwellenwerten und deren Details an
- Verfolgen und Vergleichen der LUN-Performance-Daten
- Untersuchung und Behebung von Problemen mit Schwellenwerten
- Untersuchung und Behebung von Performance-Problemen

Namespace Explorer-Seite

Die Seite Namespace Explorer bietet eine detaillierte Übersicht über die Performance aller Namespaces innerhalb eines Clusters.

Auf der Namespace Explorer-Seite können Sie die Namespace-Performance während eines bestimmten Zeitraums verfolgen und vergleichen. Dadurch können Sie die Performance Ihrer Namesaces optimieren und Fehler beheben.

Mit der Funktion „Anzeigen und Vergleichen“ können Sie die Performance dieses Namespaces mit den folgenden Eigenschaften vergleichen:

- Das Volume, auf dem sich der Namespace befindet
- Andere Namespaces, die auf dem gleichen Volume sind
- Andere Namespaces, die auf derselben SVM liegen

Auf der Namespace Explorer-Seite können Sie:

- Zeigen Sie Probleme mit Schwellenwerten und deren Details an
- Verfolgen und Vergleichen von Namespace-Performance-Daten
- Untersuchung und Behebung von Problemen mit Schwellenwerten
- Untersuchung und Behebung von Performance-Problemen
- Starten Sie System Manager, um eine Konfigurationsänderung für den Namespace vorzunehmen

  Die Schaltfläche **Namespace konfigurieren** steht zur Verfügung, wenn Sie mit der Rolle OnCommand Administrator oder Storage Administrator bei Unified Manager angemeldet sind, und wenn Sie ONTAP 9.5 oder höher verwenden.

Seite „Performance/LIF Explorer“

Die Seite „Performance/LIF Explorer“ bietet eine detaillierte Performance-Übersicht für alle LIFs innerhalb eines Clusters.

Auf der Seite „Performance/LIF Explorer“ können Sie die LIF-Performance in einem bestimmten Zeitraum nachverfolgen und vergleichen. So lassen sich Fehler finden und die LIF-Performance optimieren.

Mithilfe der Funktion „Anzeigen und Vergleichen“ können Sie die Performance dieser LIF mit vergleichen:

- Andere LIFs, die sich am gleichen Port befinden
- Andere LIFs auf derselben SVM
- Der Port, auf dem sich das LIF befindet
- Der SVM, auf der sich das LIF befindet

Auf der Seite „Performance/LIF Explorer“ können Sie:

- Zeigen Sie Probleme mit Schwellenwerten und deren Details an
- Nachverfolgung und Vergleich der LIF-Performance-Daten
- Untersuchung und Behebung von Problemen mit Schwellenwerten
- Untersuchung und Behebung von Performance-Problemen

Beschreibungen der Zählerdiagramme

Mithilfe der Zählerdiagramme des Performance Explorer können Sie Performancedaten für ausgewählte Speicherobjekte anzeigen und vergleichen. Diese Diagramme bieten einen Überblick über Performance-Trends und können Performance-Probleme isolieren und lösen.

Zählerdiagramme zur Latenz-Performance

Die Zählerdiagramme des Performance Explorer zeigen die Anzahl von Millisekunden an, die für das ausgewählte Storage-Objekt erforderlich sind, um auf Applikationsanforderungen zu reagieren.

Das Popup-Fenster, das angezeigt wird, wenn sich der Cursor im Diagrammbereich befindet, zeigt die spezifischen Zählerwerte zu bestimmten Zeiten an.

Auf der unteren Seite der Tabelle werden Informationen zur minimalen, maximalen, durchschnittlichen und 95. Perzentil-Latenz für den ausgewählten Zeitraum angezeigt.

Es stehen drei Arten von Latenzdiagrammen zur Verfügung:

Latenz: Zählerdiagramm insgesamt

Zeigt die Anzahl der Millisekunden an, die erforderlich ist, um auf Anwendungsanforderungen zu reagieren. Die durchschnittlichen Latenzwerte werden durch die I/O-Gewichtung bestimmt.

Latenz - Aufschlüsselung der Zähler

Zeigt die gleichen Latenzdaten, die in Lese-, Schreib- und sonstige Latenz getrennt sind, an.

Diese Diagrammoption wird angewendet, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume oder eine LUN ist.

Latenz: Zählerdiagramm der Cluster-Komponenten

Zeigt die Latenzdaten nach Clusterkomponente an. Damit können Sie die Cluster-Komponente identifizieren, die für die Latenz verantwortlich ist. Wenn Sie den Mauszeiger über das Diagramm halten, wird der genaue Latenzbeitrag für jede Komponente angezeigt.

Diese Diagrammoption wird angewendet, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume oder eine LUN ist.

Zoom-Ansicht-Taste

Zeigt eine vergrößerte Ansicht der Daten des Zählerdiagramms an.

- Veranstaltungen

  Das Auftreten von kritischen, Warn- und Informationsereignissen wird in den Zeitlinien über den Diagrammen angezeigt.

- Schwellenwerte

  Die horizontale, gestrichelte Zeile zeigt den in Unified Manager festgelegten Grenzwert für die Auslastungswarnung an.

  Die rote Linie zeigt den Auslastungskritischen Schwellenwert in Unified Manager an.

- Zähler

  Die Zähler im linken Teilfenster zeigen an, welche Zählerwerte angezeigt werden. Deaktivieren oder Auswählen des Das wird mit einem Zähler verknüpft, versteckt und zeigt, dass Zählerinformationen aus dem Diagramm angezeigt werden und kann beim Vergleich der Objektlatenz helfen.

Zählerdiagramme der IOPS-Performance

In den Performance Explorer IOPS-Zählerdiagrammen wird die Anzahl der vom ausgewählten Speicherobjekt verarbeiteten ein-/Ausgabevorgänge pro Sekunde angezeigt.

Das Popup-Fenster, das angezeigt wird, wenn sich der Cursor im Diagrammbereich befindet, zeigt die spezifischen Zählerwerte zu bestimmten Zeiten an.

Wenn in der Zoom-Ansicht angezeigt wird, zeigen die IOPS-Diagramme des Volumes und der LUN unter ONTAP auch Einstellungen für den maximalen und minimalen Durchsatz-Schwellenwert für Quality of Service (QoS) an. Die Diagramme für IOPS/TB zeigen QoS-Spitzenwerte und erwartete Durchsatzschwellenwerte an, falls konfiguriert.

Wenn sich ein Volume oder eine LUN befindet, das die IOPS einer Shared QoS-Richtlinie gemeinsam nutzt, wird eine Zeile für „`Total Workload IOPS`“ angezeigt, um die IOPS zu zeigen, die von allen anderen Workloads in dieser Richtlinie verwendet werden.

Unten auf der Diagrammseite werden Informationen zum IOPS-Minimum, Maximum, Durchschnitt und 95. Perzentil für den ausgewählten Zeitraum angezeigt.

Es sind vier Arten von IOPS-Diagrammen verfügbar:

IOPS – Zählerdiagramm insgesamt

Zeigt die Anzahl der pro Sekunde verarbeiteten ein-/Ausgabevorgänge an.

IOPS - Aufschlüsselung der Zähler

Zeigt die gleichen IOPS-Daten, getrennt in Lese-, Schreib- und sonstige IOPS, an.

Diese Diagrammoption wird angewendet, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume oder eine LUN ist.

IOPS – Zählerdiagramm zu Protokollen

Zeigt dieselben IOPS-Daten an. Bei SVMs werden die Performance-Daten jedoch in einzelne Komponenten für den Datenverkehr über CIFS, NFS, FCP, NVMe und iSCSI-Protokolle getrennt.

IOPS/TB – Zählerdiagramm insgesamt

Zeigt die Anzahl der pro Sekunde verarbeiteten ein-/Ausgabevorgänge basierend auf dem gesamten logischen Speicherplatz, der vom Volume in Terabyte verbraucht wird. Dieser Zähler wird auch als I/O-Dichte bezeichnet und misst, wie viel Performance mit einer bestimmten Menge an Storage-Kapazität bereitgestellt werden kann.

Diese Diagrammoption ist nur verfügbar, wenn das ausgewählte Objekt ein Volume ist. Sie zeigt Performance-Daten nur an, wenn die vom Volume genutzte logische Kapazität größer oder gleich 1 TB ist. Lücken werden im Diagramm angezeigt, wenn die genutzte Kapazität während des ausgewählten Zeitraums unter 1 TB fällt.

> In manchen Situationen kann das IOPS/TB-Diagramm große Datensspitzen anzeigen, während das IOPS-Diagramm nicht dasselbe Verhalten zeigt. Dies ist eine bekannte Beschränkung, wenn Performance-Daten weniger häufig als andere Performance-Daten erfasst werden. Dieses Diagramm kehrt in der Regel in 5 oder 10 Minuten wieder in den Normalbetrieb zurück, wenn die Erfassungszyklen synchronisiert werden.

Zoom-Ansicht-Taste

Zeigt eine vergrößerte Ansicht der Daten des Zählerdiagramms an.

- Veranstaltungen

  Das Auftreten von kritischen, Fehler-, Warn- und Informationsereignissen wird in den Zeitlinien oberhalb der Diagramme angezeigt.

- Schwellenwerte

  Die horizontale, gestrichelte Zeile zeigt den in Unified Manager festgelegten Grenzwert für die Auslastungswarnung an.

  Die rote Linie zeigt den Auslastungskritischen Schwellenwert in Unified Manager an.

- Zähler

  Die Zähler im linken Teilfenster zeigen an, welche Zählerwerte angezeigt werden. Deaktivieren oder Auswählen des Das wird einem Zähler zugeordnet, versteckt sich und zeigt, dass Zählerinformationen aus dem Diagramm angezeigt werden und kann beim Vergleich der Objekt-IOPS helfen.

MB/s-Performance-Zählerdiagramme

In den Zählerdiagrammen Performance Explorer MB/s wird die Anzahl der in das

ausgewählte Objekt pro Sekunde übertragenen Megabyte an Daten angezeigt.

Das Popup-Fenster, das angezeigt wird, wenn sich der Cursor im Diagrammbereich befindet, zeigt die spezifischen Zählerwerte zu bestimmten Zeiten an.

Wenn in der Zoom-Ansicht angezeigt wird, zeigen die Volume- und LUN-Diagramme unter ONTAP auch Einstellungen für den maximalen MB/s-Durchsatz von Quality of Service (QoS) an.

Wenn sich ein Volume oder eine LUN ansieht, das die MB/s einer gemeinsam genutzten QoS-Richtlinie teilt, wird eine Zeile mit „`Gesamt-Workload Mbps`“ angezeigt, um die MB/s anzuzeigen, die von allen anderen Workloads in dieser Richtlinie verwendet werden.

Auf der unteren Seite der Kartenseite werden Informationen für den minimalen, maximalen, durchschnittlichen und 95-perzentilen MB/s für den ausgewählten Zeitbereich angezeigt.

Es stehen zwei Arten von Mbps-Diagrammen zur Verfügung:

MB/s – Zählerdiagramm insgesamt

Zeigt die Anzahl der Megabyte an Daten an, die pro Sekunde an das ausgewählte Objekt übertragen werden.

Mbps - Aufschlüsselung des Zählerdiagramms

Zeigt dieselben MB/s-Daten an, die in Festplattenlesevorgänge, Flash Cache Lese-, Schreib- und andere Vorgänge getrennt sind.

Diese Diagrammoption wird angewendet, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume oder eine LUN ist.

Flash Cache-Daten werden nur für Nodes und nur angezeigt, wenn ein Flash Cache Modul im Node installiert ist.

Zoom-Ansicht-Taste

Zeigt eine vergrößerte Ansicht der Daten des Zählerdiagramms an.

- Veranstaltungen

  Das Auftreten von kritischen, Fehler-, Warn- und Informationsereignissen wird in den Zeitlinien oberhalb der Diagramme angezeigt.

- Schwellenwerte

  Die horizontale, gestrichelte Zeile zeigt den in Unified Manager festgelegten Grenzwert für die Auslastungswarnung an.

  Die rote Linie zeigt den Auslastungskritischen Schwellenwert in Unified Manager an.

- Zähler

  Die Zähler im linken Teilfenster zeigen an, welche Zählerwerte angezeigt werden. Deaktivieren oder Auswählen des Dies wird mit einem Zähler verknüpft, versteckt sich und zeigt die Zählerinformationen aus dem Diagramm an und kann beim Vergleich von Objekt-MB/s helfen.

Zählerdiagramm der Auslastungs-Performance

Das Zählerdiagramm zur Performance Explorer-Auslastung zeigt den durchschnittlichen Prozentsatz der ausgewählten Ressource an, die verwendet wird.

Das Popup-Fenster, das angezeigt wird, wenn sich der Cursor im Diagrammbereich befindet, zeigt die spezifischen Zählerwerte zu bestimmten Zeiten an.

Auf der unteren Seite der Kartenseite werden Informationen zur minimalen, maximalen, durchschnittlichen und 95. Perzentil-Auslastung für den ausgewählten Zeitraum angezeigt.

Auslastung – Zählerdiagramm insgesamt

Zeigt den durchschnittlichen Prozentsatz der ausgewählten Ressource an, die verwendet wird. Bei Nodes zeigt dies die Auslastung von Node-Ressourcen (CPU und RAM) an, bei Aggregaten zeigt dies die Auslastung der Festplatten im Aggregat an. Bei den Ports gibt dies die Bandbreitenauslastung des Ports an.

Diese Diagrammoption wird angewendet, wenn es sich bei dem ausgewählten Objekt um einen Node, ein Aggregat oder einen Port handelt.

Zoom-Ansicht-Taste

Zeigt eine vergrößerte Ansicht der Daten des Zählerdiagramms an.

- Veranstaltungen

  Das Auftreten von kritischen, Warn- und Informationsereignissen wird in den Zeitlinien über den Diagrammen angezeigt.

- Schwellenwerte

  Die horizontale, gestrichelte Zeile zeigt den in Unified Manager festgelegten Grenzwert für die Auslastungswarnung an.

  Die rote Linie zeigt den Auslastungskritischen Schwellenwert in Unified Manager an.

- Zähler

  Die Zähler im linken Teilfenster zeigen an, welche Zählerwerte angezeigt werden. Deaktivieren oder Auswählen des Dies wird mit einem Zähler verknüpft, versteckt und zeigt, dass Zählerinformationen aus dem Diagramm angezeigt werden und kann beim Vergleich der Objektnutzung helfen.

Zählerdiagramme mit hoher Performance-Kapazität

Die Performance ExplorerPerformance-Kapazität verwendeten Zählerdiagramme zeigen den Prozentsatz der Performance-Kapazität an, die vom Node oder Aggregat verbraucht wird.

Daten zur Performance-Kapazität sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.

Diese Diagramme gelten nur, wenn das ausgewählte Objekt ein Knoten oder Aggregat ist.

Das Popup-Fenster, das angezeigt wird, wenn sich der Cursor im Diagrammbereich befindet, zeigt die spezifischen Zählerwerte zu bestimmten Zeiten an.

Auf der unteren Seite des Diagramms werden Informationen zur minimalen, maximalen, durchschnittlichen und 95. Perzentil-Performance angezeigt, die für den ausgewählten Zeitraum verwendet wird.

Es stehen zwei Arten von Diagrammen zur Nutzung der Performance-Kapazität zur Verfügung:

Genutzte Performance-Kapazität – Zählerdiagramm insgesamt

Zeigt den Prozentsatz der Performance-Kapazität an, die vom Node oder Aggregat verbraucht wird.

- Grüner Bereich

  Der Kapazitätswert liegt unter dem in Unified Manager festgelegten Warnschwellenwert.

- Gelber Bereich

  Der Kapazitätswert nähert sich dem in Unified Manager festgelegten Warnschwellenwert.

- Roter Bereich

  Der Kapazitätswert liegt über dem Warnschwellenwert und nähert sich dem in Unified Manager festgelegten maximalen Schwellenwert.

Genutzte Performance-Kapazität – Aufschlüsselung der Zähler

Zeigt denselben Prozentsatz der Performance-Kapazität an, die in Benutzerprotokolle, System-Hintergrundprozesse und die Menge an freier Performance-Kapazität unterteilt ist.

Zoom-Ansicht-Taste

Zeigt eine vergrößerte Ansicht der Daten des Zählerdiagramms an.

- Veranstaltungen

  Das Auftreten von kritischen, Warn- und Informationsereignissen wird in den Zeitlinien über den Diagrammen angezeigt.

- Schwellenwerte

  Die horizontale, gestrichelte Zeile gibt den in Unified Manager festgelegten Kapazitätswarnschwellenwert an.

  Die rote Linie zeigt den in Unified Manager festgelegten Kapazitätsschwellenwert an.

  Der schwarze durchgezogene Linie bei 100 % ist der empfohlene Wert für die maximale Performance-Kapazität.

- Zähler

  Die Zähler im linken Teilfenster zeigen an, welche Zählerwerte angezeigt werden. Deaktivieren oder Auswählen des Das mit einem Zähler verknüpft ist, kann den Vergleich einschränken.

Verfügbares Zählerdiagramm für die IOPS-Performance

Das Performance Explorer Verfügbare IOPS-Zählerdiagramm zeigt die Anzahl der ein-/Ausgabevorgänge pro Sekunde an, die derzeit (kostenlos) auf dem ausgewählten Speicherobjekt verfügbar sind.

Das Popup-Fenster, das angezeigt wird, wenn sich der Cursor im Diagrammbereich befindet, zeigt die spezifischen Zählerwerte zu bestimmten Zeiten an.

Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt ein Knoten oder Aggregat ist.

Auf der unteren Seite des Diagramms werden Informationen zur minimalen, maximalen, durchschnittlichen und 95. Perzentil-Performance angezeigt, die für den ausgewählten Zeitraum verwendet wird.

Verfügbare IOPS: Zählerdiagramm insgesamt

Zeigt die Anzahl der ein-/Ausgabevorgänge pro Sekunde an, die derzeit auf dem ausgewählten Speicherobjekt verfügbar (frei) sind. Diese Zahl ergibt sich aus der Subtraktion der derzeit verwendeten IOPS von den IOPS-Gesamtwerten, die Unified Manager berechnet, die das Objekt ausführen kann.

Verfügbare IOPS-Daten sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.

Zoom-Ansicht-Taste

Zeigt eine vergrößerte Ansicht der Daten des Zählerdiagramms an.

- Veranstaltungen

  Das Auftreten von kritischen, Warn- und Informationsereignissen wird in den Zeitlinien über den Diagrammen angezeigt.

- Zähler

  Die Zähler im linken Teilfenster zeigen an, welche Zählerwerte angezeigt werden. Deaktivieren oder Auswählen des Dies wird mit einem Zähler verknüpft, versteckt sich und zeigt die Zählerinformationen aus dem Diagramm an und kann beim Vergleich von Objekten helfen.

Zählerdiagramm der Performance im Cache-Verhältnis

Das Zählerdiagramm im Performance Explorer Cache Miss Ratio zeigt den Prozentsatz der Leseanforderungen von Client-Anwendungen an, die von der Festplatte zurückgegeben werden, anstatt vom Cache zurückgegeben zu werden.

Das Popup-Fenster, das angezeigt wird, wenn sich der Cursor im Diagrammbereich befindet, zeigt die spezifischen Zählerwerte zu bestimmten Zeiten an.

Auf der unteren Seite der Kartenseite werden Informationen zum Mindest-, maximal-, Durchschnitts- und 95. Perzentil-Cacheverhältnis für den ausgewählten Zeitbereich angezeigt.

Cache-Miss-Verhältnis - Zählerdiagramm insgesamt

Zeigt den Prozentsatz der Leseanforderungen von Client-Anwendungen an, die von der Festplatte

zurückgegeben werden, anstatt vom Cache zurückgegeben zu werden.

Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volume ist.

Zoom-Ansicht-Taste

Zeigt eine vergrößerte Ansicht der Daten des Zählerdiagramms an.

- Veranstaltungen

  Das Auftreten von kritischen, Warn- und Informationsereignissen wird in den Zeitlinien über den Diagrammen angezeigt.

- Zähler

  Die Zähler im linken Teilfenster zeigen an, welche Zählerwerte angezeigt werden. Deaktivieren oder Auswählen des Dies wird mit einem Zähler verknüpft, versteckt sich und zeigt die Zählerinformationen aus dem Diagramm an und kann beim Vergleich von Objekten helfen.

Anzeigen von Informationen zur Objektkonfiguration

Auf den Objektinformationsseiten auf der Landing Page jedes Objekts werden die Werte für die nicht-Performance-Konfigurationsattribute der einzelnen Storage-Objekte angezeigt. Einige der Attribute sind physische Konfigurationseinstellungen, während andere Attribute die Leistung des Objekts beeinträchtigen können.

Es ist beispielsweise nützlich, die Menge an Speicherplatz zu kennen, die für ein Aggregat oder für einen Node verfügbar ist. Das Wissen über die Geschwindigkeitseinstellung für einen bestimmten Port kann helfen, wenn Sie ein Leistungsproblem diagnostizieren.

Informationsseite für Performance/Cluster

Auf der Seite „Performance/Cluster Information“ können Sie eine Liste der physischen und logischen Attribute des Clusters anzeigen. Diese Informationen könnten bei der Beantwortung von Fragen zur Leistungsfähigkeit helfen.

Cluster-Attribute

- * Management-LIF*

  Der Name der Cluster-Management-LIF und, ob das LIF derzeit verfügbar ist (up), oder nicht (Down).

- **IP-Adresse**

  Die IPv4- oder IPv6-Adresse der Cluster-Management-LIF.

- **FQDN**

  Der vollständig qualifizierte Domain-Name (FQDN) der Cluster-Management-LIF.

- **Betriebssystemversion**

  Die Version der auf dem Cluster installierten ONTAP Software.

Falls unterschiedliche Versionen der ONTAP Software auf den Nodes im Cluster installiert werden, ist die aufgeführte Version die niedrigste Versionsnummer. Überprüfen Sie die Seite Performance/Node-Informationen, um die Version der auf jedem Node installierten ONTAP Software anzuzeigen.

- **Seriennummer**

  Die eindeutige Identifikationsnummer des Clusters.

- **Modell / Familie**

  Die Modellnummer und Modellfamilie aller Nodes im Cluster.

- * Kapazität (frei/gesamt)*

  Den gesamten für den Cluster verfügbaren Speicher in Gigabyte und die derzeit verfügbare Menge an Speicherplatz.

- **Erlaubte Protokolle**

  Liste aller Protokolle, die von diesem Cluster gewartet werden können. Zu den verfügbaren Protokollen gehören FC/FCoE, iSCSI, HTTP, NVMe, NDMP, NFS und CIFS.

- **Knoten**

  Die Anzahl der Nodes in diesem Cluster. Sie können auf die Nummer klicken, um auf der Seite „Performance/Node Inventory“ die Nodes anzuzeigen.

- **Storage Virtual Machines**

  Die Anzahl der SVMs in diesem Cluster Sie können auf die Zahl klicken, um die SVMs auf der Seite „Performance/SVM Inventory“ anzuzeigen.

- **LIFs**

  Die Anzahl der LIFs in diesem Cluster. Sie können auf die Nummer klicken, um die LIFs auf der Seite „Performance/LIF-Inventar“ anzuzeigen.

- **Kontakt / Standort**

  Falls verfügbar: Der Name des Storage-Administrators, der bezüglich des Clusters und den Standort des Clusters kontaktiert werden soll.

Informationen zu Performance/Nodes

Auf der Seite Performance/Node Information können Sie eine Liste der physischen und logischen Attribute des Knotens anzeigen. Diese Informationen könnten bei der Beantwortung von Fragen zur Leistungsfähigkeit helfen.

Knotenattribute

- **IP-Adresse**

  Die IPv4- oder IPv6-Adresse der Node-Management-LIF.

- **FQDN**

  Der vollständig qualifizierte Domain-Name (FQDN) der Node-Management-LIF.

- **Betriebssystemversion**

  Die Version der auf dem Node installierten ONTAP Software.

- **Modell / Familie**

  Die Nummer des Plattformmodells des Nodes.

- * Kapazität (frei/gesamt)*

  Den gesamten für den Node verfügbaren Storage in Gigabyte und die derzeit verfügbare Menge an Speicherplatz.

- * Cluster*

  Der Name des Clusters, zu dem dieser Node gehört. Sie können auf den Namen klicken, um Cluster-Details auf der Seite „Performance/Cluster Explorer“ anzuzeigen.

- **HA-Partner**

  Ggf. der Name des HA-Partner-Node. Sie können auf den Namen klicken, um Details zu Partner-Nodes auf der Seite Performance/Node Explorer anzuzeigen.

- **Aggregate**

  Die Anzahl der Aggregate auf diesem Node. Sie können auf die Nummer klicken, um auf der Seite „Performance/Aggregates Inventory“ die Aggregate anzuzeigen.

  Die hier aufgeführte Nummer stimmt möglicherweise nicht mit der Nummer auf der Seite „Performance/Aggregates Inventory“ überein, da die Bestandsseite keine Root-Aggregate enthält.

- **Ports**

  Die Anzahl der Ports auf diesem Node. Sie können auf die Nummer klicken, um auf der Seite „Performance/Ports Inventory“ die Ports anzuzeigen.

  Die hier aufgeführte Nummer stimmt möglicherweise nicht mit der Nummer auf der Seite „Performance/Ports Inventory“ überein, da die Inventarseite keine Node-Management-Ports enthält.

- **Kontakt / Standort**

  Falls verfügbar, der Name des Administrators, der Kontakt zu diesem Node und dem Standort des Node aufnimmt.

- **# von Kernen / Geschwindigkeit**

  Falls verfügbar, die Anzahl der CPU-Kerne im Controller und die Geschwindigkeit der CPU-Kerne.

- **RAM**

  Falls verfügbar, ist der gesamte verfügbare Speicher des Controllers.

Flash-Geräte

> Flash Cache-Daten werden nur für Nodes und nur angezeigt, wenn ein Flash Cache Modul im Node installiert ist.

- **Steckplatznummer**

  Die Steckplatznummer, in der das Flash Cache-Modul installiert ist.

- **Status**

  Der Betriebsstatus des Moduls. Gültige Werte:

  - Online
  - Offline_fehlgeschlagen
  - „Offline_Schwellenwert“

- **Modell / Familie**

  Die Modellnummer des Moduls.

- **Firmware Rev.**

  Die auf dem Modul installierte Firmware-Version.

- * Kapazität*

  Die Größe des installierten Flash Cache Moduls

Informationsseite zu Performance/Aggregat

Verwenden Sie die Seite Informationen zu Performance/Aggregat, um eine Liste der physischen und logischen Attribute des Aggregats anzuzeigen. Diese Informationen könnten bei der Beantwortung von Fragen zur Leistungsfähigkeit helfen.

Aggregatattribute

- **Aggregattyp**

  Der Aggregattyp:

  - HDD
  - Hybrid

    Kombiniert HDDs und SSDs, aber Flash Pool wurde nicht aktiviert.

  - Hybrid (Flash Pool)

Kombiniert HDDs und SSDs und ermöglicht die Aktivierung von Flash Pool.

- SSD
- SSD (FabricPool)

  Kombiniert SSDs mit einer Cloud-Tier

- VMDisk (SDS)

  Virtuelle Laufwerke innerhalb einer virtuellen Maschine

- VMDisk (FabricPool)

  Kombiniert virtuelle Festplatten mit einer Cloud-Tier

- LUN (FlexArray)

- * Cluster*

  Der Name des Clusters, zu dem das Aggregat gehört. Sie können auf den Namen klicken, um in der Seite „Performance/Cluster Explorer“ Cluster-Details anzuzeigen.

- **Knoten**

  Der Name des Node, zu dem die Festplatten des Aggregats gehören. Sie können auf den Namen klicken, um Node-Details auf der Seite Performance/Node Explorer anzuzeigen.

- **Flash Pool**

  Ob es sich um ein Flash Pool Aggregat handelt: Ja oder Nein

  Ein Flash Pool Aggregat ist ein hybrides Aggregat, das sowohl aus SSDs als auch aus HDDs besteht.

- **FabricPool**

  Ob es sich dabei um ein FabricPool Aggregat handelt: Ja oder Nein

  Ein FabricPool Aggregat besteht aus SSDs und einer Cloud-Tier.

- **Inaktive Datenberichterstattung**

  Gibt an, ob die Funktion zur Berichterstellung inaktiver Daten auf diesem Aggregat aktiviert oder deaktiviert ist. Bei Aktivierung zeigen Volumes auf diesem Aggregat auf der Seite „Performance/Volumes Inventory“ den Umfang der „kalten“ Daten an.

  Der Wert in diesem Feld lautet „`N/A`“, wenn die Version von ONTAP keine inaktive Datenberichterstattung unterstützt.

Performance/Volume oder Performance/FlexGroup Informationsseite

Auf dieser Seite können Sie eine Liste der physischen und logischen Attribute des Volumes anzeigen. Diese Informationen könnten bei der Beantwortung von Fragen zur Leistungsfähigkeit helfen. Der Titel dieser Seite hängt davon ab, ob Sie ein FlexVol-Volume oder ein FlexGroup-Volume anzeigen.

Volume-Attribute

- **Typ**

  Typ des Volume, entweder Lesen/Schreiben (RW) oder Datensicherung (DP).

- **Stil**

  Stil eines Volumes, entweder FlexVol oder FlexGroup.

  Die Performance-Seiten von Unified Manager unterstützen keine Infinite Volumes.

- * Cluster*

  Der Name des Clusters, zu dem dieses FlexVol Volume oder das FlexGroup Volume gehört. Sie können auf den Namen klicken, um in der Seite „Performance/Cluster Explorer“ Cluster-Details anzuzeigen.

- **Aggregate**

  Der Name des Aggregats, auf dem sich das FlexVol Volume befindet, oder die Anzahl der Aggregate, auf denen sich dieses FlexGroup Volume befindet.

  Bei FlexVol-Volumes können Sie auf den Namen klicken, um Details zu Aggregaten auf der Seite mit dem Explorer anzuzeigen. Bei FlexGroup Volumes können Sie auf die Zahl klicken, um die Aggregate anzuzeigen, die in diesem FlexGroup Volume verwendet werden, auf der Seite „Performance/Aggregat-Inventar“.

- **Storage Virtual Machine**

  Der Name der SVM, zu der dieses FlexVol Volume oder dieses FlexGroup Volume gehört. Sie können auf der Seite „Performance/SVM Explorer“ auf den Namen klicken, um SVM-Details anzuzeigen.

- **Tiering-Richtlinie**

  Die Tiering-Richtlinie für das Volume. Die Richtlinie wirkt sich nur dann aus, wenn das Volume auf einem FabricPool Aggregat bereitgestellt wird. Folgende Richtlinien stehen zur Verfügung:

  - Keine. Die Daten für dieses Volume verbleiben immer auf der Performance-Tier.
  - Nur Snapshot. Nur Snapshot Daten werden automatisch in die Cloud-Tier verschoben. Alle anderen Daten verbleiben in der Performance-Tier.
  - Backup: Bei Datensicherungs-Volumes werden alle übertragenen Benutzerdaten in der Cloud-Tier gestartet, aber bei späteren Client-Lesevorgängen kann es dazu kommen, heiße Daten in die Performance-Tier zu verschieben.
  - Automatisch. Daten auf diesem Volume werden automatisch zwischen Performance-Tier und Cloud-Tier verschoben, wenn ONTAP feststellt, dass die Daten „`Hot`“ oder „`Cold`“ sind.

- **RAID-Typ**

  Der Redundanztyp, der auf der Performance-Tier des Aggregats verwendet wird, auf dem sich das Volume befindet. Mögliche Typen:

  - RAID0
  - RAID4

- RAID-DP
- RAID-TEC

> Der Wert „`not zutreffende`“ wird für FlexGroup Volumes angezeigt, da sich die zusammengehörigen Volumes auf Aggregaten verschiedener RAID-Typen befinden können.

- * Kapazität (frei/gesamt)*

  Der gesamte verfügbare Speicher für das Volume, in Gigabyte und die derzeit verfügbare Speichermenge.

Informationsseite zum Performance-/konstituierenden Volumen

Mithilfe der Seite Informationen zum Performance/konstituierenden Volume können Sie eine Liste der physischen und logischen Attribute des FlexGroup-Volume anzeigen. Diese Informationen könnten bei der Beantwortung von Fragen zur Leistungsfähigkeit helfen.

Attribute des konstituierenden Volumes

- **Typ**

  Typ der Komponente, entweder Lesen/Schreiben (RW) oder Datensicherung (DP).

- **Stil**

  Stil des Volume, es handelt sich um ein zusammengehörige Volume eines FlexGroup Volume.

- * Cluster*

  Der Name des Clusters, zu dem das FlexGroup-Teilvolume gehört. Sie können auf den Namen klicken, um in der Seite „Performance/Cluster Explorer“ Cluster-Details anzuzeigen.

- * Aggregat*

  Der Name des Aggregats, auf dem sich das FlexGroup-Teilvolume befindet. Sie können auf den Namen klicken, um aggregierte Details auf der Seite „Performance/Aggregate Explorer“ anzuzeigen.

- **FlexGroup**

  Der Name des FlexGroup Volume, zu dem diese Komponente gehört. Sie können auf den Namen klicken, um Details zu FlexGroup-Volumes auf der Seite „Performance/FlexGroup Explorer“ anzuzeigen.

- **Storage Virtual Machine**

  Der Name der SVM, der das FlexGroup-Teilvolume angehört. Sie können auf der Seite „Performance/SVM Explorer“ auf den Namen klicken, um SVM-Details anzuzeigen.

- **Tiering-Richtlinie**

  Die Tiering-Richtlinie für das Volume. Die Richtlinie wirkt sich nur dann aus, wenn das Volume auf einem FabricPool Aggregat bereitgestellt wird. Folgende Richtlinien stehen zur Verfügung:

  - Keine. Die Daten für dieses Volume verbleiben immer auf der Performance-Tier.

- Nur Snapshot. Nur Snapshot Daten werden automatisch in die Cloud-Tier verschoben. Alle anderen Daten verbleiben in der Performance-Tier.
- Backup: Bei Datensicherungs-Volumes werden alle übertragenen Benutzerdaten in der Cloud-Tier gestartet, aber bei späteren Client-Lesevorgängen kann es dazu kommen, heiße Daten in die Performance-Tier zu verschieben.
- Automatisch. Daten auf diesem Volume werden automatisch zwischen Performance-Tier und Cloud-Tier verschoben, wenn ONTAP feststellt, dass die Daten „`Hot`“ oder „`Cold`“ sind.

- **RAID-Typ**

  Der Redundanztyp, der auf dem Aggregat, in dem sich diese Komponente befindet, verwendet wird. Mögliche Typen:

  - RAID0
  - RAID4
  - RAID-DP
  - RAID-TEC

- * Kapazität (frei/gesamt)*

  Den insgesamt verfügbaren Storage der Komponente in Gigabyte sowie die derzeit verfügbare Menge an Speicherplatz.

Informationen zu Leistung/Anschluss

Verwenden Sie die Seite Angaben zu Leistung/Anschluss, um eine Liste der physischen und logischen Attribute des Ports anzuzeigen. Diese Informationen könnten bei der Beantwortung von Fragen zur Leistungsfähigkeit helfen.

Port-Attribute

- * WWN*

  Der WWN (World Wide Name) des Ports.

- **Knoten**

  Der Name des Node, auf dem sich der physische Port befindet. Sie können auf den Namen klicken, um Node-Details auf der Seite Performance/Node Explorer anzuzeigen.

- * Cluster*

  Der Name des Clusters, zu dem der Port gehört. Sie können auf den Namen klicken, um Cluster-Details auf der Seite „Performance/Cluster Explorer“ anzuzeigen.

- **Betriebsgeschwindigkeit**

  Die tatsächliche Geschwindigkeit, mit der der Port für die Ausführung konfiguriert ist.

  FCP-Ports sind automatisch Erkennung und werden als „`Auto`“ angezeigt.

- * Rolle*

Die Netzwerkanschlussfunktion: Entweder Data oder Cluster.

FCP-Ports können keine Rolle haben, und dieses Feld wird nicht angezeigt.

- **Typ**

  Der Porttyp: Entweder Netzwerk oder FCP (Fibre Channel Protocol).

- **Bundesland**

  Der Verbindungsstatus des Ports.

  - Bei Netzwerkports wird ein aktiver Port als „`up`“ aufgeführt und ein inaktiver Port wird als „`Down`“ aufgeführt.
  - Bei FCP-Ports wird ein aktiver Port als „`Online`“ angezeigt, und ein inaktiver Port wird als „`Link not connected`“ aufgeführt.

Informationen zu Performance/SVM

Auf der Seite „Performance/SVM Information“ können Sie eine Liste der konfigurierten Attribute der SVM anzeigen. Diese Informationen könnten bei der Beantwortung von Fragen zur Leistungsfähigkeit helfen.

SVM-Attribute

- **IP-Adresse**

  Falls definiert, ist dies die IPv4- oder IPv6-Adresse der SVM-Management-LIF.

- **IPspace**

  Der IPspace, in dem sich die SVM befindet.

- **Domain-Name**

  Der vollständig qualifizierte Domain-Name (FQDN) der SVM-Management-LIF.

- **Servicetyp**

  Der Typ der SVM.

  Mögliche Werte sind: „`Admin`“ für die Cluster-übergreifende Management-SVM, „`SSystem`“ für die Kommunikation auf Cluster-Ebene in einem IPspace, „`Data`“ für SVM mit Daten-Serving und „`Node`“ für Node Management-SVM.

- * Kapazität (frei/gesamt)*

  Den gesamten für die SVM verfügbaren Storage in Gigabyte und die Menge an aktuell verfügbarem Storage.

- * Cluster*

  Der Name des Clusters, zu dem die SVM gehört. Sie können auf den Namen klicken, um in der Seite „Performance/Cluster Explorer“ Cluster-Details anzuzeigen.

- **Bände**

  Die Anzahl der Volumes in der SVM. Sie können auf die Nummer klicken, um die Volumes auf der Seite „Performance/Volume Inventory“ anzuzeigen.

- **LIFs**

  Die Anzahl der für die SVM verfügbaren LIFs. Sie können auf die Nummer klicken, um die LIFs auf der Seite „Performance/LIFs Inventar“ anzuzeigen.

- **Daten-LIFs**

  Anzahl und Typ der für die SVM verfügbaren Daten-LIFs

- **Zulässiger Volumentyp**

  Der Typ des Volumes, der auf der SVM erstellt werden kann.

  SVMs können eine oder mehrere FlexVol Volumes oder FlexGroup Volumes enthalten. Der FlexGroup-Typ ist bei Verwendung von ONTAP 9.1 oder höher zulässig.

  Die Performance-Seiten von Unified Manager unterstützen keine Infinite Volumes.

- **Erlaubte Protokolle**

  Liste aller Protokolle, die von dieser SVM gewartet werden können Verfügbare Protokolle sind FC/FCoE, iSCSI, HTTP, NDMP, NVMe, NFS und CIFS.

- **Portsatz**

  Wenn FCP- oder iSCSI-Protokolle definiert werden, ist der Portsatz, der dieser SVM zugewiesen ist.

Informationen zu Performance/LUN

Auf der Seite „Performance/LUN Information“ können Sie eine Liste der physischen und logischen Attribute der LUN anzeigen. Diese Informationen könnten bei der Beantwortung von Fragen zur Leistungsfähigkeit helfen.

LUN-Attribute

- * WWN*

  Der WWN (World Wide Name) der LUN.

- **Pfad**

  Der vollständige Pfad der LUN, beispielsweise `/vol/vol1/lun1`.

- **Ausrichtung**

  Zeigt den Ausrichtungsstatus der LUN an. Mögliche Werte:

  - Nicht zugeordnet

- Ausgerichtet
- Falsch Ausgerichtet
- Möglicherweise falsch ausgerichtet
- Unbestimmt

- * Kapazität (frei/gesamt)*

  Der gesamte verfügbare Speicher auf der LUN, in Gigabyte und der derzeit verfügbaren Menge an Speicherplatz.

- **Lautstärke**

  Der Name des Volumes, zu dem die LUN gehört. Sie können auf den Namen klicken, um die Volume-Details auf der Seite Performance/Volume Explorer anzuzeigen.

- **Storage Virtual Machine**

  Der Name der SVM, der die LUN angehört. Sie können auf der Seite „Performance/SVM Explorer“ auf den Namen klicken, um SVM-Details anzuzeigen.

- **Knoten**

  Der Name des Node, auf dem sich die LUN befindet. Sie können auf den Namen klicken, um Node-Details auf der Seite Performance/Node Explorer anzuzeigen.

- * Cluster*

  Der Name des Clusters, zu dem die LUN gehört. Sie können auf den Namen klicken, um in der Seite „Performance/Cluster Explorer“ Cluster-Details anzuzeigen.

- **Bundesland**

  Der Zustand der LUN. Gültige Status können „Online“, „Offline“, „NV-Fehler“, „Speicherplatz-Fehler“ und „Foreign-lun-Fehler“ sein.

- * Zugeordnet*

  Gibt an, ob die LUN einer Initiatorgruppe zugeordnet ist (true), oder nicht (false).

Namespace-Informationen

Auf der Seite Namespace-Informationen können Sie eine Liste der physischen und logischen Attribute des Namespace anzeigen. Diese Informationen könnten bei der Beantwortung von Fragen zur Leistungsfähigkeit helfen.

Namespace-Attribute

- * Cluster*

  Der Name des Clusters, zu dem der Namespace gehört. Sie können auf den Namen klicken, um in der Seite „Performance/Cluster Explorer“ Cluster-Details anzuzeigen.

- * Kapazität (frei/gesamt)*

Die gesamte Storage-Kapazität des Namespace und die derzeit verfügbare Speichermenge.

- **Knoten**

  Der Name des Node, auf dem sich der Namespace befindet. Sie können auf den Namen klicken, um Node-Details auf der Seite Performance/Node Explorer anzuzeigen.

- **Pfad**

  Der vollständige Pfad des Namespace beispielsweise `/vol/vol1/namespace1`.

- **Bundesland**

  Der Status des Namespace. Gültige Status können „Online“, „Offline“, „NV-Fehler“ und „space-error“ sein.

- **Subsystem**

  Das Subsystem des Namespace.

- **Storage Virtual Machine**

  Der Name der SVM, zu der der Namespace gehört. Sie können auf der Seite „Performance/SVM Explorer“ auf den Namen klicken, um SVM-Details anzuzeigen.

- **Lautstärke**

  Der Name des Volumes, zu dem der Namespace gehört. Sie können auf den Namen klicken, um die Volume-Details auf der Seite Performance/Volume Explorer anzuzeigen.

Informationsseite für Performance/LIF

Zeigen Sie mithilfe der Seite „Performance/LIF-Informationen“ eine Liste der konfigurierten Attribute des LIF an. Diese Informationen könnten bei der Beantwortung von Fragen zur Leistungsfähigkeit helfen.

LIF-Attribute

- **IP-Adresse**

  Die dem LIF zugewiesene IPv4- oder IPv6-Adresse. Einem LIF kann mehrere IP-Adressen zugewiesen sein.

- * Rolle*

  Die Rolle bestimmt die Art des Datenverkehrs, der über das LIF unterstützt wird.

  LIFs können eine der folgenden Rollen aufweisen:

  - Daten
  - Cluster
  - Node-Management
  - Intercluster

- **Failover-Gruppe**

  Der Name der Failover-Gruppe, die dem LIF zugewiesen ist.

  Dieses Feld gilt nur für Netzwerk-LIFs, nicht für SAN (FC/ISCSI) und NVMe LIFs.

- **Failover-Richtlinie**

  Der Name der Failover-Richtlinie, die dem LIF zugewiesen ist.

  Dieses Feld gilt nur für Netzwerk-LIFs, nicht für SAN (FC/ISCSI) und NVMe LIFs.

- * Home Port*

  Der Name des Node und des Ports, der als Home-Port für diese Schnittstelle definiert wurde. Sie können auf den Namen klicken, um Einzelheiten zu den Ports auf der Seite Leistung/Port Explorer anzuzeigen.

- **Aktueller Port**

  Der Name des Node und des Ports, auf dem die Schnittstelle derzeit gehostet wird. Sie können auf den Namen klicken, um Einzelheiten zu den Ports auf der Seite Leistung/Port Explorer anzuzeigen.

Verstehen und Verwenden der Seite Node Failover Planning

Die Seite „Performance/Node Failover Planning“ schätzt die Auswirkungen auf die Performance eines Node, wenn der hochverfügbare Partner-Node des Node ausfällt. Die Schätzungen von Unified Manager beruhen auf der historischen Performance von Nodes im HA-Paar.

Die Schätzung der Auswirkungen auf die Performance bei einem Failover hilft Ihnen, die folgenden Szenarien zu planen:

- Wenn ein Failover die geschätzte Performance des übernehmenden Node immer wieder auf ein nicht akzeptables Niveau verschlechtert, können Sie Korrekturmaßnahmen ergreifen, um die Performance-Beeinträchtigung aufgrund eines Failover zu verringern.
- Vor dem Initiieren eines manuellen Failover zur Durchführung von Hardwarewartungsaufgaben können Sie einschätzen, welche Auswirkungen der Failover auf die Performance des Takeover-Nodes hat, um den optimalen Zeitpunkt für die Durchführung der Aufgabe zu bestimmen.

Verwenden der Seite Knoten-Failover-Planung, um Korrekturmaßnahmen zu ermitteln

Basierend auf den Informationen, die auf der Seite „Performance/Node Failover Planning“ angezeigt werden, können Sie Maßnahmen ergreifen, um sicherzustellen, dass ein Failover nicht dazu führt, dass die Performance eines HA-Paars unter eine akzeptable Ebene fällt.

Um beispielsweise die geschätzten Performance-Auswirkungen eines Failover zu verringern, können Sie einige Volumes oder LUNs von einem Node im HA-Paar auf andere Nodes im Cluster verschieben. So wird sichergestellt, dass der primäre Node nach einem Failover weiterhin eine akzeptable Performance liefern kann.

Komponenten der Seite Knoten-Failover-Planung

Die Komponenten der Seite Performance/Node Failover Planning werden in einem Raster und im Fenster Comparing angezeigt. In diesen Abschnitten können Sie die Auswirkungen eines Node-Failovers auf die Performance des Takeover-Nodes bewerten.

Das Raster der Performance-Statistiken

Auf der Seite „Performance/Node-Failover-Planung“ wird ein Raster mit Statistiken zu Latenz, IOPS, Auslastung und Performance-Kapazität angezeigt.

> Die IOPS-Werte, die auf dieser Seite und auf der Seite „Performance/Node Performance Explorer“ angezeigt werden, sind möglicherweise nicht dieselben.

Im Raster ist jedem Node eine der folgenden Rollen zugewiesen:

- Primär

  Der Node, der beim Ausfall des Partners für den HA-Partner übernimmt. Das Root-Objekt ist immer der primäre Node.

- Partner

  Der Node, der im Failover-Szenario ausfällt.

- Geschätzte Übernahme

  Das gleiche wie der primäre Knoten. Für diesen Node angezeigte Performance-Statistiken zeigen die Performance des Takeover-Node, nachdem der ausgefallene Partner übernommen wurde.

> Obwohl der Workload des Takeover-Node den kombinierten Workloads beider Nodes nach einem Failover entspricht, wurden die Statistiken für den geschätzten Takeover-Node nicht als Summe der Statistiken des primären Nodes und des Partner-Nodes angezeigt. Wenn zum Beispiel die Latenz des primären Node 2 ms/op beträgt und die Latenz des Partnerknotens 3 ms/op beträgt, kann der geschätzte Übernahmeknoten eine Latenz von 4 ms/op haben Dieser Wert ist eine Berechnung, die Unified Manager durchführt.

Sie können auf den Namen des Partner-Knotens klicken, wenn er das Root-Objekt werden soll. Nachdem die Seite Performance/Node Performance Explorer angezeigt wurde, können Sie auf die Registerkarte **Failover Planning** klicken, um zu sehen, wie sich die Leistung in diesem Ausfallszenario ändert. Wenn beispielsweise Node1 der primäre Node und Node2 der Partner-Node ist, können Sie auf Node2 klicken, um ihn zum primären Node zu machen. Auf diese Weise sehen Sie, wie sich die geschätzte Performance je nach dem Ausfall des Node ändert.

Teilfenster „Vergleichen“

In der folgenden Liste werden die im Teilfenster „Vergleich“ angezeigten Komponenten standardmäßig beschrieben:

- **Veranstaltungsdiagramme**

  Sie werden im gleichen Format wie auf der Seite Performance/Node Performance Explorer angezeigt. Sie beziehen sich nur auf den primären Node.

- **Counter-Charts**

  Sie zeigen historische Statistiken für den im Raster angezeigten Performance-Zähler an. In jedem Diagramm wird im Diagramm für den geschätzten Takeover-Node die geschätzte Performance angezeigt, wenn ein Failover zu einem bestimmten Zeitpunkt aufgetreten ist.

  Angenommen, das Auslastungsdiagramm zeigt 73 % des Node Estimated Takeover um 11:00 Uhr an Am 8. Februar. Wenn zu diesem Zeitpunkt ein Failover aufgetreten wäre, hätte die Auslastung des Takeover-Nodes 73 % betragen.

  Anhand der historischen Statistiken finden Sie den optimalen Zeitpunkt für das Initiieren eines Failover und minimieren so das Risiko einer Überlastung des Takeover-Nodes. Sie können einen Failover nur zu Zeiten planen, in denen die prognostizierte Performance des Takeover-Node akzeptabel ist.

Standardmäßig werden Statistiken sowohl für das Root-Objekt als auch für den Partner-Node im Teilfenster „Vergleichen“ angezeigt. Anders als auf der Seite Performance/Node Performance Explorer zeigt diese Seite nicht die Schaltfläche **Hinzufügen** an, um Objekte zum Statistikvergleich hinzuzufügen.

Sie können das vergleichende Fenster auf die gleiche Weise anpassen wie auf der Seite Performance/Node Performance Explorer. Die folgende Liste zeigt Beispiele zur Anpassung der Diagramme:

- Klicken Sie auf einen Node-Namen, um die Statistiken des Node in den Zählerdiagrammen anzuzeigen oder zu verbergen.
- Klicken Sie auf **Zoom-Ansicht**, um ein detailliertes Diagramm für einen bestimmten Zähler in einem neuen Fenster anzuzeigen.

Verwenden einer Schwellenwertrichtlinie auf der Seite Knoten-Failover-Planung

Sie können eine Node-Schwellenwertrichtlinie erstellen, sodass Sie auf der Seite „Performance/Node Failover Planning“ eine Benachrichtigung erhalten können, wenn ein potenzieller Failover die Performance des Takeover-Node auf ein inakzeptables Maß verschlechtert.

Die vom System definierte Performance-Schwellenwertrichtlinie „`Node HA-Paar Overused`“ erzeugt ein Warnereignis, wenn der Schwellenwert für sechs aufeinanderfolgende Erfassungszeiträume (30 Minuten) überschritten wird. Der Schwellenwert ist dann nicht erreicht, wenn die kombinierte Performance-Kapazität, die von den Nodes in einem HA-Paar genutzt wird, 200 % überschreitet.

Das Ereignis der vom System definierten Schwellenwertrichtlinie gibt Ihnen Warnungen vor, dass ein Failover dazu führt, dass die Latenz des Takeover-Node auf ein inakzeptables Maß erhöht wird. Wenn ein Ereignis, das von dieser Richtlinie für einen bestimmten Node generiert wird, angezeigt wird, können Sie zur Seite Performance/Node-Failover-Planung für diesen Node wechseln, um den prognostizierten Latenzwert aufgrund eines Failover anzuzeigen.

Zusätzlich zur Nutzung dieser systemdefinierten Schwellenwertrichtlinie können Sie unter Verwendung des Zählers „`Performance Capacity Used - Takeover`“ Schwellenwertrichtlinien erstellen und die Richtlinie dann auf ausgewählte Nodes anwenden. Wenn Sie einen Schwellenwert von weniger als 200 % angeben, erhalten Sie ein Ereignis, bevor der Schwellenwert für die vom System definierte Richtlinie nicht erreicht wird. Sie können auch den Mindestzeitraum angeben, für den der Schwellenwert auf weniger als 30 Minuten überschritten wird, wenn Sie benachrichtigt werden möchten, bevor das vom System definierte Richtlinienereignis generiert wird.

Sie können beispielsweise eine Schwellenwertrichtlinie zur Generierung eines Warnungsereignisses

definieren, wenn die kombinierte Performance-Kapazität der Nodes in einem HA-Paar mehr als 10 Minuten lang 175 % überschreitet. Sie können diese Richtlinie auf Node1 und Node2 anwenden, die ein HA-Paar bilden. Nachdem Sie eine Warnmeldung für Node1 oder Node2 erhalten haben, können Sie die Seite Performance/Node-Failover-Planung für diesen Node anzeigen, um die geschätzten Performance-Auswirkungen auf den Takeover-Node einzuschätzen. Sie können Korrekturmaßnahmen ergreifen, um bei einem Failover einen Überlastung des Takeover-Node zu vermeiden. Wenn Sie Maßnahmen ergreifen, wenn die kombinierte Performance-Kapazität, die von den Nodes verwendet wird, unter 200 % liegt, erreicht die Latenz des Ersatz-Node nicht ein inakzeptables Maß, selbst wenn in diesem Zeitraum ein Failover stattfindet.

Verwenden des Leistungsdiagramms zur verwendeten Kapazität zur Failover-Planung

Das Diagramm „Detailed Performance Capacity Used – Breakdown“ zeigt die für den primären Knoten und den Partner-Knoten verwendete Performance-Kapazität an. Er zeigt außerdem die Menge der freien Performance-Kapazität auf dem geschätzten Takeover-Node an. Anhand dieser Informationen können Sie ermitteln, ob bei einem Ausfall des Partner-Node möglicherweise ein Performance-Problem auftritt.

Über diese Aufgabe

Neben der Anzeige der Gesamt-Performance-Kapazität, die für die Nodes verwendet wird, unterteilt das Diagramm die Werte für jeden Knoten in Benutzerprotokolle und Hintergrundprozesse.

- Benutzerprotokolle sind die I/O-Vorgänge von Benutzerapplikationen auf und vom Cluster.
- Hintergrundprozesse sind interne Systemprozesse, die mit Storage-Effizienz, Datenreplizierung und Systemzustand verknüpft sind.

Mit dieser zusätzlichen Detailebene können Sie ermitteln, ob ein Performance-Problem auf Benutzerapplikationsaktivitäten oder auf System-Prozessen im Hintergrund verursacht wird, wie Deduplizierung, RAID rekonstruieren, Festplatte Schrubben und SnapMirror Kopien.

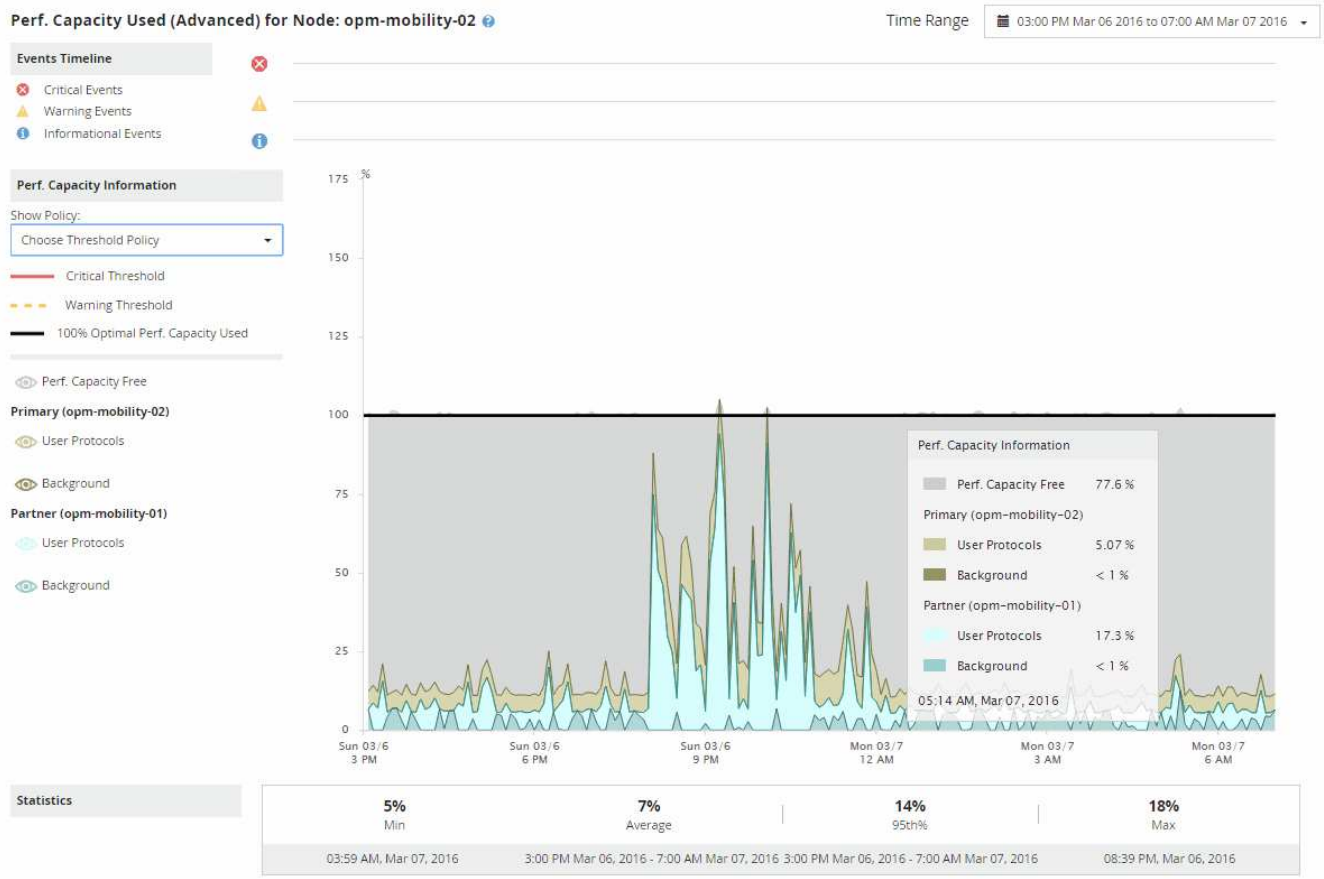
Schritte

1. Wechseln Sie zur Seite **Leistung/Knoten-Failover-Planung** für den Knoten, der als Geschätzter Übernahmeknoten dient.
2. Wählen Sie im Auswahlfeld **Zeitbereich** den Zeitraum aus, für den die historischen Statistiken im Zählerraster und in den Zählerdiagrammen angezeigt werden.

   Die Zählerdiagramme mit den Statistiken für den primären Node, den Partner-Node und den geschätzten Takeover-Node werden angezeigt.

3. Wählen Sie aus der Liste **Choose Charts** die Option **Perf. Verwendete Kapazität**.
4. Im **Perf. Verwendete Kapazität** Diagramm, wählen Sie **Breakdown** und klicken Sie auf **Zoom View**.

   Das detaillierte Diagramm für Perf. Die verwendete Kapazität wird angezeigt.



5. Bewegen Sie den Cursor über das detaillierte Diagramm, um die Informationen zur verwendeten Performance-Kapazität im Popup-Fenster anzuzeigen.

   Die Perf. Der freie Prozentsatz der Kapazität ist die am geschätzten Takeover-Node verfügbare Performance-Kapazität. Es zeigt an, wie viel Performance-Kapazität nach einem Failover auf dem Takeover-Node übrig ist. Wenn der Wert 0 % beträgt, erhöht ein Failover die Latenz auf ein inakzeptables Level auf dem Takeover-Node.

6. Ziehen Sie Korrekturmaßnahmen in Betracht, um einen freien Prozentsatz bei niedriger Performance-Kapazität zu vermeiden.

   Wenn Sie einen Failover für eine Node-Wartung initiieren möchten, wählen Sie eine Zeit zum Fehlschlagen des Partner-Node aus, wenn der freie Prozentsatz der Performance-Kapazität nicht bei 0 ist.

Erfassung von Daten und Monitoring der Workload-Performance

Unified Manager erfasst und analysiert Workload-Aktivitäten alle 5 Minuten, um Performance-Ereignisse zu identifizieren und Konfigurationsänderungen alle 15 Minuten zu erkennen. Es werden maximal 30 Tage 5 vergangener Performance- und Ereignisdaten aufbewahrt. Anhand dieser Daten wird der erwartete Bereich für alle überwachten Workloads prognostiziert.

In diesem Kapitel wird beschrieben, wie dynamische Schwellenwerte funktionieren und wie sie zur Überwachung der Workload-Performance eingesetzt werden. Dieses Kapitel gilt nicht für Statistiken oder Ereignisse, die durch benutzerdefinierte oder systemdefinierte Leistungsschwellenwerte entstehen.

Unified Manager muss die Workload-Aktivität mindestens 3 Tage lang sammeln, bevor sie mit der Analyse beginnen kann. Vor dem erwarteten Bereich für I/O-Reaktionszeiten und Vorgänge kann auf der Seite Performance/Volume Details und auf der Seite Event Details angezeigt werden. Während diese Aktivität erfasst wird, werden im erwarteten Bereich nicht alle Änderungen angezeigt, die von der Workload-Aktivität auftreten. Nach der Erfassung von 3 Tagen Aktivität passt Unified Manager den erwarteten Bereich alle 24 Stunden um 12:00 Uhr an, um Workload-Aktivitätsänderungen zu berücksichtigen und einen präziseren Leistungsschwellenwert festzulegen.

In den ersten 4 Tagen, an denen Unified Manager ein Volume überwacht, werden die Diagramme auf der Seite Performance/Volume Details nicht den erwarteten Bereich für dieses Volume angezeigt, wenn mehr als 24 Stunden seit der letzten Datenerfassung vergangen sind. Ereignisse, die vor der letzten Sammlung erkannt wurden, sind weiterhin verfügbar.

Bei der Sommerzeit (Sommerzeit) wird die Systemzeit geändert, wodurch der erwartete Bereich der Performance-Statistiken für überwachte Workloads verändert wird. Unified Manager beginnt sofort mit der Korrektur des erwarteten Bereichs, der ungefähr 15 Tage dauert. In dieser Zeit können Sie Unified Manager weiterhin verwenden. Da Unified Manager jedoch den erwarteten Bereich zum Erkennen von Ereignissen verwendet, sind einige Ereignisse möglicherweise nicht korrekt. Ereignisse, die vor der Zeitänderung erkannt wurden, werden nicht beeinträchtigt. Wenn Sie die Zeit auf einem Cluster oder auf einem Unified Manager-Server zu einem früheren Zeitpunkt manuell ändern, wirkt sich dies auch auf die Ergebnisse der Ereignisanalyse aus.

Arten von Workloads, die von Unified Manager überwacht werden

Mit Unified Manager lässt sich die Performance von zwei Workload-Typen überwachen: Benutzerdefiniert und systemdefiniert.

- ***benutzerdefinierte Workloads***

  Der I/O-Durchsatz von Applikationen zum Cluster. Dies sind Prozesse, die an Lese- und Schreibanfragen beteiligt sind. Ein FlexVol Volume oder FlexGroup Volume ist ein benutzerdefinierter Workload.

  Unified Manager überwacht nur die Workload-Aktivität auf dem Cluster. Er überwacht nicht die Applikationen, Clients oder Pfade zwischen den Applikationen und dem Cluster.

  Wenn eine oder mehrere der folgenden Optionen für einen Workload zutrifft, kann er nicht von Unified Manager überwacht werden:

  - Es handelt sich um eine Kopie der Datensicherung (DP) im schreibgeschützten Modus. (Beachten Sie, dass bei Verwendung von ONTAP 8.3 und höher DP-Volumes für vom Benutzer erzeugten Datenverkehr überwacht werden.)
  - Es handelt sich um ein Infinite Volume.
  - Ein offline-Datenklon.
  - Es handelt sich um ein gespiegeltes Volume in einer MetroCluster-Konfiguration.

- ***systemdefinierte Workloads***

Zu den internen Prozessen, die mit Storage-Effizienz, Datenreplizierung und Systemzustand verbunden sind, gehören:

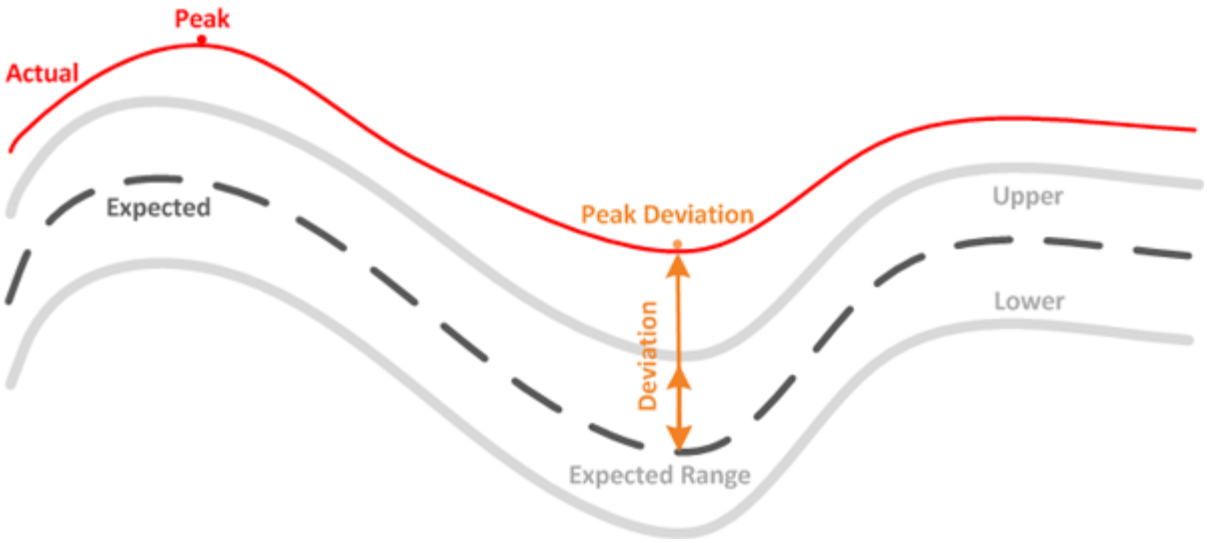
- Storage-Effizienz, z. B. Deduplizierung
- Der Zustand der Festplatte, einschließlich RAID-Rekonstruktion, Disk-Schrubben usw.
- Datenreplizierung, z. B. SnapMirror Kopien
- Management-Aktivitäten
- Systemzustand des File-Systems, der verschiedene WAFL-Aktivitäten umfasst
- Filesystem-Scanner, z. B. WAFL-Scan
- Copy-Offload, z. B. Verlagerung von Storage-Effizienzvorgängen von VMware Hosts
- Systemzustand, wie z. B. das Verschieben von Volumes, die Datenkomprimierung usw.
- Nicht überwachte Volumes

Performance-Daten für systemdefinierte Workloads werden nur in der GUI angezeigt, wenn die von diesen Workloads verwendete Cluster-Komponente mit Konflikten belegt ist. Sie können beispielsweise nicht nach dem Namen eines systemdefinierten Workloads suchen, um dessen Performance-Daten in der GUI anzuzeigen. Wenn mehrere systemdefinierte Workloads desselben Typs angezeigt werden, wird dem Workload-Namen ein Buchstabe angehängt. Das Schreiben ist für die Verwendung durch das Supportpersonal bestimmt.

Messwerte für die Workload-Performance

Unified Manager misst die Performance von Workloads auf einem Cluster basierend auf historischen und erwarteten statistischen Werten, die den erwarteten Wertebereich für die Workloads bilden. Es vergleicht die tatsächlichen statistischen Workload-Werte mit dem erwarteten Bereich, um zu ermitteln, ob die Workload-Performance zu hoch oder zu niedrig ist. Ein Workload, der nicht den erwarteten Leistung entspricht, löst einen Performance-Ereignisbericht aus, damit Sie benachrichtigt werden.

In der folgenden Abbildung stellt der tatsächliche Wert in Rot die tatsächlichen Performance-Statistiken im Zeitrahmen dar. Der tatsächliche Wert hat den Leistungsschwellenwert überschritten, der die oberen Grenzen des erwarteten Bereichs darstellt. Der Peak ist der höchste ist-Wert im Zeitrahmen. Die Abweichung misst die Änderung zwischen den erwarteten Werten und den ist-Werten, während die Peak-Abweichung die größte Änderung zwischen den erwarteten Werten und den ist-Werten angibt.



In der folgenden Tabelle sind die Messwerte zur Workload-Performance aufgeführt.

Messung	Beschreibung
Aktivität	Der Prozentsatz des QoS-Limits, der von den Workloads in der Richtliniengruppe verwendet wird Wenn Unified Manager eine Änderung an einer Richtliniengruppe erkennt, z. B. das Hinzufügen oder Entfernen eines Volumes oder das Ändern des QoS-Limits, kann der tatsächliche und erwartete Wert 100 % des festgelegten Grenzwerts überschreiten. Wenn ein Wert 100 % des festgelegten Grenzwerts überschreitet, wird er als >100 % angezeigt. Wenn ein Wert kleiner als 1 % des festgelegten Grenzwerts ist, wird er als <1 % angezeigt.
Tatsächlich	Der messbare Performance-Wert zu einem bestimmten Zeitpunkt für einen bestimmten Workload.

Messung	Beschreibung
Abweichung	Die Änderung zwischen den erwarteten Werten und den ist-Werten. Es ist das Verhältnis des ist-Wertes minus dem erwarteten Wert zum oberen Wert des erwarteten Bereichs minus dem erwarteten Wert. Ein negativer Abweichungswert zeigt, dass die Workload-Performance niedriger ist als erwartet, während ein positiver Abweichungswert darauf hinweist, dass die Workload-Performance höher ist als erwartet. Wenn die erwarteten Werte und der ist-Wert sehr gering sind, z.B. in den Hundertstel oder Tausendstel eines Prozentwerts, wird in der Abweichung N/A angezeigt
Erwartet	Die erwarteten Werte basieren auf der Analyse historischer Performance-Daten für einen bestimmten Workload. Unified Manager analysiert diese statistischen Werte, um den erwarteten Wertebereich zu bestimmen.
Erwarteter Bereich	Der erwartete Wertebereich ist eine Prognose oder Vorhersage dessen, was die oberen und unteren Leistungswerte zu einem bestimmten Zeitpunkt erwartet werden. Bei der Workload-Latenz bilden die oberen Werte den Performance-Schwellenwert. Wenn der tatsächliche Wert den Performance-Schwellenwert überschreitet, löst Unified Manager eine Warnmeldung im Rahmen des Performance-Ereignisses aus.
Spitze	Der maximale Wert, der über einen Zeitraum gemessen wird.
Maximale Abweichung	Der maximale Abweichungswert, der über einen Zeitraum gemessen wird.
Warteschlangentiefe	Die Anzahl der ausstehenden I/O-Anfragen, die an der Interconnect-Komponente warten.

Messung	Beschreibung
Auslastung	Für die Netzwerkverarbeitung, Datenverarbeitung und aggregierte Komponenten ist der prozentuale Anteil der Auslastung während eines bestimmten Zeitraums an den Workload-Vorgängen beschäftigt. Beispielsweise der prozentuale Anteil der Zeit, die für die Netzwerkverarbeitung oder Datenverarbeitung erforderlich ist, um eine I/O-Anfrage zu bearbeiten, oder an ein Aggregat, um eine Lese- oder Schreibanforderung zu erfüllen.
Schreibdurchsatz	Der Schreibdurchsatz in Megabyte pro Sekunde (MB/s), von Workloads in einem lokalen Cluster zum Partner-Cluster in einer MetroCluster-Konfiguration.

Der erwartete Leistungsbereich

Der erwartete Wertebereich ist eine Prognose oder Vorhersage dessen, was die oberen und unteren Leistungswerte zu einem bestimmten Zeitpunkt erwartet werden. Bei der Workload-Latenz bilden die oberen Werte den Performance-Schwellenwert. Wenn der tatsächliche Wert den Performance-Schwellenwert überschreitet, löst Unified Manager eine Warnmeldung im Rahmen des Performance-Ereignisses aus.

Beispiel: Während der regulären Geschäftszeiten zwischen 9:00 Uhr Bis 5:00 Uhr checken die meisten Mitarbeiter ihre E-Mail-Adresse möglicherweise zwischen 9:00 Uhr ein Und 10:30 Uhr Der erhöhte Bedarf an E-Mail-Servern bedeutet eine Zunahme der Workload-Aktivitäten im Back-End Storage während dieser Zeit. Mitarbeiter können von ihren E-Mail-Clients langsame Reaktionszeiten feststellen.

Während der Mittagspause zwischen 12:00 Uhr Und 13:00 Uhr Und am Ende des Arbeitstages nach 5:00 Uhr werden die meisten Mitarbeiter wahrscheinlich von ihren Computern weg. Der Bedarf an E-Mail-Servern sinkt in der Regel, wodurch auch der Bedarf an Back-End Storage sinkt. Alternativ können geplante Workload-Operationen wie Storage-Backups oder Virus-Scans nach 5:00 Uhr geplant werden Und erhöhen Sie die Aktivität im Back-End Storage.

Über mehrere Tage bestimmt der Anstieg und die Abnahme der Workload-Aktivität den erwarteten Aktivitätsbereich, wobei die Workloads über- und Untergrenzen verteilt sind. Wenn sich die tatsächlichen Workload-Aktivitäten für ein Objekt außerhalb der oberen oder unteren Grenzen befinden und für einen bestimmten Zeitraum außerhalb der Grenzen liegen, kann dies darauf hindeuten, dass das Objekt überlastet oder nicht ausgelastet ist.

Wie sich der erwartete Bereich bildet

Unified Manager muss mindestens 3 Tage Workload-Aktivität sammeln, bevor sie mit der Analyse beginnen kann. Anschließend kann der erwartete Bereich für I/O-Reaktionszeiten und Vorgänge auf der GUI angezeigt werden. Die erforderliche Mindesterfassung berücksichtigt nicht alle Änderungen, die von der Workload-Aktivität durchgeführt werden. Nach der Erfassung der ersten 3 Tage der Aktivität passt Unified Manager den erwarteten Bereich alle 24 Stunden um 12:00 Uhr an, um Änderungen der Workload-Aktivität widerzuspiegeln und einen genaueren Leistungsschwellenwert festzulegen.

Bei der Sommerzeit (Sommerzeit) wird die Systemzeit geändert, wodurch der erwartete Bereich der Performance-Statistiken für überwachte Workloads verändert wird. Unified Manager beginnt sofort mit der Korrektur des erwarteten Bereichs, der ungefähr 15 Tage dauert. In dieser Zeit können Sie Unified Manager weiterhin verwenden. Da Unified Manager jedoch den erwarteten Bereich zum Erkennen von Ereignissen verwendet, sind einige Ereignisse möglicherweise nicht korrekt. Ereignisse, die vor der Zeitänderung erkannt wurden, werden nicht beeinträchtigt. Wenn Sie die Zeit auf einem Cluster oder auf einem Unified Manager-Server zu einem früheren Zeitpunkt manuell ändern, wirkt sich dies auch auf die Ergebnisse der Ereignisanalyse aus.

Wie der erwartete Bereich bei der Leistungsanalyse verwendet wird

Unified Manager verwendet den erwarteten Bereich, um die typischen Aktivitäten der I/O-Latenz (Reaktionszeit) und der IOPS (Vorgänge) für überwachte Workloads darzustellen. Er benachrichtigt Sie, wenn die tatsächliche Latenz für einen Workload über dem oberen Bereich des erwarteten Bereichs liegt. Dadurch wird ein Performance-Ereignis ausgelöst, sodass Sie das Performance-Problem analysieren und Korrekturmaßnahmen ergreifen können.

Der erwartete Bereich legt die Performance-Baseline für den Workload fest. Im Laufe der Zeit lernt Unified Manager aus früheren Performance-Messungen, um die erwartete Performance und Aktivitätslevel für den Workload zu prognostizieren. Die obere Grenze des erwarteten Bereichs bestimmt den Leistungsschwellenwert. Unified Manager verwendet die Basiskapazität, um zu ermitteln, ob die tatsächliche Latenz oder der tatsächliche Betrieb über einem Schwellenwert oder außerhalb des erwarteten Bereichs liegt. Der Vergleich der ist-Werte mit den erwarteten Werten erstellt ein Performance-Profil für den Workload.

Wenn die tatsächliche Latenz für einen Workload den Performance-Schwellenwert überschreitet, aufgrund von Konflikten bei einer Cluster-Komponente, ist die Latenz hoch, und der Workload arbeitet langsamer als erwartet. Die Performance anderer Workloads, die dieselben Cluster-Komponenten nutzen, ist möglicherweise auch langsamer als erwartet.

Unified Manager analysiert das Schwellenwertüberschreitereignis und legt fest, ob es sich bei der Aktivität um ein Performance-Ereignis handelt. Wenn die hohe Workload-Aktivität über einen langen Zeitraum, z. B. mehrere Stunden, konsistent bleibt, berücksichtigt Unified Manager die Aktivität als „Normal“ und passt den erwarteten Bereich dynamisch an, um den neuen Performance-Schwellenwert zu bilden.

Einige Workloads weisen möglicherweise durchgängig niedrige Aktivitäten auf, bei denen der erwartete Bereich des Betriebs oder der Latenz im Laufe der Zeit keine hohen Änderungsraten aufweisen. Um die Anzahl der Ereignismeldungen zu minimieren, löst Unified Manager während der Analyse von Performance-Ereignissen ein Ereignis nur für Volumes mit niedriger Aktivität aus, deren Vorgänge und Latenzen erheblich höher sind als erwartet.

In diesem Beispiel weist die Latenz für ein Volume einen erwarteten Bereich auf, in Grau, von 0 Millisekunden pro Vorgang (ms/op) bei dem niedrigsten und 5 ms/op bei dem höchsten Wert auf. Wird die tatsächliche Latenz blau auf 10 ms/op plötzlich erhöht, weil der Netzwerk-Traffic oder die Konflikte einer Cluster-Komponente zeitweise zu hoch sind, liegt sie über dem erwarteten Bereich und hat den Performance-

Schwellenwert überschritten.

Wenn der Netzwerk-Traffic gesunken ist oder die Cluster-Komponente keine Konflikte mehr aufweist, wird die Latenz innerhalb des erwarteten Bereichs zurückgegeben. Wenn die Latenz für einen langen Zeitraum bei oder über 10 ms/op bleibt, müssen Sie möglicherweise Korrekturmaßnahmen ergreifen, um das Ereignis zu beheben.

Unified Manager verwendet Workload-Latenz zur Identifizierung von Performance-Problemen

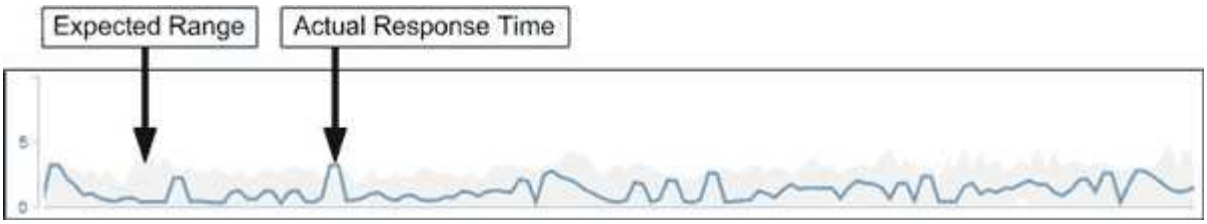
Die Workload-Latenz (Reaktionszeit) ist die Zeit, die ein Volume auf einem Cluster benötigt, um auf I/O-Anforderungen von Client-Applikationen zu reagieren. Unified Manager verwendet die Latenz, um Performance-Ereignisse zu erkennen und zu benachrichtigen.

Eine hohe Latenz bedeutet, dass Anfragen von Applikationen auf Volumes eines Clusters länger dauern als üblich. Die Ursache für die hohe Latenz könnte sich auf dem Cluster selbst befinden, aufgrund von Konflikten bei einer oder mehreren Cluster-Komponenten. Hohe Latenzzeiten könnten auch auf Probleme außerhalb des Clusters zurückzuführen sein, beispielsweise Netzwerkengpässe, Probleme mit dem Client, der die Applikationen hostet, oder Probleme mit den Applikationen selbst.

Unified Manager überwacht nur die Workload-Aktivität auf dem Cluster. Er überwacht nicht die Applikationen, Clients oder Pfade zwischen den Applikationen und dem Cluster.

Operationen im Cluster, z. B. die Erstellung von Backups oder die Durchführung von Deduplizierung, die die Anforderungen von Clusterkomponenten erhöhen, die für andere Workloads gemeinsam genutzt werden, können ebenfalls zu einer hohen Latenz beitragen. Wenn die tatsächliche Latenz den Performance-Schwellenwert des erwarteten Bereichs überschreitet, analysiert Unified Manager das Ereignis, um zu ermitteln, ob es sich um ein Performance-Ereignis handelt, das Sie möglicherweise beheben müssen. Die Latenz wird in Millisekunden pro Vorgang (ms/op) gemessen.

Auf der Seite Performance/Volume Details können Sie sich eine Analyse der Latenzstatistiken anzeigen lassen, um zu ermitteln, wie die Aktivitäten einzelner Prozesse wie Lese- und Schreibanfragen mit den Latenzstatistiken insgesamt verglichen werden. Der Vergleich hilft Ihnen dabei zu ermitteln, welche Vorgänge die höchste Aktivität haben oder ob bestimmte Vorgänge anormale Aktivitäten haben, die sich auf die Latenz eines Volumes auswirken. Bei der Analyse von Performance-Ereignissen können Sie mithilfe der Latenzstatistiken feststellen, ob ein Ereignis durch ein Problem auf dem Cluster verursacht wurde. Sie können auch die spezifischen Workload-Aktivitäten oder Cluster-Komponenten ermitteln, die am Ereignis beteiligt sind.



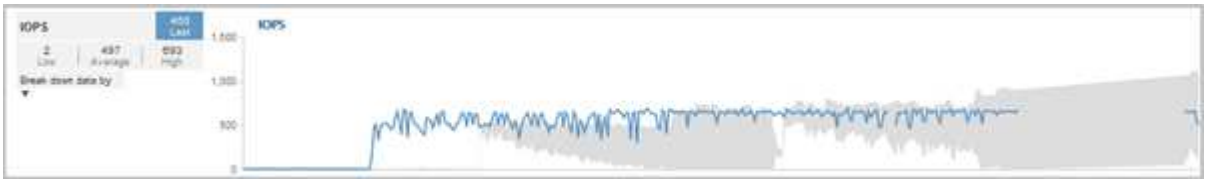
Dieses Beispiel zeigt das Latenzdiagramm auf der Seite Performance/Volume-Details. Die tatsächliche Reaktionszeit (Latenz) ist eine blaue Linie, und der erwartete Bereich ist grau.

In der blauen Zeile kann es zu Lücken kommen, wenn Unified Manager keine Daten erfassen konnte. Dies kann eintreten, da das Cluster oder Volume nicht erreichbar war, Unified Manager während dieser Zeit ausgeschaltet wurde oder die Sammlung länger als den 5-Minuten-Erfassungszeitraum nahm.

Einfluss von Cluster-Vorgängen auf die Workload-Latenz

Operationen (IOPS) stellen die Aktivität aller benutzerdefinierten und systemdefinierten Workloads auf einem Cluster dar. Die IOPS-Statistiken helfen Ihnen bei der Bestimmung, ob Cluster-Prozesse, z. B. Backups oder Deduplizierungsvorgänge, Auswirkungen auf die Workload-Latenz (Reaktionszeit) haben oder ein Performance-Ereignis verursacht haben oder dazu beigetragen haben.

Bei der Analyse von Performance-Ereignissen können Sie mithilfe der IOPS-Statistiken feststellen, ob ein Performance-Ereignis durch ein Problem auf dem Cluster verursacht wurde. Ermitteln Sie die spezifischen Workload-Aktivitäten, die möglicherweise zum Performance-Event beigetragen haben. Die IOPS werden in Operationen pro Sekunde (OPs/Sek.) gemessen.



Dieses Beispiel zeigt das IOPS-Diagramm auf der Seite „Performance/Volume Details“. Die tatsächlichen Statistiken für den Betrieb sind eine blaue Linie und der erwartete Bereich von Statistiken zum Betrieb ist grau.

In manchen Fällen, in denen ein Cluster überlastet ist, wird möglicherweise von Unified Manager die Meldung angezeigt `Data collection is taking too long on Cluster cluster_name`. Das bedeutet, dass für die Analyse von Unified Manager nicht genügend Statistiken erfasst wurden. Sie müssen die Ressourcen, die das Cluster verwendet, verringern, um Statistiken erfassen zu können.

Performance Monitoring von MetroCluster-Konfigurationen

Unified Manager ermöglicht das Monitoring des Schreibdurchsatzes zwischen Clustern in einer MetroCluster-Konfiguration, um Workloads mit einem hohen Schreibdurchsatz zu identifizieren. Falls diese hochperformanten Workloads dazu führen, dass andere Volumes auf dem lokalen Cluster hohe I/O-Reaktionszeiten aufweisen, löst Unified Manager Performance-Ereignisse aus, um Sie zu benachrichtigen.

Wenn ein lokales Cluster in einer MetroCluster-Konfiguration seine Daten auf sein Partner-Cluster spiegelt, werden die Daten in den NVRAM geschrieben und dann über die Interswitch-Links (ISLs) auf die Remote-Aggregate übertragen. Unified Manager analysiert den NVRAM, um die Workloads zu identifizieren, deren hoher Schreibdurchsatz den NVRAM übernutzt und so den NVRAM-Konflikt verursacht.

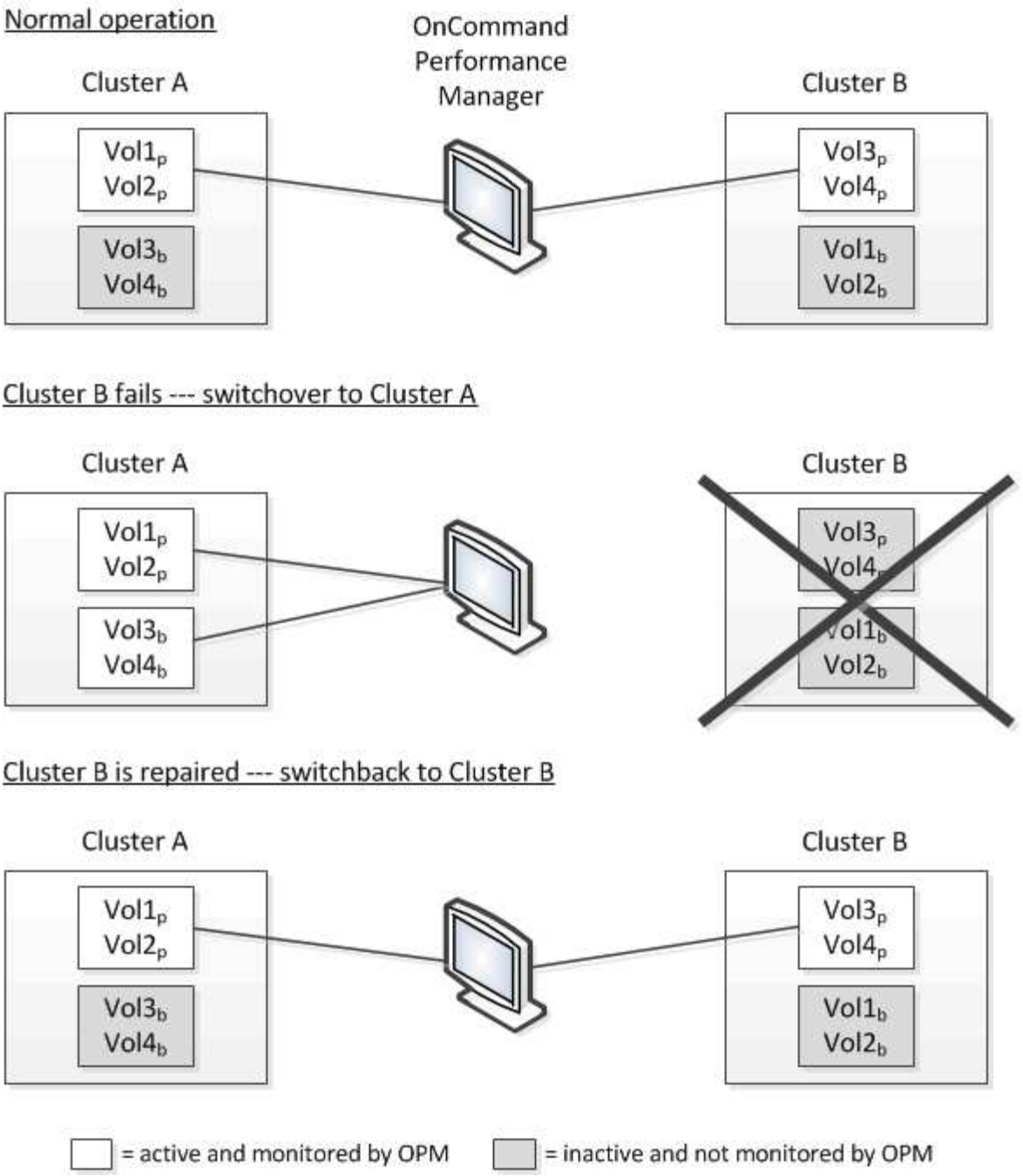
Workloads, deren Abweichung in der Reaktionszeit den Performance-Schwellenwert überschritten hat, werden als „*Opfern*“ bezeichnet. Workloads, deren Abweichung beim Schreibdurchsatz zum NVRAM höher ist als üblich, was zu den Engpässen führt, werden als *bullies* bezeichnet. Da nur Schreibanforderungen zum Partner-Cluster gespiegelt werden, analysiert Unified Manager nicht den Lesedurchsatz.

Unified Manager behandelt die Cluster in einer MetroCluster Konfiguration als einzelne Cluster. Es unterscheidet nicht zwischen Clustern, die Partner sind oder den Schreibdurchsatz von jedem Cluster korrelieren.

Volume-Verhalten während des Umschalens und Zurück

Ereignisse, die ein Switchover oder einen Switchover auslösen, bewirken, dass aktive Volumes von einem Cluster zu einem anderen Cluster in der Disaster-Recovery-Gruppe verschoben werden. Die Volumes auf dem Cluster, die aktiv waren und Clients Daten bereitstellen, werden angehalten, und die Volumes auf dem anderen Cluster sind aktiviert, und mit der Bereitstellung von Daten beginnen Sie. Unified Manager überwacht nur die Volumes, die aktiv sind und ausgeführt werden.

Da Volumes von einem Cluster zum anderen verschoben werden, wird empfohlen, beide Cluster zu überwachen. Eine einzige Instanz von Unified Manager kann beide Cluster in einer MetroCluster-Konfiguration überwachen. Manchmal erfordert die Entfernung zwischen den beiden Standorten jedoch zwei Unified Manager-Instanzen, um beide Cluster zu überwachen. Die folgende Abbildung zeigt eine einzelne Instanz von Unified Manager:



Die Volumes mit p in ihren Namen geben die primären Volumes an, und die Volumes mit b in ihren Namen sind durch SnapMirror erstellte gespiegelte Backup-Volumes.

Im Normalbetrieb:

- Cluster A verfügt über zwei aktive Volumes: Vol1p und Vol2p.
- Cluster B verfügt über 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 aktiven Volume (Statistiken, Ereignisse usw.) werden von Unified Manager erfasst. Die Statistiken zu Vol1p und Vol2p werden von Cluster A gesammelt, und die Statistiken von Vol3p und Vol4p werden von Cluster B gesammelt

Nach einem katastrophalen Ausfall verursacht eine Umschaltung aktiver Volumes von Cluster B zu Cluster A:

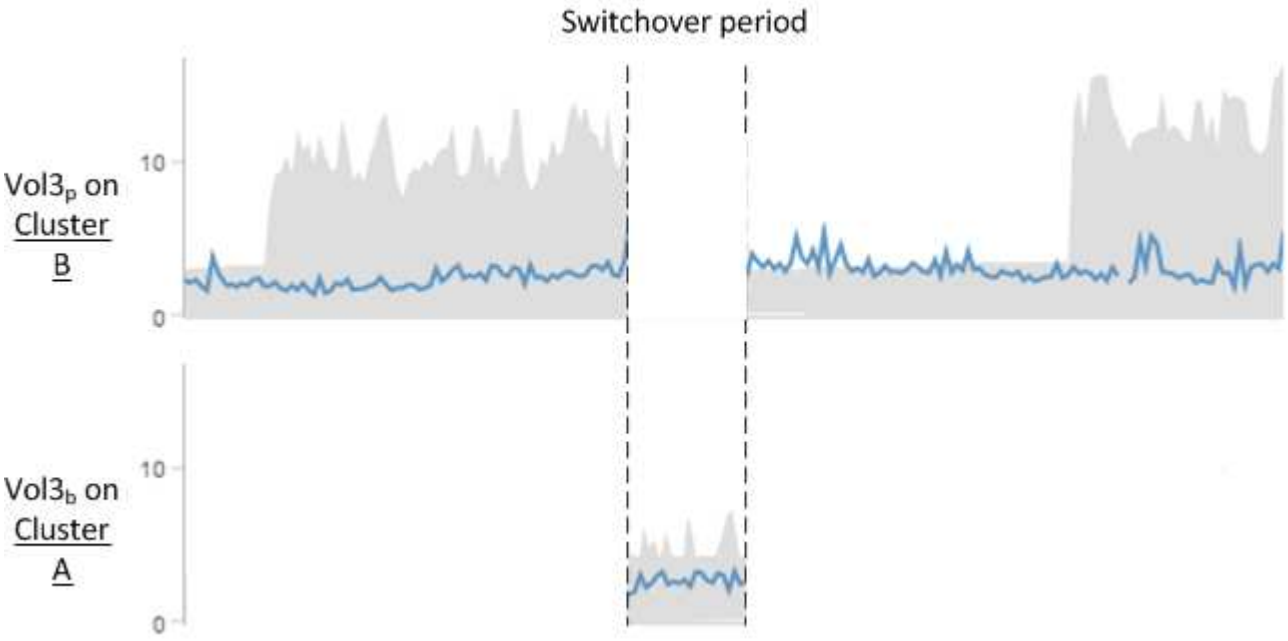
- Cluster A verfügt über vier aktive Volumes: Vol1p, Vol2p, Vol3b und Vol4b.
- Cluster B hat vier inaktive Volumes: Vol3p, Vol4p, Vol1b und Vol2b.

Wie im normalen Betrieb werden Informationen zu den aktiven Volumes von Unified Manager erfasst. Aber in diesem Fall werden die Statistiken zu Vol1p und Vol2p von Cluster A gesammelt, und die Statistiken Vol3b und Vol4b werden auch von Cluster A gesammelt

Beachten Sie, dass Vol3p und Vol3b nicht die gleichen Volumes sind, weil sie auf verschiedenen Clustern sind. Die Informationen im Unified Manager für Vol3p sind nicht identisch mit Vol3b:

- Während der Umstellung auf Cluster A sind Vol3p-Statistiken und -Ereignisse nicht sichtbar.
- Bei der ersten Umschaltung sieht Vol3b wie ein neues Volume ohne historische Informationen aus.

Wenn Cluster B repariert wird und ein Switchback durchgeführt wird, ist Vol3p wieder für Cluster B aktiv. Dies enthält die historischen Statistiken und eine Lücke zwischen den Statistiken für den Zeitraum während der Umschaltung. Vol3b kann von Cluster A nicht angezeigt werden, bis eine weitere Umschaltung erfolgt:



- MetroCluster Volumes, die inaktiv sind, z. B. Vol3b auf Cluster A nach dem Wechsel zurück, werden mit der Meldung „`Dieses Volume wurde gelöscht`“ identifiziert. Das Volume wird nicht tatsächlich gelöscht, es wird jedoch derzeit nicht von Unified Manager überwacht, da es sich nicht um das aktive Volume handelt.
- Wenn ein einziger Unified Manager beide Cluster in einer MetroCluster Konfiguration überwacht, liefert die Volume-Suche Informationen, unabhängig davon, welches Volume zu diesem Zeitpunkt aktiv ist. Eine Suche nach „`VOL3`“ gibt beispielsweise Statistiken und Ereignisse für Vol3b auf Cluster A zurück, wenn eine Umschaltung stattgefunden hat und VOL3 auf Cluster A aktiv ist

Performance-Ereignisanalyse und -Benachrichtigung

Bei Performance-Ereignissen werden Sie über Probleme mit der I/O-Performance bei

einem Volume-Workload informiert, die durch Konflikte bei einer Cluster-Komponente verursacht wurden. Unified Manager analysiert das Ereignis, um alle betroffenen Workloads zu ermitteln, die Komponente mit Konflikten zu identifizieren und ob das Ereignis weiterhin ein Problem ist, das Sie möglicherweise beheben müssen.

Unified Manager überwacht die I/O-Latenz (Reaktionszeit) und IOPS (Vorgänge) für Volumes auf einem Cluster. Wenn beispielsweise andere Workloads eine Cluster-Komponente zu hoch nutzen, liegt der Konflikt bei der Komponente und kann nicht auf einer optimalen Ebene Performance erbringen, um die Workload-Anforderungen zu erfüllen. Die Performance anderer Workloads, die dieselbe Komponente verwenden, kann beeinträchtigt werden und die Latenz steigt. Wenn die Latenz den Performance-Schwellenwert überschreitet, löst Unified Manager ein Performance-Ereignis aus und sendet eine E-Mail-Benachrichtigung, um Sie zu benachrichtigen.

Ereignisanalyse

Unified Manager führt die folgenden Analysen anhand der Performance-Statistiken der letzten 15 Tage durch, um die Opfer-Workloads, problematische Workloads und die an einem Ereignis beteiligte Cluster-Komponente zu identifizieren:

- Identifiziert Opfer-Workloads, deren Latenz den Performance-Schwellenwert überschritten hat; dies ist die obere Grenze des erwarteten Bereichs:
  - Bei Volumes auf HDD oder Flash Pool (hybride) Aggregaten werden Ereignisse nur ausgelöst, wenn die Latenz mehr als 5 Millisekunden (ms) beträgt und die IOPS mehr als 10 Operationen pro Sekunde (OPs/s) sind.
  - Bei Volumes auf reinen SSD-Aggregaten oder FabricPool (Composite)-Aggregaten werden Ereignisse nur ausgelöst, wenn die Latenz größer als 1 ms ist und die IOPS mehr als 100 OPs/s beträgt
- Identifiziert Konflikte bei der Cluster-Komponente.

  Wenn die Latenz der Opfer-Workloads am Cluster Interconnect größer als 1 ms ist, behandelt Unified Manager dies als erheblich und löst ein Ereignis für den Cluster Interconnect aus.

- Ermittelt die problematischer Workloads, die die Cluster-Komponente überbeanspruchen und sie verursachen, dass sie unkonflikte aufweisen.
- Ordnen Sie die betroffenen Workloads auf Grundlage ihrer Umlenkungen in der Auslastung oder Aktivität einer Cluster-Komponente an, um zu ermitteln, welche „Verursacher“ die höchste Nutzungsänderung der Cluster-Komponente aufweisen und welche Opfer am meisten davon betroffen sind.

Ein Ereignis kann nur für einen kurzen Moment eintreten und sich dann selbst korrigieren, nachdem die verwendete Komponente keine Konflikte mehr hat. Ein kontinuierliches Ereignis: Eine erneute Auftreten für dieselbe Cluster-Komponente innerhalb eines Intervalls von fünf Minuten, bleibt im aktiven Status. Für kontinuierliche Ereignisse löst Unified Manager eine Warnmeldung aus, nachdem dasselbe Ereignis in zwei aufeinanderfolgenden Analyseintervallen erkannt wurde. Ereignisse, die ungelöst bleiben, die einen Status von neu haben, können unterschiedliche Beschreibungsmeldungen bei den an der Ereignisänderung beteiligten Workloads anzeigen.

Wenn ein Ereignis gelöst ist, bleibt es in Unified Manager als Teil der Aufzeichnung bisheriger Performance-Probleme für ein Volume verfügbar. Jedes Ereignis verfügt über eine eindeutige ID, mit der der Ereignistyp und die beteiligten Volumes, Cluster und Cluster-Komponenten identifiziert werden.

Ein einzelnes Volume kann gleichzeitig an mehreren Ereignissen beteiligt sein.

Ereignisstatus

Ereignisse können einen der folgenden Status haben:

- * Aktiv*

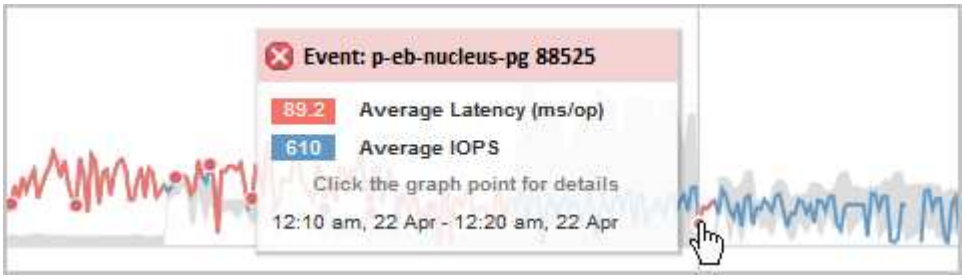
  Zeigt an, dass das Leistungsereignis aktuell aktiv ist (neu oder bestätigt). Das Problem, das das Ereignis verursacht hat, wurde nicht selbst behoben oder wurde nicht behoben. Der Performance-Zähler für das Storage-Objekt bleibt über dem Performance-Schwellenwert.

- **Veraltet**

  Zeigt an, dass das Ereignis nicht mehr aktiv ist. Das Problem, das das Ereignis verursacht hat, hat sich selbst korrigiert oder wurde behoben. Der Performance-Zähler für das Storage-Objekt liegt nicht mehr über dem Performance-Schwellenwert.

Ereignisbenachrichtigung

Die Ereignisalarme werden auf der Seite Dashboards/Übersicht, Dashboards/Leistung, Performance/Volume Details angezeigt und an angegebene E-Mail-Adressen gesendet. Sie können ausführliche Analyseinformationen zu einem Ereignis anzeigen und auf der Seite „Veranstaltungsdetails“ Vorschläge zu seiner Behebung erhalten.



In diesem Beispiel wird ein Ereignis durch einen roten Punkt (angezeigt) Auf der Latenzkarte auf der Seite Performance/Volume Details. Wenn Sie den Mauszeiger über den roten Punkt bewegen, wird ein Popup-Fenster mit weiteren Details zu dem Ereignis und Optionen zur Analyse angezeigt.

Interaktion mit Ereignissen

Auf der Seite Performance/Volume Details können Sie mit Ereignissen wie folgt interagieren:

- Wenn Sie den Mauszeiger über einen roten Punkt bewegen, wird eine Meldung angezeigt, die die Ereignis-ID zusammen mit der Latenz, der Anzahl der Operationen pro Sekunde und dem Datum und der Zeit, zu der das Ereignis erkannt wurde, anzeigt.

  Wenn für den gleichen Zeitraum mehrere Ereignisse vorliegen, wird in der Meldung die Anzahl der Ereignisse zusammen mit der durchschnittlichen Latenz und der durchschnittlichen Anzahl von Operationen pro Sekunde für das Volume angezeigt.

- Durch Klicken auf ein einzelnes Ereignis wird ein Dialogfeld angezeigt, das ausführlichere Informationen zu dem Ereignis enthält, einschließlich der involvierten Cluster-Komponenten, ähnlich dem Abschnitt „Zusammenfassung“ auf der Seite „Ereignisdetails“.

  Die Komponente in Konflikt ist eingekreist und rot hervorgehoben. Sie können entweder auf die Ereignis-ID oder **vollständige Analyse anzeigen** klicken, um die vollständige Analyse auf der Seite Ereignisdetails anzuzeigen. Wenn mehrere Ereignisse für den gleichen Zeitraum vorhanden sind, werden im Dialogfeld

Details zu den drei letzten Ereignissen angezeigt. Sie können auf eine Ereignis-ID klicken, um die Ereignisanalyse auf der Seite Ereignisdetails anzuzeigen. Wenn mehr als drei Ereignisse für den gleichen Zeitraum vorhanden sind, wird das Dialogfeld durch Klicken auf den roten Punkt nicht angezeigt.

Wie Unified Manager die Auswirkungen auf die Performance eines Ereignisses ermittelt

Unified Manager verwendet für einen Workload die Abweichung von Aktivität, Auslastung, Schreibdurchsatz, Auslastung der Clusterkomponente oder der I/O-Latenz (Reaktionszeit), um den Einfluss auf die Workload-Performance zu ermitteln. Anhand dieser Informationen wird festgelegt, welche Rolle der jeweilige Workload im Ereignis spielt und wie sie auf der Seite „Ereignisdetails“ aufgelistet werden.

Unified Manager vergleicht die zuletzt analysierten Werte für einen Workload mit dem erwarteten Wertebereich. Die Differenz zwischen den zuletzt analysierten Werten und dem erwarteten Wertebereich identifiziert die Workloads, deren Performance am stärksten von dem Ereignis beeinflusst wurde.

Nehmen Sie beispielsweise an, dass ein Cluster zwei Workloads enthält: Workload A und Workload B. Der erwartete Bereich für den Workload A beträgt 5-10 Millisekunden pro Operation (ms/op) und seine tatsächliche Latenz beträgt normalerweise etwa 7 ms/op Der erwartete Bereich für Workload B beträgt 10-20 ms/op, seine tatsächliche Latenz beträgt normalerweise etwa 15 ms/op Beide Workloads liegen deutlich innerhalb des erwarteten Latenzbereichs. Aufgrund von Konflikten im Cluster erhöht sich die Latenz beider Workloads auf 40 ms/op, indem der Performance-Schwellenwert überschritten wird. Dies ist die obere Grenze des erwarteten Bereichs und das Auslösen von Ereignissen. Die Latenzabweichung von den erwarteten Werten bis zu den Werten über dem Performance-Schwellenwert für Workload A liegt bei rund 33 ms/op, die Abweichung für Workload B liegt bei etwa 25 ms/op Die Latenz beider Workloads liegt bei 40 ms/op, doch bei Workload A hatten die größeren Auswirkungen auf die Performance, da die höhere Latenzabweichung bei 33 ms/op

Auf der Seite „Ereignisdetails“ im Abschnitt „Systemdiagnose“ können Sie Workloads nach deren Abweichung bei Aktivität, Auslastung oder Durchsatz für eine Cluster-Komponente sortieren. Sie können Workloads auch nach Latenz sortieren. Wenn Sie eine Sortieroption auswählen, analysiert Unified Manager die Abweichungen von Aktivität, Auslastung, Durchsatz oder Latenz, da das Ereignis anhand der erwarteten Werte erkannt wurde, um die Sortierreihenfolge des Workloads zu bestimmen. Für die Latenz die roten Punkte (🔴) Geben Sie einen Performance-Schwellenwert an, der durch einen Opfer-Workload und die daraus folgende Auswirkung auf die Latenz übergeht. Jeder rote Punkt weist ein höheres Maß an Latenzabweichungen auf. So können Sie die betroffenen Workloads identifizieren, deren Latenz sich am stärksten auf ein Ereignis auswirkt.

Cluster-Komponenten und warum sie über Konflikte verfügen können

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

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

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

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

- **Netzwerk**

  Zeigt die Wartezeit von I/O-Anfragen durch iSCSI-Protokolle oder Fibre Channel-Protokollen (FC) des Clusters an. Die Wartezeit liegt darin, auf die Transaktionen „iSCSI Ready to Transfer“ (R2T) oder „FCP Transfer Ready“ (XFER_RDY) zu warten, bis der Cluster auf eine I/O-Anforderung antworten kann. Wenn die Netzwerkkomponente unter einem Konflikt steht, bedeutet dies, dass hohe Wartezeiten auf der Protokollebene des Blocks die Latenz eines oder mehrerer Workloads beeinflussen.

- * Netzwerkverarbeitung*

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

- **QoS-Richtlinie**

  Steht für die Storage-Richtliniengruppe für Quality of Service (QoS), der Mitglied des Workloads ist Wenn die Richtliniengruppe Konflikte hat, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch das festgelegte Durchsatzlimit gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- * Cluster Interconnect*

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

- **Datenverarbeitung**

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

- **MetroCluster Ressourcen**

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

einer oder mehrerer Workloads auf dem lokalen Cluster. Wenn das Cluster nicht in einer MetroCluster-Konfiguration befindet, wird dieses Symbol nicht angezeigt.

- **Aggregate oder SSD Aggregate Ops**

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

- **Cloud-Latenz**

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

- **Sync SnapMirror**

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

Rollen von Workloads, die an einem Performance-Ereignis beteiligt sind

Unified Manager verwendet Rollen, um die Beteiligung eines Workloads bei einem Performance-Ereignis zu ermitteln. Zu den Rollen gehören Opfer, Bullies und Haie. Ein benutzerdefiniertes Workload kann gleichzeitig Opfer, Bully und Haifisch sein.

Rolle	Beschreibung
Opfer	Ein benutzerdefiniertes Workload, dessen Performance aufgrund anderer Workloads, sogenannte „Verursacher“, stark gesunken ist, die eine Cluster-Komponente überlasten. Es werden nur benutzerdefinierte Workloads als „Opfer“ identifiziert. Unified Manager ermittelt anhand der Latenzabweichung von Opfer-Workloads, bei der die tatsächliche Latenz während eines Ereignisses deutlich größer geworden ist als der erwartete Latenzbereich.

Rolle	Beschreibung
Bully	Ein benutzerdefiniertes oder systemdefiniertes Workload, dessen Überprovisionierung einer Cluster-Komponente die Performance anderer Workloads, genannt „Opfern“, abnimmt. Unified Manager identifiziert problematische Workloads basierend auf der abweichenden Nutzung einer Cluster-Komponente, wobei die tatsächliche Nutzung während eines Ereignisses deutlich größer ist als der erwartete Nutzungsumfang.
Hai	Einen benutzerdefinierten Workload mit der höchsten Auslastung einer Cluster-Komponente im Vergleich zu allen an einem Ereignis beteiligten Workloads. Unified Manager identifiziert Haifisch-Workloads auf der Grundlage ihrer Verwendung einer Clusterkomponente bei einem Ereignis.

Workloads auf einem Cluster können viele der Cluster-Komponenten gemeinsam nutzen, z. B. Storage-Aggregate und die CPU für Netzwerk und Datenverarbeitung. Wenn ein Workload, z. B. ein Volume, seine Nutzung einer Cluster-Komponente so erhöht, dass die Komponente die Workload-Anforderungen nicht effizient erfüllen kann, hat die Komponente Konflikte. Der Workload, der eine Cluster-Komponente übernutzt, ist ein problematischer Bestandteil. Die anderen Workloads, die diese Komponenten gemeinsam nutzen und deren Performance durch die Täter beeinträchtigt wird, sind Opfer. Aktivitäten systemdefinierter Workloads wie Deduplizierung oder Snapshot Kopien können sich auch in „`bullying`“ eskalieren.

Wenn Unified Manager ein Ereignis erkennt, werden alle betroffenen Workloads und Cluster-Komponenten identifiziert, einschließlich der problematische Workloads, die das Ereignis verursacht haben, der Clusterkomponente, die Konflikte verursacht hat, und der Opfer-Workloads, deren Performance aufgrund der gesteigerten Aktivitäten als Folge problematischer Workloads gesunken ist.

Wenn Unified Manager die problematische Workloads nicht identifizieren kann, werden nur bei den betroffenen Workloads und der betroffenen Cluster-Komponente ein Alarm ausgegeben.

Unified Manager erkennt Workloads, die Opfer problematischer Workloads sind, und ermittelt zudem, ob dieselben Workloads problematische Workloads werden. Ein Workload kann für sich selbst eine problematische sein. Ein so leistungsstarker Workload, der durch eine Richtliniengruppenbeschränkung gedrosselt wird, führt beispielsweise dazu, dass alle Workloads in der Richtliniengruppe gedrosselt werden – auch selbst. Ein Workload, der ein problematischer oder Opfer in einem laufenden Performance-Ereignis ist, kann seine Rolle ändern oder nicht mehr Teilnehmer des Ereignisses sein. Auf der Seite Performance/Volume Details in der Tabelle Ereignisliste wird das Datum und die Uhrzeit der Rollenänderung angezeigt, wenn das ausgewählte Volume seine Teilnehmerrolle ändert.

Analyse der Workload-Performance

Mit Unified Manager lässt sich die I/O-Performance von Volume-Workloads auf Clustern überwachen und analysieren. Sie können ermitteln, ob ein Performance-Problem im Cluster liegt und ob der Storage das Problem ist.

Dieses Kapitel beschreibt die Analyse der Workload-Performance mithilfe der Seite „Performance/Volume Details“ und der Seite „Ereignisdetails“.

Ermitteln, ob ein Workload ein Performance-Problem aufweist

Sie können mit Unified Manager feststellen, ob ein festgestellter Performance-Ereignis tatsächlich durch ein Performance-Problem auf dem Cluster verursacht wurde. Das Ereignis konnte beispielsweise zu einem Spitzenwert bei der Aktivität geführt haben, der die Reaktionszeit steigerte, aber jetzt ist die Reaktionszeit wieder auf das übliche Niveau zurückgekehrt.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den Namen des Volumes oder der zugehörigen LUN identifiziert haben, die Sie analysieren möchten.
- Unified Manager muss Performance-Statistiken vom Cluster mindestens fünf Tage gesammelt und analysiert haben.

Über diese Aufgabe

Wenn Sie die Seite „Ereignisdetails“ aufrufen, können Sie auf den Namenslink für ein Volume klicken, um direkt zur Seite „Performance/Volume Details“ zu gelangen.

Schritte

1. Geben Sie in der **Search**-Leiste mindestens die ersten drei Zeichen des Volume-Namens ein.

   Der Name des Volume wird in den Suchergebnissen angezeigt.

2. Klicken Sie auf den Namen des Volumes.

   Das Volume wird auf der Seite Performance/Volume Details angezeigt.

3. Klicken Sie im **Historic Data**-Diagramm auf **5d**, um die letzten fünf Tage historischer Daten anzuzeigen.
4. Lesen Sie das **Latenz**-Diagramm, um die folgenden Fragen zu beantworten:
   - Gibt es neue Performance-Ereignisse?
   - Gibt es historische Performance-Ereignisse, die darauf hindeuten, dass in der Vergangenheit Probleme mit dem Volume aufgetreten sind?
   - Gibt es Spitzen in der Reaktionszeit, auch wenn sich die Spitzen innerhalb des erwarteten Bereichs befinden?
   - Gab es Konfigurationsänderungen auf dem Cluster, die sich möglicherweise auf die Performance auswirken? Wenn bei der Antwortzeit des Volumes keine Performance-Ereignisse, Spitzenlasten oder kürzlich geänderte Konfigurationen angezeigt werden, die sich möglicherweise auf die Reaktionszeit auswirken, können Sie das durch das Cluster verursachte Performance-Problem ausschließen.

Untersuchung einer vermuteten langsamen Reaktionszeit für einen Workload

Sie können mit Unified Manager ermitteln, ob die Operationen im Cluster möglicherweise

zur langsamen Reaktionszeit (Latenz) für einen Volume-Workload beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den Namen des Volumes oder der zugehörigen LUN identifiziert haben, die Sie analysieren möchten.
- Unified Manager muss Performance-Statistiken vom Cluster mindestens fünf Tage gesammelt und analysiert haben.

Über diese Aufgabe

Wenn Sie die Seite „Ereignisdetails“ aufrufen, können Sie auf den Namen eines Volumes klicken, um direkt zur Seite „Performance/Volume Details“ zu gelangen.

Schritte

1. Geben Sie in der **Search**-Leiste den Namen des Volumens ein.

   Der Name des Volume wird in den Suchergebnissen angezeigt.

2. Klicken Sie auf den Namen des Volumes.

   Das Volume wird auf der Seite Performance/Volume Details angezeigt.

3. Klicken Sie auf der Historischen Datenkarte auf **5d**, um die letzten fünf Tage historischer Daten anzuzeigen.
4. Lesen Sie das **IOPS** Diagramm, um die folgenden Fragen zu beantworten:
   - Gibt es dramatische Spitzen in der Aktivität?
   - Gibt es dramatische Tropfen in der Aktivität?
   - Gibt es anormale Änderungen im Betriebsmuster? Wenn der Betrieb keine dramatischen Spitzen oder Aktivitätsspitzen anzeigt und während dieser Zeit keine Änderungen an der Cluster-Konfiguration vorgenommen wurden, kann der Storage-Administrator bestätigen, dass andere Workloads die Volume-Performance nicht beeinträchtigt haben.
5. Wählen Sie im Menü **break down Data by** unter **IOPS** die Option **reads/writes/other** aus.
6. Klicken Sie Auf **Absenden**.

   Das Diagramm Lese-/Schreibvorgänge/Sonstiges wird unter dem IOPS-Diagramm angezeigt.

7. Prüfen Sie das Diagramm * Lese-/Schreibvorgänge/anderes*, um dramatische Spitzen oder Abfälle in der Menge der Lese- oder Schreibvorgänge für das Volume zu identifizieren.

   Wenn keine drastischen Spitzen oder Abfälle bei Lese- oder Schreibvorgängen vorliegen, kann der Storage-Administrator bestätigen, dass die I/O-Vorgänge im Cluster normal ausgeführt werden. Möglicherweise liegen Leistungsprobleme im Netzwerk oder den verbundenen Clients vor.

Trends der I/O-Reaktionszeit bei Cluster-Komponenten erkennen

Mit Unified Manager können Sie die Performance-Trends für alle überwachten Clusterkomponenten für einen Volume Workload anzeigen. Im Laufe der Zeit können Sie

sehen, welche Komponenten die höchste Auslastung haben, ob Lese- oder Schreibanfragen die höchste Auslastung haben und wie sich die Auslastung auf die Reaktionszeit des Workloads ausgewirkt hat.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den Namen des Volumes oder der zugehörigen LUN, die Sie analysieren möchten, identifiziert haben.
- Um Performance-Statistiken von 30 Tagen anzuzeigen, muss Unified Manager mindestens 30 Tage Performance-Statistik aus dem Cluster gesammelt und analysiert haben.

Über diese Aufgabe

Anhand der Ermittlung der Performance-Trends für die Cluster-Komponenten kann der Administrator entscheiden, ob der Cluster überlastet oder nicht ausgelastet ist.

Wenn Sie die Seite „Ereignisdetails“ aufrufen, können Sie auf den Namen eines Volumes klicken, um direkt zur Seite „Performance/Volume Details“ zu gelangen.

Schritte

1. Geben Sie in der **Search**-Leiste den Namen des Volumens ein.

   Der Name des Volume wird in den Suchergebnissen angezeigt.

2. Klicken Sie auf den Namen des Volumes.

   Das Volume wird auf der Seite Performance/Volume Details angezeigt.

3. Klicken Sie auf dem Historischen Datendiagramm auf **30d**, um die letzten 30 Tage historischer Daten anzuzeigen.
4. Klicken Sie auf **Aufbrechen von Daten durch**.
5. Wählen Sie unter **Latenz Cluster-Komponenten** und **Lese-/Schreib-Latenz** aus.
6. Klicken Sie Auf **Absenden**.

   Beide Diagramme werden unter dem Latenzdiagramm angezeigt.

7. Sehen Sie sich das Diagramm * Cluster Components* an.

   Das Diagramm unterteilt die Gesamtantwortzeit nach Cluster-Komponente. Die Reaktionszeit im Aggregat ist die höchste.

8. Vergleichen Sie das Diagramm **Cluster Components** mit dem Diagramm **Latenz**.

   Das Latenzdiagramm zeigt Spitzen in der gesamten Reaktionszeit, die mit den Spitzen in der Reaktionszeit des Aggregats abgeglichen werden. Am Ende des 30-Tage-Zeitrahmens, in dem die Leistungsschwelle überschritten wurde, gibt es einige wenige.

9. Prüfen Sie das Diagramm * Lese-/Schreib-Latenz*.

   Das Diagramm zeigt eine höhere Reaktionszeit bei Schreibanfragen als Leseanforderungen, was darauf

hinweist, dass die Client-Anwendungen länger als gewöhnlich warten, um ihre Schreibanforderungen zu erfüllen.

10. Vergleichen Sie das Diagramm * Lese-/Schreib-Latenz* mit dem Diagramm * Latenz*.

    Die Spitzen bei der gesamten Antwortzeit, die auf das Aggregat im Diagramm „Cluster-Komponenten“ abgestimmt sind, werden auch auf die Schreibvorgänge im Latenzdiagramm für Lese-/Schreibvorgänge ausgerichtet. Der Administrator muss entscheiden, ob die Client-Applikationen, die den Workload verwenden, berücksichtigt werden müssen oder ob das Aggregat zu viel genutzt wird.

Analyse der Performance-Verbesserungen, die durch die Verschiebung eines Volumes erzielt wurden

Mit Unified Manager können Sie die Auswirkungen einer Verschiebung eines Volumes auf die Latenz (Reaktionszeit) anderer Volumes auf dem Cluster untersuchen. Durch die Verschiebung eines hochperformanten Volumes zu einem weniger ausgelasteten Aggregat oder eines Aggregats mit aktiviertem Flash-Storage kann das Volume effizienter ausgeführt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den Namen des Volumes oder der zugehörigen LUN identifiziert haben, die Sie analysieren möchten.
- Unified Manager muss sieben Tage Daten erfasst und analysiert haben.

Über diese Aufgabe

Unified Manager bestimmt, wann ein Volume zwischen Aggregaten verschoben wird. Es kann erkennen, wann die Volume-Verschiebung stattfindet, abgeschlossen ist oder fehlgeschlagen ist. Auf der Seite Performance/Volume Details wird für jeden Status der Volume-Verschiebung ein Änderungssymbol angezeigt. Anhand dieses Symbols können Sie feststellen, wann ein Verschiebevorgang stattgefunden hat, und Sie können feststellen, ob dieser zu einem Performance-Ereignis beigetragen hat.

Wenn Sie die Seite „Ereignisdetails“ aufrufen, können Sie auf den Namen eines Volumes klicken, um direkt zur Seite „Performance/Volume Details“ zu wechseln.

Schritte

1. Geben Sie in der **Search**-Leiste den Namen des Volumens ein.
2. Klicken Sie auf den Namen des Volumes.

   Das Volume wird auf der Seite Performance/Volume Details angezeigt.

3. Passen Sie im Diagramm * Historic Data* die Schieberegler an, um die Aktivität der letzten Arbeitswoche anzuzeigen.
4. Analysieren Sie das **Latenz**-Diagramm und das **IOPS**-Diagramm, um zu sehen, wie sich das Volumen in den letzten Tagen abspielte.

   Angenommen, Sie stellen fest, dass ein konsistentes Muster sehr hoher durchschnittlicher Antwortzeiten von über 42 Millisekunden pro Betrieb (ms/OP) mit Performance-Ereignissen jeden Tag der Woche fällt

und entscheiden, das Volume in ein weniger beschäftigtes Aggregat zu verschieben, um die Performance zu verbessern. Mit OnCommand System Manager kann das Volume zu einem Aggregat mit aktiviertem Flash Pool verschoben werden, um die Performance zu steigern. Etwa eine Stunde nach Abschluss der Volume-Verschiebung können Sie zu Unified Manager zurückkehren, um zu bestätigen, dass der Vorgang erfolgreich abgeschlossen wurde und sich die Latenz verbessert hat.

5. Wenn die Seite **Performance/Volume Details** nicht angezeigt wird, suchen Sie nach dem gewünschten Volume.
6. Klicken Sie im **Historic Data**-Diagramm auf **1d**, um die Aktivität vom letzten Tag, einige Stunden seit der Volumenbewegung, anzuzeigen.

   Im unteren Bereich der Seite in der Zeile Ereignisse Zeit wird ein Symbol für das Ereignis ändern ( ) Wird angezeigt, um die Zeit anzugeben, die der Vorgang der Volumenbewegung abgeschlossen wurde. Eine schwarze, vertikale Linie wird auch vom Änderungssymbol in das Latenzdiagramm angezeigt.

7. Zeigen Sie mit dem Cursor auf das Symbol Ereignis ändern, um Details zum Ereignis in der **Ereignisliste** anzuzeigen.

   Da das Volume zu einem Aggregat mit aktiviertem Flash Pool verschoben wurde, sehen Sie die Änderung bei Lese- und Schreib-I/O in den Cache.

8. Wählen Sie im Menü * Data by* unter **Mbps** die Option **Cache HIT Ratio** aus.

   Das Diagramm „Cache-Trefferverhältnis“ zeigt Statistiken zu den Lese- und Schreibvorgängen im Cache an.

   Das Volume wurde erfolgreich in ein Aggregat mit weniger Auslastung verschoben und das Änderungsereignis wird in der Ereignisliste rechts hervorgehoben. Die durchschnittliche Latenz sank deutlich von über 42 ms/op auf rund 24 ms/op Die derzeitige Latenz beträgt ca. 1.5 ms/op Im Cache-Trefferverhältnis-Diagramm liegt die Menge der erfolgreichen Lese- und Schreibvorgänge in den Cache jetzt bei 100 %, da sich das Volume jetzt auf einem Aggregat mit aktiviertem Flash Pool befindet.

So verschieben Sie ein FlexVol Volume

Wenn Sie wissen, wie das Verschieben eines FlexVol Volumes funktioniert, können Sie feststellen, ob die Verschiebung eines Volumes Service Level Agreements erfüllt und ermitteln, wo sich die Volume-Verschiebung befindet.

FlexVol Volumes werden von einem Aggregat oder Node zu einem anderen innerhalb derselben Storage Virtual Machine (SVM) verschoben. Durch eine Volume-Verschiebung wird der Client-Zugriff während der Verschiebung nicht unterbrochen.

Verschieben eines Volumes erfolgt in mehreren Phasen:

- Ein neues Volume wird auf dem Zielaggregat erstellt.
- Die Daten aus dem ursprünglichen Volume werden auf das neue Volume kopiert.

  Während dieser Zeit ist das ursprüngliche Volume intakt und für Clients verfügbar.

- Am Ende des Verschiebevorgangs wird der Client-Zugriff vorübergehend gesperrt.

  Während dieser Zeit führt das System eine endgültige Replikation vom Quell-Volume zum Ziel-Volume durch, tauscht die Identitäten der Quell- und Ziel-Volumes aus und ändert das Ziel-Volume in das Quell-

Volume.

- Nach Abschluss der Verschiebung wird der Client-Datenverkehr zum neuen Quell-Volume weitergeleitet und der Client-Zugriff wird fortgesetzt.

Die Verschiebung wird für den Client-Zugriff nicht unterbrochen, da die Zeit, in der der Client-Zugriff gesperrt ist, bevor Clients eine Unterbrechung oder eine Unterbrechung bemerken. Der Client-Zugriff ist standardmäßig für 35 Sekunden gesperrt. Falls der Vorgang zur Verschiebung des Volumes nicht zum Zeitpunkt des Abzugriffs abgeschlossen werden kann, bricht das System diese letzte Phase der Verschiebung des Volumes ab und erlaubt den Client-Zugriff. Das System versucht standardmäßig dreimal die letzte Phase. Nach dem dritten Versuch wartet das System eine Stunde, bevor es erneut versucht wird, die letzte Phasenfolge zu versuchen. Das System führt die letzte Phase der Verschiebung des Volumes aus, bis die Volume-Verschiebung abgeschlossen ist.

Seite Performance/Volume Details

Diese Seite enthält detaillierte Performance-Statistiken für alle I/O-Aktivitäten und Vorgänge für das ausgewählte FlexVol Volume, das FlexGroup Volume oder den FlexGroup-Komponenten-Workload. Sie können einen bestimmten Zeitrahmen auswählen, in dem die Statistiken und Ereignisse für das Volume angezeigt werden sollen. Die Ereignisse identifizieren Performance-Ereignisse und Änderungen, die sich auf die I/O-Performance auswirken können.

Historisches Diagramm

Zeigt die historischen Leistungsanalyse-Daten für das ausgewählte Volume an. Sie können auf die Schieberegler klicken und ziehen, um einen Zeitrahmen festzulegen. Die Schieberegler erhöhen und reduzieren das Zeitfenster. Die Daten außerhalb des Zeitrahmenfensters sind ausgegraut. Mit dem Schieberegler unten im Diagramm können Sie das Zeitfenster über die historischen Daten verschieben. Die gesamte Seite, einschließlich der angezeigten Diagramme und Ereignisse, gibt die Daten wieder, die im Zeitfenster verfügbar sind. Unified Manager speichert auf dieser Seite maximal 30 Tage historische Daten.

Wenn Sie auf dem historischen Datendiagramm je nach Bildschirmauflösung einen Zeitrahmen von mehr als einem Tag auswählen, werden in den Diagrammen die maximalen Werte für Reaktionszeit und IOPS über die Anzahl der Tage hinweg angezeigt.

Optionen

- **Zeitauswahl**

  Gibt den Zeitbereich an, über den die Volume-Performance-Statistiken für die gesamte Seite angezeigt werden sollen. Sie können 1 Tag (**1d**) bis 30 Tage (**30d**) anklicken oder auf **Benutzerdefiniert** klicken, um einen benutzerdefinierten Bereich auszuwählen. Für einen benutzerdefinierten Bereich können Sie ein Anfang- und Enddatum auswählen und dann auf **Aktualisieren** klicken, um die gesamte Seite zu aktualisieren.

  Wenn Sie auf der Seite Ereignisdetails auf die Seite Performance/Volume Details zugreifen, indem Sie auf den Namenslink eines Volumes klicken, wird standardmäßig automatisch ein Zeitbereich, z. B. 1 Tag oder 5 Tage vor dem aktuellen Tag, ausgewählt. Wenn Sie den Schieberegler im historischen Datendiagramm verschieben, ändert sich der Zeitbereich in einen benutzerdefinierten Bereich, aber die Auswahl **Benutzerdefiniert** Zeit ist nicht ausgewählt. Die Standardzeitauswahl bleibt ausgewählt.

- **Brechen Sie die Daten nach** auf

  Enthält eine Liste von Diagrammen, die Sie zur Seite „Performance/Volume-Details“ hinzufügen können, um detailliertere Performance-Statistiken für das ausgewählte Volume anzuzeigen.

In den Aufschlüsselung der Daten werden Performance-Statistiken angezeigt

Sie können die Diagramme verwenden, um Performance-Trends für ein Volume anzuzeigen. Sie können auch Statistiken für Lese- und Schreibvorgänge, Netzwerkprotokollaktivitäten, die Auswirkungen einer QoS-Richtliniengruppendrosselung auf Latenz, das Verhältnis von Lese- und Schreibzugriffen auf Cache Storage, die von einem Workload verwendete Cluster-CPU-Gesamtzeit und bestimmte Cluster-Komponenten anzeigen.

Diese Ansichten zeigen Statistiken von maximal 30 Tagen vom aktuellen Tag an. Wenn Sie im historischen Datendiagramm je nach Bildschirmauflösung einen Zeitrahmen von mehr als einem Tag auswählen, werden in den Diagrammen die maximalen Werte für Latenz und IOPS über die Anzahl der Tage hinweg angezeigt.

Sie können das Kontrollkästchen * Alle auswählen* verwenden, um alle aufgeführten Diagrammoptionen auszuwählen oder zu deaktivieren.

- **Latenz**

  In den folgenden Diagrammen werden Informationen zur Latenz oder Reaktionszeit für den ausgewählten Workload detailliert aufgeführt:

  - **Clusterkomponenten**

    Zeigt ein Diagramm der Zeit an, die für jede Cluster-Komponente verwendet wurde, die vom ausgewählten Volume verwendet wurde.

    Das Diagramm hilft Ihnen, die Auswirkung auf die Latenz für jede Komponente in Verbindung mit der gesamten Latenz zu bestimmen. Sie können das Kontrollkästchen neben jeder Komponente verwenden, um das Diagramm anzuzeigen und auszublenden.

    Bei QoS-Richtliniengruppen werden Daten nur für benutzerdefinierte Richtliniengruppen angezeigt. Nullen werden für systemdefinierte Richtliniengruppen angezeigt, z. B. für Standardrichtliniengruppen.

  - **Lese-/Schreib-Latenz**

    Zeigt ein Diagramm der Latenzen der erfolgreichen Lese- und Schreibanforderungen vom ausgewählten Volume-Workload im ausgewählten Zeitrahmen an.

    Schreibanforderungen sind eine orangefarbene Zeile und Leseanforderungen sind eine blaue Zeile. Die Anforderungen sind spezifisch hinsichtlich der Latenz für den ausgewählten Volume-Workload und nicht für alle Workloads im Cluster.

    Die Lese- und Schreib-Statistiken ergeben möglicherweise nicht immer die im Latenzdiagramm angezeigten Statistiken zur gesamten Latenz. Das erwartete Verhalten hängt davon ab, wie Unified Manager Statistiken zu Lese- und Schreibvorgängen für einen Workload sammelt und analysiert.

◦ **Policy Group Impact**

Zeigt ein Diagramm des prozentualen Anteils der Latenz für den ausgewählten Volume-Workload an, der durch das Durchsatzlimit seiner QoS-Richtliniengruppe beeinträchtigt wird.

Wenn der Workload gedrosselt wird, zeigt der Prozentsatz an, wie sehr die Drosselung zu einem bestimmten Zeitpunkt zur Latenz beigetragen hat. Die Prozentwerte geben die Drosselung an:

- 0% = keine Drosselung
- > 0% = Drosselung
- > 20% = kritische Drosselung Wenn der Cluster mehr Arbeit erledigen kann, können Sie die Drosselung durch Erhöhung des Richtliniengruppenlimits verringern. Eine andere Option ist es, den Workload in ein weniger stark ausgelasteten Aggregat zu verschieben.

> Das Diagramm wird nur für Workloads in einer benutzerdefinierten QoS-Richtliniengruppe mit einem festgelegten Durchsatzlimit angezeigt. Sie wird nicht angezeigt, ob sich die Workloads in einer von dem System definierten Richtliniengruppe befinden, z. B. in der Standardrichtliniengruppe, oder in einer Richtliniengruppe, die kein QoS-Limit hat. Bei einer QoS-Richtliniengruppe können Sie den Mauszeiger auf den Namen der Richtliniengruppe zeigen, um ihr Durchsatzlimit und das letzte Mal anzuzeigen. Wenn die Richtliniengruppe geändert wurde, bevor das zugehörige Cluster zu Unified Manager hinzugefügt wurde, handelt es sich bei der letzten geänderten Zeit um das Datum und die Uhrzeit, zu der Unified Manager das Cluster zum ersten Mal entdeckte.

- **IOPS**

Die folgenden Diagramme zeigen die IOPS-Daten für den ausgewählten Workload an:

◦ **Lesen/Schreiben/Sonstiges**

Zeigt ein Diagramm an, das die Anzahl der Lese- und Schreib-IOPS und anderer IOPS pro Sekunde im ausgewählten Zeitrahmen anzeigt.

Andere IOPS sind Protokollaktivitäten, die vom Client initiiert werden und keine Lese- oder Schreibvorgänge sind. In einer NFS-Umgebung könnten dies beispielsweise Metadatenvorgänge wie getattr, setattr oder fsstat sein. In einer CIFS-Umgebung könnte es sich um Attributsuchen, Verzeichnislisten oder Virenschutzprüfungen handeln. Schreib-IOPS sind eine orangefarbene Linie und Leseanforderungen sind eine blaue Linie. Die Anforderungen sind spezifisch für alle Vorgänge des ausgewählten Volume-Workloads und nicht für alle Vorgänge im Cluster.

- **Mbps**

Die folgenden Diagramme zeigen die Durchsatzdaten für den ausgewählten Workload an:

◦ **Cache Trefferquote**

Zeigt ein Diagramm des prozentualen Anteils der Leseanforderungen von Client-Applikationen an, die über den Cache im ausgewählten Zeitrahmen zufrieden sind.

Der Cache könnte sich auf Flash Cache-Karten oder Solid State-Laufwerken (SSDs) in Flash Pool Aggregaten befinden. Ein Cache-Treffer in Blau ist ein aus dem Cache gelesener Treffer. Ein Cache-Treffer in orange ist ein Lesevorgang von einer Festplatte im Aggregat. Die Anforderungen sind spezifisch für den ausgewählten Volume-Workload, nicht jedoch für alle Workloads im Cluster.

Ausführlichere Informationen zur Volume-Cache-Nutzung können Sie auf den Integritätsseiten von Unified Manager und in OnCommand System Manager anzeigen.

- **Komponenten**

  Die folgenden Diagramme zeigen die Daten nach Clusterkomponenten, die vom ausgewählten Workload verwendet werden:

  - **Cluster CPU-Zeit**

    Zeigt ein Diagramm der CPU-Nutzungszeit in ms für alle Nodes im Cluster an, die vom ausgewählten Workload verwendet werden.

    Das Diagramm zeigt die kombinierte CPU-Nutzungszeit für die Netzwerkverarbeitung und Datenverarbeitung an. Auch die CPU-Zeit für systemdefinierte Workloads, die dem ausgewählten Workload zugewiesen sind und dieselben Nodes für die Datenverarbeitung nutzen, ist inbegriffen. Anhand der Tabelle können Sie ermitteln, ob der Workload ein hoher Verbrauch der CPU-Ressourcen auf dem Cluster darstellt. Mithilfe des Diagramms können Sie auch zusammen mit dem Latenzdiagramm für Lese-/Schreibvorgänge unter dem Latenzdiagramm oder dem Diagramm „Lese-/Schreibvorgänge/anderes“ unter dem IOPS-Diagramm festlegen, wie Änderungen an der Workload-Aktivität im Laufe der Zeit die Cluster-CPU-Auslastung beeinträchtigen.

  - * Datenträgernutzung*

    Zeigt ein Diagramm an, das den Prozentsatz der Auslastung auf den Datenfestplatten im Storage-Aggregat im ausgewählten Zeitrahmen anzeigt.

  Die Auslastung schließt nur Lese- und Schreibanfragen der Festplatte aus dem ausgewählten Volume-Workload ein. Lesezugriffe aus dem Cache sind nicht enthalten. Die Auslastung ist spezifisch für den ausgewählten Volume Workload, nicht für alle Workloads auf den Festplatten. Wenn ein überwachtes Volume an einer Volume-Verschiebung beteiligt ist, beziehen sich die Auslastungswerte in diesem Diagramm auf das Zielaggregat, zu dem das Volume verschoben wurde.

Darstellung der Performance-Daten

Unified Manager verwendet Diagramme oder Diagramme, um Ihnen Volume-Performance-Statistiken und Ereignisse über einen bestimmten Zeitraum anzuzeigen.

Mithilfe der Diagramme können Sie den Zeitbereich anpassen, für den Daten angezeigt werden sollen. Die Daten werden mit dem Zeitrahmen auf der horizontalen Achse des Diagramms und den Zählern auf der vertikalen Achse angezeigt, wobei Punktintervalle entlang der Diagrammlinien angezeigt werden. Die vertikale Achse ist dynamisch; die Werte passen sich an die Spitzen der erwarteten oder tatsächlichen Werte an.

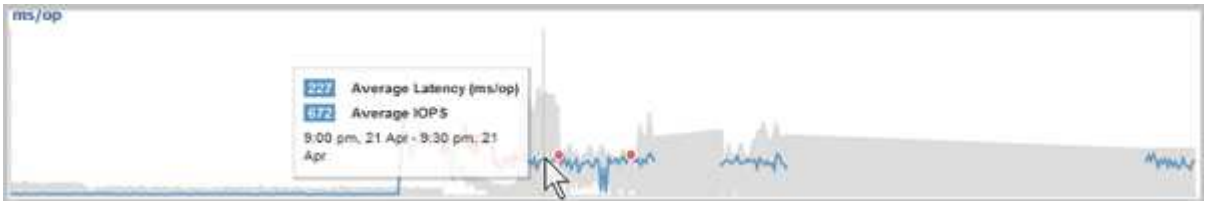
Auswählen von Zeitrahmens

Auf der Seite Performance/Volume Details können Sie im Historic Data Chart einen Zeitrahmen für alle Diagramme auf der Seite auswählen. Die schaltflächen 1d, 5d, 10d und 30d geben 1 Tag bis 30 Tage (1 Monat) an und mit der Schaltfläche **Benutzerdefiniert** können Sie einen benutzerdefinierten Zeitbereich innerhalb dieser 30 Tage festlegen. Jeder Punkt in einem Diagramm entspricht einem Erfassungsintervall von 5 Minuten, und es werden maximal 30 Tage historische Performance-Daten aufbewahrt. Beachten Sie, dass Intervalle auch Netzwerkverzögerungen und andere Anomalien berücksichtigen.

In diesem Beispiel hat das Historic Data Chart einen Zeitrahmen auf den Anfang und das Ende des Monats März eingestellt. Im ausgewählten Zeitrahmen sind alle historischen Daten vor März ausgegraut.

Anzeigen von Datenpunktinformationen

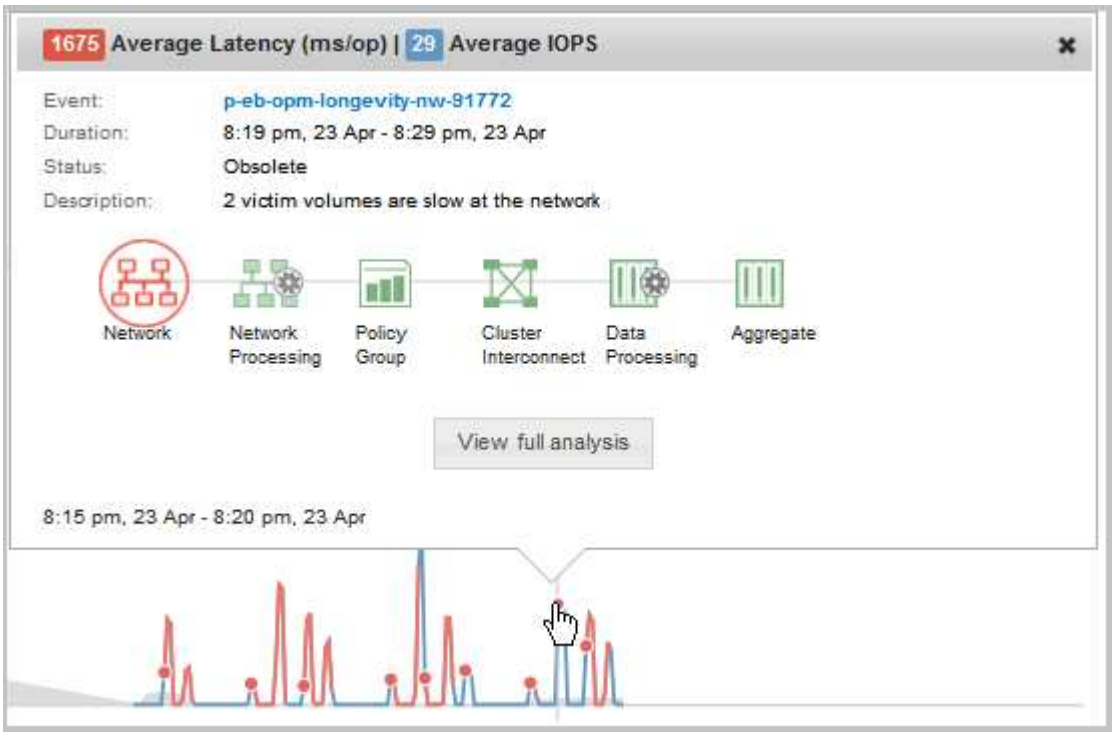
Um die Informationen zu Datenpunkten in einem Diagramm anzuzeigen, können Sie den Cursor über einen bestimmten Punkt im Diagramm positionieren, und ein Popup-Feld zeigt die Werte-, Datums- und Zeitinformationen an.



Wenn Sie in diesem Beispiel den Mauszeiger über das IOPS-Diagramm auf der Seite „Performance/Volume Details“ positionieren, werden die Reaktionszeiten und die Werte der Vorgänge zwischen 3:50 Uhr angezeigt Und 3:55 Uhr Am 20. Oktober.

Anzeigen von Performance-Ereignisinformationen

Um Event-Informationen auf einem Diagramm anzuzeigen, können Sie den Mauszeiger über ein Event-Symbol positionieren, um zusammenfassende Informationen in einem Popup-Feld anzuzeigen. Alternativ können Sie auf das Event-Symbol klicken, um ausführlichere Informationen zu erhalten.



In diesem Beispiel werden auf der Seite Performance/Volume-Details durch Klicken auf ein Ereignissymbol im Latenzdiagramm detaillierte Informationen zum Ereignis in einem Popup-Feld angezeigt. Das Ereignis wird auch in der Ereignisliste hervorgehoben.

Verwalten von Berichten

Mit OnCommand Unified Manager lassen sich Berichte erstellen und managen, sodass Kunden benutzerdefinierte Informationen über Kapazität, Auslastung und Performance von Storage-Objekten und Ereignissen für Storage-Objekte anzeigen können.

Die Implementierung der Planung und Erstellung von Berichten aus der Option Berichte im linken Navigationsbereich wird in einer zukünftigen Version abgelehnt. Mit den folgenden zusätzlichen Methoden können Sie Gesundheits- und Performance-Daten aus Unified Manager extrahieren:

- Daten direkt aus den Grid-Seiten in der GUI extrahieren
- Verwenden der Open Database für den Zugriff auf alle verfügbaren Objekte
- Ausführung von Unified Manager REST-APIs zur Rückgabe der Informationen, für die Sie interessiert sind, zu überprüfen

Planen von Berichten

Sie können Ihre Berichte auf der Seite Berichtsdetails planen und die geplanten Berichte an einen oder mehrere Empfänger in einem bestimmten Format zu einer bestimmten Häufigkeit senden. Sie können beispielsweise einen Bericht als E-Mail im PDF-Format jeden Montag planen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte** und dann auf **Bericht ausführen** für den gewünschten Bericht.

   Die Seite Berichtdetails wird angezeigt.

2. Klicken Sie Auf **Aktionen** > **Bericht Planen**.
3. Wählen Sie im Dialogfeld **Bericht planen** einen der bevorzugten Zeitpläne für Ihren Bericht aus:

Ihr Ziel ist	Dann…
Wählen Sie einen Zeitplan aus der bestehenden Liste von Zeitplänen aus	Klicken Sie auf **vorhandenen Zeitplan verwenden** und wählen Sie den Zeitplan aus.

Ihr Ziel ist	Dann…
Erstellen Sie einen neuen Zeitplan	Klicken Sie auf **Neuen Zeitplan erstellen**, geben Sie dann den Terminplannamen ein, geben Sie die E-Mail-Adresse an, wählen Sie das Berichtsformat und die Berichtsfrequenz aus, und geben Sie eine Zeit oder einen Tag ein, die der Bericht ausführen soll. Sie können eine oder mehrere E-Mail-Adressen angeben, die durch Kommas getrennt sind. Die Option *PDF* ist als Standardreport-Format ausgewählt. Als Standardfrequenz wird die Option *hourly* ausgewählt.

4. Klicken Sie Auf **Zeitplan**.

Gemeinsame Nutzung von Berichten

Sie können Ihre Berichte per E-Mail versenden und mit einem oder mehreren Benutzern teilen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte** und dann auf **Bericht ausführen** für den gewünschten Bericht.

   Die Seite Berichtdetails wird angezeigt.

2. Klicken Sie Auf **Aktionen** > **Teilen**.
3. Geben Sie im Dialogfeld **Bericht teilen** die E-Mail-Adresse des Empfängers an, mit dem Sie den Bericht teilen möchten.

   Sie können eine oder mehrere E-Mail-Adressen angeben, die durch Kommas getrennt sind.

4. Geben Sie den Betreff der E-Mail an.

   Standardmäßig wird der Name des Berichts als Betreff der E-Mail angezeigt.

5. Wählen Sie das Berichtsformat aus.

   Die Option *PDF* ist als Standardreport-Format ausgewählt. Wenn das XHTML-Format ausgewählt ist, muss der Empfänger den Bericht öffnen, der per E-Mail über einen unterstützten Webbrowser gesendet wird.

6. Klicken Sie Auf **Teilen**.

Verwalten von Berichtzeitplänen

Sie können Ihre Berichtspläne im Dialogfeld Berichtszeitpläne verwalten verwalten verwalten verwalten verwalten. Sie können einen neuen Zeitplan hinzufügen und vorhandene Zeitpläne anzeigen, ändern oder löschen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte** und dann auf **Berichtszeitpläne verwalten**.
2. Im Dialogfeld **Berichtszeitpläne verwalten**

Ihr Ziel ist	Dann…
Vorhandenen Zeitplan anzeigen oder ändern	a. Wählen Sie den Zeitplan aus der Liste im linken Fensterbereich aus. Die Zeitplandetails werden angezeigt. b. Nehmen Sie die erforderlichen Änderungen vor. c. Klicken Sie auf **Speichern** oder **Speichern und Schließen**.
Einen vorhandenen Zeitplan löschen	a. Wählen Sie den Zeitplan aus der Liste im linken Fensterbereich aus. Die Zeitplandetails werden angezeigt. b. Klicken Sie Auf **Zeitplan Löschen**.
Fügen Sie einen neuen Zeitplan hinzu	a. Klicken Sie Auf **Zeitplan Hinzufügen**. b. Im rechten Fensterbereich wird ein neues Planungsformular angezeigt. c. Geben Sie den Terminnamen, die E-Mail-Adresse des Empfängers, das Berichtsformat und die Häufigkeit ein, und wählen Sie die Berichte aus, die Sie planen möchten. d. Klicken Sie Auf **Speichern**. Der neue Zeitplan wird in die Liste „Zeitpläne“ eingefügt.

Anpassen eines Berichts

Sie können Berichte auf der Seite Berichtsdetails anpassen und den benutzerdefinierten Bericht mit einem anderen Namen speichern.

Über diese Aufgabe

Nachdem Sie einen benutzerdefinierten Bericht gespeichert haben, können Sie keinen der Filter ändern, die Sie zum Erstellen des Berichts angewendet haben, da der Bericht als „`New`“ gilt. Stellen Sie also sicher, dass Sie mit allen Änderungen zufrieden sind, bevor Sie den Bericht speichern. Sie können jedoch neue Filter auf den Bericht anwenden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte** und dann auf **Bericht ausführen** für den Bericht, den Sie anpassen möchten.

Die Seite Berichtdetails wird angezeigt.

2. Passen Sie den Bericht nach Bedarf an, und klicken Sie dann auf **Aktionen** > **Customized Report speichern unter**.
3. Geben Sie im Dialogfeld **Customized Report as** speichern einen Namen für den angepassten Bericht und eine kurze Beschreibung der Anpassung ein, damit andere verstehen, was der Bericht anzeigt.

   Standardmäßig wird der aktuelle Berichtname angezeigt.

4. Klicken Sie Auf **Speichern**.

   Wenn Sie die Fehlermeldung „`konnte den benutzerdefinierten Bericht nicht speichern. Die gewünschte Datei wurde nicht`" erstellt, warten einige Momente und klicken dann erneut auf **Speichern**. Dieses Problem tritt auf, wenn die Verbindung zwischen dem Webbrowser und dem Unified Manager-Server langsam ist.

Ergebnisse

Der benutzerdefinierte Bericht wird gespeichert und in seiner jeweiligen Berichtskategorie auf der Seite Berichtdetails angezeigt.

Bearbeiten eines benutzerdefinierten Berichts

Sie können weitere Änderungen an einem bereits angepassten Bericht vornehmen und den Bericht speichern. Sie können den Namen des Berichts nicht ändern, nachdem Sie ihn gespeichert haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte** und dann auf **Bericht ausführen** für den Bericht, den Sie bearbeiten möchten.

   Die Seite Berichtdetails wird angezeigt.

2. Ändern Sie den Bericht nach Bedarf, und klicken Sie dann auf **Aktionen** > **Benutzerdefinierter Bericht speichern**.
3. Geben Sie im Dialogfeld **Benutzerdefinierter Bericht speichern** eine kurze Beschreibung der Änderungen im benutzerdefinierten Bericht ein und klicken Sie auf **Speichern**.

Berichte werden importiert

Wenn Sie einen Bericht außerhalb von Unified Manager erstellt haben, können Sie die Berichtsdatei importieren und speichern, die mit Unified Manager verwendet werden soll.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Sie müssen sicherstellen, dass der zu importierende Bericht von Unified Manager unterstützt wird.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte** und dann auf **Bericht importieren**.
2. Klicken Sie im Dialogfeld **Bericht importieren** auf **Durchsuchen** und wählen Sie die Datei aus, die Sie importieren möchten, und geben Sie dann einen Namen und eine kurze Beschreibung des Berichts ein.
3. Klicken Sie Auf **Import**.

   Wenn Sie den Bericht nicht importieren können, können Sie die Protokolldatei überprüfen, um den Fehler zu finden, der das Problem verursacht.

Weitere Informationen zu Berichten

Sie können die Option zum Ausführen, Löschen, Exportieren und Importieren von Berichten verwenden. Sie können auch benutzerdefinierte Berichte erstellen und den benutzerdefinierten Bericht speichern. Sie können weitere Vorgänge wie Filtern, Sortieren, Gruppieren und Formatieren ausführen.

Was Berichte tun

In Berichten werden detaillierte Informationen zu Storage-Objekten angezeigt, mit denen Sie potenzielle Probleme prüfen und identifizieren können.

Sie können Berichte speichern, löschen, freigeben, planen und importieren. Sie können auch nach bestimmten Berichten suchen. Sie können Berichte an bestimmte Anwendungsfälle anpassen und den individuell angepassten Bericht für zukünftige Zwecke speichern. Sie können weitere Vorgänge wie Filtern, Sortieren, Gruppieren und Formatieren ausführen.

Standardmäßig wird jede Berichtsgruppe nach Berichtstyp und -Beschreibung angezeigt. Sie können Berichte ausführen, um eine bestimmte Berichtsgruppe anzuzeigen.

Nachdem Sie einen Bericht erstellt haben, können Sie ihn weiter anpassen und den angepassten Bericht speichern. Sie können die benutzerdefinierten Berichte anzeigen, die auf der Seite Berichte unter der spezifischen Berichtskategorie gespeichert werden.

Sie können Berichte so planen, dass sie gesendet werden, oder Berichte in einem der unterstützten Formate teilen: PDF, XHTML, CSV, XLS oder Text.

Sie können Berichte in verschiedenen Formaten exportieren und auf Ihrem Desktop speichern. Sie können einzelne Spaltendaten aus den generierten Berichten exportieren.

Sie können Berichtsdesign-Dateien importieren (`.rptdesign` Dateien), und speichern Sie die importierten Berichte auf der Seite Berichte. Sie können benutzerdefinierte und importierte Berichte löschen.

Sie können die folgenden Berichte importieren:

- Berichte mit mehreren Kopfzeilen, für die ein Spaltbereich auf einen gesetzt ist
- Berichte nur mit Diagrammen
- Berichte nur mit Listen und Raster

Berichte im Text-, CSV- und Excel-Format werden in den folgenden Szenarien unterstützt:

- Tabellenelement nur in `.rptdesign` Datei
- Eine Tabelle mit nur einer Kopfzeile als Zeile

Sie können Berichte, die über einen Spaltbereich von mehr als einem verfügen, nicht importieren. Wenn ein Bericht im Text-, CSV- oder Excel-Format mehr als eine Kopfzeile enthält, wird nur die erste Kopfzeile berücksichtigt und die verbleibenden Zeilen werden ignoriert.

Auf Unified Manager-Datenbanken kann für individuelle Berichte zugegriffen werden

Unified Manager verwendet eine MySQL Datenbank, um Daten von den überwachten Clustern zu speichern. Die Daten werden in verschiedenen Schemata in der MySQL-Datenbank gespeichert.

Ab Unified Manager 7.3 werden weitere Schemata bereitgestellt, die den Zugriff auf zusätzliche Tabellendaten ermöglichen.

Alle Tabellendaten aus den folgenden Datenbanken sind verfügbar:

Datenbank	Beschreibung
netapp_Modell_Ansicht	Daten zu den Objekten auf ONTAP Controllern.
netapp_Performance	Cluster-spezifische Performance-Zähler.
Okum	Daten und Informationen zu Unified Manager Applikationen unterstützen das Filtern, Sortieren und Berechnen einiger abgeleiteter Felder.
Ocum_Report	Daten für die Bestandskonfiguration und Informationen zur Kapazität.
Ocum_Report_birt	Wie oben beschrieben, aber diese Datenbank wird von integrierten BIRT-Berichten belegt.
opm	Einstellungen für Performance-Konfiguration und Schwellenwertinformationen.
Skalemonitor	Daten zu Zustand- und Performance-Problemen der Unified Manager Applikation

Ein Berichtbenutzer – ein Datenbankbenutzer mit der Rolle „Berichtschema“ – kann auf die Daten in diesen Tabellen zugreifen. Dieser Benutzer hat schreibgeschützten Zugriff auf Reporting- und andere Datenbankansichten direkt aus der Unified Manager-Datenbank. Beachten Sie, dass dieser Benutzer nicht berechtigt ist, auf Tabellen zuzugreifen, die Benutzerdaten oder Cluster-Anmeldeinformationen enthalten.

Siehe "Technischer Bericht zu Unified Manager Reporting" (TR-4565).

Die Berichtsplanung ist

Sie können einen Bericht für ein bestimmtes Datum und eine bestimmte Uhrzeit mithilfe

der Option **Zeitplan** erstellen. Der Bericht wird automatisch per E-Mail an einen oder mehrere Empfänger gemäß dem Zeitplan gesendet.

Wenn Sie einen Bericht planen, können Sie den Aufwand für die manuelle Erstellung und das manuelle Senden von Berichten minimieren. Sie können sicherstellen, dass der aktuelle Status des Speichers in festgelegten Intervallen von den Administratoren überwacht wird, die nicht anderweitig von Unified Manager benachrichtigt werden.

Die Weitergabe von Berichten ist wichtig

Sie können einen Bericht über E-Mail mit der Option **Teilen** an einen oder mehrere Benutzer weitergeben.

Sie müssen den Bericht vor der Freigabe speichern, um sicherzustellen, dass die letzten Änderungen, die Sie an dem Bericht vorgenommen haben, angezeigt werden.

Sie können den Bericht in jedem gewünschten Format freigeben. Mit der Option **Share** können Sie Berichte sofort per E-Mail teilen, auch mit Personen, die keinen Zugang zu Unified Manager haben, aber über eine gültige E-Mail-Adresse verfügen.

Der Import des Berichts ist

Sie können einen Bericht mit der Option **Bericht importieren** aus Unified Manager importieren und den importierten Bericht mit einem Namen und einer kurzen Beschreibung speichern. Durch das Importieren von Berichten können Sie zusätzlich zu den Standardberichten von Unified Manager benutzerdefinierte Berichte zu Ihrer Umgebung hinzufügen.

Sie können ein importieren `.rptdesign` Datei, die bereits erstellt wurde. Sie können einen importierten Bericht ausführen, freigeben, planen und löschen.

Unified Manager speichert die Importprotokolldateien in den Dateien jboss.log, ocum-Report.log und ocumserver-debug.log.

Der Kunden-Support hilft Ihnen nicht bei der Erstellung von Berichten, aber er unterstützt Sie bei Problemen, die während eines Berichtsimports auftreten.

Die Funktion Importbericht umfasst die folgende Unterstützung:

- Berichte mit mehreren Kopfzeilen, in denen der Spaltbereich auf 1 gesetzt ist (`colspan=1`)
- Berichte nur mit Diagrammen
- Berichte nur mit Listen und Raster
- Passwörter, die in Berichten verwendet werden, müssen im Format „`base64`“ codiert werden. Berichte, die andere Codierung verwenden, z. B. das Format „`jce`“, verursachen während des Importvorgangs einen Fehler.
- Berichte, die die Datenaggregation enthalten, sollten das aggregierte Spaltenelement in den Tabellendaten des Berichts enthalten.

Berichte im Text-, CSV- und Excel-Format werden in den folgenden Szenarien unterstützt:

- Tabellenelement nur in `.rptdesign` Datei
- Eine Tabelle mit nur einer Kopfzeile

Sie können Berichte, die über einen Spaltbereich von mehr als 1 verfügen, nicht importieren. Wenn ein Bericht im Text-, CSV- oder Excel-Format mehr als eine Kopfzeile enthält, wird nur die erste Kopfzeile berücksichtigt und der Rest wird ignoriert.

Berichtanpassung

Verschiedene Unified Manager Berichte können anhand von Storage- und Nutzungskapazität, Ereignissen, Cluster-Inventar, NFS-Exporten oder SVM-Inventar angepasst werden. .

Anpassungen für Berichte der Storage-Zusammenfassung

Sie können Storage-Übersichtsberichte anpassen, um Informationen zur Storage-Kapazität in HA-Paaren anzuzeigen und zu analysieren. Mit Filtern können Sie die Storage-Auslastung nach Cluster-Modell, die Kapazität der am meisten nicht zugewiesenen LUNs und die Kapazität verfügbarer HA-Paare anzeigen, um neue Volumes und LUNs bereitzustellen.

Anpassen des Storage Summary-Berichts zur Anzeige der Kapazität nach Cluster-Modellen

Sie können den Storage-Übersichtsbericht anpassen, um die Storage-Kapazität und Auslastung von Clustern zu analysieren und die in der Gesamt-Rohkapazität enthaltenen Aggregate anzuzeigen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach einem Cluster:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das ⋮ Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. So gruppieren Sie den Bericht anhand des Modellnamens:
   a. Klicken Sie in die Spalte **Modell**, und klicken Sie auf ⋮ Symbol.
   b. Wählen Sie **Gruppe** > **Gruppe Hinzufügen**.
3. Führen Sie die folgenden Schritte aus, um der gesamten Rohkapazität Aggregate hinzuzufügen:
   a. Klicken Sie in die Spalte **Gesamt Rohkapazität** und klicken Sie auf ⋮ Symbol.
   b. Wählen Sie **Aggregation**.

c. Deaktivieren Sie im Dialogfeld **Aggregation** das Kontrollkästchen **Tabellenebene** und aktivieren Sie das Kontrollkästchen **Gruppenebene**.

d. Geben Sie ggf. einen Namen in das Feld **Etikett eingeben** ein.

4. Klicken Sie auf **OK**.
5. Um den anderen Spalten im Bericht Aggregate hinzuzufügen, wiederholen Sie die Schritte 3 und 4.

Anpassen des Storage Summary-Berichts zur Analyse der Clusterkapazität auf Grundlage der ONTAP-Version

Sie können den Bericht zur Storage-Übersicht so anpassen, dass Cluster nach ONTAP-Version gruppiert werden. Auch Aggregate mit Bezug auf die gesamte Rohkapazität lassen sich anzeigen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie Gruppierung nach Cluster:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie Auf (Menüsymbol).
   c. Wählen Sie **Gruppe** > **Option Innere Gruppe löschen**.
2. So gruppieren Sie den Bericht nach der ONTAP-Version:
   a. Klicken Sie in die Spalte **OS Version** und wählen Sie die aus Symbol.
   b. Wählen Sie **Gruppe** > **Gruppe Hinzufügen**.
3. Führen Sie die folgenden Schritte aus, um der gesamten Rohkapazität Aggregate hinzuzufügen:
   a. Klicken Sie in die Spalte **Gesamt Rohkapazität** und klicken Sie auf Symbol.
   b. Wählen Sie **Aggregation**.
   c. Deaktivieren Sie im Dialogfeld **Aggregation** das Kontrollkästchen **Tabellenebene** und aktivieren Sie das Kontrollkästchen **Gruppenebene**.
   d. Geben Sie ggf. einen Namen in das Feld **Etikett eingeben** ein.
4. Klicken Sie auf **OK**.

Anpassen des Berichts „Storage Summary“ zur Analyse von Clustern mit der am meisten nicht zugewiesenen LUN-Kapazität

Sie können den Bericht „Storage Summary“ anpassen, um die Storage-Auslastung von Clustern zu analysieren, sodass Sie die LUNs mit der am meisten nicht zugewiesenen Kapazität finden können.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den

entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie Gruppierung nach Cluster:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das ••• Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um HA-Paare mit der am meisten nicht zugewiesenen LUN-Kapazität zu sortieren, klicken Sie in die Spalte **nicht zugewiesene LUN-Kapazität (TB)** und klicken Sie auf ••• Symbol.
3. Wählen Sie **Filter** > **Oben/Unten N**.
4. Wählen Sie im Dialogfeld **Top/Bottom N** aus dem Feld **Filter** die Option **Top N** aus, und geben Sie einen Wert in das Textfeld ein.
5. Klicken Sie auf **OK**.

Anpassen des Storage Summary Reports zur Analyse von HA-Paaren für die verfügbare Kapazität, um neue Volumes und LUNs bereitzustellen

Sie können den Bericht „Storage Summary“ anpassen, um verfügbare HA-Paare mit Kapazität anzuzeigen, sodass Sie neue Volumes und LUNs bereitstellen können. Im Bericht werden HA-Paare sortiert, um die ungenutzte Gesamtkapazität des Aggregats zu verringern.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie Gruppierung nach Cluster:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das ••• Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um HA-Paare mit verfügbarer Kapazität zu sortieren, klicken Sie in die Spalte **Aggregat unbenutzte Kapazität (TB)** und klicken Sie auf die ••• Symbol.
3. Wählen Sie **Filter** > **Oben/Unten N**.
4. Wählen Sie im Dialogfeld **Top/Bottom N** aus dem Feld **Filter** die Option **Top N** aus, und geben Sie einen Wert in das Textfeld ein.
5. Klicken Sie auf **OK**.

Anpassungen im Bericht zur Kapazität und Auslastung von Aggregaten

Sie können Berichte anpassen, um zahlreiche Informationen zu Aggregaten anzuzeigen.

Anpassen des Berichts zur Kapazität und Auslastung des Aggregats, um alle Aggregate anzuzeigen, die die volle Kapazität erreichen

Sie können den Aggregat-Kapazitäts- und Auslastungsbericht anpassen, um Aggregate anzuzeigen, sortiert nach wachsender Anordnung der Kapazitätsauslastung des Aggregats. So können Sie die volle Kapazität der Aggregate anzeigen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie Gruppierung nach Cluster und nach HA-Paar:
   a. Klicken Sie in die Spalten, die die Gruppierung aufheben müssen.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Option Innere Gruppe löschen**.
2. Um die volle Kapazität der Aggregate zu sortieren, klicken Sie in die Spalte **Tage bis voll** und klicken Sie auf das Symbol.
3. Wählen Sie **Filter** > **Oben/Unten N**.
4. Wählen Sie im Dialogfeld **Oben/Unten N** aus dem Feld **Filter** die Option **bottom N** aus, und geben Sie einen Wert in das Textfeld ein.
5. Klicken Sie auf **OK**.

Anpassung des Berichts zur Aggregatskapazität und -Auslastung, um Aggregate mit dem Schwellenwert, der erreicht wurde, anzuzeigen

Sie können den Aggregat-Kapazitäts- und Auslastungsbericht anpassen, um die Top-Aggregate anzuzeigen, sortiert nach sinkender Reihenfolge des Überlaufs von Snapshot Kopien. So können Sie den Speicherplatz anzeigen, der in den Aggregaten noch verfügbar ist.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach Cluster oder HA-Paar:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um die Differenz zwischen dem Prozentsatz der verwendeten Daten und dem Schwellenwert für fast volle Werte anzuzeigen, fügen Sie eine neue Spalte hinzu:

a. Wählen Sie eine Spalte aus, und klicken Sie auf die Symbol.
b. Wählen Sie **Spalte** > **Neue Berechnete Spalte**.
c. Geben Sie im Dialogfeld * Neue berechnete Spalte* eine Spaltenbezeichnung ein.
d. Wählen Sie in der Liste Kategorie auswählen die Option **Math** aus.
e. Wählen Sie aus der Liste **Funktion auswählen** die Option **UNTERSCHIED**.
f. Wählen Sie in der Liste Spalte 1 die Option **Space nahezu Full Threshold (%)** aus.
g. Wählen Sie aus der Liste Spalte 2 die Option **verwendete Daten%** aus.
h. Klicken Sie auf **OK**.

3. Um die Werte größer 0 in der neuen Spalte zu filtern, klicken Sie in die Spalte **Neu berechnet** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
4. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **größer als** aus.
5. Geben Sie im Feld **Wert** ein `0` Und klicken Sie auf **OK**.
6. Um die Werte zu sortieren, klicken Sie in der Spalte **Neu berechnet** auf und klicken Sie auf das Symbol.
7. Wählen Sie **Filter** > **Oben/Unten N**.
8. Wählen Sie im Dialogfeld **Top/Bottom N** aus dem Feld **Filter** die Option **Top N** aus, und geben Sie einen Wert in das Textfeld ein.
9. Klicken Sie auf **OK**.

Anpassung des Aggregat-Kapazitäts- und Auslastungsberichts, um Aggregate mit überhöhten Schwellenwerten anzuzeigen

Sie können den Aggregat-Kapazitäts- und Auslastungsbericht anpassen, um die Aggregate anzuzeigen, sortiert nach dem Prozentsatz der überbelegten Kapazität, sodass Sie den noch in den Aggregaten verfügbaren Speicherplatz anzeigen können.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach Cluster oder HA-Paar:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um den Unterschied zwischen dem übernused used prozentual und dem überzugestodenen Schwellenwert anzuzeigen, fügen Sie eine neue Spalte hinzu.
   a. Wählen Sie eine Spalte aus, und klicken Sie auf .

b. Wählen Sie **Spalte** > **Neue Berechnete Spalte**.
c. Geben Sie im Dialogfeld * Neue berechnete Spalte* eine Spaltenbezeichnung ein.
d. Wählen Sie in der Liste Kategorie auswählen die Option **Math** aus.
e. Wählen Sie aus der Liste **Funktion auswählen** die Option **UNTERSCHIED**.
f. Wählen Sie in der Liste Spalte 1 die Option **Überbeplante Schwelle (%)** aus.
g. Wählen Sie aus der Liste Spalte 2 die Option **überzugestogene Kapazität %** aus.
h. Klicken Sie auf **OK**.

3. Um die Werte größer als Null in der neuen Spalte zu filtern, klicken Sie in die Spalte **Neu berechnet** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
4. Wählen Sie aus der Liste **Bedingung** die Option **größer als** aus.
5. Geben Sie im Feld **Wert** ein `0` Und klicken Sie auf **OK**.
6. Um die Werte zu sortieren, klicken Sie in **Neue berechnete Spalte** und klicken Sie auf das Symbol.
7. Wählen Sie **Filter** > **Oben/Unten N**.
8. Wählen Sie im Dialogfeld **Top/Bottom N** aus dem Feld **Filter** die Option **Top N** aus, und geben Sie einen Wert in das Textfeld ein.
9. Klicken Sie auf **OK**.

Anpassung des Berichts zur Aggregatskapazität und -Auslastung, um Aggregate mit nicht-konformen Konfigurationen anzuzeigen

Sie können den Aggregat-Kapazitäts- und Auslastungsbericht anpassen, um die Aggregate anzuzeigen, die nach dem vollständigen Schwellenwert gefiltert sind. So können Sie Aggregate anzeigen, die möglicherweise nicht den Unternehmensrichtlinien entsprechen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach Cluster oder HA-Paar:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um den Aggregatschwellenwert von maximal 85 % zu filtern, klicken Sie in die Spalte **Space Full Threshold** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
3. Wählen Sie aus der Liste **Bedingung** die Option **größer als** aus.
4. Klicken Sie auf **Werte auswählen** und wählen Sie **85**.
5. Klicken Sie auf **OK**.

Anpassungen der Volume-Kapazität und -Auslastung

Sie können Berichte erstellen, um verschiedene Kapazitäts- und Auslastungsinformationen über Volumes zu überwachen. Sie können z. B. Berichte erstellen, um genutzte Volumes, Gesamtkapazität, tägliche Wachstumsrate und Kapazität von Snapshot-Kopien anzuzeigen. Dadurch können Sie feststellen, ob genügend Speicherplatz auf einem Volume vorhanden ist oder ob diese zu stark genutzt werden oder nicht ausgelastet sind.

Anpassen des Volume-Kapazitäts- und Auslastungsberichts zur Anzeige von Volumes, die sich der vollen Kapazität nähern, bei ausgeschaltetem Snapshot Autodelete

Sie können den Volume-Kapazitäts- und Auslastungsbericht anpassen, um Volumes anzuzeigen, die nach einer besseren Anordnung der Volume-Kapazitätsauslastung sortiert sind. So können Sie Volumes anzeigen, die ihre volle Kapazität erreichen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach SVM, Cluster oder Volume:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um Volumen zu sortieren, die sich der vollen Kapazität nähern, klicken Sie in der Spalte **Tage bis voll** auf, und klicken Sie auf Symbol.
3. Um Volumen zu filtern, bei denen der Snapshot Autodelete deaktiviert ist, klicken Sie in die Spalte **Snapshot Autodelete** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
4. Wählen Sie aus der Liste **Bedingung** die Option **gleich** aus.
5. Klicken Sie auf **Werte auswählen** und wählen Sie **deaktiviert**.
6. Klicken Sie auf **OK**.

Anpassen des Berichts zur Volume-Kapazität und -Auslastung, um die am wenigsten verbrauchten Volumes mit deaktiviertem Thin Provisioning anzuzeigen

Sie können den Volume-Kapazitäts- und Auslastungsbericht anpassen, um Volumes basierend auf ihrem Volume-Verbrauch anzuzeigen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach SVM, Cluster oder Volume:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um die Volumen anhand des verbrauchten Prozentsatzes zu sortieren, klicken Sie in die Spalte **verwendete Daten %** und klicken Sie auf das Symbol.
3. Um Volumes mit deaktiviertem Thin Provisioning zu filtern, klicken Sie in die Spalte **Thin Provisioning** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
4. Wählen Sie aus der Liste **Bedingung** die Option **gleich** aus.
5. Klicken Sie auf **Werte auswählen** und wählen Sie **Nein**.
6. Klicken Sie auf **OK**.

Anpassen des Berichts zur Kapazität und Auslastung des Volumes, um Volumes mit nicht-konformen Konfigurationen anzuzeigen

Sie können den Volume-Kapazitäts- und Auslastungsbericht anpassen, um Volumes anzuzeigen, die den Unternehmensrichtlinien nicht entsprechen. Wenn beispielsweise die Deduplizierung für alle Volumes aktiviert sein muss, können Sie einen Bericht mit allen Volumes erstellen, in denen die Deduplizierung deaktiviert ist.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach SVM, Cluster oder Volume:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Alle Spalten ausblenden mit Ausnahme der Spalten Cluster, Storage Virtual Machine, Volume, Deduplication and Deduplication Space Savings (GB):
   a. Klicken Sie in die Spalte, und klicken Sie auf Symbol.
   b. Wählen Sie im Menü die Option **Spalte** > **Spalte ausblenden**.
3. Um Volumes zu filtern, die die Deduplizierung deaktiviert haben, klicken Sie in der Spalte **Deduplizierung** auf und öffnen Sie das Dialogfeld **Filter**, indem Sie auf das klicken Symbol.
4. Wählen Sie aus der Liste **Bedingung** die Option **gleich** aus.
5. Klicken Sie auf **Werte auswählen** und wählen Sie **deaktiviert**.

6. Klicken Sie auf **OK**.
7. Um Volumes basierend auf den Platzeinsparungen durch die Deduplizierung zu sortieren, klicken Sie in der Spalte **Deduplication Space Savings (GB)** auf das Symbol.

Anpassungen hinsichtlich Kapazität und Auslastung von qtree

Sie können benutzerdefinierte Berichte erstellen, um die Kapazität und Auslastung der qtrees des Systems zu analysieren. Beispielsweise können Sie Berichte erstellen, um qtrees zu sortieren und zu bestimmen, ob gegen die Festplatten- oder DateiSoft-Limits verstoßen wurde.

Anpassung des Qtree-Kapazitäts- und Auslastungsberichts zur Anzeige von qtrees, die das weiche Limit der Festplatte überschritten haben

Sie können den Qtree-Kapazitäts- und Auslastungsbericht anpassen, um qtrees anzuzeigen, die die Softgrenzen der Festplatte überschritten haben. Sie können nach verwendeter Festplatte, Festplatten-Limit und Festplatten-Softlimit filtern und sortieren.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach SVM, Cluster oder Volume:
   a. Klicken Sie in die Spalten, die die Gruppierung aufheben müssen.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um qtrees zu filtern, die nicht über eine unbegrenzte Anzahl von Festplatten verfügen, klicken Sie in die Spalte **Disk Hard Limit** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf das klicken Symbol.
   a. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **nicht gleich** aus.
   b. Klicken Sie auf **Werte auswählen** und wählen Sie **unbegrenzt**.
   c. Klicken Sie Auf **Ok**.
3. Um qtrees zu filtern, die nicht über einen unbegrenzten Wert verfügen, klicken Sie in die Spalte **Disk Soft Limit** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf das klicken Symbol.
   a. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **nicht gleich** aus.
   b. Klicken Sie auf **Werte auswählen** und wählen Sie **unbegrenzt**.
   c. Klicken Sie Auf **Ok**.
4. So fügen Sie eine Spalte für qtrees hinzu, die das weiche Limit für die Festplatte nicht überschritten haben:
   a. Klicken Sie in der Spalte **Disk Soft Limit** auf Und wählen Sie **Spalte** > **Neue berechnete Spalte**

b. Geben Sie im Dialogfeld * Neue berechnete Spalte* ein `Breached Disk Soft Limit Capacity` Im Feld **Spaltenbeschriftung**.

c. Wählen Sie in der Liste Kategorie auswählen die Option **Text** aus.

d. Wählen Sie aus der Dropdown-Liste **Funktion auswählen** die Option **Erweitert** aus.

e. Geben Sie im Feld **Ausdruck eingeben** ein `IF(([qtreeDiskUsedPercent] *[diskLimit]/100 > [softDiskLimit]), "Yes", "No").`

f. Klicken Sie auf **OK**.

5. Um qtrees zu filtern, die das Limit für weiche Festplatten überschritten haben, klicken Sie in die Spalte **nicht mehr belegte Datenträgerweiche Grenzkapazität** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf das klicken Symbol.

a. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **gleich** aus.

b. Klicken Sie auf **Werte auswählen** und wählen Sie **Ja**.

c. Klicken Sie Auf **Ok**.

Anpassung des Qtree-Kapazitäts- und Auslastungsberichts zur Anzeige von qtrees, die das Softlimit der Dateien überschritten haben

Sie können den Qtree-Kapazitäts- und Auslastungsbericht anpassen, um qtrees anzuzeigen, die die Softlimit von Dateien überschritten haben. Sie können nach verwendeter Datei, hartem Limit und Softlimit für Dateien filtern und sortieren.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach SVM, Cluster oder Volume:

a. Klicken Sie in die Spalten, die die Gruppierung aufheben müssen.

b. Klicken Sie auf das Symbol.

c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.

2. Um qtrees zu filtern, die nicht über eine unbegrenzte Anzahl von Dateien verfügen, klicken Sie in die Spalte **File Hard Limit** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.

a. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **nicht gleich** aus.

b. Klicken Sie auf **Werte auswählen** und wählen Sie **unbegrenzt**.

c. Klicken Sie Auf **Ok**.

3. Um qtrees zu filtern, die kein unbegrenztes Dateilimit haben, klicken Sie in die Spalte **Dateiweicher Grenzwert** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf das klicken Symbol.

a. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **nicht gleich** aus.

b. Klicken Sie auf **Werte auswählen** und wählen Sie **unbegrenzt**.

c. Klicken Sie Auf **Ok**.

4. So fügen Sie eine Spalte für qtrees hinzu, die das Softlimit der Datei überschritten haben:
   a. Klicken Sie in der Spalte **Dateiweicher Grenzwert** auf das Und wählen Sie **Spalte** > **Neue berechnete Spalte**
   b. Geben Sie im Dialogfeld * Neue berechnete Spalte* ein `Breached File Soft Limit Capacity` Im Feld **Spaltenbeschriftung**.
   c. Wählen Sie in der Liste Kategorie auswählen die Option **Text** aus.
   d. Wählen Sie aus der Dropdown-Liste **Funktion auswählen** die Option **Erweitert** aus.
   e. Geben Sie im Feld **Ausdruck eingeben** ein `IF(([qtreeFileUsedPercent]*[fileLimit]/100 > [softFileLimit]), "Yes", "No").`
   f. Klicken Sie auf **OK**.
5. Um qtrees zu filtern, die das Limit für weiche Dateien überschritten haben, klicken Sie in die Spalte **undurchbrochen Dateiweicher Grenzwert Kapazität** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf das klicken Symbol.
   a. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **gleich** aus.
   b. Klicken Sie auf **Werte auswählen** und wählen Sie **Ja**.
   c. Klicken Sie Auf **Ok**.

Anpassungen für Ereignisberichte

Sie können Berichte erstellen, um ausstehende Ereignisse auf einem Cluster zu überwachen.

Anpassen des Ereignisberichts zur Anzeige von Ereignissen mit einem kritischen Schweregrad

Sie können den Ereignisbericht so anpassen, dass Ereignisse angezeigt werden, die nach ihrem Schweregrad gefiltert sind, und nach den Ereignissen, die für den längsten Zeitraum nicht gelöst wurden.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Um Ereignisse mit dem Schweregrad kritisch zu filtern, klicken Sie in die Spalte **Status** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
2. Wählen Sie aus der Liste **Bedingung** die Option **gleich** aus.
3. Klicken Sie auf **Werte auswählen** und wählen Sie **kritisch**.
4. Klicken Sie auf **OK**.
5. Um die Ereignisse zu sortieren, die für den längsten Zeitraum nicht aufgelöst wurden, klicken Sie in die Spalte **Tage ausstehen** und klicken Sie auf das Symbol.

6. Wählen Sie **Filter** > **Oben/Unten N**.
7. Wählen Sie im Dialogfeld **Top/Bottom N** aus dem Feld **Filter** die Option **Top N** aus, und geben Sie einen Wert in das Textfeld ein.
8. Klicken Sie auf **OK**.

Anpassen des Ereignisberichts zur Anzeige von Ereignissen auf unternehmenskritischen Objekten

Sie können den Ereignisbericht so anpassen, dass Ereignisse, die nach Priorität geschäftskritischer Daten gefiltert wurden, angezeigt werden.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Um Ereignisse mit unternehmenskritischer Datenpriorität zu filtern, klicken Sie in die Spalte **Datenpriorität** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
2. Wählen Sie aus der Liste **Bedingung** die Option **gleich** aus.
3. Klicken Sie auf **Werte auswählen** und wählen Sie **unternehmenskritisch**.
4. Klicken Sie auf **OK**.

Anpassen des Berichts „Veranstaltungen“ zur Anzeige der am häufigsten diskutierten Ereignisse

Sie können den Ereignisbericht so anpassen, dass Ereignisse, die am meisten besprochen werden, angezeigt werden.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Um die Ereignisse zu sortieren, die am meisten diskutiert werden, klicken Sie in die Spalte **Hinweise** und klicken Sie auf die Symbol.
2. Wählen Sie **Filter** > **Oben/Unten N**.
3. Wählen Sie im Dialogfeld **Top/Bottom N** aus dem Feld **Filter** die Option **Top N** aus, und geben Sie einen Wert in das Textfeld ein.
4. Klicken Sie auf **OK**.

Anpassen des Ereignisberichts zur Anzeige der dem Administrator zugewiesenen Ereignisse

Sie können den Ereignisbericht so anpassen, dass dem Administrator zugewiesene Ereignisse angezeigt werden, die nach der Auswirkungs-Ebene und dem Administratornamen gefiltert sind.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Um Ereignisse zu filtern, klicken Sie in der Spalte **Impact Level** auf und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
2. Wählen Sie aus der Liste **Bedingung** die Option **gleich** aus.
3. Klicken Sie auf **Werte auswählen** und wählen Sie **Vorfall**.
4. Klicken Sie auf **OK**.
5. Um diese Vorfälle dem Administrator zuzuweisen, klicken Sie in der Spalte **Assigned to** auf und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
6. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **gleich** aus.
7. Klicken Sie auf **Werte auswählen** und wählen Sie **Admin-Name**.
8. Klicken Sie auf **OK**.

Anpassen des Ereignisberichts zur Anzeige von Ereignissen, die die Verfügbarkeit beeinträchtigen

Sie können den Ereignisbericht so anpassen, dass Ereignisse angezeigt werden, die nach den meisten Vorfällen kategorisiert und dem Administrator zugewiesen sind. Sie können den Bericht nach den Auswirkungen und dem Admin-Namen filtern.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Um Verfügbarkeitsereignisse zu filtern, klicken Sie in die Spalte **Impact Area** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
2. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **gleich** aus.
3. Klicken Sie auf **Werte auswählen** und wählen Sie **Vorfall**.
4. Klicken Sie auf **OK**.

Anpassen des Berichts „Ereignisse“ zur Anzeige der am häufigsten bestätigten nicht behobenen Ereignisse

Sie können den Ereignisbericht so anpassen, dass die am stärksten bestätigten Ereignisse, gefiltert nach dem Ereignisstatus, angezeigt werden. Sie können sie in abnehmender Reihenfolge sortieren, um die Anzahl der ausstehenden Tage anzuzeigen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Um bestätigte Ereignisse zu filtern, klicken Sie in die Spalte **Status** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
2. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **gleich** aus.
3. Klicken Sie auf **Werte auswählen** und wählen Sie **bestätigt**.
4. Klicken Sie auf **OK**.
5. Um den Bericht weiter zu filtern, klicken Sie in die Spalte **bestätigt durch** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
6. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **gleich** aus.
7. Klicken Sie auf **Werte auswählen** und wählen Sie **Name**.
8. Klicken Sie auf **OK**.
9. Um die Ereignisse, die für die meisten Tage ausstehen, zu sortieren, klicken Sie in die Spalte **Tage Outstanding** und klicken Sie auf .
10. Wählen Sie **Filter** > **Oben/Unten N**.
11. Wählen Sie im Dialogfeld **Top/Bottom N** aus dem Feld **Filter** die Option **Top N** aus, und geben Sie einen Wert in das Textfeld ein.
12. Klicken Sie auf **OK**.

Anpassungen für Cluster Inventory Report

Sie können Inventarberichte anpassen, um zu überwachen, ob für Clusterkomponenten unzureichende Ressourcen vorhanden sind. Beispielsweise können Sie Berichte so anpassen, dass Informationen wie Cluster, die sich der SVM-Anzahl nähern, Nodes, die ältere Versionen von ONTAP ausführen, und Nodes, die das maximale Limit für Festplatten erreichen, überwacht werden.

Sie können den Bericht „Cluster Inventory“ anpassen, um Cluster anzuzeigen, die das Limit für die SVM-Anzahl erreichen

Sie können den Bericht „Cluster Inventory“ so anpassen, dass Cluster angezeigt werden. Dieser Bericht sortiert nach klassifikation der Reihenfolge ihrer SVM-Anzahl.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach Cluster oder Node:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. So sortieren Sie Cluster nach SVM-Anzahl:
   a. Klicken Sie in die Spalte **SVM Count**.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Option Innere Gruppe löschen**.
3. Wählen Sie **Filter** > **Oben/Unten N**.
4. Wählen Sie im Dialogfeld **Top/Bottom N** aus dem Feld **Filter** die Option **Top N** aus, und geben Sie einen Wert in das Textfeld ein.
5. Klicken Sie auf **OK**.

Sie können den Cluster-Inventory-Bericht anpassen, um Nodes anzuzeigen, auf denen ältere Versionen der ONTAP Software ausgeführt werden

Sie können den Cluster-Inventory-Bericht so anpassen, dass nach älteren ONTAP-Versionen gefiltert werden.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach Cluster oder Node:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um Knoten zu filtern, die nicht ONTAP 8.3 ausführen, klicken Sie auf die Spalte **ONTAP Version** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
3. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **nicht gleich** aus.
4. Klicken Sie auf **Werte auswählen** und wählen Sie **8.3**.
5. Klicken Sie auf **OK**.

Sie können den Cluster-Inventory-Bericht so anpassen, dass Nodes angezeigt werden, die das maximale Festplattenslimit erreichen

Sie können den Cluster-Bestandsbericht so anpassen, dass eine Liste der Nodes angezeigt wird, die das maximale Festplattenlimit erreichen und nach zunehmender

Reihenfolge sortiert werden.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach Cluster oder Node:
   a. Klicken Sie in die Spalten, die nicht gruppiert werden müssen.
   b. Klicken Sie auf das ••• Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. So verschieben Sie die Spalte **Datenträgeranzahl** neben der Spalte **Modell**:
   a. Klicken Sie in die Spalte **Datenträgeranzahl**.
   b. Klicken Sie auf das ••• Symbol und wählen Sie **Spalte** > **Spalten neu ordnen**.
   c. Verwenden Sie im Dialogfeld **Spalten neu ordnen** die Pfeiltasten nach oben* und **nach unten**, um die Spalte an die gewünschte Position zu verschieben.
3. So fügen Sie eine neue berechnete Spalte hinzu:
   a. Wählen Sie eine Spalte aus, und klicken Sie auf ••• Und wählen Sie **Spalte** > **Neue berechnete Spalte**.
   b. Geben Sie im Dialogfeld * Neue berechnete Spalte* ein `Maximum Disk Limit` Im Feld **Spaltenbeschriftung**.
   c. Wählen Sie aus der Liste Kategorie auswählen die Option **Vergleich**.
   d. Wählen Sie aus der Liste **Funktion auswählen** die Option **Erweitert**.
   e. Geben Sie im Feld **Ausdruck eingeben** ein `IF([model]="FAS3250" , 960, 0).`
   f. Klicken Sie auf **OK**.
4. So fügen Sie eine zweite neue Spalte hinzu:
   a. Wählen Sie die Spalte **Maximum Disk Limit** aus, und klicken Sie auf ••• Und wählen Sie **Spalte** > **Neue berechnete Spalte**.
   b. Geben Sie im Dialogfeld * Neue berechnete Spalte* ein `Available Volume` Im Feld **Spaltenbeschriftung**.
   c. Wählen Sie in der Liste Kategorie auswählen die Option **Math** aus.
   d. Wählen Sie aus der Liste **Funktion auswählen** die Option **UNTERSCHIED**.
   e. Wählen Sie in der Liste Spalte 1 die Option **Maximum Disk Limit** aus.
   f. Wählen Sie in der Liste Spalte 2 die Option **Datenträgeranzahl** aus.
   g. Klicken Sie auf **OK**.
5. Um die Werte zu sortieren, klicken Sie in der Spalte **Verfügbare Volumen** auf und klicken Sie auf ••• Symbol.

6. Wählen Sie **Filter** > **Oben/Unten N**.
7. Wählen Sie im Dialogfeld **Top/Bottom N** aus dem Feld **Filter** die Option **Top N** aus, und geben Sie einen Wert in das Textfeld ein.
8. Klicken Sie auf **OK**.

Anpassungen des NFS-Exportberichts

Sie können NFS-Exportberichte anpassen, um Informationen über NFS-Exportrichtlinien und Regeln für Volumes auf Ihren Storage-Systemen zu analysieren. So können Sie z. B. Berichte anpassen, um Volumes mit nicht zugänglichen Verbindungspfaden und Volumes mit der Standard-Exportrichtlinie anzuzeigen.

Anpassen des Berichts NFS-Exporte, um eine Liste von Volumes anzuzeigen, die über einen nicht zugänglichen Verbindungspfad verfügen

Sie können den Bericht NFS Exports anpassen, um eine Liste von Volumes anzuzeigen, die über einen nicht zugänglichen Verbindungspfad verfügen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach Cluster oder Volumes:
   a. Klicken Sie in die Spalten, die die Gruppierung aufheben müssen.
   b. Klicken Sie auf das ••• Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um Volumes mit einem nicht zugänglichen Verbindungspfad zu filtern, klicken Sie in die Spalte **Junction Path Active** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
3. Wählen Sie aus der Liste **Bedingung** die Option **gleich** aus.
4. Klicken Sie auf **Werte auswählen** und wählen Sie **Nein**.
5. Klicken Sie auf **OK**.

Anpassen des Berichts NFS-Exporte zur Anzeige einer Liste von Volumes mit Standard-Exportrichtlinie

Sie können den Bericht NFS-Exporte anpassen, um eine Liste von Volumes mit der Standard-Exportrichtlinie anzuzeigen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach Cluster oder Volumes:
   a. Klicken Sie in die Spalten, die die Gruppierung aufheben müssen.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um Volumes mit Standard-Exportrichtlinie zu filtern, klicken Sie auf die Spalte **Richtlinie exportieren** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
3. Wählen Sie aus der Liste **Bedingung** die Option **gleich** aus.
4. Klicken Sie auf **Werte auswählen** und wählen Sie **Standard**.
5. Klicken Sie auf **OK**.

Anpassungen des SVM-Inventarberichts

Sie können SVM-Bestandsberichte erstellen, um Volume-Informationen zu analysieren und die allgemeine Integrität und Storage-Verfügbarkeit anzuzeigen. Sie können beispielsweise Berichte erstellen, um SVMs die maximale Volume-Anzahl zu erreichen und beendete SVMs zu analysieren.

Sie können den SVM-Bestandsbericht anpassen, um eine Liste der SVMs anzuzeigen, die die maximale Volume-Begrenzung erreichen

Sie können den SVM-Bestandsbericht anpassen, um eine Liste der SVMs anzuzeigen, die die maximale Volume-Grenze erreichen, indem Sie die Volumes in steigender Reihenfolge sortieren.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. So entfernen Sie die Gruppierung nach einem Cluster:
   a. Klicken Sie in die Spalte, die nicht gruppiert werden muss.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um SVMs zu filtern, die keine unbegrenzten zulässigen Volumen haben, klicken Sie auf die Spalte **Maximum allowed Volumes** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
3. Wählen Sie im Feld **Datentyp** die Option **String** aus, und klicken Sie auf **OK**.
4. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **nicht gleich** aus.
5. Klicken Sie auf **Werte auswählen** und wählen Sie **unbegrenzt**.
6. So fügen Sie eine neue berechnete Spalte hinzu:

a. Wählen Sie eine Spalte aus, und klicken Sie auf Und wählen Sie **Spalte** > **Neue berechnete Spalte**.

b. Geben Sie im Dialogfeld * Neue berechnete Spalte* ein `Available Volume` Im Feld **Spaltenbeschriftung**.

c. Wählen Sie in der Liste Kategorie auswählen die Option **Math** aus.

d. Wählen Sie aus der Dropdown-Liste **Funktion auswählen** die Option **Erweitert** aus.

e. Geben Sie im Feld **Ausdruck eingeben** ein `[maximumVolumes]-[volumeCount].`

f. Klicken Sie auf **OK**.

7. Um SVMs in aufsteigender Reihenfolge zu sortieren, klicken Sie in der Spalte **Available Volume** auf und klicken Sie auf Symbol.
8. Wählen Sie **Filter** > **Oben/Unten N**.
9. Wählen Sie im Dialogfeld **Oben/Unten N** aus dem Feld **Filter** die Option **bottom N** aus, und geben Sie einen Wert in das Textfeld ein.
10. Klicken Sie auf **OK**.

Sie können den SVM-Bestandsbericht anpassen, um eine Liste der angehalten SVMs anzuzeigen

Sie können den SVM-Bestandsbericht anpassen, um eine Liste der angehalten SVMs anzuzeigen. Der Bericht filtert die SVMs nach ihrem Status.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Um SVMs nach Status zu filtern, klicken Sie auf die Spalte **Status** und öffnen Sie das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
2. Wählen Sie aus der Liste **Bedingung** die Option **gleich** aus.
3. Klicken Sie auf **Werte auswählen** und wählen Sie **angehalten**.
4. Klicken Sie auf **OK**.

Inventarisierung von Volume-Beziehungen – Berichte

Sie können den Bestandsbericht zu Volume-Beziehungen anpassen, um die Volume-Details anzuzeigen, die basierend auf der Fehlerquelle gefiltert werden. Mithilfe von Filtern können Sie Inventardetails zu Volume-Beziehungen basierend auf Zeitplänen anzeigen und Details zum Volume-Bestand basierend auf Problemen gruppieren.

Anpassen des Berichts „Volume Relationships Inventory“ zur Anzeige von Volumes, die nach Fehlerquelle gruppiert sind

Sie können den Bestandsbericht zu Volume-Beziehungen anpassen, um Volumes anzuzeigen, die nach Fehlerquelle gruppiert sind.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Wählen Sie die Spalte **Relationship Health** aus.
2. Um die Volume-Details für fehlerhafte Volumes anzuzeigen, klicken Sie auf das — Zeichen neben der Spalte **Bad**.
3. Um die Volume-Details für gute Volumes anzuzeigen, klicken Sie auf das — Zeichen neben der Spalte **gut**.

Anpassen des Berichts „Volume Relationships Inventory“, um nach Problem gruppierte Volumes anzuzeigen

Sie können den Bestandsbericht zu Volume-Beziehungen anpassen, um Volumes anzuzeigen, die nach dem Integritätsstatus der Volume-Beziehung gruppiert werden.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Um Volumen nach dem Status der Volume-Beziehung zu filtern, wählen Sie die Spalte **Relationship Health** aus, und klicken Sie auf die Symbol.
2. Klicken Sie im Dialogfeld **Filter** auf **Werte auswählen** und wählen Sie dann den gewünschten Wert aus der Dropdown-Liste aus.

   Die Volume-Details für den ausgewählten Wert werden angezeigt.

Anpassung des Berichts Volume Transfer Status (Historical)

Sie können den Bericht „Volume Transfer Status“ (Verlauf) anpassen, um Informationen zu Volume-Transfers in bestimmten Zeitabständen anzuzeigen und zu analysieren. Mithilfe von Filtern können Sie Details zur Volume-Übertragung zwischen zwei Daten anzeigen.

Anpassen der Berichtspläne für den Volume Transfer Status (Historical)

Sie können die Zeitpläne für den Bericht „Volume Transfer Status“ (Historischer Bericht) anpassen, um die Volume-Details auf Basis verschiedener Zeitpläne anzuzeigen. Sie können vorhandene Berichtspläne anzeigen, ändern oder löschen und neue Zeitpläne für Berichte hinzufügen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Klicken Sie auf der Berichtsseite **Volume Transfer Status (Historical)** auf **Berichtszeitpläne verwalten**.
2. Geben Sie im Dialogfeld **Berichtszeitpläne verwalten** bestimmte Details ein, wie z. B. Name des Empfängerplans, E-Mail-Adresse, Berichtsformat, Häufigkeit und Berichte.
3. Wählen Sie als Berichtskategorie * Inventory* aus.
4. Klicken Sie auf **Speichern und Schließen**.

   Der Bericht zum Volume Transfer Status (Historical) wird automatisch per E-Mail an einen oder mehrere Empfänger gemäß dem Zeitplan gesendet.

Anpassen des Berichts zum Volume Transfer Status (Historical), um Volumes in bestimmten Zeitintervallen anzuzeigen

Sie können den Bericht „Volume Transfer Status“ (Historischer Bericht) anpassen, um die Volume-Details in bestimmten Zeitintervallen anzuzeigen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Gruppierung nach Cluster entfernen:
   a. Klicken Sie in die Spalte, die die Gruppierung aufheben soll.
   b. Klicken Sie auf das Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um die Volume-Details zu einem bestimmten Zeitintervall anzuzeigen, klicken Sie in die Spalte **Startzeit** und klicken Sie dann auf Symbol.
3. Klicken Sie im Dialogfeld **Filter** auf **Werte auswählen** und wählen Sie dann das Datum und die Uhrzeit aus der Dropdown-Liste aus.

   Die Volume-Details für den ausgewählten Zeitbereich werden angezeigt.

Anpassen des Berichts zum Volume Transfer Status (Historical) zur Anzeige von Volumes, die nach Zeitpunkt des Auftretens gruppiert sind

Sie können den Bericht „Volume Transfer Status“ (Historischer Bericht) so anpassen, dass die Liste der Volumes angezeigt wird, die nach dem Zeitpunkt des Eintretens zwischen zwei Daten gruppiert sind.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Gruppierung nach Cluster entfernen:
   a. Klicken Sie in der Spalte, die nicht gruppiert werden muss, auf die ••• Symbol.
   b. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Öffnen Sie in der Spalte **Startzeit** das Dialogfeld **Filter**, indem Sie auf klicken Symbol.
3. Wählen Sie aus der Dropdown-Liste **Bedingung** die Option **Zwischen** aus.
4. Klicken Sie auf **Werte auswählen**, und wählen Sie die Werte **Datum von** und **Datum bis** aus.
5. Klicken Sie auf **OK**.

Anpassen des Berichts zum Volume Transfer Status (Historical), um fehlgeschlagene oder erfolgreiche Volume-Transfers anzuzeigen

Sie können den Bericht zum Volume Transfer Status (Historical) anpassen, um die Details zu fehlgeschlagenen oder erfolgreichen Volume-Transfers anzuzeigen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Gruppierung nach Cluster entfernen:
   a. Wählen Sie die Spalte aus, die die Gruppierung aufheben soll.
   b. Klicken Sie auf das ••• Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um die Volume-Transfers nach Fehlschlag oder Erfolg zu sortieren, klicken Sie in der Spalte **Operationelles Ergebnis** auf und klicken Sie dann auf das ••• Symbol.
3. Wählen Sie **Filter**.
4. Klicken Sie im Dialogfeld **Filter** auf **Werte auswählen** und wählen Sie dann entweder **Erfolg** oder **Fehler** aus.

Anpassung des Berichts Volume Transfer Rate (Historical

Sie können den Bericht „Volume Transfer Rate“ (Historischer Bericht) anpassen, um Details zur Volume-Übertragung basierend auf der Gesamtgröße des Volumes anzuzeigen. Sie können auch die Volume-Transfers für einen bestimmten Wochentag anzeigen.

Anpassen des Berichts zur Volume Transfer Rate (Historical), um Volume-Transfers basierend auf der Transfergröße anzuzeigen

Sie können den Bericht „Volume Transfer Rate“ (Historischer Bericht) anpassen, um die Volume-Transferdetails entsprechend der Gesamtübertragungsgröße des Volumes

anzuzeigen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Gruppierung nach Cluster entfernen:
   a. Wählen Sie die Spalte aus, die die Gruppierung aufheben soll.
   b. Klicken Sie auf das ••• Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um die Volume-Transfers entsprechend der Volume-Transfergröße zu sortieren, klicken Sie auf die Spalte **Total Transfer Size (GB)**.

Anpassen des Berichts zur Volume Transfer Rate (Historical), um Volume Transfers nach Tag gruppiert anzuzeigen

Sie können den Bericht Volume Transfer Rate (Historical) anpassen, um die nach Tag sortierten Volume-Transferdetails anzuzeigen.

Über diese Aufgabe

Sie können diese Aufgabe auch ausführen, indem Sie auf der Seite Berichte auf **Bericht ausführen** für den entsprechenden Bericht klicken.

Schritte

1. Gruppierung nach Cluster entfernen:
   a. Wählen Sie die Spalte aus, die die Gruppierung aufheben soll.
   b. Klicken Sie auf das ••• Symbol.
   c. Wählen Sie **Gruppe** > **Innengruppe Löschen**.
2. Um die Volume-Transfers für einen bestimmten Tag anzuzeigen, klicken Sie auf die Spalte **Tag**.

Beschreibung der Berichtsfenster und Dialogfelder

Mit den Optionen können Sie die Berichte planen, freigeben, verwalten, speichern und importieren.

Berichtsseite

Auf der Seite Berichte können Sie detaillierte Informationen zu den von Ihnen erstellten Berichten anzeigen. Sie können nach einem bestimmten Bericht suchen, einen Bericht speichern und einen Bericht löschen. Sie können auch einen Bericht planen, freigeben und importieren.

Auf der Seite Berichte werden kategorisierte Berichtsgruppen angezeigt, zu denen Sie spezifische

Berichtsdetails erhalten können. Standardmäßig werden die Berichtsgruppen erweitert, um die Berichtstypen, eine Berichtsübersicht und Links anzuzeigen, mit denen Sie Berichte anpassen können. Es kann jeweils nur ein Bericht angezeigt werden. Sie können auf die Schaltfläche **Bericht ausführen** klicken, um einen Bericht für eine bestimmte Gruppe von Berichten anzuzeigen.

Die Implementierung der Planung und Erstellung von Berichten auf der Seite Berichte wird in einer zukünftigen Version veraltet sein. Mit den folgenden zusätzlichen Methoden können Sie Gesundheits- und Performance-Daten aus Unified Manager extrahieren:

- Daten direkt aus den Grid-Seiten in der GUI extrahieren
- Verwenden der Open Database für den Zugriff auf alle verfügbaren Objekte
- Ausführung von Unified Manager REST-APIs zur Rückgabe der Informationen, für die Sie interessiert sind, zu überprüfen

Die folgende Liste enthält Berichtsgruppen und Berichtstypen, die auf der Seite Berichte angezeigt werden:

- Berichte Zur Kapazitätsauslastung
  - Zusammenfassung
  - Kapazität und Auslastung aggregieren
  - Volume-Kapazität und -Auslastung
  - Kapazität und Auslastung von qtree
- Betriebsberichte - Ereignisse
- Bestandsberichte
  - Cluster-Inventar
  - NFS Exporte
  - SVM-Inventar
- Importierte Berichte
- Datensicherungsberichte
  - Konfiguration Der Volume Data Protection
  - Inventarisierung Von Volume-Beziehungen
  - Volume-Transferstatus (Historisch)
  - Volume-Übertragungsrate (Historisch)

Zusammenfassungsbericht über Storage

Mit dem Bericht „Storage Summary“ können Sie zusammengefasste Informationen zur Storage-Kapazität in den HA-Paaren anzeigen. Anhand dieser Informationen erhalten Sie Einblick in mögliche Kapazitätsrisiken und können geeignete Maßnahmen zur Neuverteilung des Workloads ergreifen. Cluster-Informationen mit einem Node sind im Bericht nicht sichtbar.

Übersicht Storage-Bericht – Diagrammansicht

Der Bericht „Speicherübersicht“ wird in zwei Formaten angezeigt:

- Übersicht Storage-Bericht – Diagrammansicht
- Tabellarische Ansicht des Berichts „Storage Summary“

Das Diagramm zeigt den Kapazitätstrends der genutzten und nicht genutzten Datenkapazität der Aggregate für einen bestimmten Zeitraum. Die Gesamtkapazität wird auf der vertikalen (y) Achse und dem Cluster-Namen auf der horizontalen (x)-Achse angezeigt. Daher stellt jeder Balken im Diagramm einen Cluster dar. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Punkt positionieren.

- * Clustername*

  Zeigt den Cluster-Namen an.

- **HA-Paar**

  Zeigt den HA-Paar-Wert an, der durch die Bildung von zwei Nodes ermittelt wird.

- **Modell**

  Zeigt den Namen des Modells an.

- **Betriebssystemversion**

  Zeigt die Version des verwendeten ONTAP an.

- **Gesamtbruttokapazität**

  Zeigt die gesamte physische Kapazität aller Festplatten im Array an.

- **Unkonfigurierte Rohkapazität**

  Zeigt die nicht konfigurierte Kapazität von Festplatten an, deren Containertyp nicht „Aggregate“, „Broken“, „Spare“ oder „Shared“ ist. Diese Kapazität ist immer höher als die physische Kapazität der Festplatte in ONTAP. Nehmen Sie beispielsweise eine 2-TB-Festplatte in Betracht. Die physische Kapazität der Festplatte beträgt 1.6 TB in ONTAP, während die nicht konfigurierte Rohkapazität in Unified Manager 1.8 TB beträgt.

- **Gesamtkapazität**

  Zeigt die Gesamtgröße der verfügbaren Aggregate für den Benutzer an. Dies schließt die Snapshot Kopie-Reserve ein.

- **Verwendete Gesamtkapazität**

  Zeigt die Kapazität an, die bereits in Aggregaten verwendet wird. Dies schließt die Kapazität ein, die von Volumes, LUNs und anderen Technologieköpfen für Storage-Effizienz verbraucht wird.

- * Nicht Genutzte Kapazität Aggregieren*

  Zeigt die Kapazität an, die möglicherweise zum Speichern zusätzlicher Daten im Aggregat verfügbar ist. Dies schließt die Snapshot Kopie-Reserve ein.

- **Zugewiesene LUN-Kapazität**

  Zeigt die Kapazität der zugeordneten LUNs an.

- **Nicht zugewiesene LUN-Kapazität**

  Zeigt die Kapazität aller LUNs an, die dem Host nicht zugeordnet sind.

- **Volumen Gesamtkapazität**

  Zeigt die Gesamtkapazität der Volumes an (verwendet plus nicht genutzt).

- **Volumen Genutzte Kapazität**

  Zeigt die verwendete Kapazität der Volumes an.

- **Volumen Ungenutzte Kapazität**

  Zeigt die ungenutzte Kapazität der Volumes an.

- **Volume Protection Kapazität**

  Zeigt die Kapazität der Volumes an, für die SnapMirror und SnapVault aktiviert sind.

- * Cluster Lizenzierte Cloud Stufe Gesamt*

  Zeigt die Gesamtkapazität an, die im Cloud-Tier lizenziert wurde. Dieses Feld wird für Storage-Provider angezeigt, die eine FabricPool-Lizenz benötigen, z. B. Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud oder Alibaba Cloud Object Storage.

- * Clusterlizenzierte Cloud-Stufe Verwendet*

  Zeigt den Speicherplatz an, der von Daten im Cloud-Tier für Storage-Provider verwendet wird, die eine FabricPool Lizenz benötigen.

- **Verwendete Cluster-StorageGRID-Kapazität**

  Zeigt den Speicherplatz an, der von Daten im Cloud-Tier für Storage-Provider verwendet wird, die keine FabricPool Lizenz benötigen, z. B. StorageGRID.

Bericht über Kapazität und Auslastung aggregieren

Der Bericht zur Aggregatskapazität und -Auslastung ermöglicht es Ihnen, Informationen zur Kapazität und Auslastung von Aggregaten in einem Cluster anzuzeigen. Diese Informationen geben Ihnen die Möglichkeit, mögliche Kapazitätsrisiken zu verstehen und die konfigurierte, genutzte und nicht genutzte Kapazität von Aggregaten anzuzeigen.

Tabellarische Ansicht der Berichte für Kapazität und Auslastung des Aggregats

- * Cluster*

  Zeigt den Cluster-Namen an.

- **HA-Paar**

  Zeigt den HA-Paar-Wert an, der durch die Bildung von zwei Nodes ermittelt wird.

- * Aggregat*

Zeigt den Aggregatnamen an.

- **Datenkapazität (GB)**

  Zeigt die Gesamtkapazität der Daten an (genutzt plus verfügbar).

- **Genutzte Datenkapazität (GB)**

  Zeigt die genutzte Datenkapazität an.

- **Verwendete Daten %**

  Zeigt die genutzte Datenkapazität als Prozentsatz an.

- **Verfügbare Datenkapazität (GB)**

  Zeigt die verfügbare Datenkapazität an.

- * Verfügbare Daten %*

  Zeigt die verfügbare Datenkapazität als Prozentsatz an.

- * Tägliche Zuwachsrate %*

  Zeigt die Wachstumsrate an, die alle 24 Stunden im Volumen stattfindet.

- **Tage Bis Voll**

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor die volle Kapazität des Aggregats erreicht ist.

- **Space Full Threshold**

  Zeigt den Prozentsatz an, bei dem ein Aggregat voll ist.

- **Space Fast Voll Schwellenwert**

  Zeigt den Prozentsatz an, bei dem ein Aggregat fast voll ist.

- **Schwellenwert Der Wachstumsrate**

  Gibt an, dass die Wachstumsrate des Aggregats als normal angesehen wird, bevor das System ein ungewöhnliches Ereignis für die aggregierte Wachstumsrate generiert.

- **Schwellenwert Für Die Empfindlichkeit Der Wachstumsrate**

  Gibt den Faktor an, der auf die Standardabweichung der Wachstumsrate eines Volumens angewendet wird. Wenn die Wachstumsrate die faktorierte Standardabweichung überschreitet, wird ein ungewöhnliches Ereignis der Volumenwachstumsrate generiert.

- **Tage Bis Zur Vollständigen Schwelle**

  Gibt die Anzahl der verbleibenden Tage an, bevor die volle Kapazität des Aggregats erreicht ist.

- **Snapshot Reserve Gesamtkapazität (GB)**

Zeigt die Gesamtkapazität der Snapshot Reserve des Aggregats an.

- **Verwendete Snapshot-Reserve Kapazität (GB)**

  Zeigt den Speicherplatz an, der von Snapshot-Kopien aus der Snapshot-Reserve verwendet wird.

- **Snapshot Reserve Verwendet %**

  Zeigt die Menge an Speicherplatz an, die von Snapshot Kopien aus der Snapshot Reserve als Prozentsatz verwendet wird.

- **Snapshot Reserve verfügbare Kapazität (GB)**

  Zeigt die Menge an Speicherplatz an, die für Snapshot Kopien verfügbar ist.

- **Snapshot Reserve Verfügbar %**

  Zeigt die Menge an Speicherplatz, die für Snapshot Kopien verfügbar ist, als Prozentsatz an.

- **Snapshot Kopien Reserve Full Threshold**

  Gibt den Prozentsatz an, an dem ein Aggregat den gesamten reservierten Speicherplatz für Snapshot Kopien verbraucht hat.

- **Überengagierte Kapazität %**

  Zeigt die Überbelegung des Aggregats als Prozentsatz an.

- **Überbeplante Schwelle %**

  Zeigt den Prozentsatz an, zu dem ein Aggregat überbelegt ist.

- **Nahezu Überhöhte Schwelle %**

  Zeigt den Prozentsatz an, bei dem ein Aggregat fast überbelegt ist.

- **Typ**

  Zeigt den Aggregattyp an:

  - HDD
  - Hybrid

    Kombiniert HDDs und SSDs, aber Flash Pool wurde nicht aktiviert.

  - Hybrid (Flash Pool)

    Kombiniert HDDs und SSDs und ermöglicht die Aktivierung von Flash Pool.

  - SSD
  - SSD (FabricPool)

    Kombiniert SSDs mit einer Cloud-Tier

  - VMDisk (SDS)

Virtuelle Laufwerke innerhalb einer virtuellen Maschine

- VMDisk (FabricPool)

  Kombiniert virtuelle Festplatten mit einer Cloud-Tier

- LUN (FlexArray) bei Standardfestplatten und SSD-Festplatten ist diese Spalte leer, wenn auf dem überwachten Speichersystem eine ONTAP-Version vor 8.3 ausgeführt wird.

- **RAID-Typ**

  Zeigt den RAID-Konfigurationstyp an.

- **Gesamtzustand**

  Zeigt den aktuellen Status des Aggregats an.

- **SnapLock Typ**

  Gibt an, ob es sich um ein SnapLock- oder ein nicht-SnapLock-Aggregat handelt.

- **Cloud Tier verwendeter Speicherplatz (GB)**

  Zeigt die Datenmenge an, die aktuell im Cloud-Tier verwendet wird.

- * Cloud Tier*

  Zeigt den Namen des Cloud-Tiers an, als er von ONTAP erstellt wurde.

Bericht zur Volume-Kapazität und -Auslastung

Der Bericht zur Volume-Kapazität und -Auslastung ermöglicht eine Anzeige von Informationen zur Kapazität und Auslastung von Volumes in einem Cluster. Diese Informationen geben Ihnen die Möglichkeit, mögliche Kapazitätsrisiken zu verstehen und die konfigurierte, genutzte und nicht genutzte Kapazität von Aggregaten anzuzeigen. Darüber hinaus können Sie in dem Bericht Entscheidungen zur Aktivierung speicherplatzsparender Funktionen wie Deduplizierung und Thin Provisioning treffen.

Tabellarische Ansicht der Volume-Kapazität und Auslastung

- * Cluster*

  Zeigt den Cluster-Namen an.

- **Storage Virtual Machine**

  Zeigt den Namen der Storage Virtual Machine (SVM) an, die das Volume enthält.

- **Lautstärke**

  Zeigt den Namen des Volumes an.

- **Gesamtkapazität Der Daten**

Zeigt die Gesamtkapazität (genutzt plus verfügbar) in einem Volume an.

- **Genutzte Datenkapazität**

  Zeigt die genutzte Datenkapazität in einem Volume an.

- **Verwendete Daten %**

  Zeigt die verwendeten Daten in einem Volume in Prozent an.

- **Verfügbare Datenkapazität**

  Zeigt die verfügbare Datenkapazität in einem Volume an.

- * Verfügbare Daten %*

  Zeigt die verfügbare Datenkapazität in einem Volume als Prozentsatz an.

- * Tägliche Zuwachsrate %*

  Zeigt die Wachstumsrate an, die alle 24 Stunden im Volumen stattfindet.

- **Tage Bis Voll**

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

- **Space Full Threshold %**

  Gibt das Limit für das als voll betrachtete Volume an.

- **Space Fast Voll Schwellenwert %**

  Gibt das Limit für das Volumen an, das als fast voll betrachtet wird.

- **Wachstumsquote Schwellenwert %**

  Gibt an, dass die Wachstumsrate des Aggregats als normal angesehen wird, bevor das System ein ungewöhnliches Ereignis für die aggregierte Wachstumsrate generiert.

- **Schwellenwert Für Die Empfindlichkeit Der Wachstumsrate**

  Gibt den Faktor an, der auf die Standardabweichung der Wachstumsrate eines Volumens angewendet wird. Wenn die Wachstumsrate die faktorierte Standardabweichung überschreitet, wird ein ungewöhnliches Ereignis der Volumenwachstumsrate generiert.

- **Tage Bis Zur Vollständigen Schwelle**

  Gibt die Anzahl der verbleibenden Tage an, bevor die volle Kapazität erreicht wurde.

- **Snapshot-Überlauf %**

  Zeigt den Prozentsatz des Speicherplatzes an, der von den Snapshot Kopien verbraucht wird.

- **Verwendete Snapshot-Reserve Kapazität**

  Zeigt die Menge an Speicherplatz an, der von Snapshot Kopien im Volume verwendet wird.

- **Snapshot Reserve Verwendet %**

  Zeigt die Menge an Speicherplatz an, der von Snapshot Kopien im Volume in Prozent verwendet wird.

- **Snapshot Reserve Verfügbare Kapazität**

  Zeigt die Menge an Speicherplatz an, die für Snapshot Kopien im Volume verfügbar ist.

- **Snapshot Reserve Verfügbar %**

  Zeigt die Menge an Speicherplatz, die für Snapshot Kopien im Volume verfügbar ist, als Prozentsatz an.

- **Snapshot Reserve Gesamtkapazität**

  Zeigt die Gesamtkapazität der Snapshot Kopien im Volume an.

- **Snapshot Kopien Reservieren Voller Schwellenwert %**

  Gibt den Prozentsatz an, mit dem der für Snapshot Kopien reservierte Speicherplatz als voll betrachtet wird.

- **Schwellenwert Für Anzahl Der Snapshot-Kopien**

  Gibt die Anzahl der Snapshot Kopien auf einem Volume an, die als zu viele Kopien gelten.

- **Snapshot Kopiert Tage Bis Vollschwellenwert**

  Gibt die Anzahl der Tage an, die noch verbleiben, bevor der für Snapshot Kopien reservierte Speicherplatz mit der vollen Kapazität erreicht wird.

- * Anzahl Inodes*

  Zeigt die Anzahl der Inodes im Volume an.

- **Auslastung Von Nodes %**

  Gibt den Prozentsatz des Inode-Speicherplatzes an, der im Volume verwendet wird.

- **Inodes Full Threshold**

  Gibt den Prozentsatz an, bei dem ein Volume als verbraucht wurde, alle Inodes verbraucht zu haben.

- **Inodes Fast Volle Schwelle**

  Gibt den Prozentsatz an, bei dem ein Volume als den Großteil seiner Inodes verbraucht wurde.

- **Quote Zugesagt Kapazität**

  Zeigt den Speicherplatz an, der in den Volumes reserviert ist.

- **Quote Überzuviel Kapazität**

  Zeigt die Menge an Speicherplatz an, die verwendet werden kann, bevor das System das überzustrapaziertes Ereignis für die Volume-Quota generiert.

- **Überschreitungsschwellenwert Für Quote %**

Gibt den Prozentsatz an, bei dem das Volumen fast überbelegt ist.

- **Quote Nahezu Überfordert Schwellenwert %**

  Gibt den Prozentsatz an, bei dem der Volume-Speicherplatz fast überbelegt ist.

- **Snapshot Autodelete**

  Zeigt an, ob das automatische Löschen von Snapshot Kopien aktiviert oder deaktiviert ist.

- **Deduplizierung**

  Zeigt an, ob die Deduplizierung für das Volume aktiviert oder deaktiviert ist.

- **Deduplizierungseinsparungen**

  Anzeige der Menge an Speicherplatz, die in einem Volume durch Deduplizierung eingespart wurde

- **Komprimierung**

  Zeigt an, ob die Komprimierung für das Volume aktiviert oder deaktiviert ist.

- **Komprimierung Raumeinsparungen**

  Zeigt die Menge an Speicherplatz an, die in einem Volume mithilfe der Komprimierung eingespart wurde.

- **Caching-Richtlinie**

  Zeigt die Caching-Richtlinie an, die dem ausgewählten Volume zugeordnet ist. Diese Richtlinie gibt Informationen darüber, wie Flash Pool Caching für das Volume stattfindet. Weitere Informationen zu Caching-Richtlinien finden Sie auf der Seite „Systemzustand/Volumes-Inventar“.

- **Cache-Aufbewahrungspriorität**

  Zeigt die Priorität an, die für die Aufbewahrung von zwischengespeicherten Pools verwendet wird.

- **Thin Provisioning**

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

- **Autogrow**

  Zeigt an, ob das FlexVol-Volume automatisch wächst, wenn es über keinen freien Speicherplatz verfügt.

- * Raumgarantie*

  Zeigt die FlexVol-Lautstärkeregelung an, wenn ein Volume freie Blöcke aus einem Aggregat entfernt.

- **Bundesland**

  Zeigt den Status des Volumes an, das exportiert wird.

- **SnapLock Typ**

  Gibt an, ob es sich um ein SnapLock- oder ein nicht-SnapLock-Volume handelt.

- **Ablaufdatum**

  Das Verfalldatum des SnapLock.

- **Tiering-Richtlinie**

  Wenn dieses Volume auf einem FabricPool-fähigen Aggregat implementiert wird, wird die für das Volume festgelegte Tiering-Richtlinie angezeigt.

Bericht zur Kapazität und Auslastung von qtree

Mit dem Kapazitäts- und Auslastungsbericht von Qtree können Sie die Kapazität und Auslastung der qtrees des Systems analysieren, um mögliche Risiken, die aufgrund der reduzierten Cluster-Kapazität auftreten können, zu verstehen.

Die tabellarische Ansicht des Berichts zur Kapazität und Auslastung von qtree

- * Cluster*

  Zeigt den Namen des Clusters an, der den qtree enthält.

- **Storage Virtual Machine**

  Zeigt den Namen der Storage Virtual Machine (SVM) an, die den qtree enthält.

- **Lautstärke**

  Zeigt den Namen des Volumes an, das den qtree enthält.

- **Qtree**

  Zeigt den Namen des qtree an.

- **Quotentyp**

  Gibt an, ob das Kontingent für einen Benutzer, eine Benutzergruppe oder einen qtree ist.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Für jeden Benutzer und jede Benutzergruppe werden mehrere Zeilen angezeigt. Wenn der Kontingenttyp qtree ist, wird *Not anwendbare* angezeigt. Wenn das Kontingent nicht festgelegt ist, ist die Spalte leer.

- **Verwendete Festplatte %**

  Zeigt den Prozentsatz des verwendeten Festplattenspeichers an. Wenn ein Festplattenlimit festgelegt ist, basiert dieser Wert auf dem Festplattenlimit. Wenn das Kontingent ohne Festplattenlimit festgelegt wird, basiert der Wert auf dem Volume-Datenraum. Wenn das Kontingent nicht gesetzt ist oder wenn die Quoten auf dem Volumen liegen, zu dem der qtree gehört, dann wird *nicht anwendbar* angezeigt.

- **Festplatten-Hard-Limit**

  Zeigt den maximalen Festplattenspeicher an, der für den qtree zugewiesen ist. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht wird und keine weiteren Festplattenschreibvorgänge mehr zulässig sind. Der Wert wird als *Unlimited* angezeigt, wenn das Kontingent ohne eine

Festplattenbegrenzung festgelegt ist, wenn die Quote nicht festgelegt ist, oder wenn die Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört.

- **Soft Limit Für Festplatten**

  Zeigt den für den qtree zugewiesenen Festplattenspeicher an, bevor ein Warnereignis generiert wird. Der Wert wird als *Unlimited* angezeigt, wenn das Kontingent ohne eine feste Plattengrenze eingestellt ist, wenn die Quote nicht festgelegt ist, oder wenn die Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im qtree verwendeten Dateien an. Wenn das harte Limit für die Datei festgelegt ist, basiert dieser Wert auf dem harten Limit der Datei. Der Wert wird als *not anwendbares* angezeigt, wenn das Kontingent nicht gesetzt ist, oder wenn das Kontingent ohne eine feste Dateigrenze festgelegt ist, oder wenn die Quoten auf dem Volumen deaktiviert sind, zu dem qtree gehört.

- **Harte Dateibegrenzung**

  Zeigt das endgültige Limit für die Anzahl der Dateien an, die auf den qtrees zulässig sind. Der Wert wird als *Unlimited* angezeigt, wenn das Kontingent ohne eine harte Dateibegrenzung festgelegt ist, wenn die Quote nicht festgelegt ist, oder wenn die Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört.

- **Soft Limit Für Dateien**

  Zeigt den Softlimit für die Anzahl der Dateien an, die auf qtrees zulässig sind. Der Wert wird als *Unlimited* angezeigt, wenn das Kontingent ohne eine Datei-Softlimit gesetzt wird, wenn das Kontingent nicht gesetzt ist, oder wenn die Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört.

Ereignisbericht

Im Ereignisbericht können Sie Informationen zu Ereignistrends über einen bestimmten Zeitraum anzeigen. Anhand dieser Informationen können Sie aktuelle Aktivitäten mit früheren betrieblichen Aktivitäten vergleichen, z. B. Konfigurationsänderungen, Upgrades usw. Die Informationen helfen Ihnen auch, ausstehende Ereignisse zu bestimmen.

Diagrammansicht des Ereignisberichts

Der Ereignisbericht wird in zwei Formaten angezeigt:

- Diagrammansicht des Ereignisberichts
- Tabellarische Ansicht Ereignisbericht

Das Ereignisdiagramm wird in zwei Formaten angezeigt:

- Ereignisse Severity Trend (Alle offenen Ereignisse)
- Trend Zum Ereignisstatus

Das Diagramm zeigt die Schweregrade für alle geöffneten Ereignisse innerhalb eines Zeitraums an. Auf der vertikalen Achse (y) wird eine Anzahl von Ereignissen angezeigt, und das Datum wird auf der horizontalen Achse (x) angezeigt. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Punkt positionieren. Die Details zeigen den Schweregrad des Ereignisses, die Anzahl der Ereignisse des bestimmten Schweregrads und das Datum des Ereignisses an.

Die angezeigten Schweregrade sind kritisch, Fehler und Warnung. Die Ereignisabtrennungen werden durch verschiedene Farben unterschieden. Es kann die gleiche Anzahl von Ereignissen am gleichen Datum in verschiedenen Status sein.

- * Anzahl*

  Zeigt eine Anzahl von Ereignissen an.

- **Datum**

  Zeigt das Datum an. Die x-Achse zeigt Daten von dem Zeitpunkt an, zu dem das Ereignis bis zum aktuellen Datum aufgetreten ist. Sie können auf das Diagramm klicken und vergrößern, um weitere Informationen zu erhalten.

Das Diagramm zeigt den Trend des Ereignisstatus pro Tag über einen bestimmten Zeitraum. Auf der vertikalen Achse (y) wird eine Anzahl von Ereignissen angezeigt, und das Datum wird auf der horizontalen Achse (x) angezeigt. Die Details zeigen den Ereignisstatus, die Anzahl der Ereignisse des spezifischen Status und das Datum des Ereignisses an.

Der Ereignisstatus lautet „Neu“, „bestätigt“ und „gelöst“. Der Ereignisstatus wird durch unterschiedliche Farben unterschieden.

Das Diagramm zeigt die täglich neu erzeugten Ereignisse auf kumulativer Basis in einem Balkendiagramm, dargestellt in grüner Farbe. Die Anzahl der bestätigten und gelösten Ereignisse wird angezeigt, als und wann sie täglich anerkannt und gelöst werden.

In den Diagrammen stehen eine Zoom-Funktion zur Verfügung. Sie können diese Funktion verwenden, um einen bestimmten Punkt in der Grafik zu vergrößern, um mehr Klarheit zu erzielen.

- **Quelle**

  Zeigt die Quelle eines Ereignisses an.

- **Status**

  Zeigt den Schweregrad des Ereignisses an. Sie können diese Spalte filtern, um Ereignisse mit einem bestimmten Schweregrad anzuzeigen. Die Schweregrade des Ereignisses sind kritisch, Fehler oder Warnung.

- **Bundesland**

  Zeigt den Ereignisstatus an: Neu, bestätigt, aufgelöst oder veraltet. Sie können diese Spalte filtern, um Ereignisse eines bestimmten Status anzuzeigen.

- **Veranstaltung**

  Zeigt die Ereignisnamen an.

- **Auslösezeit**

  Zeigt die Uhrzeit an, zu der das Ereignis generiert wurde. Sowohl die Uhrzeit als auch das Datum werden angezeigt.

- **Tage Herausragend**

Zeigt die Anzahl der Tage zwischen einem Ereignis und seiner Auflösung oder Bezeichnung als veraltet an.

- **Quelltyp**

  Zeigt den Objekttyp (z. B. Storage Virtual Machine (SVM), Volume oder qtree) an, mit dem das Ereignis verknüpft ist.

- * Datenpriorität*

  Zeigt den Anmerkungstyp an, der auf der Priorität der Daten des Speicherobjekts basiert.

- **Impact Level**

  Zeigt an, ob das Ereignis als Vorfall, Risiko oder Information kategorisiert ist.

- **Aufprallbereich**

  Zeigt an, ob es sich um ein Kapazitäts-, Verfügbarkeits-, Performance-, Schutz- oder Konfigurationsereignis handelt.

- * Zugewiesen Zu*

  Zeigt den Namen des Benutzers an, dem das Ereignis zugeordnet ist.

- **Zugewiesene Zeit**

  Zeigt die Zeit an, zu der das Ereignis einem Benutzer zugewiesen wurde.

- **Hinweise**

  Zeigt die Anzahl der Notizen an, die für ein Ereignis hinzugefügt werden.

- * Bestätigt Durch*

  Zeigt den Namen des Benutzers an, der das Ereignis bestätigt hat. Das Feld ist leer, wenn das Ereignis nicht bestätigt wird.

- * Quittierte Zeit*

  Zeigt die Zeit an, die seit der Quittierung des Ereignisses verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, wann das Ereignis bestätigt wurde.

- * Gelöst Von*

  Zeigt den Namen des Benutzers an, der das Ereignis gelöst hat. Das Feld ist leer, wenn das Ereignis nicht aufgelöst wird.

- * Zeit Gelöst*

  Zeigt die Zeit an, die seit dem Auflösen des Ereignisses verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, wann das Ereignis aufgelöst wurde.

- **Veraltete Zeit**

  Zeigt die Zeit an, zu der der Status des Ereignisses veraltet wurde.

Cluster-Inventory-Bericht

Cluster-Bestandsbericht enthält Informationen zu verfügbaren Ressourcen für Cluster-Komponenten, um mögliche Risiken zu verstehen, die durch unzureichende Ressourcen verursacht werden.

Cluster-Bestandsbericht – tabellarische Ansicht

- * Cluster*

  Zeigt den Namen des Clusters an.

- **HA-Paar**

  Zeigt den HA-Paar-Wert an, der durch die Bildung von zwei Nodes ermittelt wird.

- **Knoten**

  Zeigt den Namen der Nodes an.

- **Modell**

  Zeigt den Namen des Modells an.

- **Betriebssystemversion**

  Zeigt die Version des verwendeten ONTAP an.

- * All Flash Optimiert*

  Zeigt an, ob ein Node nur Solid State Drives (SSDs) unterstützt.

- **Seriennummer**

  Zeigt die Seriennummer des Node an.

- **Firmware-Version**

  Zeigt die Firmware-Version des Node an.

- **SVM-Anzahl**

  Zeigt die Anzahl der SVM an, die vom Cluster enthalten ist.

- * FC Port Anzahl*

  Zeigt die Anzahl der vom Node enthaltenen FC-Ports an.

- **FCoE Port Anzahl**

  Zeigt die Anzahl der vom Node enthaltenen FCoE-Ports an.

- * Anzahl Ethernet-Ports*

  Zeigt die Anzahl der vom Node enthaltenen ethernet-Ports an.

- * Anzahl Der Flash-Karten*

  Zeigt die Anzahl der auf den Nodes in Ihrem Datacenter installierten Flash-Karten an, sodass Sie auf mögliche Probleme überwachen können.

- **Flash-Kartengröße (GB)**

  Zeigt die Größe der auf den Nodes installierten Flash-Karten an.

- * Anzahl Festplatten-Shelfs*

  Zeigt die Anzahl der vom Node enthaltenen Platten-Shelfs an.

- * Datenträgeranzahl*

  Zeigt die Anzahl der Festplatten in einem Node an.

Bericht NFS Exporte

Der Bericht NFS Exports ermöglicht es Ihnen, Informationen über NFS-Exportrichtlinien und die zugehörigen Regeln für Volumes in Ihrem Storage-System zu prüfen.

Tabellarische Ansicht des NFS Exports-Berichts

- * Cluster*

  Zeigt den Namen des Clusters an.

- **Storage Virtual Machine**

  Zeigt den Namen der SVM mit NFS-Exportrichtlinien an.

- **Lautstärke**

  Zeigt den Namen des Volumes mit NFS-Exportrichtlinien an.

- **Qtree**

  Zeigt den Namen des qtree auf einem Volume mit NFS-Exportrichtlinien an.

- **Volume-Status**

  Zeigt den aktuellen Status des Volumes an. Der Status kann Offline, Online oder beschränkt sein.

  - Offline

    Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

  - Online

    Lese- und Schreibzugriff auf das Volume ist zulässig.

  - Eingeschränkt

    Begrenzte Vorgänge, wie etwa die Paritätsrekonstruktion, sind zulässig, der Datenzugriff jedoch nicht.

- **Verbindungspfad**

  Zeigt den Pfad an, auf dem das Volume angehängt ist.

- **Verbindungspfad Aktiv**

  Zeigt an, ob der Pfad für den Zugriff auf das bereitgestellte Volume aktiv oder inaktiv ist.

- **Exportrichtlinie**

  Zeigt die Regeln an, die die Zugriffsberechtigung für exportierte Volumes definieren.

- **Regelindex**

  Zeigt die Regeln an, die der Exportrichtlinie zugeordnet sind, z. B. die Authentifizierungsprotokolle und die Zugriffsberechtigung.

- **Zugriffsprotokolle**

  Zeigt die Protokolle an, die für die Regeln für die Exportrichtlinie aktiviert sind.

- * Client Match*

  Zeigt die Clients an, die über die Berechtigung zum Zugriff auf Daten auf den Volumes verfügen.

- **Nur-Lese-Zugriff**

  Zeigt das Authentifizierungsprotokoll an, das zum Lesen von Daten auf den Volumes verwendet wird.

- **Schreibzugriff Lesen**

  Zeigt das Authentifizierungsprotokoll an, das zum Lesen oder Schreiben von Daten auf den Volumes verwendet wird.

- **Sicherheitsstil**

  Zeigt die Zugriffsberechtigung für Volumes an, die exportiert werden. Der Sicherheitsstil kann UNIX, Unified, NTFS oder gemischt sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume haben UNIX Berechtigungen.

  - Virtualisierung

    Dateien und Verzeichnisse im Volume weisen einen einheitlichen Sicherheitsstil auf.

  - NTFS (CIFS-Clients)

    Dateien und Verzeichnisse im Volume haben Windows NTFS-Berechtigungen.

  - Gemischt

    Dateien und Verzeichnisse auf dem Volume können entweder UNIX Berechtigungen oder Windows NTFS Berechtigungen haben.

- **Unix-Erlaubnis**

  Zeigt die UNIX-Berechtigungsbits in einem Oktal-String-Format an, das für die exportierten Volumes festgelegt ist. Es ähnelt den Berechtigungsbits im UNIX-Stil.

SVM-Inventarbericht

Mit diesem SVM-Bestandsbericht können Sie SVM-Volume-Konfigurationsgrenzwerte und allgemeine Integritätswerte analysieren, um Risiken für die zukünftige Storage-Verfügbarkeit zu ermitteln.

Tabellenansicht des SVM-Bestandsberichts

- * Cluster*

  Zeigt den Namen des Clusters an, der die SVM enthält.

- **Storage Virtual Machine**

  Zeigt den Namen der SVM an.

- **Bundesland**

  Zeigt den aktuellen Administrationsstatus der SVM an. Der Status kann ausgeführt, angehalten, gestartet, angehalten, beendet, nicht zugeordnet, Initialisierung oder Löschen.

- **Volumenzahl**

  Zeigt die Anzahl der Volumes an, die von der SVM enthalten sind.

- **Maximal Zulässige Volumen**

  Zeigt die maximal zulässigen Volumes an, die auf der SVM konfiguriert werden können.

- **Root Volume**

  Zeigt den Namen des Root-Volumes der SVM an.

- **Erlaubte Protokolle**

  Zeigt den Typ der Protokolle an, die für die SVM konfiguriert werden können.

- **DNS-Domäne**

  Zeigt den DNS-Domänennamen an.

- **NIS-Domäne**

  Zeigt den NIS-Domänennamen (Network Information Service) an. Diese Spalte ist leer, wenn der NIS-Server (Network Information Service) deaktiviert oder nicht konfiguriert ist.

- **LDAP aktiviert**

  Zeigt an, ob das LDAP-Protokoll aktiviert ist oder nicht.

- **Name Service Switch**

  Zeigt den Informationstyp an, der von Hosts erfasst wurde. Mögliche Werte sind Datei, LDAP oder NIS.

Bericht zur Konfiguration der Volume-Datensicherung

Der Bericht zur Konfiguration der Volume-Datensicherung ermöglicht Ihnen, die ungesicherten Volumes und Storage Virtual Machines (SVMs) anzuzeigen, die in einem Node oder Cluster verwendet werden. Diese Informationen geben Ihnen einen Überblick über die Datensicherungsrisiken für Ihr System und zeigen die Details der geschützten Volumes und ungeschützten Volumes in Ihrem System an.

Der Bericht Volume Data Protection Configuration wird in zwei Formaten angezeigt:

- Diagramm „geschützte und ungesicherte Volumes“
- Tabellarische Ansicht der ungeschützten Volume-Daten

Diagramm „geschützte und ungesicherte Volumes“

Zeigt den relativen Prozentsatz der geschützten Volumes und der ungesicherten Volumes im System an.

Tabellarische Ansicht der ungeschützten Volume-Daten

- * Cluster*

  Zeigt den Cluster-Namen an.

- **Storage Virtual Machine**

  Zeigt den Namen der Storage Virtual Machine (SVM) an, die das Volume enthält.

- **Lautstärke**

  Zeigt den Namen des Volumes an.

- **Datenkapazität (GB)**

  Zeigt die Gesamtkapazität (genutzt plus verfügbar) in GB an.

- **Genutzte Datenkapazität (GB)**

  Zeigt die genutzte Datenkapazität (in GB) an.

- **Verwendete Daten %**

  Zeigt die genutzte Datenkapazität als Prozentsatz an.

- **Verfügbare Datenkapazität (GB)**

  Zeigt die verfügbare Datenkapazität (in GB) an.

- * Verfügbare Daten %*

  Zeigt die verfügbare Datenkapazität als Prozentsatz an.

- **Verwendete Snapshot-Reserve Kapazität (GB)**

  Zeigt die Menge an Speicherplatz an, die von Snapshot Kopien aus der Snapshot Reserve (in GB) verwendet wird.

- **Snapshot Reserve Verwendet %**

  Zeigt die Menge an Speicherplatz an, die von Snapshot Kopien aus der Snapshot Reserve als Prozentsatz verwendet wird.

- **Snapshot Reserve verfügbare Kapazität (GB)**

  Zeigt die Menge an Speicherplatz an, die für Snapshot Kopien verfügbar ist (in GB).

- **Snapshot Reserve Verfügbar %**

  Zeigt die Menge an Speicherplatz an, die in Prozent für Snapshot Kopien verfügbar ist.

- **Snapshot Reserve Gesamtkapazität (GB)**

  Zeigt die Gesamtkapazität der Snapshot-Reserve des Aggregats (in GB) an.

- **Tage Bis Voll**

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor die volle Kapazität des Aggregats erreicht ist.

- **Space Full Threshold %**

  Zeigt den Prozentsatz an, bei dem ein Aggregat voll ist.

- **Space Fast Voll Schwellenwert %**

  Zeigt den Prozentsatz an, bei dem ein Aggregat fast voll ist.

- * Tägliche Zuwachsrate %*

  Zeigt die Wachstumsrate an, die alle 24 Stunden im Volumen stattfindet.

- **Gesamtanzahl Der Inodes**

  Zeigt die Gesamtanzahl der Inodes im Volume an.

- * Auslastung Des Ikens*

  Gibt den Inode-Speicherplatz an, der im Volume verwendet wird.

- **Quote Zugesagt Kapazität**

  Zeigt den Speicherplatz an, der in den Volumes reserviert ist.

- **Quote überzuviel Kapazität (GB)**

  Zeigt den Speicherplatz an, der verwendet werden kann (in GB), bevor das System das Ereignis Volume Quota Overmited generiert.

- **Snapshot Autodelete**

  Zeigt an, ob das automatische Löschen von Snapshot Kopien aktiviert oder deaktiviert ist.

- **Deduplizierung**

  Zeigt an, ob die Deduplizierung für das Volume aktiviert oder deaktiviert ist.

- **Deduplizierungseinsparungen (GB)**

  Zeigt die Menge an Speicherplatz an, die in einem Volume mithilfe der Deduplizierung eingespart wird (in GB).

- **Komprimierung**

  Zeigt an, ob die Komprimierung für das Volume aktiviert oder deaktiviert ist.

- **Komprimierung Raumeinsparungen (GB)**

  Zeigt die Menge an Speicherplatz an, die durch Komprimierung (in GB) in einem Volume gespeichert wird.

- **Thin Provisioning**

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

- **Autogrow**

  Zeigt an, ob das FlexVol-Volume automatisch wächst, wenn es über keinen freien Speicherplatz verfügt.

- * Raumgarantie*

  Zeigt die FlexVol-Lautstärkeregelung an, wenn ein Volume freie Blöcke aus einem Aggregat entfernt.

- **Bundesland**

  Zeigt den Status des Volumes an, das exportiert wird.

- **SnapLock Typ**

  Gibt an, ob es sich um ein SnapLock- oder ein nicht-SnapLock-Volume handelt.

- **Ablaufdatum**

Bestandsbericht zu Volume-Beziehungen

Der Bericht zum Bestand von Volume-Beziehungen ermöglicht Ihnen die Analyse der Details zum Storage-Inventar in einem Cluster, die Analyse des für Volumes erforderlichen Schutzes sowie die Filterung der Volume-Details basierend auf den Fehlerquellen, Mustern und Zeitplänen.

Der Bericht „Bestandsaufnahme der Volume-Beziehungen“ wird in zwei Formaten angezeigt:

- Diagramm „SnapMirror Beziehungen“ und „SnapVault Beziehungen“
- Berichtstabellenansicht „Volume Relationships Inventory“

Tortendiagramme mit SnapMirror und SnapVault

Zeigt die Konfigurationsdetails der Volume-Beziehungen an, die im Storage-System vorhanden sind.

Bestandsinformationen zu Volume-Beziehungen

- **Gesundheit Der Beziehung**

  Zeigt den Systemzustand der Beziehung des Clusters an.

- * Beziehungsstatus*

  Zeigt den Mirror-Status der SnapMirror Beziehung an.

- **Transferstatus**

  Zeigt den Status der SnapMirror-Beziehung an.

- **Lag-Status**

  Zeigt den Verzögerungsstatus des Volumes an.

- * Quellcluster*

  Zeigt den Namen des Quell-Clusters für die SnapMirror Beziehung an.

- **Quell-SVM**

  Zeigt den Namen der Quell-Storage Virtual Machine (SVM) für die SnapMirror Beziehung an.

- **Quellvolumen**

  Zeigt den Namen des Quell-Volume für die SnapMirror Beziehung an.

- **Zielcluster**

  Zeigt den Namen des Ziel-Clusters für die SnapMirror Beziehung an.

- **Ziel-SVM**

  Zeigt den Namen der Ziel-Storage Virtual Machine (SVM) für die SnapMirror Beziehung an.

- **Zielvolumen**

  Zeigt den Namen des Ziel-Volume für die SnapMirror Beziehung an.

- **Beziehungstyp**

  Zeigt alle Beziehungstypen an, einschließlich SnapMirror oder SnapVault.

- **Letzte Erfolgreiche Aktualisierungszeit**

  Zeigt die Zeit des letzten erfolgreichen SnapMirror oder SnapVault Vorgangs an.

- **Letzte Transferdauer (Std.)**

Zeigt die Zeit an, die für den letzten Datentransfer benötigt wurde.

- **Letzte Transfergröße (MB)**

  Zeigt die Größe der letzten Datenübertragung in Byte an.

- **Endzeit Der Letzten Übertragung**

  Zeigt die Zeit an, zu der der letzte erfolgreiche SnapMirror oder SnapVault Vorgang abgeschlossen wurde.

- * Ungesunde Gründe*

  Der Grund, warum die Beziehung in einem ungesunden Zustand ist.

- **Dauer (Std.)**

  Zeigt die Zeitspanne an, die die Daten auf dem Spiegel hinter der Quelle hinkt.

- **Version Flexible Replikation**

  Zeigt entweder Ja, Ja mit Sicherungsoption oder Keine an.

Bericht „Volume Transfer Status“ (Historischer Bericht)

Im Bericht Volume Transfer Status (Historical) können Sie die Trends bei der Volume-Übertragung über einen bestimmten Zeitraum analysieren. Sie können den Bericht so konfigurieren, dass der Transferstatus des Volumes für ein bestimmtes Zeitintervall angezeigt wird. Der Bericht zeigt außerdem an, ob die Volume-Übertragung erfolgreich oder fehlgeschlagen ist.

Der Bericht zum Volume Transfer Status (Historical) wird in zwei Formaten angezeigt:

- Liniendiagramm für Volume Transfer Status
- Berichtstabellen für Volume Transfer Status (Historical)

Liniendiagramm für Volume Transfer Status

Das Liniendiagramm zeigt die Details der Volume-Übertragung an, indem die Transferanzahl anhand des Datums gezeichnet wird. Sie können auch anzeigen, ob eine bestimmte Volume-Übertragung erfolgreich oder fehlgeschlagen ist.

Tabellenansicht Volume Transfer Status

- **Quellcluster-Name**

  Zeigt den Quellcluster-Namen an.

- **Quell-SVM**

  Zeigt den Namen der Storage Virtual Machine (SVM) an.

- **Name Des Quellvolumens**

  Zeigt den Namen des Quell-Volumes an.

- **Zielcluster-Name**

  Zeigt den Ziel-Cluster-Namen an.

- **Ziel-SVM**

  Zeigt den Namen der Ziel-SVM an.

- **Zielvolumenname**

  Zeigt den Namen des Zieldatenträgers an.

- **Operationsergebnis**

  Zeigt an, ob die Volume-Übertragung erfolgreich war.

- **Startzeit**

  Zeigt die Startzeit der Volume-Übertragung an.

- **Endzeit**

  Zeigt die Endzeit der Volume-Übertragung an.

- **Übertragungsdauer (hh:mm:ss)**

  Zeigt die Zeit an, die für die Durchführung der Volume-Übertragung benötigt wurde (in Stunden).

- **Transfergröße (MB)**

  Zeigt die Größe (in MB) des übertragenen Volumes an.

- **Operationstyp**

  Zeigt den Typ der Volume-Übertragung an.

Bericht „Volume Transfer Rate“ (Historical)

Der Bericht zur Volume-Übertragungsrate (Historical) ermöglicht es Ihnen, die Menge des täglich übertragenen Datenvolumens zu analysieren. Der Bericht enthält außerdem Details zu den täglichen Volume-Transfers und die Zeit, die für den Abschluss des Transfervorgangs erforderlich ist.

Der Bericht zur Volumenübertragungsrate (Historischer Bericht) wird in zwei Formaten angezeigt:

- Balkendiagramm für Volumenübertragungsraten
- Tabellenansicht Volumenübertragungsrate

Balkendiagramm für Volumenübertragungsraten

Zeigt die Details der Übertragungsrate des Volumes an, indem die Gesamtübertragungsgröße mit der Anzahl der Stunden verglichen wird. Sie können auch die Details der Datenmenge anzeigen, die täglich übertragen wird.

Tabellenansicht Volumenübertragungsrate

- **Gesamtübertragungsgröße (GB)**

  Zeigt die Gesamtgröße der Volume-Übertragung in Gigabyte an.

- **Tag**

  Zeigt den Tag an, an dem die Volume-Übertragung initiiert wurde.

- **Endzeit**

  Zeigt die Endzeit der Volume-Übertragung mit dem Datum an.

Dialogfeld „Bericht planen“

Sie können die zu erstellenden Berichte in einer bestimmten Frequenz im Dialogfeld Bericht planen, die wiederholt erstellt werden sollen. Der Bericht wird per E-Mail an einen oder mehrere Benutzer gesendet, die im Dialogfeld Bericht planen angegeben sind.

Eigenschaften

Sie können einen Bericht planen, indem Sie Eigenschaften wie die E-Mail-Adresse des Benutzers, das Format des Berichts und die Häufigkeit, mit der der Bericht generiert wird, angeben.

- **Verwendung Eines Vorhandenen Zeitplans**
  - **Terminplanname**

    Zeigt alle vorhandenen Planungsnamen an. Hier können Sie einen bestehenden Zeitplan für Ihre Berichte auswählen.

- **Neuer Zeitplan Erstellen**
  - **Terminplanname**

    Ermöglicht die Eingabe des Planungsnamens beim Erstellen eines neuen Zeitplans.

  - * Empfänger-E-Mail-Adresse*

    Gibt die E-Mail-Adresse des Benutzers an den der Bericht gesendet werden soll an. Sie können einen oder mehrere Einträge angeben, getrennt durch Kommas. Dies ist ein Pflichtfeld.

  - **Berichtsformat**

    Gibt das Format an, in dem der Bericht geplant werden soll. Die Option *PDF* ist standardmäßig ausgewählt.

  - **Frequenz**

    Gibt die Häufigkeit an, mit der der Bericht geplant werden soll. Die Option *hourly* ist standardmäßig ausgewählt.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Zeitplan**

  Plant den Bericht mit der gespeicherten oder aktualisierten Vorlage und schließt das Dialogfeld Bericht planen.

- **Abbrechen**

  Schließt das Dialogfeld Bericht planen, während eine Meldung angezeigt wird, um die Vorlage für Planungsberichte zu speichern.

Dialogfeld „Bericht freigeben“

Sie können einen Bericht per E-Mail an einen oder mehrere Benutzer freigeben. Nachdem Sie einen Bericht angepasst haben, müssen Sie die Änderungen speichern, bevor Sie den Bericht freigeben, um sicherzustellen, dass die Änderungen angezeigt werden.

Eigenschaften

Sie können einen Bericht freigeben, indem Sie Eigenschaften wie die E-Mail-Adresse des Benutzers, Betreff der E-Mail und das Format des Berichts angeben.

- * Empfänger-E-Mail-Adresse*

  Gibt die E-Mail-Adresse des Benutzers an, an den der Bericht weitergegeben werden soll. Sie können einen oder mehrere Einträge angeben, getrennt durch Kommas. Dies ist ein Pflichtfeld.

- **Betreff**

  Gibt den Betreff der E-Mail an. Standardmäßig wird der Name des Berichts angezeigt.

- **Berichtsformat**

  Gibt das Format an, in dem der Bericht gemeinsam genutzt werden soll. Die Option *PDF* ist standardmäßig ausgewählt. Wenn das XHTML-Format ausgewählt ist, öffnen Sie den Bericht, der per E-Mail über einen unterstützten Webbrowser gesendet wird.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Anteil**

  Teilt den Bericht mit der gespeicherten Konfiguration und schließt das Dialogfeld Bericht freigeben.

- **Abbrechen**

  Schließt das Dialogfeld Bericht freigeben, während eine Meldung angezeigt wird, um die Berichtskonfiguration zu speichern.

Dialogfeld „Berichtszeitpläne verwalten“

Sie können vorhandene Berichtspläne anzeigen, ändern oder löschen und neue Zeitpläne für Ihre Berichte über das Dialogfeld Berichtszeitpläne verwalten hinzufügen.

Eigenschaften

Sie können einen vorhandenen Zeitplan auswählen oder einen neuen Zeitplan für Ihre Berichte erstellen. Sie können Ihre Berichtspläne anzeigen, ändern oder löschen.

- **Linker Fensterbereich**
  - **Terminplanname**

    Zeigt die vorhandenen Zeitpläne an. Wenn Sie auf einen beliebigen Zeitplan klicken, können Sie die Terminplandetails im rechten Fensterbereich anzeigen. Bei der ersten Anmeldung sind keine Zeitpläne vorhanden.

  - **Zeitplan Hinzufügen**

    Zeigt das neue Planungsformular im rechten Fensterbereich an. Sie können jetzt einen neuen Zeitplan hinzufügen.

- **Rechter Fensterbereich**
  - **Terminplanname**

    Zeigt den Planungsnamen an.

  - * Empfänger-E-Mail-Adresse*

    Zeigt die E-Mail-Adresse des Benutzers an den der Bericht gesendet werden muss. Sie können mehrere E-Mail-Adressen eingeben, die durch Kommas getrennt sind.

  - **Berichtsformat**

    Zeigt das Format an, in dem der Bericht dargestellt werden muss. Die PDF-Option ist als Standardreport-Format ausgewählt. Wenn das XHTML-Format ausgewählt ist, öffnen Sie den Bericht, der per E-Mail über einen unterstützten Webbrowser gesendet wird.

  - **Frequenz**

    Zeigt die Häufigkeit an, mit der der Bericht geplant ist.

  - **Kategorie Melden**

    Zeigt die Gruppen der Berichtskategorie an. Wenn Sie eine Berichtskategorie aus der Liste auswählen, werden in der Spalte Verfügbare Berichte die Berichte angezeigt, die zu dieser Berichtskategorie gehören.

  - **Verfügbare Berichte**

    Zeigt nur die Berichte an, die zur ausgewählten Berichtskategorie gehören.

  - **Ausgewählte Berichte**

    Zeigt die ausgewählten Berichte an, auf die Sie den Zeitplan anwenden möchten. Sie können die

gewünschten Berichte in der Spalte Verfügbare Berichte auswählen. Es muss mindestens ein Bericht ausgewählt werden

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Zeitplan Hinzufügen**

  Ermöglicht Ihnen das Hinzufügen eines neuen Zeitplans.

- **Zeitplan Löschen**

  Ermöglicht das Löschen des aktuell angezeigten Zeitplans. Wenn Sie einen neuen Zeitplan erstellen, ist diese Schaltfläche nicht verfügbar.

- **Speichern**

  Speichert den angezeigten, geänderten oder hinzugefügten Zeitplan.

- **Speichern und Schließen**

  Speichert den angezeigten, geänderten oder hinzugefügten Zeitplan und schließt das Dialogfeld Berichtspläne verwalten.

- **Abbrechen**

  Schließt das Dialogfeld Berichtszeitpläne verwalten, während eine Meldung angezeigt wird, die den Zeitplan speichern soll.

Dialogfeld „Customized Report speichern unter“

Sie können im Dialogfeld Customized Report unter speichern einen Bericht nach der Anpassung speichern.

Eigenschaften

Sie können einen Bericht anpassen und speichern, indem Sie Eigenschaften wie den Namen und die Beschreibung angeben.

- **Berichtsname**

  Zeigt den Namen des Berichts an. Der ursprüngliche Berichtname wird standardmäßig angezeigt. Sie können den Berichtsnamen gemäß den Einstellungen ändern. Der Berichtname darf nicht mehr als 255 Zeichen enthalten.

- **Beschreibung**

  Gibt die Beschreibung der Anpassung an den Bericht an. Beschreibung darf nicht mehr als 150 Zeichen enthalten.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Speichern**

  Speichert den angepassten Bericht .

- **Abbrechen**

  Bricht die letzten Änderungen ab und schließt das Dialogfeld „Customized Report as speichern“.

Dialogfeld „Benutzerdefinierter Bericht speichern“

Im Dialogfeld „Benutzerdefinierter Bericht speichern“ können Sie einen benutzerdefinierten Bericht speichern, nachdem Sie zusätzliche Änderungen am benutzerdefinierten Bericht vorgenommen haben.

Eigenschaften

Sie können einen benutzerdefinierten Bericht speichern, indem Sie Eigenschaften wie die Beschreibung angeben.

- **Berichtsname**

  Zeigt den Namen des benutzerdefinierten Berichts an. Dieses Feld kann nicht bearbeitet werden.

- **Beschreibung**

  Gibt die Beschreibung der Anpassungen an, die im benutzerdefinierten Bericht vorgenommen wurden. Beschreibung darf nicht mehr als 150 Zeichen enthalten.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Speichern**

  Speichert den benutzerdefinierten Bericht .

- **Abbrechen**

  Bricht die letzten Änderungen ab und schließt das Dialogfeld „Benutzerdefinierter Bericht speichern“.

Dialogfeld „Bericht importieren“

Sie können das Dialogfeld Bericht importieren verwenden, um Berichte aus zu importieren `.rptdesign` Dateien:

Eigenschaften

Sie können einen Bericht importieren, indem Sie den Namen der Berichtsdatei, den Berichtsnamen und die Berichtsbeschreibung angeben.

- **Wählen Sie Berichtsdatei**

  Ermöglicht Ihnen die Auswahl des `.rptdesign` Datei, die importiert werden soll.

In Google Chrome, die `fakepath` Des `.rptdesign` Datei wird angezeigt. In Mozilla Firefox, nur die `.rptdesign` Dateiname wird angezeigt. In Internet Explorer den vollständigen Pfad des `.rptdesign` Datei wird angezeigt.

- **Name**

  Zeigt den Namen des Berichts an. Dieses Feld ist standardmäßig leer. Sie können einen Namen für den importierten Bericht eingeben.

- **Beschreibung**

  Gibt die Beschreibung des importierten Berichts an. Die Beschreibung darf nicht mehr als 150 Zeichen enthalten.

- **Wählen Sie Datenbankbenutzer mit der Rolle des Berichtsschemas** aus

  Wählen Sie einen Datenbankbenutzer aus, oder erstellen Sie ihn, wenn Sie Berichte aus dem Storage Automation Store importieren möchten.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Import**

  Validiert die ausgewählte `.rptdesign` Datei und importiert den Bericht.

- **Abbrechen**

  Bricht den Importvorgang ab und schließt das Dialogfeld „Importbericht“.

Konfiguration von Backup- und Restore-Vorgängen

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

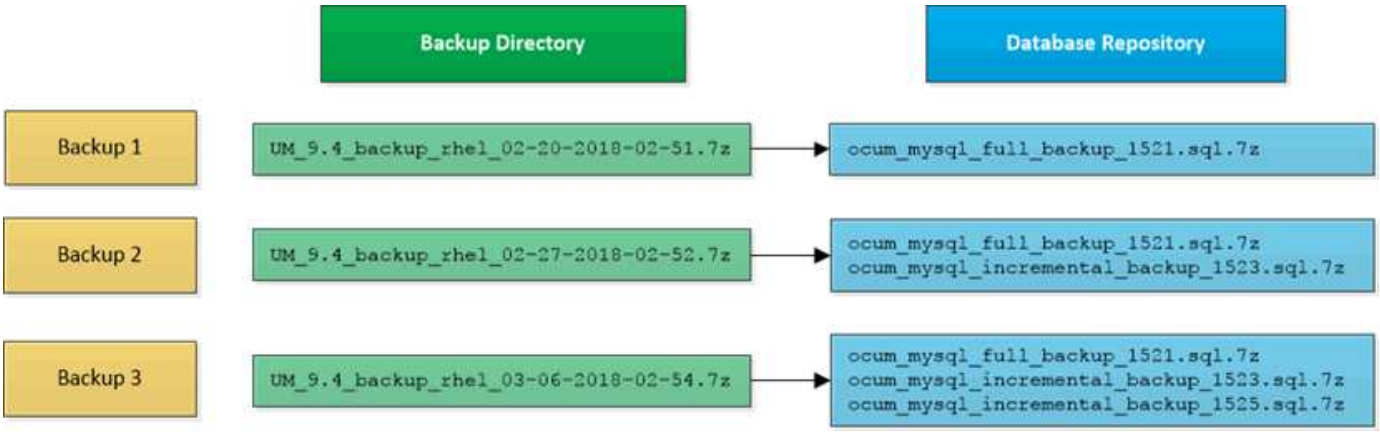
Was ist ein Datenbank-Backup

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

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

Beim ersten Generieren eines Backups wird im Backup-Verzeichnis eine einzelne Datei erstellt und im

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



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

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

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

Beachten Sie, dass Sie ein Backup nur auf derselben Version von Unified Manager wiederherstellen können. Wenn Sie beispielsweise ein Backup auf Unified Manager 9.4 erstellt haben, kann das Backup nur auf Unified Manager 9.4 Systemen wiederhergestellt werden.

Konfigurieren von Backup-Einstellungen für Datenbanken

Sie können die Backup-Einstellungen für die Unified Manager Datenbank so konfigurieren, dass der Datenbank-Backup-Pfad, die Aufbewahrungsanzahl und der Backup-Zeitplan festgelegt werden. Sie können tägliche oder wöchentliche geplante Backups aktivieren. Standardmäßig sind geplante Backups deaktiviert.

Bevor Sie beginnen

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

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

- Wenn Unified Manager auf einem Linux-System installiert ist, stellen Sie sicher, dass der Benutzer „`jboss`“

über Schreibberechtigungen in das Backup-Verzeichnis verfügt.

- Sie sollten Backup-Vorgänge nicht so planen, dass sie unmittelbar nach dem Hinzufügen eines neuen Clusters ausgeführt werden, während Unified Manager historische Performance-Daten von 15 Tagen erfasst.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Datenbank-Backup**.
2. Klicken Sie auf der Seite **Management/Datenbank-Backup** auf **Aktionen** > **Einstellungen für die Datenbanksicherung**.
3. Konfigurieren Sie die entsprechenden Werte für einen Backup-Pfad und die Anzahl der Aufbewahrung.

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

4. Wählen Sie im Abschnitt **Terminhäufigkeit** das Kontrollkästchen **Aktivieren** aus, und geben Sie dann einen täglichen oder wöchentlichen Zeitplan an.
   - * Daily*

     Wenn Sie diese Option auswählen, müssen Sie eine Zeit im 24-Stunden-Format eingeben, um das Backup zu erstellen. Wenn Sie beispielsweise 18:30 angeben, wird täglich um 6:30 Uhr ein Backup erstellt.

   - **Wöchentlich**

     Wenn Sie diese Option auswählen, müssen Sie die Uhrzeit und den Tag für die Erstellung des Backups angeben. Wenn Sie beispielsweise den Tag als Montag und die Zeit als 16:30 angeben, wird jeden Montag um 4:30 Uhr ein wöchentliches Backup erstellt.

5. Klicken Sie auf **Speichern und Schließen**.

Was ist ein Datenbank-Restore

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

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

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

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

- Virtuelle Appliance auf virtuelle Appliance
- Virtuelle Appliance für Red hat Enterprise Linux oder CentOS
- Red hat Enterprise Linux auf Red hat Enterprise Linux oder CentOS
- Windows zu Windows

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

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

Backup- und Wiederherstellungsverfahren für virtuelle Appliances – Übersicht

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

Da der Backup-Vorgang von Unified Manager auf der virtuellen Appliance keine Möglichkeit bietet, die Backup-Datei aus der vApp zu verschieben, können Sie mit den folgenden Aufgaben ein Backup der virtuellen Appliance durchführen:

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

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

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

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

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

Wiederherstellen einer Datenbanksicherung auf einer virtuellen Maschine

Bei Datenverlust oder Datenbeschädigung kann Unified Manager mit der Wiederherstellungsfunktion in den vorherigen stabilen Zustand bei minimalem Verlust wiederhergestellt werden. Sie können die Unified Manager-Datenbank auf einer virtuellen

Maschine über die Wartungskonsole von Unified Manager wiederherstellen.

Bevor Sie beginnen

- Sie müssen über die Anmeldeinformationen für den Wartungs-Benutzer verfügen.
- Die Backup-Dateien von Unified Manager müssen sich auf dem lokalen System befinden.
- Die Sicherungsdateien müssen aus sein `.7z` Typ.

Über diese Aufgabe

Die Backup-Kompatibilität ist Plattform- und versionsabhängig. Das Wiederherstellen eines Backups von einer virtuellen Appliance auf einer anderen virtuellen Appliance oder von einer virtuellen Appliance auf einem Red hat Enterprise Linux oder CentOS System ist möglich.

Wenn Sie einen Wiederherstellungsvorgang auf einer anderen virtuellen Appliance durchführen als auf dem System, von dem die ursprüngliche Sicherungsdatei erstellt wurde, müssen der Wartungsbenutzername und das Kennwort auf der neuen vApp identisch sein mit den Anmeldeinformationen der ursprünglichen vApp.

Schritte

1. Suchen Sie im vSphere-Client die virtuelle Unified Manager-Maschine und wählen Sie dann die Registerkarte **Konsole** aus.
2. Klicken Sie auf das Konsolenfenster, und melden Sie sich dann mit Ihrem Benutzernamen und Passwort an der Wartungskonsole an.
3. Geben Sie im **Hauptmenü** die Nummer für die Option **Systemkonfiguration** ein.
4. Geben Sie im Menü * Systemkonfiguration* die Nummer für die Option **aus einem OCUM-Backup** wiederherstellen ein.
5. Geben Sie bei entsprechender Aufforderung den absoluten Pfad der Sicherungsdatei ein.

   ```
   Bundle to restore from: opt/netapp/data/ocum-
   backup/UM_9.4.N151112.0947_backup_unix_02-25-2018-11-41.7z
   ```

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

Nachdem Sie fertig sind

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

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

Wiederherstellen einer Datenbanksicherung auf einem Linux-System

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

Bevor Sie beginnen

- Unified Manager muss auf einem Server installiert sein.
- Sie müssen über die Stammbenutzeranmeldeinformationen für den Linux-Host verfügen, auf dem Unified Manager installiert ist.
- Sie müssen die Backup-Datei von Unified Manager und den Inhalt des Datenbank-Repository-Verzeichnisses auf das System kopiert haben, auf dem Sie den Wiederherstellungsvorgang ausführen möchten.

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

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

Über diese Aufgabe

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

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

Schritte

1. Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager die UI nicht oder konfigurieren Sie nach Abschluss der Installation keine Cluster, Benutzer oder Authentifizierungseinstellungen. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.
2. Melden Sie sich als Root-Benutzer an dem Host an, auf dem Unified Manager installiert ist.
3. Wenn Unified Manager in VCS Setup installiert ist, stoppen Sie die Unified Manager ocie und ocieau Services mit Veritas Operations Manager.
4. Stellen Sie an der Eingabeaufforderung das Backup wieder her: `um backup restore -f <backup_file_path>/<backup_file_name>`

   ```
   um backup restore -f /data/ocum-backup/UM_9.4.N151113.1348_backup_rhel_02-20-2018-04-45.7z
   ```

Nachdem Sie fertig sind

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

Wiederherstellen einer Datenbanksicherung unter Windows

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

Bevor Sie beginnen

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

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

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

Über diese Aufgabe

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

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

Schritte

1. Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager die UI nicht oder konfigurieren Sie nach Abschluss der Installation keine Cluster, Benutzer oder Authentifizierungseinstellungen. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.
2. Melden Sie sich als Administrator bei der Unified Manager-Konsole an: `um cli login -u maint_username`
3. Stellen Sie an der Eingabeaufforderung das Backup wieder her: `um backup restore -f <backup_file_path>/<backup_file_name>`

   ```
   um backup restore -f
   \ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.4.N151118.2300_backup_windows_02-20-2018-02-51.7z
   ```

Nachdem Sie fertig sind

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

Beschreibung der Backup-Fenster und Dialogfelder

Sie können die Liste der Backups von der Backup-Seite in Unified Manager anzeigen. Sie können den Backup-Namen, die Größe und die Erstellungszeit für die auf dieser Seite aufgeführten Backups anzeigen. Sie können die Einstellungen für die Datenbank-Sicherung auf der Seite Einstellungen für die Datenbank-Sicherung ändern.

Management/Datenbank-Backup Seite

Die Seite Management/Datenbank-Backup zeigt eine Liste der von Unified Manager erstellten Backups an und enthält Informationen über den Backup-Namen, die Größe, die Erstellungszeit und den Zeitplan.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Befehlsschaltflächen

- **Aktionen**

  Zeigt das Dialogfeld Datenbank-Backup-Einstellungen an, in dem Sie einen Backup-Pfad, die Anzahl der Aufbewahrung und den Backup-Zeitplan festlegen können.

Listenansicht

In der Listenansicht werden Informationen über die von Unified Manager erstellten Backups in Tabellenformat angezeigt. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen.

- **Name**

  Zeigt den Namen des ausgewählten Backups an.

- **Größe**

  Zeigt die Größe des ausgewählten Backups an.

- **Erstellungszeit**

  Zeigt das Erstellungsdatum und die Uhrzeit der ausgewählten Sicherung an.

- **Zeitplan**

  Zeigt den Status des Sicherungsvorgangs an. Gibt außerdem an, ob es sich um ein geplantes Backup handelt oder nicht.

Dialogfeld „Einstellungen für die Datenbanksicherung“

Über das Dialogfeld Einstellungen für die Datenbanksicherung können Sie einen Backup-Pfad und die Anzahl der Aufbewahrung angeben und einen Backup-Zeitplan für eine

ausgewählte Backupinstanz aktivieren.

Sie können die folgenden Datenbank-Backup-Einstellungen ändern:

- **Pfad**

  Gibt den Pfad zum Speicherort der Sicherungsdateien an. Die folgende Tabelle gibt das Format des Backup-Pfads und die Standardstandorte für verschiedene Betriebssysteme an:

Host-Betriebssystem	Format des Backup-Pfads
Virtuelle Appliance	`/opt/netapp/data/ocum-backup`
Red hat Enterprise Linux oder CentOS	`/data/ocum-backup`
Microsoft Windows	`C:\ProgramData\NetApp\OnCommandAppData\ocum\backup\`

- **Anzahl Der Einbehalt**

  Gibt die maximale Anzahl von Backups an, die von Unified Manager beibehalten werden sollen. Der Standardwert ist zehn.

- **Zeitplanhäufigkeit Aktivieren**

  Mit dieser Option können Sie festlegen, wann ein Backup geplant werden soll; Sie können täglich oder wöchentlich wählen.

- * Daily*

  Gibt den täglichen Backup-Zeitplan mit der Zeit an.

- **Wöchentlich**

  Gibt den wöchentlichen Backup-Zeitplan mit dem Tag und der Uhrzeit an.

Befehlsschaltflächen

- **Speichern und Schließen**

  Speichert die Sicherungsdatei und schließt das Dialogfeld. Unified Manager speichert die Sicherungsdatei im folgenden Format: `um_um_version_backup_os_timestamp.7z`.

- **Abbrechen**

  Schließt das Dialogfeld Einstellungen für die Datenbanksicherung, ohne Ihre Änderungen zu speichern.

Verwendung von Unified Manager REST-APIs

Über REST-APIs lassen sich die von Unified Manager erfassten Daten zu Zustand, Kapazität und Performance anzeigen, um die Cluster zu managen.

Zugriff auf REST-APIs über die Swagger API-Webseite

REST-APIs sind über die Swagger Webseite zugänglich. Sie können auf die Swagger-Webseite zugreifen, um die Rest-API-Dokumentation von Unified Manager anzuzeigen und einen API-Aufruf manuell zu tätigen.

Bevor Sie beginnen

- Sie müssen über eine der folgenden Rollen verfügen: Operator, Storage Administrator oder OnCommand Administrator.
- Sie müssen die IP-Adresse oder den vollqualifizierten Domänennamen des Unified Manager Servers kennen, auf dem Sie die REST APIs ausführen möchten.

Über diese Aufgabe

Für jede REST-API auf der Swagger-Webseite wird ein Beispiel zur Erläuterung der Objekte und Attribute bereitgestellt, mit denen Sie die Informationen zurückgeben können, die Sie für die Überprüfung interessieren.

Schritte

1. Zugriff auf die Unified Manager REST-APIs

Option	Beschreibung
Über die Web-UI von Unified Manager:	Klicken Sie in der Menüleiste auf die Schaltfläche **Hilfe** und wählen Sie dann **API-Dokumentation** aus.
Im Browser-Fenster:	Geben Sie unter Verwendung der IP-Adresse oder des FQDN des Unified Manager-Servers die URL ein, um auf die REST-API-Seite im Format zuzugreifen `https://<Unified_Manager_IP_address_or_name>/apidocs/`. Beispiel: `https://10.10.10.10/apidocs/`

   Eine Liste der API-Ressourcentypen oder -Kategorien wird angezeigt.

2. Klicken Sie auf einen API-Ressourcentyp, um die APIs in diesem Ressourcentyp anzuzeigen.

Liste der verfügbaren REST-APIs

Sie sollten über die verfügbaren REST-APIs in Unified Manager informiert sein, damit Sie planen können, wie Sie die APIs verwenden können. Die API-Aufrufe sind unter den verschiedenen Ressourcentypen oder -Kategorien organisiert.

Auf der Swagger-Webseite finden Sie eine vollständige Liste der verfügbaren API-Aufrufe sowie die Details jedes Anrufs.

Die Management-API-Aufrufe sind nach den folgenden Kategorien organisiert:

- Aggregate
- Cluster
- Veranstaltungen
- LIFs
- LUNs
- Namespaces
- Knoten
- Ports
- SVMs
- Volumes

Wenn Sie eine der Kategorien auswählen, wird eine Liste angezeigt, die die Unterkategorie API zusammen mit einer versionierten Unterkategorie anzeigt, z. B.:

- /Aggregate
- /V1/Aggregate

Die neueste Version der REST-APIs wird ohne Versionsnummer in der URL aufgeführt. Zur Integration mit Unified Manager sollten Sie immer die neueste Version der API verwenden.

Management und Monitoring von Infinite Volumes

Überwachen Sie mit Infinite Volume die Kapazität und Verfügbarkeit Ihrer Storage Virtual Machines (SVMs). Durch die Erstellung von Regeln und Datenrichtlinien können Sie die Content-Platzierung in Ihrer Storage Virtual Machine (SVM) mit Infinite Volume managen.

Betrachtung der Details zu SVMs mit Infinite Volume

Auf der Seite „Health/Storage Virtual Machines Inventory“ können Sie detaillierte Informationen zu Storage Virtual Machines (SVMs) mit Infinite Volume anzeigen, die von Unified Manager überwacht werden. Sie können Details wie Kapazität, Konfiguration und Datenrichtlinien sowie Regeln im Zusammenhang mit dem Infinite Volume anzeigen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Der Cluster, der die SVM mit Infinite Volume enthält, muss der Unified Manager Datenbank hinzugefügt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Verwenden Sie auf der Seite **Health/Storage Virtual Machines** Inventory den Spaltenfilter in **zulässiger Volume Type**, um die zu überwachenden Infinite Volumes aufzulisten.
3. Alle Details zu SVM mit Infinite Volume können Sie anzeigen, indem Sie auf den SVM-Namen klicken.

Anzeigen der Komponenten eines Infinite Volume

Über die Seite „Health/Volumes Inventory“ können Sie die Liste der Komponenten in Ihrem Infinite Volume anzeigen. Sie können Details wie den Komponentenstatus, die SVM mit Infinite Volume anzeigen, die die Komponente, den Verbindungspfad der Komponente, das Aggregat mit der Komponente sowie die verfügbare, genutzte und die gesamte Datenkapazität der Komponente enthält.

Bevor Sie beginnen

Folgende Anforderungen müssen erfüllt werden:

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Der Cluster, der die SVM mit Infinite Volume enthält, muss der Unified Manager Datenbank hinzugefügt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Klicken Sie auf den Namen einer SVM mit Infinite Volume.
3. Klicken Sie auf der Seite **Health/Storage Virtual Machine** Details auf **Volumes** im rechten Fensterbereich **Related Devices**.

   Die Liste der Komponenten wird auf der Seite „Inventar für Funktionsdaten/Volumes“ angezeigt.

Bearbeiten der Schwellenwerteinstellungen des Infinite Volume

Wenn Sie Probleme im Storage-Bereich Ihres Infinite Volume beheben müssen, können Sie die Schwellenwerteinstellungen der Kapazität des Infinite Volume entsprechend den Anforderungen Ihres Unternehmens bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Ereignisse generiert und Sie erhalten Benachrichtigungen, wenn Sie für solche Ereignisse konfiguriert haben.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory eine SVM mit Infinite Volume aus.
3. Klicken Sie auf der Seite **Health/Storage Virtual Machine** Details auf **Actions** > **Schwellenwerte bearbeiten**.
4. Ändern Sie im Dialogfeld **SVM mit Infinite Volume Schwellenwerten** die Schwellenwerte nach Bedarf.
5. Klicken Sie auf **Speichern und Schließen**.

Bearbeiten der Schwellenwerteinstellungen von Speicherklassen

Wenn Sie Probleme im Zusammenhang mit dem Speicherplatz in Ihren Storage-Klassen beheben müssen, können Sie die Schwellenwerteinstellungen der Storage-Kapazität entsprechend den Anforderungen Ihres Unternehmens bearbeiten. Wenn der Schwellenwert überschritten wird, werden Ereignisse generiert und Sie erhalten Benachrichtigungen, wenn Sie für solche Ereignisse konfiguriert haben.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory eine SVM mit Infinite Volume aus.
3. Klicken Sie auf der Seite **Health/Storage Virtual Machine** Details auf **Actions** > **Schwellenwerte bearbeiten**.
4. Ändern Sie im Dialogfeld **Schwellenwerte für Speicherklassen bearbeiten** die Schwellenwerte nach Bedarf.
5. Klicken Sie auf **Speichern und Schließen**.

Infinite Volumes Verstehen

Ein Infinite Volume ist eine logische Storage-Einheit, mit der Sie einen großen, skalierbaren Daten-Container mit einem einzelnen Namespace und einem einzelnen Mount-Punkt bereitstellen können. Wenn Sie sich über einige der grundlegenden Konzepte von Infinite Volumes informieren, können Sie Ihre SVMs mit Infinite Volume überwachen und managen.

Was ist ein Infinite Volume

Ein Infinite Volume ist ein einzelnes, skalierbares Volume, das bis zu 2 Milliarden Dateien und Petabyte an Daten speichern kann.

Mit einem Infinite Volume können Sie mehrere Petabyte an Daten in einer großen logischen Einheit managen. Clients können mehrere Petabyte an Daten auf einem einzigen Verbindungspfad für das gesamte Volume abrufen.

Ein Infinite Volume nutzt Storage von mehreren Aggregaten auf mehreren Nodes. Beginnen Sie mit einem kleinen Infinite Volume und erweitern Sie die Technologie unterbrechungsfrei, indem Sie den Aggregaten weitere Festplatten hinzufügen oder mehr Aggregate nutzen.

Maximale Anzahl an Dateien, die ein Infinite Volume speichern kann

In den meisten Fällen kann ein Infinite Volume bis zu 2 Milliarden Dateien speichern. Ist ein Infinite Volume relativ klein, kann die maximale Anzahl an Dateien weniger als 2 Milliarden betragen.

Die maximale Anzahl an Dateien, die ein Infinite Volume enthalten kann, wird durch die Größe der Namespace-Komponente festgelegt. Wenn die Namespace-Komponente 10 TB beträgt, kann das Infinite Volume 2 Milliarden Dateien enthalten. Wenn die Namespace-Komponente weniger als 10 TB beträgt, kann das Infinite Volume proportional weniger Dateien enthalten.

Die Größe der Namespace-Komponente ist in etwa proportional zur Größe des Infinite Volume. Dies hängt von verschiedenen Faktoren ab, beispielsweise der Maximalgröße der Namespace-Komponente 10 TB, dem verfügbaren Speicherplatz im Aggregat, das die Namespace-Komponente enthält, und der SnapDiff-Einstellung.

Bei einem Infinite Volume mit zwei Nodes oder einem Infinite Volume mit mehreren Nodes ohne SnapDiff erstellt das Infinite Volume eine Größe von mindestens 80 TB in der Regel eine Namespace-Komponente von 10 TB.

Die Anzahl der Dateien beinhaltet nicht nur reguläre Dateien, sondern auch andere Dateisystemstrukturen wie Verzeichnisse und symbolische Links.

Was für eine Storage-Klasse

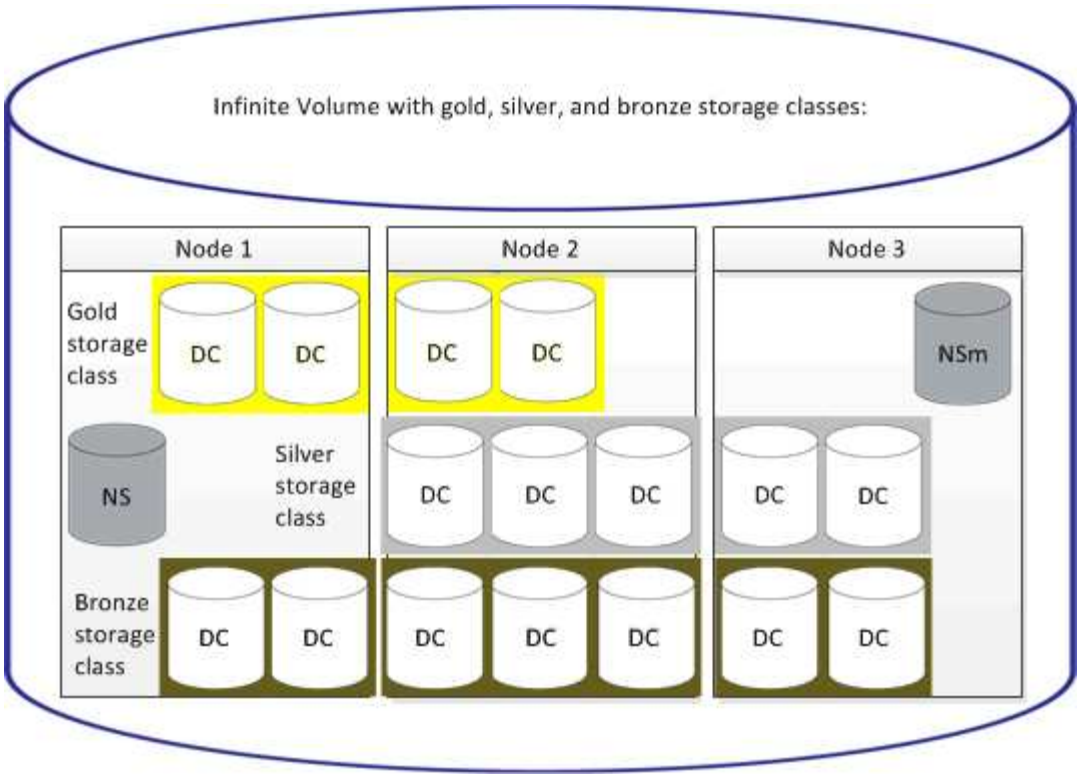
Eine Storage-Klasse ist eine Definition von Aggregateigenschaften und Volume-Einstellungen. Sie können verschiedene Storage-Klassen definieren und eine oder mehrere Storage-Klassen einem Infinite Volume zuordnen. Sie müssen OnCommand Workflow Automation verwenden, um Workflows für Ihre Anforderungen an die Storage-Klasse zu definieren und Infinite Volumes Storage-Klassen zuzuweisen.

Sie können folgende Merkmale für eine Speicherklasse definieren:

- Aggregatmerkmale, z. B. die zu verwendende Festplattenart
- Volume-Einstellungen wie Komprimierung, Deduplizierung und Volume-Garantie

Sie können beispielsweise eine Storage-Klasse definieren, die nur Aggregate mit SAS Festplatten und den folgenden Volume-Einstellungen verwendet: Thin Provisioning mit aktivierter Komprimierung und Deduplizierung.

Das folgende Diagramm zeigt ein Infinite Volume, das sich über mehrere Nodes erstreckt und folgende Storage-Klassen verwendet: Gold, Silber und Bronze. Jede Storage-Klasse kann zwei oder mehr Nodes innerhalb eines Infinite Volume umfassen. In der Abbildung ist auch die Platzierung von Datenkomponenten in jeder Storage-Klasse dargestellt.



Was für eine Namespace-Komponente ist

Jedes Infinite Volume verfügt über eine einzelne Namespace-Komponente, die Verzeichnisinformationen und Dateinamen dem physischen Speicherort der Datei im Infinite Volume zuordnet.

Die Clients kennen die Namespace-Komponente nicht und interagieren nicht direkt mit ihr. Die Namespace-Komponente ist eine interne Komponente des Infinite Volume.

Was Datenkomponenten sind

In einem Infinite Volume werden Daten in mehreren separaten Datenkomponenten gespeichert. Datenkomponenten speichern nur die Daten aus einer Datei, nicht den Namen der Datei.

Die Clients kennen Datenkomponenten nicht. Wenn ein Client eine Datei von einem Infinite Volume anfordert, ruft der Node die Daten der Datei von einer Datenkomponente ab und gibt die Datei an den Client zurück.

Jedes Infinite Volume verfügt über Dutzende Datenkomponenten. Ein Infinite Volume mit 6 PB, das eine Milliarde Dateien enthält, kann beispielsweise 60 Datenkomponenten in Aggregaten von 6 Nodes enthalten.

Eine Namespace-Spiegelkomponente ist das

Eine Namespace-Spiegelkomponente ist eine Kopie der Namespace-Komponente eines Clusters, die innerhalb eines Infinite Volume zu einer Spiegelung für die Datensicherung eingesetzt wird. Die Namespace-Spiegelkomponente übernimmt zwei Rollen: Sie sorgt für die Datensicherung der Namespace-Komponente und unterstützt SnapDiff für inkrementelles Tape Backup von Infinite Volumes.

Regeln werden erstellt

Sie können Ihrer Datenrichtlinie neue Regeln hinzufügen, um die Platzierung der Daten zu bestimmen, die auf das Infinite Volume geschrieben werden. Sie können Regeln entweder mithilfe von Regelvorlagen erstellen, die in Unified Manager definiert sind, oder benutzerdefinierte Regeln erstellen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Der Cluster, der die SVM mit Infinite Volume mit Storage-Klassen enthält, muss der Unified Manager Datenbank hinzugefügt werden.

Erstellen von Regeln mithilfe von Vorlagen

Neue Regeln lassen sich mithilfe von von Unified Manager definierten Regelvorlagen hinzufügen, um die Platzierung von Daten, die auf die SVM mit Infinite Volume geschrieben werden, zu bestimmen. Regeln lassen sich auf Basis von Dateitypen, Verzeichnispfaden oder Eigentümern erstellen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Der Cluster, der die SVM mit Infinite Volume mit Storage-Klassen enthält, muss der Unified Manager Datenbank hinzugefügt werden.

Über diese Aufgabe

Die Registerkarte Datenrichtlinie ist nur für eine SVM mit Infinite Volume sichtbar.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory die entsprechende SVM aus.
3. Klicken Sie auf die Registerkarte **Datenrichtlinie**.

   Es wird eine Liste der Regeln in der Datenrichtlinie für die ausgewählte SVM mit Infinite Volume angezeigt.
4. Klicken Sie Auf **Erstellen**.
5. Wählen Sie im Dialogfeld **Regel erstellen** eine entsprechende Regelvorlage aus der Dropdown-Liste aus.

   Die Vorlage basiert auf drei Kategorien: Dateityp, Eigentümer oder Verzeichnispfad.
6. Fügen Sie auf der Grundlage der ausgewählten Vorlage die notwendigen Bedingungen im Bereich **passende Kriterien** hinzu.
7. Wählen Sie aus der Dropdown-Liste **Platzieren Sie den passenden Inhalt in der Storage Class** aus.
8. Klicken Sie Auf **Erstellen**.

   Die neue Regel, die Sie erstellt haben, wird auf der Registerkarte Datenrichtlinie angezeigt.

9. Vorschau aller anderen Änderungen an der Datenrichtlinie.
10. Klicken Sie auf **Aktivieren**, um die Änderungen in den Regeleigenschaften in der SVM zu aktivieren.

Benutzerdefinierte Regeln werden erstellt

Je nach Anforderungen im Datacenter können Sie benutzerdefinierte Regeln erstellen und einer Datenrichtlinie hinzufügen, um die Platzierung von Daten zu bestimmen, die mit Infinite Volume auf die SVM geschrieben werden. Sie können benutzerdefinierte Regeln im Dialogfeld Regel erstellen erstellen erstellen ohne vorhandene Vorlagen zu verwenden.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Der Cluster, der die SVM mit Infinite Volume mit Storage-Klassen enthält, muss der Unified Manager Datenbank hinzugefügt werden.

Über diese Aufgabe

Die Registerkarte Datenrichtlinie ist nur für eine SVM mit Infinite Volume sichtbar.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory die entsprechende SVM aus.
3. Klicken Sie Auf **Datenrichtlinie**.
4. Klicken Sie Auf **Erstellen**.
5. Wählen Sie im Dialogfeld **Regel erstellen** die Option **Benutzerdefinierte Regel** aus der Liste **Vorlage** aus.
6. Fügen Sie im Bereich **passende Kriterien** die Bedingungen bei Bedarf hinzu.

   Unter Bedingungen können Sie eine Regel erstellen, die auf Dateitypen, Verzeichnispfaden oder Besitzern basiert. Eine Kombination dieser Bedingungen sind die Bedingungssätze. Zum Beispiel können Sie eine Regel haben: “Platzieren Sie alle .mp3 im Besitz von John in Bronze-Speicherklasse.”

7. Wählen Sie aus der Dropdown-Liste **Platzieren Sie den passenden Inhalt in der Storage Class** aus.
8. Klicken Sie Auf **Erstellen**.

   Die neu erstellte Regel wird auf der Registerkarte Datenrichtlinie angezeigt.

9. Vorschau aller anderen Änderungen an der Datenrichtlinie.
10. Klicken Sie auf **Aktivieren**, um die Änderungen in den Regeleigenschaften in der SVM zu aktivieren.

Anzeigen von Regeln

Sie können eine Liste der auf der Registerkarte Datenrichtlinie erstellten Regeln anzeigen, bevor Sie die Datenrichtlinie für Ihre SVM mit Infinite Volume ändern.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Der Cluster, der die SVM mit Infinite Volume mit Storage-Klassen enthält, muss der Unified Manager Datenbank hinzugefügt werden.

Über diese Aufgabe

Die Registerkarte Datenrichtlinie ist nur für eine SVM mit Infinite Volume sichtbar.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory die entsprechende SVM aus.
3. Klicken Sie Auf **Datenrichtlinie**.

Ergebnisse

Es wird eine Liste der Regeln in der Datenrichtlinie für die ausgewählte SVM angezeigt. Mit Filtern nach Storage Class können Sie Regeln zu bestimmten Speicherklassen anzeigen.

Vorlagenbasierte Regeln werden bearbeitet

Im Dialogfeld Regel bearbeiten können Sie eine Regel bearbeiten, die mithilfe der Regelvorlagen erstellt wurde. Sie können Regeleigenschaften wie Verzeichnispfade, Dateitypen und Eigentümer hinzufügen, ändern oder löschen. Sie können auch den Regelnamen und die der Regel zugeordnete Speicherklasse ändern.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory eine geeignete SVM aus.
3. Klicken Sie Auf **Datenrichtlinie**.

   Es wird eine Liste der Regeln in der Datenrichtlinie für die ausgewählte SVM mit Infinite Volume angezeigt.

4. Wählen Sie die Regel aus, für die neue Bedingungen oder Bedingungssätze einbezogen werden sollen.
5. Klicken Sie Auf **Bearbeiten**.
6. Bearbeiten Sie die Regel im Dialogfeld **Regel bearbeiten** nach Bedarf:

Ihr Ziel ist	Tun Sie das…
Fügen Sie eine neue Regeleigenschaft hinzu	Klicken Sie Auf **Hinzufügen**.

Ihr Ziel ist	Tun Sie das…
Löschen einer Regeleigenschaft	Klicken Sie auf **Löschen**, indem Sie die entsprechende Regeleigenschaft auswählen.
Ändern Sie eine Regeleigenschaft	Doppelklicken Sie auf die entsprechende Regeleigenschaft, und ändern Sie sie nach Bedarf.

7. Klicken Sie Auf **Aktualisieren**.
8. Überprüfen Sie, ob Ihre Änderungen auf die Regel angewendet werden, indem Sie die Regel auf der Registerkarte **Datenrichtlinie** erweitern.
9. Vorschau aller anderen Änderungen an der Datenrichtlinie.
10. Klicken Sie auf **Aktivieren**, um die Änderungen an den Regeleigenschaften in der SVM zu aktivieren.

Bearbeiten benutzerdefinierter Regeln

Sie können eine Regel bearbeiten, um neue Bedingungen oder Bedingungssätze in die Regel aufzunehmen. Wenn Sie beispielsweise neue Verzeichnispfade zusammen mit den Besitzernamen aufnehmen möchten, können Sie dies im Dialogfeld Regel bearbeiten tun.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die Registerkarte Datenrichtlinie ist nur für eine SVM mit Infinite Volume sichtbar.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory eine geeignete SVM aus.
3. Klicken Sie Auf **Datenrichtlinie**.

   Es wird eine Liste der Regeln in der Datenrichtlinie für die ausgewählte SVM mit Infinite Volume angezeigt.
4. Wählen Sie die Regel aus, für die neue Bedingungen oder Bedingungssätze einbezogen werden sollen.
5. Klicken Sie Auf **Bearbeiten**.
6. Fügen Sie im Dialogfeld **Regel bearbeiten** neue Bedingungen oder Bedingungssätze hinzu:

Sie möchten Folgendes hinzufügen:	Klicken Sie Auf…
Eine neue Bedingung	Der Symbol.
Ein neuer Bedingungssatz	**Bedingungssatz Hinzufügen**.

7. Klicken Sie Auf **Aktualisieren**.
8. Überprüfen Sie, ob Ihre Änderungen auf die Regel angewendet werden, indem Sie die Regel auf der Registerkarte **Datenrichtlinie** erweitern.
9. Vorschau aller anderen Änderungen an der Datenrichtlinie.
10. Klicken Sie auf **Aktivieren**, um die Änderungen in den Regeleigenschaften in der SVM zu aktivieren.

Regeln werden gelöscht

Sie können eine Regel aus einer Datenrichtlinie löschen, wenn sie nicht mehr benötigt wird. Beispielsweise möchten Sie eine Regel für ein bestimmtes Verzeichnis löschen, das nicht mehr gültig ist.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die Registerkarte Datenrichtlinie ist nur für eine SVM mit Infinite Volume sichtbar.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory eine geeignete SVM aus.
3. Klicken Sie Auf **Datenrichtlinie**.

   Es wird eine Liste der Regeln in der Datenrichtlinie für die ausgewählte SVM mit Infinite Volume angezeigt.

4. Wählen Sie die Regel aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.

   Sie können die Standardregel nicht löschen.

5. Vorschau aller anderen Änderungen an der Datenrichtlinie.
6. Klicken Sie auf **Aktivieren**, um die Änderungen in den Regeleigenschaften in der SVM zu aktivieren.

Anzeigen von Änderungen an Ihrer Datenrichtlinie

Sie sollten alle Änderungen an Ihren Regeln in einer Datenrichtlinie in einer Vorschau anzeigen, bevor Sie die Änderungen in der Datenrichtlinie mit Infinite Volume zur Aktivierung an der SVM übermitteln.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die Registerkarte Datenrichtlinie ist nur für eine SVM mit Infinite Volume sichtbar.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory die entsprechende SVM aus.
3. Klicken Sie Auf **Datenrichtlinie**.

   Es wird eine Liste der Regeln in der Datenrichtlinie für die ausgewählte SVM mit Infinite Volume angezeigt.

4. Ändern Sie die Datenrichtlinie nach Bedarf.

   Änderungen an Datenrichtlinien können das Erstellen neuer Regeln, das Bearbeiten vorhandener Regeln, das Löschen vorhandener Regeln oder das Neuanordnen der Regeln umfassen.

5. Klicken Sie Auf **Aktivieren**.
6. Im Fenster **Summary of Changes to Data Policy Configuration** können Sie die Änderungen an Ihrer Datenrichtlinie in der Vorschau anzeigen und dann auf **Activate** klicken, um die Änderungen der Datenrichtlinie in der SVM mit Infinite Volume zu aktivieren.

Konfiguration einer Datenrichtlinie exportieren

Sie können eine Konfiguration einer Datenrichtlinie aus Unified Manager in eine Datei exportieren. Nachdem Sie beispielsweise das erforderliche Backup erstellt haben und im Notfall die Konfiguration der Datenrichtlinie aus dem primären Storage exportiert haben.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die Registerkarte Datenrichtlinie, die bei dieser Aufgabe verwendet wird, wird nur für SVMs mit Infinite Volume angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory die entsprechende SVM aus.
3. Klicken Sie Auf **Datenrichtlinie**.

   Es wird eine Liste der Regeln in der Datenrichtlinie für die ausgewählte SVM mit Infinite Volume angezeigt.

4. Klicken Sie Auf **Exportieren**.
5. Geben Sie im browserspezifischen Dialogfeld den Speicherort an, an den die Konfiguration der Datenrichtlinie exportiert werden soll.

Ergebnisse

Die Konfiguration der Datenrichtlinien wird als JSON-Datei an den angegebenen Speicherort exportiert.

Importieren einer Konfiguration für Datenrichtlinien

Sie können eine Richtlinienkonfiguration aus einer Datei importieren, die Datenrichtlinie ändern und die Änderungen in der SVM mit Infinite Volume aktivieren. Im Falle eines Ausfalls können Sie beispielsweise eine bereits definierte Datenrichtlinie in die sekundäre importieren und die Richtlinie nach Bedarf ändern.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Wenn Sie eine Konfiguration einer Datenrichtlinie importieren, werden Ihre vorhandenen Regeln überschrieben.

Die Registerkarte Datenrichtlinie wird nur für SVMs mit Infinite Volume angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory die entsprechende SVM aus.
3. Klicken Sie Auf **Datenrichtlinie**.

   Es wird eine Liste der Regeln in der Datenrichtlinie für die ausgewählte SVM mit Infinite Volume angezeigt.
4. Klicken Sie Auf **Import**.
5. Geben Sie im Dialogfeld **Datenrichtlinie importieren** die Datenrichtlinie an, die Sie importieren möchten, indem Sie den absoluten Pfad der Datenrichtliniendatei angeben.
6. Klicken Sie Auf **Import**.
7. Klicken Sie auf **Aktivieren**, um die importierten Regeln in der SVM zu aktivieren.

Allgemeines zu Regeln und Datenrichtlinien

Wenn Sie die Konzepte zu Regeln und Datenrichtlinien kennen, können Sie Ihre Infinite Volumes effizient managen.

Was sind Regeln und Datenrichtlinien

Eine *Regel* legt die Platzierung von Dateien (Daten) in einer Storage Virtual Machine (SVM) mit Infinite Volume fest. Eine Sammlung solcher Regeln ist als *Datenrichtlinie* bekannt.

- **Regel**

  Regeln bestehen im Wesentlichen aus einer Reihe vordefinierter Bedingungen und Informationen, die bestimmen, wo Dateien im Infinite Volume abgelegt werden sollen. Wird eine Datei im Infinite Volume abgelegt, werden die Attribute dieser Datei mit der Liste der Regeln abgeglichen. Wenn Attribute mit den Regeln übereinstimmen, werden durch die Platzierungsinformationen dieser Regel die Speicherklasse bestimmt, in der die Datei abgelegt wird. Eine Standardregel in der Datenrichtlinie wird verwendet, um die

Platzierung von Dateien zu bestimmen, wenn die Attribute keiner der Regeln in der Regelliste entsprechen.

Wenn Sie zum Beispiel eine Regel haben, “Platzieren Sie alle Dateien vom Typ .mp3 in der Bronze-Speicherklasse.”, würden alle .mp3-Dateien, die auf das Infinite Volume geschrieben werden, in der Bronze-Speicherklasse platziert werden.

- **Datenrichtlinie**

  Eine Datenrichtlinie ist eine Liste von Regeln. Jede SVM mit Infinite Volume verfügt über eine eigene Datenrichtlinie. Jede Datei, die dem Infinite Volume hinzugefügt wird, wird mit den Regeln seiner Datenrichtlinie verglichen, um den Speicherort dieser Datei zu bestimmen. Die Datenrichtlinie ermöglicht es Ihnen, eingehende Dateien auf Basis der Dateiattribute zu filtern und diese Dateien in den entsprechenden Speicherklassen zu platzieren.

Die Standardregel ist

Die Standardregel dabei ist die Regel, die in der Datenrichtlinie einer Storage Virtual Machine (SVM) mit Infinite Volume vorhanden ist. Sie bestimmt die Platzierung der Daten, die auf das Infinite Volume geschrieben werden, wenn keine der Bedingungen in den vorhandenen Regeln mit den zu schreibenden Daten übereinstimmen.

Die Standardregel ist immer die letzte Regel in einer Datenrichtlinie und kann nicht neu angeordnet werden. Nehmen wir zum Beispiel eine Datenrichtlinie mit drei Regeln. Regel-1 speichert alle .pdf-Dateien in der Klasse *High_Performance*Storage. Regel-2 speichert alle Dateien, die dem Administrator gehören, und Dateinamen, die mit *.xls enden, in der Speicherklasse *Archive_CONFIR*. Die dritte Regel ist die Standardregel für die Storage-Klasse *low_Performance*.

Wenn eine Reihe von *.jpg-Dateien, die nicht dem Administrator gehören, in das Infinite Volume geschrieben wird, wird die Standardregel verwendet, um diese .jpg-Dateien in der Speicherklasse *low_Performance* zu platzieren. Regel-1 und Regel-2 werden nicht verwendet, da die geschriebenen Daten nicht mit diesen Regeln übereinstimmen.

Filtern einer Datenrichtlinie nach Daten, die auf ein Infinite Volume geschrieben wurden

Eine Datenrichtlinie filtert automatisch auf das Infinite Volume geschriebene Daten in verschiedenen Storage-Klassen. Alle Dateien werden im Namespace des Infinite Volume auf das einzelne File-System geschrieben. Anhand der Regeln der Datenrichtlinie wird festgelegt, welche Storage-Klasse die Daten für die Dateien speichert.

Bei der Erstellung des Infinite Volume wird automatisch eine Datenrichtlinie für eine Storage Virtual Machine (SVM) mit Infinite Volume erstellt. Die Datenrichtlinie ist aktiv und enthält eine Standardregel. Die Standardregel speichert eingehende Daten für Dateien wie folgt für Infinite Volumes mit und ohne Storage-Klassen:

Für ein Infinite Volume…	Die standardmäßige Datenrichtlinie führt dies aus…
Ohne Storageklassen	Alle eingehenden Daten für Dateien werden auf dem Infinite Volume gespeichert

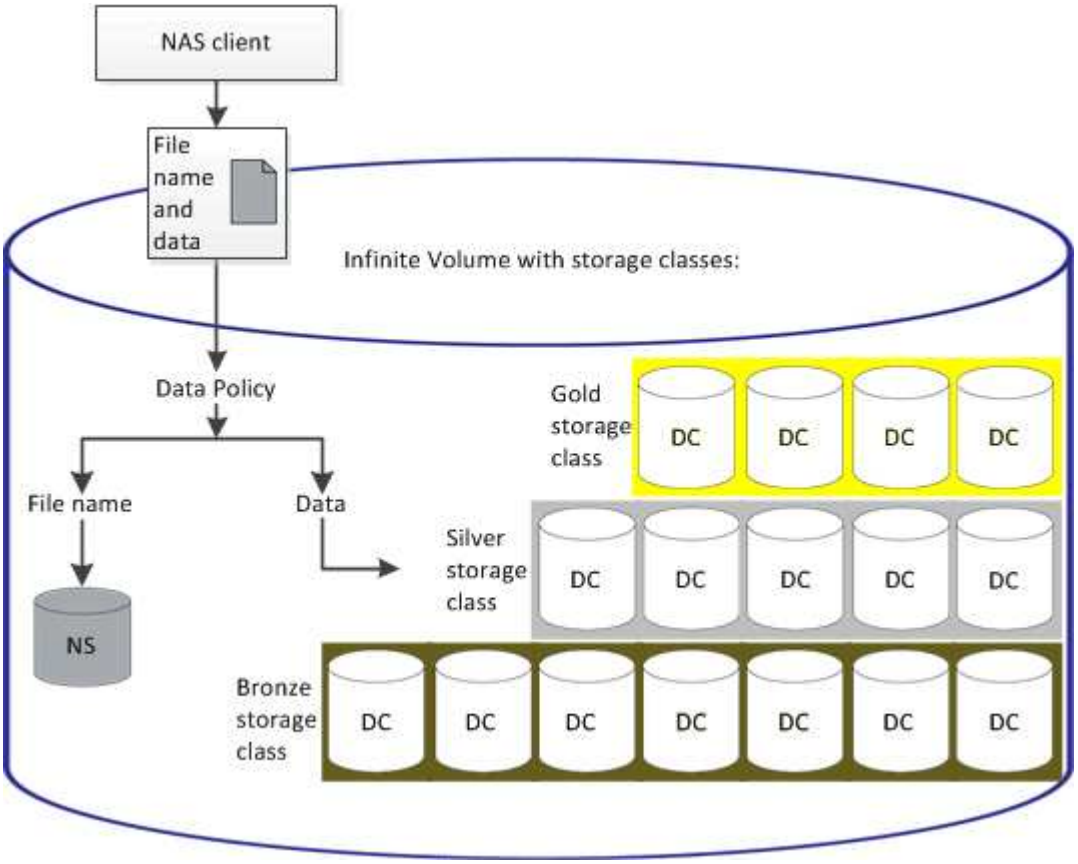
Für ein Infinite Volume…	Die standardmäßige Datenrichtlinie führt dies aus…
Mit einer Storage-Klasse	Alle eingehenden Daten für Dateien werden in die Speicherklasse gespeichert
Mit einer oder mehreren Speicherklassen	Alle eingehenden Daten für Dateien werden in die erste erstellte Speicherklasse gespeichert

Bei einem Infinite Volume mit zwei oder mehr Storage-Klassen sollten Sie die So bald wie möglich der Datenrichtlinien ändern, um Regeln zu erstellen, die Daten nach verschiedenen Dateitypen in die verschiedenen Storage-Klassen filtern. Sie sollten die Datenrichtlinie unter Verwendung von Unified Manager ändern.

Die Datenrichtlinie hat keine Auswirkung auf den Speicherort der Dateien im Filesystem im Namespace des Infinite Volume, und die Storage-Klassen sind für Client-Applikationen transparent. Das Dateisystem im Namespace enthält die Dateinamen. Die Datenrichtlinie beeinflusst nur, welche Storage-Klassen zur Speicherung der Daten für die Dateien verwendet werden. Datenrichtlinien sind nützlich, wenn Sie einem Infinite Volume zwei oder mehr Storage-Klassen zuweisen.

Sie können die Datenrichtlinie ändern, um zusätzliche Regeln zu erstellen, aber Sie können die Datenrichtlinie oder die Standardregel nicht löschen.

Im folgenden Diagramm wird dargestellt, wie eine Datenrichtlinie die Daten eines Infinite Volume filtert. Der Dateiname wird in der Namespace-Komponente gespeichert, und die Regeln in der Datenrichtlinie geben an, dass Daten für diese bestimmte Datei in der Silber-Speicherklasse gespeichert werden.



Was ist eine Regelvorlage

Eine Regelvorlage ist eine vordefinierte Vorlage, die zum Erstellen von Regeln in einer Datenrichtlinie verwendet werden kann. Mit einer Regelvorlage können Sie eine Regel erstellen, die auf drei Kategorien basiert: Eigentümer, Dateityp und Verzeichnispfad.

Beispiel für eine Regelvorlage für Dateitypen

Die Regelvorlage “Platzieren Sie alle Dateien mit den angegebenen Erweiterungen in einer geeigneten Speicherklasse” speichert alle .mp3 Dateien, die auf das Infinite Volume geschrieben werden, in einer Speicherklasse, die Sie angeben.

Welche Bedingungen und Bedingungssätze sind

Conditions sind ein Satz von übereinstimmenden Kriterien, die auf Regeleigenschaften basieren - wie Dateiname, Verzeichnispfad und Eigentümer -, die eine Regel definieren. Eine Sammlung solcher Bedingungen ist als *condition Set* bekannt. Sie können Bedingungen und Bedingungssätze nur für benutzerdefinierte Regeln verwenden, um zu bestimmen, wo Inhalte in Ihr Infinite Volume geschrieben werden.

Bestimmten Bedingungen

Für eine benutzerdefinierte Regel können Sie Bedingungen festlegen, die auf Regeleigenschaften wie Dateiname, Verzeichnispfad oder Eigentümer oder einer Kombination aller Regeleigenschaften basieren. Die Logik ähnelt einem Booleschen Vorgang UND einer Operation. Durch die Verwendung von Bedingungen können Sie beispielsweise eine benutzerdefinierte Regel erstellen, mit der Dateien gespeichert werden `.mp3` Erweiterungen und Dateien im Besitz von John im Verzeichnispfad beginnend mit `/NS/`.

Bedingungssätze

Die für Bedingungssätze verwendete Logik ähnelt einem Booleschen Wert ODER einer Operation. Durch die Verwendung von Bedingungen und Bedingungssätzen können Sie beispielsweise eine komplexe benutzerdefinierte Regel erstellen, die einer der folgenden Bedingungen entspricht:

- Zustand-1

  Alle Dateien im Besitz von Mary und werden in abgelegt `/NS/Eng/`

- Zustand-2

  Alle Dateien mit Namen, die mit enden `.pdf`Und im Besitz von Mary

Beschreibung der Fenster und Dialogfelder von Infinite Volume

Sie können SVMs mit Infinite Volume über die entsprechende Detailseite für den Systemzustand/Storage Virtual Machine überwachen. Über das Dialogfeld Regel erstellen können Sie Regeln und Datenrichtlinien verwalten. Sie können die Schwellenwerte der Speicherklasse auch im Dialogfeld Schwellenwerte für Speicherklassen bearbeiten ändern.

Dialogfeld Regel erstellen

Im Dialogfeld Regel erstellen können Sie neue Regeln für Ihre Datenrichtlinie erstellen. Wenn Sie beispielsweise die Platzierung des Inhalts eines bestimmten Dateityps festlegen möchten, können Sie im Dialogfeld Regel erstellen die Regel für Ihre Datenrichtlinie erstellen verwenden.

Regelname

Gibt den Namen der neuen Regel an.

Bereich Vorlagen

Zeigt die Liste der Regelvorlagen an. Sie können eine entsprechende Regelvorlage aus der Liste auswählen, um eine Regel für die Datenrichtlinie zu erstellen.

Übereinstimmende Kriterien

Zeigt eine Liste der Bedingungen an, die sich auf die ausgewählte Regelvorlage beziehen. Die Bedingungsliste ändert sich basierend auf der ausgewählten Regelvorlage. Wenn Sie beispielsweise “Platzieren Sie alle Dateien mit den angegebenen Besitzernamen in einer geeigneten Speicherklasse”, wird **Liste des Eigentümers, die…** in übereinstimmenden Kriterien angezeigt.

- **Hinzufügen**

  Ermöglicht das Hinzufügen einer neuen Regeleigenschaft auf Grundlage der ausgewählten Regelvorlage. Wenn Sie beispielsweise die Regelvorlage „`Legen Sie alle Dateien mit den angegebenen Besitzernamen in eine geeignete Speicherklasse`“, können Sie über die Schaltfläche **Hinzufügen** den Namen des Eigentümers hinzufügen.

- **Löschen**

  Ermöglicht das Löschen einer ausgewählten Regeleigenschaft.

Platzierung Von Inhalten

Ermöglicht Ihnen die Auswahl einer geeigneten Speicherklasse für Ihre Regel aus der Liste.

Befehlsschaltflächen

- **Erstellen**

  Erstellt eine neue Regel für die Datenrichtlinie und schließt das Dialogfeld Regel erstellen.

- **Abbrechen**

  Bricht die letzten Änderungen an der Regel ab und schließt das Dialogfeld Regel erstellen.

Dialogfeld Regel bearbeiten

Über das Dialogfeld Regel bearbeiten können Sie die Eigenschaften einer Regel bearbeiten, z. B. Dateitypen, Verzeichnispfade oder Eigentümer. Sie können auch eine geeignete Speicherklasse für die Regel auswählen. Wenn beispielsweise ein bestimmter

Dateipfad nicht mehr gültig ist, können Sie den Dateipfad aus der entsprechenden Regel löschen.

Regelname

Zeigt den Namen der Regel an.

Übereinstimmende Kriterien

Zeigt eine Liste der Bedingungen an, die sich auf die ausgewählte Regelvorlage beziehen. Die Bedingungsliste ändert sich basierend auf der ausgewählten Regelvorlage.

- **Hinzufügen**

  Ermöglicht das Hinzufügen einer neuen Regeleigenschaft, eines neuen Dateityps, eines Dateipfads oder eines neuen Besitzers. Wenn Sie beispielsweise die Regelvorlage „`Platzieren Sie alle Dateien mit den angegebenen Besitzernamen in eine geeignete Speicherklasse`“ angegeben haben, können Sie über die Schaltfläche Hinzufügen den Namen des Besitzers hinzufügen.

- **Löschen**

  Ermöglicht das Löschen einer ausgewählten Regeleigenschaft.

Bereich der Content-Platzierung

Zeigt die Liste der Speicherklassen an. Sie können eine geeignete Speicherklasse für die ausgewählte Regel auswählen.

Befehlsschaltflächen

- **Aktualisierung**

  Aktualisiert die an der Regel vorgenommenen Änderungen und schließt das Dialogfeld Regel bearbeiten.

- **Abbrechen**

  Bricht die letzten Änderungen an der Regel ab und schließt das Dialogfeld Regel bearbeiten.

Dialogfeld „Regel bearbeiten“ (Erweitert bearbeiten)

Im Dialogfeld Regel bearbeiten können Sie die Eigenschaften einer Regel bearbeiten, die nicht mit einer Vorlage erstellt wurde. Die zu bearbeitenden Regeleigenschaften umfassen die Dateitypen, Verzeichnispfade, übereinstimmende Kriterien oder Eigentümer. Sie können eine geeignete Speicherklasse für die Regel auswählen. Sie können beispielsweise die Bedingungen bearbeiten, die in den übereinstimmenden Kriterien einer Regel angegeben sind.

Regelname

Zeigt den Namen der Regel an.

Übereinstimmende Kriterien

Zeigt eine Liste der Bedingungen an, die sich auf die ausgewählte Regelvorlage beziehen. Die Bedingungsliste ändert sich basierend auf der ausgewählten Regelvorlage. Sie können die Regeln erweitern und die Regeleigenschaften nach Bedarf ändern.

Bereich der Content-Platzierung

Zeigt die Liste der Speicherklassen an. Sie können eine geeignete Speicherklasse für die ausgewählte Regel auswählen.

Befehlsschaltflächen

- **Aktualisierung**

  Aktualisiert die an der Regel vorgenommenen Änderungen und schließt das Dialogfeld Regel bearbeiten.

- **Abbrechen**

  Bricht die letzten Änderungen an der Regel ab und schließt das Dialogfeld Regel bearbeiten.

Das Dialogfeld „SVM mit Infinite Volume Schwellenwerten“ bearbeiten

Im Dialogfeld „SVM mit Infinite Volume Schwellenwerten bearbeiten“ können Sie die standardmäßigen Schwellwerte jeder SVM je nach Unternehmensanforderung mit Infinite Volume ändern. Die Standardschwellenwerte geben die Aktivitätsebene an, die auf der SVM erreicht werden muss, bevor ein Ereignis ausgelöst wird.

Kapazität

Im Bereich Kapazität können Sie mit Infinite Volume für die ausgewählte SVM einen Kapazitätsschwellenwert festlegen:

- **Raum Fast Voll**

  Gibt den Prozentsatz an, bei dem die SVM mit Infinite Volume als nahezu voll erachtet wird. Außerdem wird der entsprechende Speicherplatz (in GB, MB oder TB) im Infinite Volume angezeigt. Wenn Sie beispielsweise ein Infinite Volume mit einer Größe von 10 GB haben und der Schwellenwert für fast voll Speicherplatz 80 % beträgt, werden folgende Informationen angezeigt: (8 GB von 10 GB).

  Sie können auch den Schieberegler verwenden, um den Schwellenwert festzulegen.

- **Raum Voll**

  Gibt den Prozentsatz an, bei dem die SVM mit Infinite Volume als voll erachtet wird. Außerdem wird der entsprechende Speicherplatz (in GB, MB oder TB) im Infinite Volume angezeigt. Wenn Sie beispielsweise ein Infinite Volume mit Größe 10 GB haben und der Schwellenwert für „Space Full“ 90 % beträgt, werden folgende Informationen angezeigt: (9 GB von 10 GB).

  Sie können auch den Schieberegler verwenden, um den Schwellenwert festzulegen.

- **Limit Für Snapshot-Nutzung**

  Gibt das Limit des in Prozent reservierten Speicherplatzes für Snapshot Kopien im Infinite Volume an.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Auf globale Standards zurücksetzen**

  Ermöglicht es Ihnen, die Schwellenwerteinstellungen auf die aktuellen Werte zurückzusetzen, die auf globaler Ebene festgelegt sind.

- **Speichern**

  Speichert alle Schwellwerteinstellungen.

- **Speichern und Schließen**

  Speichert alle Schwellenwerteinstellungen und schließt dann das Dialogfeld „SVM mit Infinite Volume-Schwellenwerten bearbeiten“.

- **Abbrechen**

  Ignoriert alle Änderungen an den Schwellenwerten und schließt das Dialogfeld „SVM mit Infinite Volume Schwellenwerten bearbeiten“.

Dialogfeld „Schwellenwerte für Speicherklasse bearbeiten“

Sie können im Dialogfeld Schwellenwerte der Storage-Klasse bearbeiten die Standardschwellenwerte verschiedener Storage-Klassen in jeder SVM mit Infinite Volume basierend auf den Anforderungen Ihres Unternehmens ändern. Die Standardschwellenwerte geben an, welche Aktivität in einer Storage-Klasse erreicht werden muss, bevor ein Ereignis ausgelöst wird.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Kapazität

Im Kapazitätsbereich können Sie Grenzwerte für die Kapazität für die ausgewählte Speicherklasse festlegen.

- **Raum Fast Voll**

  Gibt den Prozentsatz an, bei dem eine Storage-Klasse in der SVM mit Infinite Volume als nahezu voll erachtet wird. Es zeigt auch den entsprechenden Speicherplatz (in GB, MB oder TB) in der Speicherklasse an. Beispiel: Wenn Sie eine Speicherklasse von Größe 10 GB haben und der Schwellenwert für Speicherplatz fast voll 80% beträgt, werden folgende Informationen angezeigt: (8 GB von 10 GB).

  Sie können auch den Schieberegler verwenden, um den Schwellenwert festzulegen.

- **Raum Voll**

  Gibt den Prozentsatz an, bei dem die Storage-Klasse in der SVM mit Infinite Volume als voll erachtet wird. Es zeigt auch den entsprechenden Speicherplatz (in GB, MB oder TB) in der Speicherklasse an. Wenn Sie beispielsweise eine Speicherklasse mit einer Größe von 10 GB haben und der Schwellenwert für „Space Full“ 90 % beträgt, werden folgende Informationen angezeigt: (9 GB von 10GB).

  Sie können auch den Schieberegler verwenden, um den Schwellenwert festzulegen.

- **Limit Für Snapshot-Nutzung**

  Gibt das Limit in Prozent im Speicherplatz an, der für Snapshot Kopien in der Storage-Klasse reserviert ist.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie Aufgaben für ein ausgewähltes Volume ausführen.

- **Auf globale Standards zurücksetzen**

  Ermöglicht es Ihnen, die Schwellenwerteinstellungen auf die aktuellen Werte zurückzusetzen, die auf globaler Ebene festgelegt sind.

- **Speichern**

  Speichert alle Schwellwerteinstellungen.

- **Speichern und Schließen**

  Speichert alle Schwellenwerteinstellungen und schließt dann das Dialogfeld „Schwellenwerte für Speicherklasse bearbeiten“.

- **Abbrechen**

  Bricht Änderungen (falls vorhanden) an den Schwellenwerteinstellungen ab und schließt das Dialogfeld „Schwellenwerte für Speicherklasse bearbeiten“.

Verwalten von Clustern

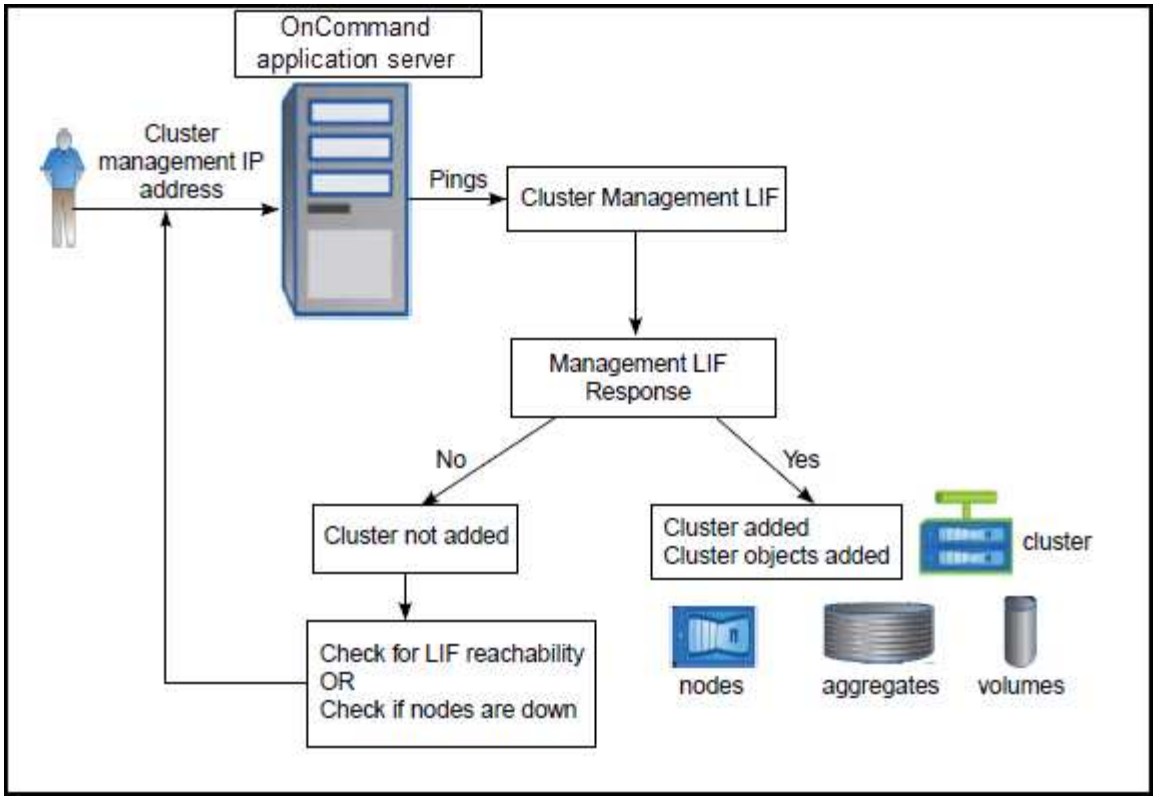
ONTAP-Cluster können mit Unified Manager gemanagt werden, um Cluster zu überwachen, hinzuzufügen, zu bearbeiten und zu entfernen.

Funktionsweise der Cluster-Erkennung

Nachdem Sie Unified Manager einen Cluster hinzugefügt haben, erkennt der Server die Cluster-Objekte und fügt sie seiner Datenbank hinzu. Wenn Sie verstehen, wie der Erkennungsvorgang funktioniert, können Sie die Cluster und ihre Objekte im Unternehmen managen.

Das Monitoring-Intervall zum Erfassen von Cluster-Konfigurationsinformationen beträgt 15 Minuten. Beispielsweise dauert es nach dem Hinzufügen eines Clusters 15 Minuten, bis die Cluster-Objekte in der UI von Unified Manager angezeigt werden. Dieser Zeitrahmen trifft auch zu, wenn Sie die Änderungen an einem Cluster vornehmen. Wenn Sie beispielsweise einer SVM in einem Cluster zwei neue Volumes hinzufügen, werden diese neuen Objekte in der UI nach dem nächsten Abfrageintervall bis zu 15 Minuten angezeigt.

Das folgende Image veranschaulicht den Erkennungsvorgang:



Nachdem alle Objekte für ein neues Cluster erkannt wurden, sammelt Unified Manager historische Performance-Daten für die letzten 15 Tage. Diese Statistiken werden mithilfe der Funktionalität zur Datenerfassung erfasst. Diese Funktion bietet Ihnen sofort nach dem Hinzufügen mehr als zwei Wochen Performance-Informationen für einen Cluster. Nach Abschluss des Datenerfassungszyklus werden Cluster-Performance-Daten in Echtzeit standardmäßig alle fünf Minuten erfasst.

Da die Sammlung von 15 Tagen Leistungsdaten CPU-intensiv ist, empfiehlt es sich, das Hinzufügen neuer Cluster zu staffeln, so dass Datenkontinuitätssammlung nicht auf zu vielen Clustern zur gleichen Zeit laufen.

Anzeigen der Liste der überwachten Cluster

Auf der Seite Configuration/Cluster Data Sources können Sie das Inventar der Cluster anzeigen. Sie können Details zu den Clustern anzeigen, z. B. ihren Namen oder ihre IP-Adresse und ihren Kommunikationsstatus.

Bevor Sie beginnen

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

Über diese Aufgabe

Die Liste der Cluster wird nach der Spalte „Sammlungsstatus“ sortiert. Sie können auf eine Spaltenüberschrift klicken, um die Cluster nach unterschiedlichen Spalten zu sortieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Cluster-Datenquellen**.

Hinzufügen von Clustern

Sie können OnCommand Unified Manager um ein Cluster erweitern, sodass Sie das Cluster überwachen können. Dazu gehört beispielsweise die Möglichkeit, Cluster-Informationen wie Systemzustand, Kapazität, Performance und Konfiguration des Clusters abzurufen, damit Sie etwaige auftretende Probleme finden und beheben können.

Bevor Sie beginnen

- Sie müssen die OnCommand-Administratorrolle oder die Speicheradministratorrolle besitzen.
- Sie müssen den Host-Namen oder die Cluster-Management-IP-Adresse (IPv4 oder IPv6) für das Cluster haben.

  Bei Verwendung des Host-Namens muss dieser für die Cluster-Management-IP-Adresse für die Cluster-Management-LIF aufgelöst werden. Wenn Sie eine Node-Management-LIF verwenden, schlägt der Vorgang fehl.

- Sie müssen Benutzername und Passwort besitzen, um auf das Cluster zugreifen zu können.

  Für dieses Konto muss die Rolle *admin* mit dem Anwendungszugriff auf *ontapi*, *ssh* und *http* eingestellt sein.

- Sie müssen den Protokolltyp (HTTP oder HTTPS) kennen, der für das Cluster konfiguriert werden soll, und die Portnummer, mit der eine Verbindung zum Cluster hergestellt wird.
- Auf dem Unified Manager-Server muss ausreichend Speicherplatz vorhanden sein. Sie können dem Server kein Cluster hinzufügen, wenn bereits mehr als 90 % des Speicherplatzes belegt sind.

> Sie können Cluster hinzufügen, die sich hinter einer NAT/Firewall befinden, indem Sie die Unified Manager NAT IP-Adresse verwenden. Alle angeschlossenen Workflow-Automatisierungs- oder SnapProtect-Systeme müssen sich auch hinter der NAT/Firewall befinden, und SnapProtect-API-Aufrufe müssen die NAT-IP-Adresse verwenden, um den Cluster zu identifizieren.

Über diese Aufgabe

- Jedes Cluster in einer MetroCluster Konfiguration muss separat hinzugefügt werden.
- Eine einzelne Instanz von Unified Manager kann eine bestimmte Anzahl Nodes unterstützen. Wenn Sie eine Umgebung überwachen müssen, die die Anzahl der unterstützten Nodes überschreitet, müssen Sie eine zusätzliche Instanz von Unified Manager installieren, um einige der Cluster zu überwachen.
- Sie können ein einzelnes Cluster durch zwei Instanzen von Unified Manager überwachen, vorausgesetzt, Sie haben eine zweite Cluster-Management-LIF im Cluster konfiguriert, sodass jede Instanz von Unified Manager über eine andere LIF verbunden ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Cluster-Datenquellen**.
2. Klicken Sie auf der Seite **Konfiguration/Cluster-Datenquellen** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Cluster hinzufügen** die Werte nach Bedarf an, und klicken Sie dann auf **Absenden**.

4. Wenn HTTPS ausgewählt ist, führen Sie die folgenden Schritte aus:

   a. Klicken Sie im Dialogfeld **Autorisieren Host** auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.

   b. Klicken Sie Auf **Ja**.

      Unified Manager überprüft das Zertifikat nur, wenn das Cluster zunächst hinzugefügt wird. Unified Manager überprüft nicht das Zertifikat für jeden API-Aufruf an ONTAP.

   Wenn das Zertifikat abgelaufen ist, können Sie kein neues Cluster hinzufügen. Sie müssen zuerst das SSL-Zertifikat erneuern und dann den Cluster hinzufügen.

Ergebnisse

Nachdem alle Objekte für ein neues Cluster erkannt wurden (ca. 15 Minuten), erfasst Unified Manager die historischen Performance-Daten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktionalität zur Datenerfassung erfasst. Diese Funktion bietet Ihnen sofort nach dem Hinzufügen mehr als zwei Wochen Performance-Informationen für einen Cluster. Nach Abschluss des Datenerfassungszyklus werden Cluster-Performance-Daten in Echtzeit standardmäßig alle fünf Minuten erfasst.

Da die Sammlung von 15 Tagen Leistungsdaten CPU-intensiv ist, empfiehlt es sich, das Hinzufügen neuer Cluster zu staffeln, so dass Datenkontinuitätssammlung nicht auf zu vielen Clustern zur gleichen Zeit laufen. Wenn Sie Unified Manager während des Datenerfassungszeitraums neu starten, wird die Sammlung angehalten, und es werden für den fehlenden Zeitraum Lücken in den Leistungsdiagrammen angezeigt.

Wenn Sie eine Fehlermeldung erhalten, dass Sie das Cluster nicht hinzufügen können, prüfen Sie, ob die folgenden Probleme vorhanden sind:

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

Cluster werden bearbeitet

Sie können die Einstellungen eines vorhandenen Clusters, z. B. Host-Name oder IP-Adresse, Benutzername, Passwort, Protokoll und Port, ändern. Über das Dialogfeld Cluster bearbeiten.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle oder die Speicheradministratorrolle besitzen.

Über diese Aufgabe

Wenn Sie die IP-Adresse eines Clusters in eine IP-Adresse eines vorhandenen überwachten Clusters ändern, gehen alle Daten des vorhandenen Clusters verloren, wenn das frühere Cluster erkannt wird. Es wird keine Fehlermeldung angezeigt, um Sie zu warnen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Cluster-Datenquellen**.
2. Wählen Sie auf der Seite **Konfiguration/Cluster-Datenquellen** den Cluster aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Cluster bearbeiten** die Werte nach Bedarf.
4. Klicken Sie Auf **Absenden**.

Cluster werden entfernt

Sie können ein Cluster mithilfe der Seite Configuration/Cluster Data Sources aus Unified Manager entfernen. Beispielsweise können Sie ein Cluster entfernen, wenn die Cluster-Erkennung ausfällt oder wenn Sie ein Storage-System stilllegen möchten.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle oder die Speicheradministratorrolle besitzen.

Über diese Aufgabe

Durch diese Aufgabe wird das ausgewählte Cluster aus Unified Manager entfernt. Nachdem ein Cluster entfernt wurde, wird er nicht mehr überwacht. Die beim entfernten Cluster registrierte Instanz des Unified Manager wird auch vom Cluster nicht registriert.

Durch das Entfernen eines Clusters werden auch alle seine Storage-Objekte, historischen Daten, Storage-Services und alle zugehörigen Ereignisse aus Unified Manager gelöscht. Diese Änderungen werden auf den Bestandsseiten und den Detailseiten nach dem nächsten Datenerfassungszyklus angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Cluster-Datenquellen**.
2. Wählen Sie auf der Seite **Konfiguration/Cluster-Datenquellen** den Cluster aus, den Sie entfernen möchten, und klicken Sie auf **Entfernen**.
3. Klicken Sie im Dialogfeld **Datenquelle entfernen** auf **Entfernen**, um die Anforderung zum Entfernen zu bestätigen.

Cluster-Erkennung neu ermitteln

Sie können ein Cluster manuell auf der Seite „Configuration/Cluster Data Sources“ wiederfinden, um die neuesten Informationen über den Systemzustand, den Überwachungsstatus und den Performance-Status des Clusters abzurufen.

Über diese Aufgabe

Sie können ein Cluster manuell wiederentdecken, wenn Sie den Cluster aktualisieren möchten - z. B. indem

Sie die Größe eines Aggregats erhöhen, wenn der Speicherplatz nicht ausreicht - und Sie möchten, dass Unified Manager die Änderungen entdeckt, die Sie vornehmen.

Wenn Unified Manager mit OnCommand Workflow Automation (WFA) kombiniert wird, löst das Pairing die Neuerfassung der von WFA gecachten Daten aus.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Cluster-Datenquellen**.
2. Klicken Sie auf der Seite **Konfiguration/Cluster-Datenquellen** auf **Wiederentdecken**.

   Unified Manager erkennt das ausgewählte Cluster erneut und zeigt den neuesten Zustand und Performance-Status an.

   Sie können den Überwachungsstatus des Clusters im rechten Bereich der Seite Dashboards/Cluster-Ansicht abrufen.

Seitenbeschreibungen zur Datenquellenverwaltung

Cluster lassen sich anzeigen und verwalten, einschließlich Hinzufügen, Bearbeiten, Neuerkennen und Entfernen von Clustern. Von einer einzelnen Seite aus.

Seite „Configuration/Cluster Data sources“

Auf der Seite Configuration/Cluster Data Sources werden Informationen über die Cluster angezeigt, die von Unified Manager derzeit überwacht werden. Auf dieser Seite können Sie weitere Cluster hinzufügen, Cluster-Einstellungen bearbeiten und Cluster entfernen.

Eine Nachricht am Ende der Seite gibt an, wie häufig Unified Manager Performance-Daten aus den Clustern sammelt. Das Standard-Erfassungsintervall beträgt fünf Minuten, Sie können dieses Intervall jedoch über die Wartungskonsole ändern, wenn Sammlungen von großen Clustern nicht rechtzeitig abgeschlossen werden.

Befehlsschaltflächen

- **Hinzufügen**

  Öffnet das Dialogfeld Cluster hinzufügen, in dem Sie Cluster hinzufügen können.

- **Bearbeiten**

  Öffnet das Dialogfeld Cluster bearbeiten, in dem Sie die Einstellungen des ausgewählten Clusters bearbeiten können.

- **Entfernen**

  Entfernt das ausgewählte Cluster und alle zugehörigen Ereignisse und Storage-Objekte. Nachdem der Cluster entfernt wurde, wird er nicht mehr überwacht.

  Der Cluster, die zugehörigen Storage-Objekte und alle zugehörigen Ereignisse werden entfernt und das Cluster wird nicht mehr von Unified Manager überwacht. Auch die beim entfernten Cluster registrierte Instanz des Unified Manager wird vom Cluster nicht registriert.

- * Wiederentdecken*

  Erzwingt eine Neuentdeckung des Clusters, damit Sie die Erfassung von Gesundheits- und Performance-Daten aktualisieren können.

Cluster-Liste

In der Liste Cluster werden die Eigenschaften aller erkannten Cluster angezeigt. Sie können auf eine Spaltenüberschrift klicken, um die Cluster nach dieser Spalte zu sortieren.

- **Status**

  Zeigt den aktuellen Erkennungsstatus der Datenquelle an. Der Status kann fehlgeschlagen sein ( ), Abgeschlossen ( ), oder in Arbeit ( ).

- **Name**

  Zeigt den Cluster-Namen an.

  Beachten Sie, dass der Name möglicherweise fünfzehn Minuten oder länger dauern kann, bis er nach dem ersten Hinzufügen des Clusters angezeigt wird.

- **Wartungsmodus**

  Ermöglicht Ihnen, den Zeitrahmen oder „`maintential window`“ anzugeben, wenn ein Cluster zu Wartungszwecken ausfällt, damit Sie während des Wartungszeitraums keine Warnmeldungen vom Cluster erhalten.

  Wenn der Wartungsmodus für die Zukunft geplant ist, wird in diesem Feld „`Scheduled`“ angezeigt. Mit dem Mauszeiger über das Feld können Sie die geplante Zeit anzeigen. Wenn sich das Cluster im Wartungsfenster befindet, wird in diesem Feld „`aktiv`“ angezeigt.

- **Hostname oder IP-Adresse**

  Zeigt den Hostnamen, den vollqualifizierten Domänennamen (FQDN), den Kurznamen oder die IP-Adresse der Cluster-Management-LIF an, die zur Verbindung mit dem Cluster verwendet wird.

- **Protokoll**

  Zeigt den Protokolltyp an, der auf dem Cluster konfiguriert werden kann: HTTP oder HTTPS (für eine sichere Verbindung).

  Wenn mit beiden Protokollen eine Verbindung zum Cluster hergestellt wird, wird HTTPS über HTTP ausgewählt. Die Standardeinstellung ist HTTPS.

- **Port**

  Zeigt die Portnummer des Clusters an.

  Wenn der Port nicht angegeben wird, wird der Standardport für das ausgewählte Protokoll verwendet (80 für HTTP oder 443 für HTTPS).

- **Benutzername**

  Zeigt den Benutzernamen an, der zur Anmeldung beim Cluster verwendet werden kann.

- **Betrieb**

  Zeigt den aktuellen Vorgang an, der von der Cluster-Datenquelle unterstützt wird.

  Die Datenquelle unterstützt folgende Vorgänge:

  - Ermitteln

    Gibt den Vorgang an, wenn die Datenquelle erkannt wird.

  - Gesundheitsabfrage

    Gibt den Vorgang an, wenn die Datenquelle erfolgreich erkannt wurde und die Probenahme gestartet wurde.

  - Löschen

    Gibt den Vorgang an, wenn die Datenquelle (Cluster) aus der jeweiligen Liste der Speicherobjekte gelöscht wird.

- **Betriebszustand**

  Zeigt den Status des aktuellen Vorgangs an. Der Status kann ausgefallen, abgeschlossen oder in Bearbeitung sein.

- **Startzeit Der Operation**

  Das Datum und die Uhrzeit, zu der der Vorgang gestartet wurde.

- **Endzeit Der Operation**

  Datum und Uhrzeit des Vorgangs.

- **Beschreibung**

  Alle Nachrichten im Zusammenhang mit dem Vorgang.

Dialogfeld Cluster hinzufügen

Sie können ein vorhandenes Cluster hinzufügen, sodass Sie das Cluster überwachen und Informationen zu dessen Zustand, Kapazität, Konfiguration und Performance erhalten können.

Sie können einen Cluster hinzufügen, indem Sie die folgenden Werte angeben:

- **Hostname oder IP-Adresse**

  Ermöglicht Ihnen die Angabe des Host-Namens (bevorzugte) oder der IP-Adresse (IPv4 oder IPv6) der Cluster-Management-LIF, die zum Herstellen einer Verbindung zum Cluster verwendet wird. Durch die Angabe des Host-Namens können Sie den Namen des Clusters über die Web-Benutzeroberfläche abstimmen, anstatt zu versuchen, eine IP-Adresse auf einer Seite mit einem Hostnamen auf einer anderen Seite zu korrelieren.

- **Benutzername**

Ermöglicht Ihnen, einen Benutzernamen anzugeben, der zum Anmelden beim Cluster verwendet werden kann.

- **Passwort**

  Ermöglicht Ihnen die Angabe eines Passworts für den angegebenen Benutzernamen.

- **Protokoll**

  Ermöglicht Ihnen die Angabe des Protokolltyps, der im Cluster konfiguriert werden kann. Sie können HTTP oder HTTPS aktivieren (für eine sichere Verbindung). Die Verbindung mit dem Cluster wird über beide Protokolle hergestellt, und HTTPS wird über HTTP ausgewählt. Standardmäßig ist HTTPS mit dem Standardport 443 aktiviert.

- **Port**

  Ermöglicht Ihnen, die Portnummer anzugeben, die zum Herstellen der Verbindung mit dem Cluster verwendet wird. Wenn der Port nicht angegeben wird, wird der Standardport für das ausgewählte Protokoll verwendet (80 für HTTP oder 443 für HTTPS).

Dialogfeld Cluster bearbeiten

Im Dialogfeld Cluster bearbeiten können Sie die Verbindungseinstellungen eines vorhandenen Clusters, einschließlich IP-Adresse, Port und Protokoll, ändern.

Sie können die folgenden Felder bearbeiten:

- **Hostname oder IP-Adresse**

  Ermöglicht Ihnen, den FQDN, den Kurznamen oder die IP-Adresse (IPv4 oder IPv6) der Cluster-Management-LIF anzugeben, die zum Herstellen einer Verbindung zum Cluster verwendet wird.

- **Benutzername**

  Ermöglicht Ihnen, einen Benutzernamen anzugeben, der zum Anmelden beim Cluster verwendet werden kann.

- **Passwort**

  Ermöglicht Ihnen die Angabe eines Passworts für den angegebenen Benutzernamen.

- **Protokoll**

  Ermöglicht Ihnen die Angabe des Protokolltyps, der im Cluster konfiguriert werden kann. Sie können HTTP oder HTTPS aktivieren (für eine sichere Verbindung). Die Verbindung mit dem Cluster wird über beide Protokolle hergestellt, und HTTPS wird über HTTP ausgewählt. Standardmäßig ist HTTPS mit dem Standardport 443 aktiviert.

- **Port**

  Ermöglicht Ihnen, die Portnummer anzugeben, die zum Herstellen der Verbindung mit dem Cluster verwendet wird. Wenn der Port nicht angegeben wird, wird der Standardport für das ausgewählte Protokoll verwendet (80 für HTTP oder 443 für HTTPS).

Verwalten des Benutzerzugriffs

Sie können Rollen erstellen und Funktionen zuweisen, um den Benutzerzugriff auf ausgewählte Cluster-Objekte zu steuern. Sie können Benutzer identifizieren, die über die erforderlichen Funktionen für den Zugriff auf ausgewählte Objekte in einem Cluster verfügen. Nur diese Benutzer haben Zugriff, um Cluster-Objekte zu managen.

Benutzer hinzufügen

Sie können lokale Benutzer oder Datenbankbenutzer über die Seite Verwaltung/Benutzer hinzufügen. Sie können auch Remote-Benutzer oder -Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Sie können diesen Benutzern Rollen zuweisen. Anhand der Berechtigungen der Rollen können Benutzer Storage-Objekte und -Daten mit Unified Manager managen oder die Daten in einer Datenbank anzeigen.

Bevor Sie beginnen

- Sie müssen die OnCommand-Administratorrolle besitzen.
- Um einen Remote-Benutzer oder eine Remotegruppe hinzuzufügen, müssen Sie die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsserver konfiguriert haben.
- Wenn Sie die SAML-Authentifizierung so konfigurieren möchten, dass ein Identitäts-Provider (IdP) Benutzer authentifiziert, die auf die grafische Schnittstelle zugreifen, stellen Sie sicher, dass diese Benutzer als „`remote`“-Benutzer definiert sind.

  Der Zugriff auf die Benutzeroberfläche ist Benutzern vom Typ „`local`“ oder „`maintBuße`“ nicht erlaubt, wenn die SAML-Authentifizierung aktiviert ist.

Über diese Aufgabe

Wenn Sie eine Gruppe aus Windows Active Directory hinzufügen, können sich alle direkten Mitglieder und geschachtelten Untergruppen bei Unified Manager authentifizieren, es sei denn, geschachtelte Untergruppen sind deaktiviert. Wenn Sie eine Gruppe von OpenLDAP oder anderen Authentifizierungsdiensten hinzufügen, können sich nur die direkten Mitglieder dieser Gruppe bei Unified Manager authentifizieren.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.
2. Klicken Sie auf der Seite **Verwaltung/Benutzer** auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld **Benutzer hinzufügen** den Benutzertyp aus, den Sie hinzufügen möchten, und geben Sie die erforderlichen Informationen ein.

   Wenn Sie die erforderlichen Benutzerinformationen eingeben, müssen Sie eine E-Mail-Adresse angeben, die für diesen Benutzer eindeutig ist. Sie müssen vermeiden, E-Mail-Adressen anzugeben, die von mehreren Benutzern gemeinsam verwendet werden.

4. Klicken Sie Auf **Hinzufügen**.

Bearbeiten der Benutzereinstellungen

Sie können Benutzereinstellungen bearbeiten, z. B. die E-Mail-Adresse und die Rolle, die jeder Benutzer angegeben hat. Beispielsweise können Sie die Rolle eines Benutzers, der ein Speicheroperator ist, ändern und dem Benutzer Berechtigungen für Speicheradministratoren zuweisen.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Wenn Sie die Rolle ändern, die einem Benutzer zugewiesen ist, werden die Änderungen angewendet, wenn eine der folgenden Aktionen ausgeführt wird:

- Der Benutzer meldet sich bei Unified Manager ab und meldet sich zurück.
- Das Sitzungszeitlimit von 24 Stunden wird erreicht.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.
2. Wählen Sie auf der Seite **Verwaltung/Benutzer** den Benutzer aus, für den Sie die Einstellungen bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
3. Bearbeiten Sie im Dialogfeld **Benutzer bearbeiten** die entsprechenden Einstellungen, die für den Benutzer angegeben sind.
4. Klicken Sie Auf **Speichern**.

Testen eines Remote-Benutzers oder einer Remote-Gruppe

Sie können überprüfen, ob ein Remote-Benutzer oder eine Remote-Gruppe auf den Unified Manager-Server zugreifen kann, indem Sie die für Ihre Authentifizierungsserver festgelegten Authentifizierungseinstellungen verwenden.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert und die Authentifizierungseinstellungen so konfiguriert haben, dass der Unified Manager-Server den Remote-Benutzer oder die Remote-Gruppe validieren kann.
- Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.
2. Wählen Sie auf der Seite * Management/Users* einen Remote-Benutzer oder eine Remote-Gruppe aus, die Sie validieren möchten, und klicken Sie dann auf **Test**.

Anzeigen von Benutzern

Sie können die Seite „Management/Benutzer“ verwenden, um die Liste der Benutzer

anzuzeigen, die Storage-Objekte und Daten mit Unified Manager managen. Sie können Details zu den Benutzern anzeigen, z. B. den Benutzernamen, den Benutzertyp, die E-Mail-Adresse und die Rolle, die den Benutzern zugewiesen ist.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.

   Die Liste der Benutzer wird auf der Seite Verwaltung/Benutzer angezeigt.

Benutzer oder Gruppen werden gelöscht

Sie können einen oder mehrere Benutzer aus der Management-Server-Datenbank löschen, um den Zugriff bestimmter Benutzer auf Unified Manager zu verhindern. Sie können auch Gruppen löschen, sodass alle Benutzer der Gruppe nicht mehr auf den Verwaltungsserver zugreifen können.

Bevor Sie beginnen

- Wenn Sie Remote-Gruppen löschen, müssen Sie die Ereignisse neu zugewiesen haben, die den Benutzern der Remote-Gruppen zugewiesen sind.

  Wenn Sie lokale Benutzer oder Remote-Benutzer löschen, werden die diesen Benutzern zugewiesenen Ereignisse automatisch aufgehoben.

- Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.
2. Wählen Sie auf der Seite **Verwaltung/Benutzer** die Benutzer oder Gruppen aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie auf **Ja**, um den Löschvorgang zu bestätigen.

Ändern des lokalen Benutzerpassworts

Sie können Ihr lokales Benutzeranmeldeswort ändern, um potenzielle Sicherheitsrisiken zu vermeiden.

Bevor Sie beginnen

Sie müssen als lokaler Benutzer angemeldet sein.

Über diese Aufgabe

Die Passwörter für den Wartungsbenutzer und für Remote-Benutzer können mit diesen Schritten nicht geändert werden. Wenden Sie sich an Ihren Passwortadministrator, um ein Kennwort für Remote-Benutzer zu

ändern. Informationen zum Ändern des Wartungs-Benutzerpassworts finden Sie unter "Verwenden der Wartungskonsole".

Schritte

1. Melden Sie sich bei Unified Manager an.
2. Klicken Sie in der oberen Menüleiste auf das Benutzersymbol und dann auf **Passwort ändern**.

   Die Option **Passwort ändern** wird nicht angezeigt, wenn Sie ein Remote-Benutzer sind.

3. Geben Sie im Dialogfeld **Passwort ändern** das aktuelle Passwort und das neue Passwort ein.
4. Klicken Sie Auf **Speichern**.

Nachdem Sie fertig sind

Wenn Unified Manager in einer Hochverfügbarkeitskonfiguration konfiguriert ist, müssen Sie das Passwort auf dem zweiten Node des Setup ändern. Beide Instanzen müssen dasselbe Passwort haben.

Was der Wartungsbenutzer tut

Der Wartungbenutzer wird während der Installation von Unified Manager auf einem Red hat Enterprise Linux oder CentOS System erstellt. Der Wartungs-Benutzername ist der Benutzer „`umadmin`“. Der Wartungsbenutzer hat die OnCommand-Administratorrolle in der Web-UI, und dieser Benutzer kann nachfolgende Benutzer erstellen und ihnen Rollen zuweisen.

Der Wartungsbenutzer oder umadmin-Benutzer kann auch auf die Unified Manager Wartungskonsole zugreifen.

Was RBAC ist

RBAC (rollenbasierte Zugriffssteuerung) bietet die Möglichkeit, zu steuern, wer Zugriff auf verschiedene Funktionen und Ressourcen im OnCommand Unified Manager Server hat.

Was ist die rollenbasierte Zugriffssteuerung

Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) ermöglicht Administratoren das Management von Benutzergruppen, indem sie Rollen definieren. Wenn Sie den Zugriff auf bestimmte Funktionen auf ausgewählte Administratoren beschränken müssen, müssen Sie Administratorkonten für diese einrichten. Wenn Sie die Informationen beschränken möchten, die Administratoren anzeigen können, und die Vorgänge, die sie ausführen können, müssen Sie Rollen auf die von Ihnen erstellten Administratorkonten anwenden.

Der Verwaltungsserver verwendet RBAC für Benutzeranmeldung und Rollenberechtigungen. Wenn Sie die Standardeinstellungen des Managementservers für den Administratorbenutzerzugriff nicht geändert haben, müssen Sie sich nicht anmelden, um sie anzuzeigen.

Wenn Sie einen Vorgang initiieren, der bestimmte Berechtigungen benötigt, fordert der Verwaltungsserver Sie zur Anmeldung auf. Zum Erstellen von Administratorkonten müssen Sie sich z. B. mit Administrator-

Kontozugriff anmelden.

Definitionen der Benutzertypen

Ein Benutzertyp gibt die Art des Kontos an, das der Benutzer besitzt und umfasst Remote-Benutzer, Remote-Gruppen, lokale Benutzer, Datenbankbenutzer und Wartungbenutzer. Jeder dieser Typen hat seine eigene Rolle, die von einem Benutzer mit der Rolle „OnCommand Administrator“ zugewiesen wird.

Unified Manager-Benutzertypen sind wie folgt:

- **Benutzer der Wartung**

  Erstellt während der Erstkonfiguration von Unified Manager. Der Wartungsbenutzer erstellt dann weitere Benutzer und weist Rollen zu. Der Benutzer der Wartung ist außerdem der einzige Benutzer, der Zugriff auf die Wartungskonsole hat. Wenn Unified Manager auf einem Red hat Enterprise Linux- oder CentOS-System installiert ist, erhält der Wartungbenutzer den Benutzernamen „`umadmin`.“.

- **Lokaler Benutzer**

  Greift auf die Unified Manager-Benutzeroberfläche zu und führt Funktionen basierend auf der Rolle durch, die der Wartungsbenutzer oder Benutzer mit der OnCommand-Administratorrolle angegeben hat.

- **Remote-Gruppe**

  Eine Gruppe von Benutzern, die mit den auf dem Authentifizierungsserver gespeicherten Anmeldeinformationen auf die Benutzeroberfläche von Unified Manager zugreifen. Der Name dieses Kontos muss mit dem Namen einer auf dem Authentifizierungsserver gespeicherten Gruppe übereinstimmen. Allen Benutzern innerhalb der Remote-Gruppe wird über ihre individuellen Benutzeranmeldeinformationen der Zugriff auf die Unified Manager-Benutzeroberfläche gewährt. Remote-Gruppen können Funktionen entsprechend ihren zugewiesenen Rollen ausführen.

- **Remote-Benutzer**

  Greift über die auf den Authentifizierungsserver gespeicherten Anmeldeinformationen auf die Unified Manager-UI zu. Ein Remote-Benutzer führt Funktionen basierend auf der Rolle aus, die der Wartungsbenutzer oder ein Benutzer mit der OnCommand-Administratorrolle zugewiesen hat.

- **Datenbankbenutzer**

  Hat schreibgeschützten Zugriff auf Daten in der Unified Manager-Datenbank, hat keinen Zugriff auf die Unified Manager-Webschnittstelle oder die Wartungskonsole und kann keine API-Aufrufe ausführen.

Definitionen von Benutzerrollen

Der Wartungs-Benutzer oder der OnCommand-Administrator weist jedem Benutzer eine Rolle zu. Jede Rolle enthält bestimmte Berechtigungen. Der Umfang der Aktivitäten, die Sie in Unified Manager ausführen können, hängt von der Ihnen zugewiesenen Rolle ab und welchen Berechtigungen die Rolle enthält.

Unified Manager enthält die folgenden vordefinierten Benutzerrollen:

- **Betreiber**

  Anzeige von Storage-Systeminformationen und anderen von Unified Manager erfassten Daten, einschließlich Verläufe und Kapazitätstrends Mit dieser Rolle kann der Speicherbetreiber Notizen zu den Ereignissen anzeigen, zuweisen, bestätigen, auflösen und hinzufügen.

- * Storage Administrator*

  Konfiguration von Storage-Managementvorgängen in Unified Manager Diese Rolle ermöglicht es dem Storage-Administrator, Schwellenwerte zu konfigurieren und Alarme sowie andere für das Storage-Management spezifische Optionen und Richtlinien zu erstellen.

- **OnCommand-Administrator**

  Konfiguriert Einstellungen, die in keinem Zusammenhang mit dem Storage-Management stehen. Diese Rolle ermöglicht das Management von Benutzern, Sicherheitszertifikaten, Datenbankzugriff und Verwaltungsoptionen, einschließlich Authentifizierung, SMTP, Networking und AutoSupport.

  Wenn Unified Manager auf Linux-Systemen installiert wird, heißt der ursprüngliche Benutzer mit der OnCommand-Administratorrolle automatisch „`umadmin`“.

- **Integrationsschema**

  Diese Rolle bietet schreibgeschützten Zugriff auf Unified Manager Datenbankansichten für die Integration von Unified Manager mit OnCommand Workflow Automation (WFA).

- **Schema Melden**

  Diese Rolle ermöglicht einen schreibgeschützten Zugriff auf Reporting und andere Datenbankansichten direkt aus der Unified Manager Datenbank. Folgende Datenbanken stehen zur Verfügung:

  - netapp_Modell_Ansicht
  - netapp_Performance
  - Okum
  - Ocum_Report
  - Ocum_Report_birt
  - opm
  - Skalemonitor

Unified Manager Benutzer-Rollen und -Funktionen

Anhand der Ihnen zugewiesenen Benutzerrolle können Sie festlegen, welche Vorgänge Sie in Unified Manager ausführen können.

In der folgenden Tabelle sind die Funktionen aufgeführt, die die einzelnen Benutzerrollen ausführen können:

Funktion	Operator	Storage-Administrator	OnCommand Administrator	Integrationsschema	Berichtschema
Anzeigen von Speichersysteminformationen	•	•	•	•	•
Andere Daten wie Verläufe und Kapazitätstrends anzeigen	•	•	•	•	•
Ereignisse anzeigen, zuweisen und lösen	•	•	•		
Anzeigen von Storage-Serviceobjekten, z. B. SVM-Zuordnungen und Ressourcenpools	•	•	•		
Anzeigen von Schwellenwertrichtlinien	•	•	•		
Management von Storage-Serviceobjekten wie SVM-Zuordnungen und Ressourcenpools		•	•		
Definieren von Warnmeldungen		•	•		
Optionen für das Storage Management managen		•	•		

Funktion	Operator	Storage-Administrator	OnCommand Administrator	Integrationsschema	Berichtschema
Storage Management-Richtlinien managen		•	•		
Benutzer managen			•		
Management von Verwaltungsoptionen			•		
Definieren Sie Schwellenwertrichtlinien			•		
Datenbankzugriff managen			•		
Managen Sie die Integration in WFA und erhalten Sie Zugriff auf die Datenbankansichten				•	
Schreibgeschützter Zugriff auf Berichte und andere Datenbankansichten					•
Planen und Speichern von Berichten	•	•	•		
Importierte Berichte importieren und löschen			•		

Beschreibung der Benutzerzugriffsfenster und Dialogfelder

Basierend auf den RBAC-Einstellungen können Sie Benutzer auf der Seite

Management/Users hinzufügen und diesen Benutzern geeignete Rollen zuweisen, um die Cluster aufzurufen und zu überwachen.

Management-/Benutzerseite

Auf der Seite Verwaltung/Benutzer wird eine Liste Ihrer Benutzer und Gruppen angezeigt und enthält Informationen wie den Namen, den Benutzertyp und die E-Mail-Adresse. Auf dieser Seite können Sie auch Aufgaben wie das Hinzufügen, Bearbeiten, Löschen und Testen von Benutzern ausführen.

Befehlsschaltflächen

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

- **Hinzufügen**

  Zeigt das Dialogfeld Benutzer hinzufügen an, in dem Sie einen lokalen Benutzer, einen Remote-Benutzer, eine Remote-Gruppe oder einen Datenbankbenutzer hinzufügen können.

  Sie können Remote-Benutzer oder -Gruppen nur hinzufügen, wenn Ihr Authentifizierungsserver aktiviert und konfiguriert ist.

- **Bearbeiten**

  Zeigt das Dialogfeld Benutzer bearbeiten an, in dem Sie die Einstellungen für den ausgewählten Benutzer bearbeiten können.

- **Löschen**

  Löscht die ausgewählten Benutzer aus der Management-Server-Datenbank.

- **Test**

  Hiermit können Sie überprüfen, ob ein Remote-Benutzer oder eine Gruppe im Authentifizierungsserver vorhanden ist.

  Sie können diese Aufgabe nur ausführen, wenn Ihr Authentifizierungsserver aktiviert und konfiguriert ist.

Listenansicht

Die Listenansicht zeigt in tabellarischer Form Informationen zu den erstellten Benutzern an. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen.

- **Name**

  Zeigt den Namen des Benutzers oder der Gruppe an.

- **Typ**

  Zeigt den Benutzertyp an: Lokaler Benutzer, Remote-Benutzer, Remote-Gruppe, Datenbankbenutzer oder Wartungbenutzer.

- **E-Mail**

Zeigt die E-Mail-Adresse des Benutzers an.

- * Rolle*

  Zeigt den Typ der Rolle an, die dem Benutzer zugewiesen ist: Operator, Storage Administrator, OnCommand Administrator, Integrations- Schema oder Berichtschema.

Dialogfeld Benutzer hinzufügen

Sie können lokale Benutzer oder Datenbankbenutzer erstellen, Remote-Benutzer oder Remote-Gruppen hinzufügen und Rollen zuweisen, sodass diese Benutzer Storage-Objekte und Daten mit Unified Manager managen können.

Sie können einen Benutzer hinzufügen, indem Sie die folgenden Felder ausfüllen:

- **Typ**

  Ermöglicht die Angabe des Benutzertyps, den Sie erstellen möchten.

- **Name**

  Ermöglicht Ihnen, einen Benutzernamen anzugeben, mit dem sich ein Benutzer bei Unified Manager anmelden kann.

- **Passwort**

  Ermöglicht Ihnen die Angabe eines Passworts für den angegebenen Benutzernamen. Dieses Feld wird nur angezeigt, wenn Sie einen lokalen Benutzer oder einen Datenbankbenutzer hinzufügen.

- **Passwort Bestätigen**

  Ermöglicht Ihnen die erneute Eingabe Ihres Kennworts, um die Genauigkeit der Angaben im Feld „Kennwort“ sicherzustellen. Dieses Feld wird nur angezeigt, wenn Sie einen lokalen Benutzer oder einen Datenbankbenutzer hinzufügen.

- **E-Mail**

  Ermöglicht Ihnen die Angabe einer E-Mail-Adresse für den Benutzer; die angegebene E-Mail-Adresse muss eindeutig dem Benutzernamen entsprechen. Dieses Feld wird nur angezeigt, wenn Sie einen Remote-Benutzer oder einen lokalen Benutzer hinzufügen.

- * Rolle*

  Ermöglicht es Ihnen, dem Benutzer eine Rolle zuzuweisen und den Umfang der Aktivitäten festzulegen, die der Benutzer durchführen kann. Als Rolle können OnCommand-Administrator, Storage-Administrator, Operator, Integrations-Schema oder das Berichtschema verwendet werden.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Hinzufügen**

  Fügt den Benutzer hinzu und schließt das Dialogfeld Benutzer hinzufügen.

- **Abbrechen**

  Bricht die Änderungen ab und schließt das Dialogfeld Benutzer hinzufügen.

Dialogfeld „Benutzer bearbeiten“

Im Dialogfeld Benutzer bearbeiten können Sie je nach ausgewähltem Benutzer nur bestimmte Einstellungen bearbeiten.

Details

Im Bereich Details können Sie die folgenden Informationen über einen ausgewählten Benutzer bearbeiten:

- **Typ**

  Dieses Feld kann nicht bearbeitet werden.

- **Name**

  Dieses Feld kann nicht bearbeitet werden.

- **Passwort**

  Ermöglicht Ihnen das Bearbeiten des Kennworts, wenn der ausgewählte Benutzer ein Datenbankbenutzer ist.

- **Passwort Bestätigen**

  Hiermit können Sie das bestätigte Kennwort bearbeiten, wenn der ausgewählte Benutzer ein Datenbankbenutzer ist.

- **E-Mail**

  Ermöglicht Ihnen die Bearbeitung der E-Mail-Adresse des ausgewählten Benutzers. Dieses Feld kann bearbeitet werden, wenn der ausgewählte Benutzer ein lokaler Benutzer, ein LDAP-Benutzer oder ein Wartungbenutzer ist.

- * Rolle*

  Ermöglicht Ihnen die Bearbeitung der Rolle, die dem Benutzer zugewiesen ist. Dieses Feld kann bearbeitet werden, wenn der ausgewählte Benutzer ein lokaler Benutzer, ein Remote-Benutzer oder eine Remote-Gruppe ist.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Speichern**

  Speichert die Änderungen und schließt das Dialogfeld Benutzer bearbeiten.

- **Abbrechen**

  Bricht die Änderungen ab und schließt das Dialogfeld Benutzer bearbeiten.

Verwalten der Authentifizierung

Sie können die Authentifizierung mit LDAP oder Active Directory auf dem Unified Manager-Server aktivieren und so konfigurieren, dass sie mit Ihren Servern zur Authentifizierung von Remote-Benutzern verwendet werden kann.

Darüber hinaus können Sie die SAML-Authentifizierung aktivieren, damit Remote-Benutzer über einen sicheren Identitäts-Provider (IdP) authentifiziert werden, bevor sie sich in der Web-UI von Unified Manager anmelden können.

Aktivieren der Remote-Authentifizierung

Sie können die Remote-Authentifizierung aktivieren, damit der Unified Manager-Server mit Ihren Authentifizierungsservern kommunizieren kann. Die Benutzer des Authentifizierungsservers können auf die grafische Schnittstelle von Unified Manager zugreifen, um Storage-Objekte und Daten zu managen.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

> Der Unified Manager-Server muss direkt mit dem Authentifizierungsserver verbunden sein. Sie müssen alle lokalen LDAP-Clients wie SSSD (System Security Services Daemon) oder NSLCD (Name Service LDAP Caching Daemon) deaktivieren.

Über diese Aufgabe

Sie können die Remote-Authentifizierung entweder über Open LDAP oder Active Directory aktivieren. Wenn die Remote-Authentifizierung deaktiviert ist, können Remote-Benutzer nicht auf Unified Manager zugreifen.

Die Remote-Authentifizierung wird über LDAP und LDAPS (Secure LDAP) unterstützt. Unified Manager verwendet 389 als Standardport für nicht sichere Kommunikation und 636 als Standardport für sichere Kommunikation.

> Das Zertifikat, das zur Authentifizierung von Benutzern verwendet wird, muss dem X.509-Format entsprechen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** die Option **Remote-Authentifizierung aktivieren** aus.
3. Wählen Sie im Feld **Authentifizierungsdienst** den Diensttyp aus und konfigurieren Sie den Authentifizierungsdienst.

Für Authentifizierungstyp…	Geben Sie die folgenden Informationen ein…
Active Directory	• Administratorname des Authentifizierungsservers in einem der folgenden Formate: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (Mit der entsprechenden LDAP-Schreibweise) • Administratorpasswort • Basisname (unter Verwendung der entsprechenden LDAP-Notation)
Öffnen Sie LDAP	• Distinguished Name binden (in der entsprechenden LDAP-Notation) • Kennwort binden • Basisname mit Distinguished Name

Wenn die Authentifizierung eines Active Directory-Benutzers sehr viel Zeit oder Zeit in Anspruch nimmt, benötigt der Authentifizierungsserver wahrscheinlich eine lange Zeit, um darauf zu reagieren. Wenn Sie die Unterstützung für verschachtelte Gruppen in Unified Manager deaktivieren, wird die Authentifizierungszeit möglicherweise verkürzt.

Wenn Sie die Option Sichere Verbindung verwenden für den Authentifizierungsserver auswählen, kommuniziert Unified Manager mit dem Authentifizierungsserver über das SSL-Protokoll (Secure Sockets Layer).

4. Fügen Sie Authentifizierungsserver hinzu, und testen Sie die Authentifizierung.
5. Klicken Sie auf **Speichern und Schließen**.

Deaktivieren verschachtelter Gruppen von der Remote-Authentifizierung

Wenn die Remote-Authentifizierung aktiviert ist, können Sie die verschachtelte Gruppenauthentifizierung deaktivieren, sodass sich nur einzelne Benutzer und nicht Gruppenmitglieder im Remote-Zugriff auf Unified Manager authentifizieren können. Sie können verschachtelte Gruppen deaktivieren, wenn Sie die Reaktionszeit der Active Directory-Authentifizierung verbessern möchten.

Bevor Sie beginnen

- Sie müssen die OnCommand-Administratorrolle besitzen.
- Das Deaktivieren verschachtelter Gruppen ist nur bei Verwendung von Active Directory anwendbar.

Über diese Aufgabe

Wenn Sie die Unterstützung für verschachtelte Gruppen in Unified Manager deaktivieren, wird die Authentifizierungszeit möglicherweise verkürzt. Wenn die Unterstützung verschachtelter Gruppen deaktiviert ist

und eine Remote-Gruppe zu Unified Manager hinzugefügt wird, müssen einzelne Benutzer Mitglieder der Remote-Gruppe sein, um sich bei Unified Manager zu authentifizieren.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Aktivieren Sie auf der Seite **Setup/Authentifizierung** das Kontrollkästchen **Nested Group Lookup deaktivieren**.
3. Klicken Sie Auf **Speichern**.

Einrichten von Authentifizierungsservices

Authentifizierungsservices ermöglichen die Authentifizierung von Remote-Benutzern oder Remotegruppen in einem Authentifizierungsserver, bevor sie ihnen den Zugriff auf Unified Manager gewähren. Sie können Benutzer mithilfe von vordefinierten Authentifizierungsdiensten (z. B. Active Directory oder OpenLDAP) authentifizieren, oder indem Sie Ihren eigenen Authentifizierungsmechanismus konfigurieren.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert haben.
- Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Klicken Sie auf der Seite **Setup** Optionen auf **Management Server** > **Authentifizierung**.
3. Wählen Sie einen der folgenden Authentifizierungsdienste aus:

Wenn Sie die Option…	Dann tun Sie das…
Active Directory	a. Geben Sie den Administratornamen und das Kennwort ein. b. Geben Sie den Basisnamen des Authentifizierungsservers an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, lautet der Name der Basisunterscheidungname `cn=ou,dc=domain,dc=com`.

Wenn Sie die Option…	Dann tun Sie das…
OpenLDAP	a. Geben Sie den Distinguished Name und das Bind-Passwort ein. b. Geben Sie den Basisnamen des Authentifizierungsservers an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, lautet der Name der Basisunterscheidungname `cn=ou,dc=domain,dc=com`.
Andere	a. Geben Sie den Distinguished Name und das Bind-Passwort ein. b. Geben Sie den Basisnamen des Authentifizierungsservers an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, lautet der Name der Basisunterscheidungname `cn=ou,dc=domain,dc=com`. c. Geben Sie die vom Authentifizierungsserver unterstützte LDAP-Protokollversion an. d. Geben Sie den Benutzernamen, die Gruppenmitgliedschaft, die Benutzergruppe und die Mitgliedsattribute ein.

Wenn Sie den Authentifizierungsdienst ändern möchten, müssen Sie alle vorhandenen Authentifizierungsserver löschen und dann neue Authentifizierungsserver hinzufügen.

4. Klicken Sie auf **Speichern und Schließen**.

Hinzufügen von Authentifizierungsservern

Sie können Authentifizierungsserver hinzufügen und die Remote-Authentifizierung auf dem Verwaltungsserver aktivieren, sodass Remote-Benutzer innerhalb des Authentifizierungsservers auf Unified Manager zugreifen können.

Bevor Sie beginnen

- Folgende Informationen müssen zur Verfügung stehen:
  - Hostname oder IP-Adresse des Authentifizierungsservers
  - Portnummer des Authentifizierungsservers
- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst so konfiguriert haben, dass der Verwaltungsserver Remote-Benutzer oder -Gruppen im Authentifizierungsserver

authentifizieren kann.

- Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Wenn der neue Authentifizierungsserver Teil eines Hochverfügbarkeitspaars (HA-Paar) ist (unter Verwendung derselben Datenbank), können Sie auch den Authentifizierungsserver des Partners hinzufügen. Dadurch kann der Management-Server mit dem Partner kommunizieren, wenn einer der Authentifizierungsserver nicht erreichbar ist.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Klicken Sie auf der Seite **Setup/Authentifizierung** auf **Management Server** > **Authentifizierung**.
3. Aktivieren oder Deaktivieren der Option * Sichere Verbindungsauthentifizierung verwenden*:

Ihr Ziel ist	Dann tun Sie das…
Aktivieren Sie sie	a. Aktivieren Sie im Kontrollkästchen Remoteauthentifizierung aktivieren die Option **Sichere Verbindung verwenden**. b. Klicken Sie im Bereich Authentication Servers auf **Add**. c. Geben Sie im Dialogfeld Authentifizierungsserver hinzufügen den Authentifizierungsnamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein. d. Klicken Sie im Dialogfeld Host autorisieren auf Zertifikat anzeigen. e. Überprüfen Sie im Dialogfeld Zertifikat anzeigen die Zertifikatinformationen und klicken Sie dann auf **Schließen**. f. Klicken Sie im Dialogfeld Host autorisieren auf **Ja**. Wenn Sie die Option **Sichere Verbindungsauthentifizierung verwenden** aktivieren, kommuniziert Unified Manager mit dem Authentifizierungsserver und zeigt das Zertifikat an. Unified Manager verwendet 636 als Standardport für sichere Kommunikation und Portnummer 389 für nicht sichere Kommunikation.

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren	a. Deaktivieren Sie im Kontrollkästchen Remoteauthentifizierung aktivieren die Option **Sichere Verbindung verwenden**. b. Klicken Sie im Bereich Authentication Servers auf **Add**. c. Geben Sie im Dialogfeld Authentifizierungsserver hinzufügen entweder den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) des Servers und die Portdetails an. d. Klicken Sie Auf **Hinzufügen**.

Der hinzugefügte Authentifizierungsserver wird im Bereich Server angezeigt.

4. Führen Sie eine Testauthentifizierung durch, um zu bestätigen, dass Sie Benutzer im hinzugefügten Authentifizierungsserver authentifizieren können.

Die Konfiguration der Authentifizierungsserver wird getestet

Sie können die Konfiguration Ihrer Authentifizierungsserver überprüfen, um sicherzustellen, dass der Verwaltungsserver mit diesen Servern kommunizieren kann. Sie können die Konfiguration validieren, indem Sie von Ihren Authentifizierungsservern nach einem Remote-Benutzer oder einer Remotegruppe suchen und diese unter Verwendung der konfigurierten Einstellungen authentifizieren.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst so konfiguriert haben, dass der Unified Manager-Server den Remote-Benutzer oder die Remote-Gruppe authentifizieren kann.
- Sie müssen Ihre Authentifizierungsserver hinzugefügt haben, damit der Verwaltungsserver von diesen Servern nach dem Remote-Benutzer oder der Remote-Gruppe suchen und diese authentifizieren kann.
- Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Wenn der Authentifizierungsservice auf Active Directory festgelegt ist und Sie die Authentifizierung von Remote-Benutzern validieren, die zur primären Gruppe des Authentifizierungsservers gehören, werden in den Authentifizierungsergebnissen keine Informationen zur primären Gruppe angezeigt.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Klicken Sie auf der Seite **Setup/Authentifizierung** auf **Testauthentifizierung**.
3. Geben Sie im Dialogfeld **Testbenutzer** den Benutzernamen und das Kennwort des Remote-Benutzers oder den Benutzernamen der Remote-Gruppe an und klicken Sie dann auf **Test**.

Wenn Sie eine Remote-Gruppe authentifizieren, müssen Sie das Kennwort nicht eingeben.

Bearbeiten von Authentifizierungsservern

Sie können den Port ändern, den der Unified Manager-Server für die Kommunikation mit Ihrem Authentifizierungsserver verwendet.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Aktivieren Sie auf der Seite **Setup/Authentifizierung** das Kontrollkästchen **Nested Group Lookup deaktivieren**.
3. Wählen Sie im Bereich **Authentifizierungsserver** den Authentifizierungsserver aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
4. Bearbeiten Sie im Dialogfeld **Authentifizierungsserver bearbeiten** die Portdetails.
5. Klicken Sie Auf **Speichern**.

Authentifizierungsserver werden gelöscht

Sie können einen Authentifizierungsserver löschen, wenn Sie verhindern möchten, dass der Unified Manager-Server mit dem Authentifizierungsserver kommuniziert. Wenn Sie beispielsweise einen Authentifizierungsserver ändern möchten, mit dem der Verwaltungsserver kommuniziert, können Sie den Authentifizierungsserver löschen und einen neuen Authentifizierungsserver hinzufügen.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Wenn Sie einen Authentifizierungsserver löschen, können Remote-Benutzer oder -Gruppen des Authentifizierungsservers nicht mehr auf Unified Manager zugreifen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** einen oder mehrere Authentifizierungsserver aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie auf **Ja**, um die Löschanforderung zu bestätigen.

   Wenn die Option **Sichere Verbindung verwenden** aktiviert ist, werden die mit dem Authentifizierungsserver verknüpften Zertifikate zusammen mit dem Authentifizierungsserver gelöscht.

Authentifizierung mit Active Directory oder OpenLDAP

Sie können die Remote-Authentifizierung auf dem Verwaltungsserver aktivieren und den Verwaltungsserver so konfigurieren, dass er mit Ihren Authentifizierungsservern kommuniziert, damit Benutzer innerhalb der Authentifizierungsserver auf Sie zugreifen können. Außerdem können Sie die Remote-Authentifizierung auf dem Verwaltungsserver aktivieren und den Verwaltungsserver so konfigurieren, dass er mit Ihren Authentifizierungsservern kommunizieren kann Dass Benutzer innerhalb der Authentifizierungsserver auf Unified Manager zugreifen können.

Sie können einen der folgenden vordefinierten Authentifizierungsservices verwenden oder Ihren eigenen Authentifizierungsservice angeben:

- Microsoft Active Directory

  Sie können Microsoft Lightweight Directory Services nicht verwenden.

- OpenLDAP

Sie können den erforderlichen Authentifizierungsservice auswählen und die entsprechenden Authentifizierungsserver hinzufügen, damit die Remote-Benutzer im Authentifizierungsserver auf Unified Manager zugreifen können. Die Anmeldeinformationen für Remote-Benutzer oder -Gruppen werden vom Authentifizierungsserver verwaltet. Der Verwaltungsserver verwendet das Lightweight Directory Access Protocol (LDAP) zur Authentifizierung von Remote-Benutzern innerhalb des konfigurierten Authentifizierungsservers.

Für lokale Benutzer, die in Unified Manager erstellt werden, behält der Verwaltungsserver eine eigene Datenbank mit Benutzernamen und Kennwörtern. Der Verwaltungsserver führt die Authentifizierung durch und verwendet Active Directory oder OpenLDAP nicht zur Authentifizierung.

Aktivieren der SAML-Authentifizierung

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

Bevor Sie beginnen

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

Über diese Aufgabe

Nachdem Sie die SAML-Authentifizierung von Unified Manager aktiviert haben, können Benutzer erst dann auf die grafische Benutzeroberfläche zugreifen, wenn das IdP mit den Hostinformationen des Unified Manager-Servers konfiguriert wurde. Daher müssen Sie darauf vorbereitet sein, beide Teile der Verbindung

abzuschließen, bevor Sie mit dem Konfigurationsprozess beginnen. Das IdP kann vor oder nach der Konfiguration von Unified Manager konfiguriert werden.

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

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML Authentication** aus.
3. Aktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.

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

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

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

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

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

6. Klicken Sie Auf **Speichern**.

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

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

Ergebnisse

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

Nachdem Sie fertig sind

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

Wenn Sie ADFS als Identitäts-Provider verwenden, wird die Unified Manager-GUI nicht das ADFS-Timeout-Timeout erfüllt und funktioniert weiter, bis das Timeout der Unified Manager-Sitzung erreicht ist. Wenn Unified Manager auf Windows, Red hat oder CentOS bereitgestellt wird, kann das Timeout der GUI-Sitzung mit dem folgenden Unified Manager CLI-Befehl geändert werden: `um option set absolute.session.timeout=00:15:00`Mit diesem Befehl wird das Zeitlimit für die Unified Manager GUI-Sitzung auf 15 Minuten festgelegt.

Anforderungen an Identitätsanbieter

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

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

Unterstützte Verschlüsselungsstandards

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

Validierte Identitätsanbieter

- Shibboleth
- Active Directory Federation Services (ADFS)

ADFS-Konfigurationsanforderungen

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

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

- Sie müssen die Authentifizierungsmethode auf „`Forms Authentication`“ festlegen, oder Benutzer erhalten möglicherweise einen Fehler beim Abmelden von Unified Manager, wenn Sie Internet Explorer verwenden. Führen Sie hierzu folgende Schritte aus:
  a. Öffnen Sie die ADFS-Verwaltungskonsole.
  b. Klicken Sie in der linken Strukturansicht auf den Ordner Authentication Policies.
  c. Klicken Sie unter Aktionen auf der rechten Seite auf Globale primäre Authentifizierungsrichtlinie bearbeiten.

d. Setzen Sie die Intranet-Authentifizierungsmethode auf „`Forms Authentication`“ anstatt auf die Standardauthentifizierung „`Windows Authentication`“.

- In einigen Fällen wird die Anmeldung über das IdP abgelehnt, wenn das Unified Manager-Sicherheitszertifikat CA-signiert ist. Es gibt zwei Problemumgehungen zur Lösung dieses Problems:
  - Befolgen Sie die Anweisungen im Link, um die Widerrufs-Prüfung auf dem ADFS-Server für verkettete CA-Zertifikat zugeordnete abhängige Partei zu deaktivieren:

    http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

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

Sonstige Konfigurationsanforderungen

- Die Unified Manager-Taktskew ist auf 5 Minuten eingestellt, sodass der Zeitunterschied zwischen dem IdP-Server und dem Unified Manager-Server nicht mehr als 5 Minuten betragen kann oder die Authentifizierung fehlschlägt.
- Wenn Benutzer versuchen, mit Internet Explorer auf Unified Manager zuzugreifen, wird möglicherweise die Meldung angezeigt **die Webseite kann die Seite nicht anzeigen**. Stellen Sie in diesem Fall sicher, dass diese Benutzer die Option „`Sso freundliche HTTP-Fehlermeldungen`“ in **Tools** > **Internetoptionen** > **Erweitert** deaktivieren.

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML Authentication** aus.
3. Geben Sie die neue IdP-URI und die IdP-Metadaten ein, die erforderlich sind, um den Unified Manager-Server mit dem IdP zu verbinden.

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

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

5. Klicken Sie Auf **Konfiguration Speichern**.

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

6. Klicken Sie auf **OK**.

Nachdem Sie fertig sind

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

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

Deaktivieren der SAML-Authentifizierung

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

Über diese Aufgabe

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

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

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML Authentication** aus.
3. Deaktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.
4. Klicken Sie Auf **Speichern**.

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

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

Ergebnisse

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

IdP-Anmeldeseite ein.

Nachdem Sie fertig sind

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

Beschreibung der Authentifizierungsfenster und Dialogfelder

Sie können die LDAP-Authentifizierung über die Seite Setup/Authentifizierung aktivieren.

Seite „Einrichtung/Authentifizierung“

Mithilfe der Seite Setup/Authentifizierung kann Unified Manager für die Authentifizierung von Remote-Benutzern konfiguriert werden, die versuchen, sich in der Web-UI von Unified Manager anzumelden.

Über die Seite Remote Authentication können Sie Unified Manager für die Kommunikation mit Ihrem Authentifizierungsserver konfigurieren, um Remote-Benutzer zu authentifizieren.

Über die Seite SAML Authentication können Sie Unified Manager für die Kommunikation mit einem sicheren Identitäts-Provider (IdP) zur Authentifizierung von Remote-Benutzern konfigurieren.

Seite „Remote Authentication“

Mithilfe der Seite Remote Authentication kann Unified Manager für die Kommunikation mit Ihrem Authentifizierungsserver konfiguriert werden, um Remote-Benutzer zu authentifizieren, die versuchen, sich in der Web-UI von Unified Manager anzumelden.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Nachdem Sie das Kontrollkästchen Remote-Authentifizierung aktivieren aktiviert haben, können Sie die Remote-Authentifizierung über einen Authentifizierungsserver aktivieren.

- **Authentifizierungsdienst**

  Ermöglicht Ihnen, den Verwaltungsserver so zu konfigurieren, dass Benutzer in Verzeichnisdienstanbietern wie Active Directory, OpenLDAP authentifiziert werden oder dass Sie Ihren eigenen Authentifizierungsmechanismus festlegen. Sie können einen Authentifizierungsservice nur festlegen, wenn Sie die Remote-Authentifizierung aktiviert haben.

  - **Active Directory**
    - Administratorname

      Gibt den Administratornamen des Authentifizierungsservers an.

    - Passwort

      Gibt das Kennwort für den Zugriff auf den Authentifizierungsserver an.

    - Name Der Basisstation

      Gibt den Speicherort der Remote-Benutzer im Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, lautet der Name der

Basisunterscheidungname `cn=ou,dc=domain,dc=com`.

- Deaktivieren Sie Die Suche Nach Verschachtelter Gruppe

  Gibt an, ob die Option für die Suche nach verschachtelten Gruppen aktiviert oder deaktiviert werden soll. Diese Option ist standardmäßig deaktiviert. Wenn Sie Active Directory verwenden, können Sie die Authentifizierung beschleunigen, indem Sie die Unterstützung für verschachtelte Gruppen deaktivieren.

- Verwenden Sie Secure Connection

  Gibt den Authentifizierungsservice an, der für die Kommunikation mit Authentifizierungsservern verwendet wird.

◦ **OpenLDAP**

- Distinguished Name Binden

  Gibt den Distinguished BIND-Namen an, der zusammen mit dem angegebenen Basisnamen zum Suchen von Remote-Benutzern im Authentifizierungsserver verwendet wird.

- Kennwort Binden

  Gibt das Kennwort für den Zugriff auf den Authentifizierungsserver an.

- Name Der Basisstation

  Gibt den Speicherort der Remote-Benutzer im Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, lautet der Name der Basisunterscheidungname `cn=ou,dc=domain,dc=com`.

- Verwenden Sie Secure Connection

  Gibt an, dass Secure LDAP für die Kommunikation mit LDAPS-Authentifizierungsservern verwendet wird.

◦ **Andere**

- Distinguished Name Binden

  Gibt den Distinguished BIND-Namen an, der zusammen mit dem angegebenen Basisnamen verwendet wird, um Remote-Benutzer auf dem von Ihnen konfigurierten Authentifizierungsserver zu finden.

- Kennwort Binden

  Gibt das Kennwort für den Zugriff auf den Authentifizierungsserver an.

- Name Der Basisstation

  Gibt den Speicherort der Remote-Benutzer im Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, lautet der Name der Basisunterscheidungname `cn=ou,dc=domain,dc=com`.

- Protokollversion

  Gibt die LDAP-Version (Lightweight Directory Access Protocol) an, die von Ihrem

Authentifizierungsserver unterstützt wird. Sie können festlegen, ob die Protokollversion automatisch erkannt werden muss oder ob die Version auf 2 oder 3 eingestellt werden muss.

- Attribut Benutzername

  Gibt den Namen des Attributs im Authentifizierungsserver an, der Benutzeranmeldungsnamen enthält, die vom Verwaltungsserver authentifiziert werden sollen.

- Eigenschaft „Gruppenmitgliedschaft“

  Gibt einen Wert an, der die Mitgliedschaft der Managementservergruppe Remote-Benutzern auf der Grundlage eines im Authentifizierungsserver des Benutzers angegebenen Attributs und Wertes zuweist.

- UGID

  Wenn die Remote-Benutzer als Mitglieder einer Gruppe OfUniqueNames-Objekt im Authentifizierungsserver enthalten sind, können Sie mit dieser Option die Mitgliedschaft der Management-Servergruppe den Remotebenutzern basierend auf einem bestimmten Attribut in dieser GroupOfUniqueNames-Objekt zuweisen.

- Deaktivieren Sie Die Suche Nach Verschachtelter Gruppe

  Gibt an, ob die Option für die Suche nach verschachtelten Gruppen aktiviert oder deaktiviert werden soll. Diese Option ist standardmäßig deaktiviert. Wenn Sie Active Directory verwenden, können Sie die Authentifizierung beschleunigen, indem Sie die Unterstützung für verschachtelte Gruppen deaktivieren.

- Mitglied

  Gibt den Attributnamen an, den Ihr Authentifizierungsserver zum Speichern von Informationen über die einzelnen Mitglieder einer Gruppe verwendet.

- Benutzerobjektklasse

  Gibt die Objektklasse eines Benutzers im Remote-Authentifizierungsserver an.

- Objektklasse Gruppieren

  Gibt die Objektklasse aller Gruppen im Remote-Authentifizierungsserver an.

- Verwenden Sie Secure Connection

  Gibt den Authentifizierungsservice an, der für die Kommunikation mit Authentifizierungsservern verwendet wird.

> Wenn Sie den Authentifizierungsservice ändern möchten, müssen Sie sicherstellen, dass Sie alle vorhandenen Authentifizierungsserver löschen und neue Authentifizierungsserver hinzufügen.

Bereich Authentifizierungsserver

Im Bereich Authentifizierungsserver werden die Authentifizierungsserver angezeigt, mit denen der Verwaltungsserver kommuniziert, um Remotebenutzer zu finden und zu authentifizieren. Die Anmeldeinformationen für Remote-Benutzer oder -Gruppen werden vom Authentifizierungsserver verwaltet.

- **Befehlsschaltflächen**

  Ermöglicht das Hinzufügen, Bearbeiten oder Löschen von Authentifizierungsservern.

  - Zusatz

    Ermöglicht das Hinzufügen eines Authentifizierungsservers.

  Wenn der hinzugefügte Authentifizierungsserver Teil eines Hochverfügbarkeitspaars ist (unter Verwendung derselben Datenbank), können Sie auch den Authentifizierungsserver des Partners hinzufügen. Dadurch kann der Management-Server mit dem Partner kommunizieren, wenn einer der Authentifizierungsserver nicht erreichbar ist.

  - Bearbeiten

    Ermöglicht die Bearbeitung der Einstellungen für einen ausgewählten Authentifizierungsserver.

  - Löschen

    Löscht die ausgewählten Authentifizierungsserver.

- **Name oder IP-Adresse**

  Zeigt den Hostnamen oder die IP-Adresse des Authentifizierungsservers an, der zur Authentifizierung des Benutzers auf dem Verwaltungsserver verwendet wird.

- **Port**

  Zeigt die Portnummer des Authentifizierungsservers an.

- **Testauthentifizierung**

  Mit dieser Schaltfläche wird die Konfiguration Ihres Authentifizierungsservers durch Authentifizierung eines Remotebenutzers oder einer -Gruppe validiert.

  Wenn Sie beim Testen nur den Benutzernamen angeben, sucht der Verwaltungsserver im Authentifizierungsserver nach dem Remote-Benutzer, authentifiziert den Benutzer jedoch nicht. Wenn Sie sowohl den Benutzernamen als auch das Passwort angeben, sucht der Verwaltungsserver den Remote-Benutzer und authentifiziert diesen.

  Sie können die Authentifizierung nicht testen, wenn die Remote-Authentifizierung deaktiviert ist.

Seite SAML Authentication

Mithilfe der Seite SAML Authentication kann Unified Manager für die Authentifizierung von Remote-Benutzern mit SAML über einen sicheren Identitäts-Provider (IdP) konfiguriert werden, bevor sie sich in der Web-UI von Unified Manager anmelden können.

- Sie müssen über die OnCommand-Administratorrolle verfügen, um die SAML-Konfiguration erstellen oder ändern zu können.
- Sie müssen die Remote-Authentifizierung konfiguriert haben.
- Sie müssen mindestens einen Remote-Benutzer oder eine Remote-Gruppe konfiguriert haben.

Nachdem die Remote-Authentifizierung und Remote-Benutzer konfiguriert wurden, können Sie das

Kontrollkästchen SAML-Authentifizierung aktivieren aktivieren aktivieren auswählen, um die Authentifizierung über einen sicheren Identitätsanbieter zu aktivieren.

- **IdP URI**

  Der URI für den Zugriff auf das IdP vom Unified Manager-Server aus. Beispiel-URIs sind unten aufgeführt.

  ADFS-Beispiel-URI:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Shibboleth Beispiel URI:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **IdP-Metadaten**

  Die IdP-Metadaten im XML-Format.

  Wenn über den Unified Manager-Server auf die IdP-URL zugegriffen werden kann, können Sie auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um dieses Feld auszufüllen.

- **Host-System (FQDN)**

  Der FQDN des Unified Manager-Hostsystems, wie bei der Installation definiert. Sie können diesen Wert bei Bedarf ändern.

- **Host-URI**

  Die URI für den Zugriff auf das Unified Manager-Hostsystem von der IdP aus.

- **Host-Metadaten**

  Die Metadaten des Host-Systems im XML-Format.

Verwalten von Sicherheitszertifikaten

Sie können HTTPS im Unified Manager-Server konfigurieren, um Ihre Cluster über eine sichere Verbindung zu überwachen und zu verwalten.

Anzeigen des HTTPS-Sicherheitszertifikats

Sie können die HTTPS-Zertifikatsdetails mit dem abgerufenen Zertifikat in Ihrem Browser vergleichen, um sicherzustellen, dass die verschlüsselte Verbindung Ihres Browsers mit Unified Manager nicht abgefangen wird.

Bevor Sie beginnen

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

Über diese Aufgabe

Durch das Anzeigen des Zertifikats können Sie den Inhalt eines neu erstellten Zertifikats oder alternative URL-Namen anzeigen, von denen aus Sie auf Unified Manager zugreifen können.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Setup** auf **HTTPS-Zertifikat**.

   Das HTTPS-Zertifikat wird oben auf der Seite angezeigt

Nachdem Sie fertig sind

Wenn Sie ausführlichere Informationen zum Sicherheitszertifikat als auf der Seite HTTPS-Zertifikat anzeigen müssen, können Sie das Verbindungszertifikat in Ihrem Browser anzeigen.

Erstellen eines HTTPS-Sicherheitszertifikats

Sie können aus mehreren Gründen ein neues HTTPS-Sicherheitszertifikat generieren, z. B. wenn Sie mit einer anderen Zertifizierungsstelle signieren möchten oder wenn das aktuelle Sicherheitszertifikat abgelaufen ist. Das neue Zertifikat ersetzt das vorhandene Zertifikat.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Wenn Sie keinen Zugriff auf die Web-UI von Unified Manager haben, können Sie mithilfe der Wartungskonsole das HTTPS-Zertifikat mit den gleichen Werten neu generieren.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Setup** auf **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikat erneut erstellen**.

   Das Dialogfeld „HTTPS-Zertifikat neu erstellen“ wird angezeigt.

3. Wählen Sie je nach Erstellung des Zertifikats eine der folgenden Optionen aus:

Ihr Ziel ist	Tun Sie das…
Generieren Sie das Zertifikat mit den aktuellen Werten neu	Klicken Sie auf die Option **regenerieren mit aktuellen Zertifikatattributen**.

Ihr Ziel ist	Tun Sie das…
Generieren Sie das Zertifikat mithilfe anderer Werte	Click the *Update the Current Certificate Attributes* option. Die Felder allgemeiner Name und Alternative Namen verwenden die Werte aus dem vorhandenen Zertifikat, wenn Sie keine neuen Werte eingeben. Die anderen Felder benötigen keine Werte, aber Sie können Werte eingeben, z. B. für Stadt, Bundesland und Land, wenn diese Werte in das Zertifikat eingetragen werden sollen. Sie können das Kontrollkästchen „lokale Identifizierungsdaten ausschließen (z. B. localhost)“ aktivieren, wenn Sie die lokalen Identifizierungsdaten aus dem Feld Alternative Namen im Zertifikat entfernen möchten. Wenn dieses Kontrollkästchen aktiviert ist, werden nur die Daten verwendet, die Sie in das Feld Alternative Namen eingeben. Wenn das Zertifikat leer gelassen wird, hat das resultierende Zertifikat überhaupt kein Feld alternativer Namen.

4. Klicken Sie auf **Ja**, um das Zertifikat erneut zu generieren.
5. Starten Sie den Unified Manager-Server neu, damit das neue Zertifikat wirksam wird.

Nachdem Sie fertig sind

Überprüfen Sie die neuen Zertifikatinformationen, indem Sie das HTTPS-Zertifikat anzeigen.

Starten Sie die Virtual Machine von Unified Manager neu

Sie können die virtuelle Maschine von der Wartungskonsole von Unified Manager aus neu starten. Sie müssen neu starten, nachdem Sie ein neues Sicherheitszertifikat erstellt haben oder wenn ein Problem mit der virtuellen Maschine auftritt.

Bevor Sie beginnen

Die virtuelle Appliance wird eingeschaltet.

Sie sind als Maintenance-Benutzer bei der Wartungskonsole angemeldet.

Über diese Aufgabe

Sie können die virtuelle Maschine von vSphere auch mit der Option **Neustart Gast** neu starten. Weitere Informationen finden Sie in der VMware Dokumentation.

Schritte

1. Öffnen Sie die Wartungskonsole.
2. Wählen Sie **Systemkonfiguration** > **Virtuelle Maschine Neu Starten**.

Herunterladen einer Anforderung zum Signieren eines HTTPS-Zertifikats

Sie können eine Zertifizierungsanfrage für das aktuelle HTTPS-Sicherheitszertifikat herunterladen, so dass Sie die Datei einer Zertifizierungsstelle zum Signieren bereitstellen können. Ein von einer Zertifizierungsstelle signiertes Zertifikat hilft bei der Verhinderung von man-in-the-Middle-Angriffen und bietet besseren Schutz als ein selbstsigniertes Zertifikat.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Setup** auf **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikatsignierungsanforderung herunterladen**.
3. Speichern Sie die `<hostname>.csr` Datei:

Nachdem Sie fertig sind

Sie können die Datei einer Zertifizierungsstelle zum Signieren bereitstellen und dann das signierte Zertifikat installieren.

Installieren eines HTTPS-Sicherheitszertifikats

Sie können ein Sicherheitszertifikat hochladen und installieren, nachdem eine Zertifizierungsstelle unterschrieben und zurückgesendet wurde. Die Datei, die Sie hochladen und installieren, muss eine signierte Version des vorhandenen selbstsignierten Zertifikats sein. Ein CA-signiertes Zertifikat hilft bei der Verhinderung von man-in-the-Middle-Angriffen und bietet besseren Schutz als ein selbstsigniertes Zertifikat.

Bevor Sie beginnen

Sie müssen die folgenden Aktionen durchgeführt haben:

- Laden Sie die Zertifikatsignierungsanforderungsdatei herunter und lassen Sie sie von einer Zertifizierungsstelle signiert werden
- Die Zertifikatskette wurde im PEM-Format gespeichert
- Alle Zertifikate in der Kette enthalten, vom Unified Manager-Serverzertifikat bis zum Stammzertifikat, einschließlich aller vorhandenen Zwischenzertifikate

Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Setup** auf **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikat installieren**.
3. Klicken Sie im angezeigten Dialogfeld auf **Datei auswählen…**, um die hochzuladende Datei zu suchen.
4. Wählen Sie die Datei aus und klicken Sie dann auf **Installieren**, um die Datei zu installieren.

Beispiel für eine Zertifikatskette

Das folgende Beispiel zeigt, wie die Zertifikatkettendatei angezeigt werden kann:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 \(if present\)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 \(if present\)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Seitenbeschreibungen zur Zertifikatverwaltung

Auf der Seite HTTPS-Zertifikat können Sie die aktuellen Sicherheitszertifikate anzeigen und neue HTTPS-Zertifikate erstellen.

Seite „HTTPS-Zertifikat“

Auf der Seite HTTPS-Zertifikat können Sie das aktuelle Sicherheitszertifikat anzeigen, eine Anforderung zum Signieren von Zertifikaten herunterladen, ein neues HTTPS-Zertifikat erstellen oder ein neues HTTPS-Zertifikat installieren.

Wenn Sie kein neues HTTPS-Zertifikat generiert haben, wird auf dieser Seite das Zertifikat angezeigt, das während der Installation generiert wurde.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Vorgänge ausführen:

- **HTTPS-Zertifikatsignierungsanforderung herunterladen**

  Lädt eine Zertifizierungsanfrage für das aktuell installierte HTTPS-Zertifikat herunter. Sie werden vom Browser aufgefordert, das zu speichern `<hostname>.csr` Datei so, dass Sie die Datei an eine Zertifizierungsstelle zum Signieren zur Verfügung stellen können.

- **HTTPS-Zertifikat installieren**

  Ermöglicht es Ihnen, ein Sicherheitszertifikat hochzuladen und zu installieren, nachdem eine Zertifizierungsstelle unterschrieben und zurückgesendet wurde. Das neue Zertifikat wird wirksam, nachdem Sie den Verwaltungsserver neu gestartet haben.

- **HTTPS-Zertifikat neu erstellen**

  Ermöglicht Ihnen das Generieren eines HTTPS-Zertifikats, das das aktuelle Sicherheitszertifikat ersetzt. Das neue Zertifikat wird wirksam, nachdem Sie Unified Manager neu gestartet haben.

Dialogfeld „HTTPS-Zertifikat neu erstellen“

Das Dialogfeld „HTTPS-Zertifikat neu erstellen“ ermöglicht Ihnen, die Sicherheitsinformationen anzupassen und anschließend ein neues HTTPS-Zertifikat mit diesen Informationen zu erstellen.

Die aktuellen Zertifikatinformationen werden auf dieser Seite angezeigt.

Mit der Auswahl „`regenerieren mit aktuellen Zertifikatattributen`“ und „`Aktuellen Zertifikatattributen aktualisieren`“ können Sie das Zertifikat mit den aktuellen Informationen neu generieren oder ein Zertifikat mit neuen Informationen generieren.

- **Gemeinsamer Name**

  Erforderlich. Der vollständig qualifizierte Domänenname (FQDN), den Sie sichern möchten.

  Verwenden Sie in den Hochverfügbarkeitskonfigurationen von Unified Manager die virtuelle IP-Adresse.

- **E-Mail**

  Optional Eine E-Mail-Adresse, an die Sie sich mit Ihrem Unternehmen wenden können, in der Regel die E-Mail-Adresse des Zertifikatadministrators oder DER IT-Abteilung.

- **Unternehmen**

  Optional In der Regel wird der Name Ihres Unternehmens eingetragen.

- **Abteilung**

  Optional Der Name der Abteilung in Ihrem Unternehmen.

- **Stadt**

  Optional Der Standort der Stadt Ihrer Firma.

- **Bundesland**

  Optional Der Ort des Staates oder der Provinz, nicht abgekürzt, Ihrer Firma.

- **Land**

  Optional Der Standort Ihres Unternehmens in Ihrem Land. Dies ist in der Regel ein zweistelliger ISO-Code des Landes.

- **Alternative Namen**

  Erforderlich. Zusätzliche, nicht primäre Domain-Namen, die verwendet werden können, um auf diesen Server zusätzlich zu den vorhandenen localhost oder anderen Netzwerkadressen zugreifen. Trennen Sie jeden alternativen Namen durch ein Komma.

  Aktivieren Sie das Kontrollkästchen „`lokale Identifizierungsdaten ausschließen (z. B. localhost)`“, wenn Sie die lokalen Identifizierungsdaten aus dem Feld Alternative Namen im Zertifikat entfernen möchten. Wenn dieses Kontrollkästchen aktiviert ist, werden nur die Daten verwendet, die Sie in das Feld Alternative Namen eingeben. Wenn das Zertifikat leer gelassen wird, hat das resultierende Zertifikat überhaupt kein Feld alternativer Namen.

Fehlerbehebung

Mithilfe von Informationen zur Fehlerbehebung können Sie Probleme identifizieren und beheben, die bei Verwendung von Unified Manager auftreten.

Ändern des Unified Manager-Host-Namens

Irgendwann möchten Sie möglicherweise den Host-Namen des Systems ändern, auf dem Unified Manager installiert ist. Beispielsweise möchten Sie den Host umbenennen, um Ihre Unified Manager-Server nach Typ, Arbeitsgruppe oder überwachten Cluster-Gruppen einfacher zu identifizieren.

Je nachdem, ob Unified Manager auf einem VMware ESXi Server, auf einem Red hat oder CentOS Linux Server oder auf einem Microsoft Windows Server ausgeführt wird, sind die zum Ändern des Host-Namens erforderlichen Schritte unterschiedlich.

Ändern des Host-Namens der virtuellen Unified Manager-Appliance

Dem Netzwerk-Host wird ein Name zugewiesen, wenn die virtuelle Unified Manager-Appliance zuerst bereitgestellt wird. Sie können den Host-Namen nach der Bereitstellung ändern. Wenn Sie den Hostnamen ändern, müssen Sie auch das HTTPS-Zertifikat neu generieren.

Bevor Sie beginnen

Sie müssen bei Unified Manager als Wartungbenutzer angemeldet sein oder Ihnen die Rolle „OnCommand Administrator“ zugewiesen haben, um diese Aufgaben ausführen zu können.

Über diese Aufgabe

Sie können den Host-Namen (oder die Host-IP-Adresse) verwenden, um auf die Unified Manager Web-UI zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, hätten Sie einen Namen für den Netzwerk-Host zugewiesen. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollte der Host-Name aus dem DNS übernommen werden. Wenn DHCP oder DNS nicht richtig konfiguriert ist, wird der Hostname „`OnCommand`“ automatisch zugewiesen und dem Sicherheitszertifikat zugeordnet.

Unabhängig davon, wie der Hostname zugewiesen wurde, wenn Sie den Host-Namen ändern und beabsichtigen, den neuen Hostnamen zum Zugriff auf die Unified Manager Web-UI zu verwenden, müssen Sie ein neues Sicherheitszertifikat generieren.

Wenn Sie über die IP-Adresse des Servers und nicht über den Hostnamen auf die Web-Benutzeroberfläche zugreifen, müssen Sie kein neues Zertifikat generieren, wenn Sie den Hostnamen ändern. Es empfiehlt sich jedoch, das Zertifikat so zu aktualisieren, dass der Hostname im Zertifikat dem tatsächlichen Hostnamen entspricht.

Wenn Sie den Host-Namen in Unified Manager ändern, müssen Sie den Hostnamen in OnCommand Workflow Automation (WFA) manuell aktualisieren. Der Host-Name wird in WFA nicht automatisch aktualisiert.

Das neue Zertifikat wird erst wirksam, wenn die virtuelle Unified Manager-Maschine neu gestartet wird.

Schritte

1. Generieren eines HTTPS-Sicherheitszertifikats

   Wenn Sie den neuen Hostnamen zum Zugriff auf die Web-UI von Unified Manager verwenden möchten, müssen Sie das HTTPS-Zertifikat neu generieren, um es mit dem neuen Hostnamen zu verknüpfen.

2. Starten Sie die Virtual Machine von Unified Manager neu

   Nachdem Sie das HTTPS-Zertifikat erneut generiert haben, müssen Sie die virtuelle Unified Manager-Maschine neu starten.

Ändern des Unified Manager Host-Namens auf Linux-Systemen

Irgendwann möchten Sie den Host-Namen von Red hat Enterprise Linux oder CentOS Rechner ändern, auf dem Unified Manager installiert ist. Sie möchten beispielsweise den Host umbenennen, um Ihre Unified Manager-Server nach Typ, Arbeitsgruppe oder überwachten Cluster-Gruppen einfacher zu identifizieren, wenn Sie Ihre Linux-Maschinen auflisten.

Bevor Sie beginnen

Sie müssen über Root-Benutzerzugriff auf das Linux-System verfügen, auf dem Unified Manager installiert ist.

Über diese Aufgabe

Sie können den Host-Namen (oder die Host-IP-Adresse) verwenden, um auf die Unified Manager Web-UI zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, hätten Sie einen Namen für den Netzwerk-Host zugewiesen. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollte der Hostname vom DNS-Server übernommen werden.

Unabhängig davon, wie der Hostname zugewiesen wurde, müssen Sie ein neues Sicherheitszertifikat erstellen, wenn Sie den Hostnamen ändern und den neuen Hostnamen für den Zugriff auf die Unified Manager Web-UI verwenden möchten.

Wenn Sie über die IP-Adresse des Servers und nicht über den Hostnamen auf die Web-Benutzeroberfläche zugreifen, müssen Sie kein neues Zertifikat generieren, wenn Sie den Hostnamen ändern. Es empfiehlt sich jedoch, das Zertifikat zu aktualisieren, sodass der Hostname im Zertifikat dem tatsächlichen Hostnamen entspricht. Das neue Zertifikat wird erst wirksam, wenn der Linux-Rechner neu gestartet wird.

Wenn Sie den Host-Namen in Unified Manager ändern, müssen Sie den Hostnamen in OnCommand Workflow Automation (WFA) manuell aktualisieren. Der Host-Name wird in WFA nicht automatisch aktualisiert.

Schritte

1. Melden Sie sich als Root-Benutzer beim Unified Manager-System an, das Sie ändern möchten.
2. Beenden Sie die Unified Manager Software und die zugehörige MySQL Software, indem Sie die folgenden Befehle in der angezeigten Reihenfolge eingeben:
3. Ändern Sie den Host-Namen mit Linux `hostnamectl` Befehl: `hostnamectl set-hostname new_FQDN`

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Generieren Sie das HTTPS-Zertifikat für den Server erneut:`/opt/netapp/essentials/bin/cert.sh create`
5. Netzwerkdienst neu starten: `service network restart`
6. Überprüfen Sie nach dem Neustart des Dienstes, ob der neue Hostname selbst pingen kann: `ping new_hostname`

   ```
   ping nuhost
   ```

   Dieser Befehl sollte dieselbe IP-Adresse zurückgeben, die zuvor für den ursprünglichen Hostnamen festgelegt wurde.

7. Nachdem Sie die Änderung Ihres Host-Namens abgeschlossen und überprüft haben, starten Sie Unified Manager neu, indem Sie in der angezeigten Reihenfolge die folgenden Befehle eingeben:

Hinzufügen von Festplattenspeicher zum Datenbankverzeichnis von Unified Manager

Das Datenbankverzeichnis von Unified Manager enthält sämtliche Gesundheits- und Performance-Daten, die von ONTAP Systemen erfasst wurden. Unter bestimmten Umständen kann es erforderlich sein, dass Sie die Größe des Datenbankverzeichnisses erhöhen.

Das Datenbankverzeichnis kann beispielsweise voll erhalten, wenn Unified Manager Daten von einer großen Anzahl von Clustern erfasst, in denen jedes Cluster über viele Nodes verfügt. Sie erhalten ein Warnereignis, wenn das Datenbankverzeichnis zu 90 % voll ist, und ein kritisches Ereignis, wenn das Verzeichnis zu 95 % voll ist.

Nach 95 % Auslastung des Verzeichnisses werden keine zusätzlichen Daten aus Clustern erfasst.

Je nachdem, ob Unified Manager auf einem VMware ESXi Server, auf einem Red hat oder CentOS Linux Server oder auf einem Microsoft Windows Server ausgeführt wird, welche Schritte zum Hinzufügen von Kapazität zum Datenverzeichnis erforderlich sind, unterscheiden sie sich.

Hinzufügen von Speicherplatz zur Datenfestplatte der virtuellen VMware-Maschine

Wenn Sie die Menge an Speicherplatz auf der Datenfestplatte für die Unified Manager-Datenbank erhöhen müssen, können Sie nach der Installation Kapazität hinzufügen, indem Sie den Festplattenspeicher erhöhen `disk 3`.

Bevor Sie beginnen

- Sie müssen Zugriff auf den vSphere Client haben.
- Auf der virtuellen Maschine dürfen keine Snapshots lokal gespeichert werden.
- Sie müssen über die Anmeldeinformationen für den Wartungs-Benutzer verfügen.

Über diese Aufgabe

Wir empfehlen, dass Sie Ihre virtuelle Maschine sichern, bevor Sie die Größe der virtuellen Laufwerke erhöhen.

Schritte

1. Wählen Sie im vSphere-Client die Virtual Machine Unified Manager aus und fügen Sie den Daten dann weitere Festplattenkapazität hinzu `disk 3`. Details finden Sie in der VMware Dokumentation.
2. Wählen Sie im vSphere-Client die virtuelle Unified Manager-Maschine aus und wählen Sie dann die Registerkarte **Konsole** aus.
3. Klicken Sie auf das Konsolenfenster, und melden Sie sich dann mit Ihrem Benutzernamen und Passwort an der Wartungskonsole an.
4. Geben Sie im **Hauptmenü** die Nummer für die Option **Systemkonfiguration** ein.
5. Geben Sie im Menü * Systemkonfiguration* die Nummer für die Option **Datenfestplattengröße erhöhen** ein.

Hinzufügen von Speicherplatz zum Datenverzeichnis des Linux-Hosts

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

Bevor Sie beginnen

Sie müssen Root-Benutzerzugriff auf die Red hat Enterprise Linux oder CentOS Linux Maschine haben, auf der Unified Manager installiert ist.

Über diese Aufgabe

Wir empfehlen, dass Sie ein Backup der Unified Manager-Datenbank erstellen, bevor Sie die Größe des Datenverzeichnisses vergrößern.

Schritte

1. Melden Sie sich als Root-Benutzer an dem Linux-Rechner an, auf dem Sie Speicherplatz hinzufügen möchten.
2. Beenden Sie den Unified Manager-Service und die zugehörige MySQL-Software in der folgenden Reihenfolge:
3. Erstellen eines temporären Sicherungsordners (z. B. `/backup-data`) Mit genügend Speicherplatz, um die Daten im aktuellen zu enthalten `/opt/netapp/data` Verzeichnis.
4. Kopieren Sie den Inhalt und die Berechtigungskonfiguration des vorhandenen `/opt/netapp/data` Verzeichnis zum Verzeichnis der Sicherungsdaten: `cp -rp /opt/netapp/data/* /backup-data`
5. Wenn SE Linux aktiviert ist:

   a. Holen Sie sich den SE Linux-Typ für Ordner auf bestehenden `/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 wie die folgende aus:

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Führen Sie die aus `chcon` Befehl zum Festlegen des SE Linux-Typs für das Backup-Verzeichnis: `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 750 GB über LVM-Befehle oder durch Hinzufügen zusätzlicher Festplatten.

   Montieren des `/opt/netapp/data` Das Verzeichnis in einem NFS-Export oder einer CIFS-Freigabe wird nicht unterstützt.
8. Bestätigen Sie das `/opt/netapp/data` Verzeichnis-Inhaber (mysql) und Gruppe (root) bleiben unverändert: `ls -ltr / | grep opt/netapp/data`

   Das System gibt eine Bestätigung wie die folgende aus:

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

9. Wenn SE Linux aktiviert ist, bestätigen Sie den Kontext für das `/opt/netapp/data` Verzeichnis ist noch auf mysqld_db_t eingestellt: `touch /opt/netapp/data/abc``ls -Z /opt/netapp/data/abc`

   Das System gibt eine Bestätigung wie die folgende aus:

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

10. Kopieren Sie den Inhalt von `backup-data`, Zurück zu den erweiterten `/opt/netapp/data` Verzeichnis: `cp -rp /backup-data/* /opt/netapp/data/`
11. Starten Sie den MySQL-Dienst: `service mysqld start`
12. Nachdem der MySQL-Dienst gestartet wurde, starten sie die ocie- und ocieau-Dienste in der folgenden Reihenfolge: `service ocie start``service ocieau start`
13. Löschen Sie nach dem Start aller Dienste den Sicherungsordner `/backup-data`: `rm -rf /backup-data`

Hinzufügen von Speicherplatz zum logischen Laufwerk des Microsoft Windows-Servers

Wenn Sie mehr Festplattenspeicher für die Unified Manager-Datenbank benötigen, können Sie das logische Laufwerk, auf dem Unified Manager installiert ist, um Kapazität erweitern.

Bevor Sie beginnen

Sie müssen über Administratorrechte für Windows verfügen.

Über diese Aufgabe

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

Schritte

1. Melden Sie sich als Administrator beim Windows-Server an, auf dem Sie Speicherplatz hinzufügen möchten.
2. Befolgen Sie den Schritt, der der Methode entspricht, die Sie verwenden möchten, um mehr Speicherplatz hinzuzufügen:

Option	Beschreibung
Fügen Sie auf einem physischen Server die Kapazität des logischen Laufwerks hinzu, auf dem der Unified Manager-Server installiert ist.	Folgen Sie den Schritten im Microsoft Thema: "Erweitern Sie ein Basisvolume"
Fügen Sie auf einem physischen Server ein Festplattenlaufwerk hinzu.	Folgen Sie den Schritten im Microsoft Thema: "Hinzufügen Von Festplattenlaufwerken"

Option	Beschreibung
Erhöhen Sie auf einer virtuellen Maschine die Größe einer Laufwerkspartition.	Folgen Sie den Schritten im VMware Thema: "Vergrößern einer Laufwerkspartition"

Ändern des Erfassungsintervalls der Performance-Statistiken

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

Bevor Sie beginnen

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

Über diese Aufgabe

Das Problem der Performance-Statistiken-Sammlungen, die nicht rechtzeitig beenden, wird durch die Banner-Meldungen angezeigt `Unable to consistently collect from cluster <cluster_name>` Oder `Data collection is taking too long on cluster <cluster_name>`.

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

> Wenn Sie diesen Wert ab der Standardeinstellung von 5 Minuten ändern, kann sich dies auf die Anzahl und Häufigkeit von Performance-Ereignissen auswirken, die Unified Manager meldet. So werden z. B. durch systemdefinierte Performance-Schwellenwerte Ereignisse ausgelöst, wenn die Richtlinie 30 Minuten lang überschritten wird. Bei der Verwendung von 5-minütigen Sammlungen muss die Richtlinie für sechs aufeinanderfolgende Sammlungen überschritten werden. Bei 15-minütigen Sammlungen muss die Richtlinie nur für zwei Sammelzeiträume überschritten werden.

Eine Meldung am Ende der Seite „Cluster Data Sources“ zeigt das aktuelle Intervall zur Erfassung statistischer Daten an.

Schritte

1. Loggen Sie sich mit SSH als Wartungsbenutzer beim Unified Manager Host ein.

   Die Eingabeaufforderungen für die Unified ManagerMaintenance-Konsole werden angezeigt.

2. Geben Sie die Nummer der Menüoption **Konfiguration des Leistungsintervalls** ein, und drücken Sie dann die Eingabetaste.
3. Geben Sie bei der entsprechenden Aufforderung das Wartungs-Benutzerpasswort erneut ein.
4. Geben Sie die Nummer für das neue Abfrageintervall ein, das Sie einstellen möchten, und drücken Sie dann die Eingabetaste.

Nachdem Sie fertig sind

Wenn Sie das Einfassungsintervall von Unified Manager auf 10 oder 15 Minuten geändert haben und eine aktuelle Verbindung zu einem externen Datenanbieter (z. B. Graphite) besteht, müssen Sie das Übertragungsintervall des Datenanbieters so ändern, dass es dem Erfassungsintervall von Unified Manager entspricht oder größer ist.

Aktivieren von regelmäßigen AutoSupport

Es besteht die Möglichkeit, bestimmte, vorab definierte Meldungen automatisch an den technischen Support zu senden, um den ordnungsgemäßen Betrieb der Umgebung sicherzustellen und die Integrität der Umgebung zu wahren.

Bevor Sie beginnen

Sie müssen als Wartungbenutzer angemeldet sein.

Über diese Aufgabe

Sie müssen AutoSupport aktivieren, um von den Vorteilen der NetApp Active IQ profitieren zu können.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Einrichtung** auf **AutoSupport**.
2. Aktivieren Sie das Kontrollkästchen **Periodensystem AutoSupport** aktivieren.
3. Geben Sie bei Bedarf den Namen, den Port und die Authentifizierungsinformationen für den HTTP Proxy-Server an.
4. Klicken Sie Auf **Speichern**.

Senden von On-Demand AutoSupport Nachrichten

Sie können Unified Manager Systeminformationen an den technischen Support senden, um Hilfe bei der Fehlerbehebung zu erhalten. Die Meldung AutoSupport enthält Diagnosesystem-Informationen und detaillierte Daten zum Unified Manager Server.

Bevor Sie beginnen

Sie müssen als Wartungbenutzer angemeldet sein.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Einrichtung** auf **AutoSupport**.
2. Führen Sie eine oder beide der folgenden Aktionen aus:

AutoSupport-Nachricht an…	Tun Sie das…
Technischer Support	Aktivieren Sie das Kontrollkästchen **an technischen Support senden**.

AutoSupport-Nachricht an…	Tun Sie das…
Einen bestimmten E-Mail-Empfänger	Aktivieren Sie das Kontrollkästchen **an E-Mail-Empfänger** und geben Sie die E-Mail-Adresse des Empfängers ein.

3. Definieren Sie bei Bedarf den Namen, Port und die Authentifizierungsinformationen für den HTTP Proxy-Server und klicken Sie auf **Speichern**.
4. Klicken Sie auf **AutoSupport generieren und senden**.

Setup-/AutoSupport-Seite

Auf der Seite Setup/AutoSupport können Sie die Beschreibung der AutoSupport anzeigen, regelmäßige AutoSupport aktivieren oder On-Demand AutoSupport Nachrichten senden.

Informationsbereich

- **System-ID**

  Zeigt die System-ID für diesen Unified Manager-Server an.

Bereich „Periodensystem AutoSupport“

Mit dieser Funktion können Sie dem technischen Support spezifische, vordefinierte Meldungen zur periodischen Problemdiagnose und -Behebung senden.

- **Periodensystem-AutoSupport aktivieren**

  Gibt an, dass Sie die Funktion „Periodensystem AutoSupport“ aktivieren möchten.

On-Demand AutoSupport Bereich

Sie können eine On-Demand-Nachricht an den technischen Support, einen bestimmten E-Mail-Empfänger oder beides generieren und senden:

- **An technischen Support senden**

  Zeigt an, dass Sie bei aufgetretenen Problemen eine On-Demand-Nachricht an den technischen Support senden möchten.

- **An E-Mail-Empfänger senden**

  Gibt an, dass Sie für alle aufgetretenen Probleme eine On-Demand-Nachricht an einen bestimmten Empfänger senden möchten.

- * AutoSupport generieren und senden*

  Generiert und sendet eine On-Demand-Nachricht an den technischen Support, einen angegebenen E-Mail-Empfänger oder beides, wenn Fehler aufgetreten sind.

HTTP-Proxy-Bereich

Sie können einen Proxy für den Internetzugriff festlegen, um AutoSupport-Inhalte zu unterstützen, falls Ihre Umgebung keinen direkten Zugriff vom Unified Manager-Server bietet.

- **HTTP Proxy verwenden**

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

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

- **Authentifizierung verwenden**

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

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

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

Unbekannter Authentifizierungsfehler

- **Ausgabe**

  Wenn Sie einen Authentifizierungsvorgang wie das Hinzufügen, Bearbeiten, Löschen oder Testen von Remote-Benutzern oder -Gruppen durchführen, wird möglicherweise die folgende Fehlermeldung angezeigt: `Unknown authentication error`.

- **Ursache**

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

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

- **Korrekturmaßnahmen**

  a. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Setup** > **Authentifizierung**.

  b. Geben Sie basierend auf dem ausgewählten Authentifizierungsservice die entsprechenden Informationen für den Administratornamen oder den Namen der Bind Distinguished Name ein.

  c. Klicken Sie auf **Authentifizierung testen**, um die Authentifizierung mit den von Ihnen angegebenen Details zu testen.

  d. Klicken Sie auf **Speichern und Schließen**.

Der Benutzer wurde nicht gefunden

- **Ausgabe**

  Wenn Sie einen Authentifizierungsvorgang wie das Hinzufügen, Bearbeiten, Löschen oder Testen von

Remote-Benutzern oder -Gruppen durchführen, wird die folgende Fehlermeldung angezeigt: `User not found`.

- **Ursache**

  Dieses Problem kann auftreten, wenn der Benutzer im AD-Server oder LDAP-Server existiert und wenn Sie den Distinguished Base-Namen auf einen falschen Wert gesetzt haben.

- **Korrekturmaßnahmen**

  a. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Setup** > **Authentifizierung**.

  b. Geben Sie die entsprechenden Informationen für den Basisnamen ein.

  c. Klicken Sie auf **Speichern und Schließen**.

Problem beim Hinzufügen von LDAP über andere Authentifizierungsdienste

- **Ausgabe**

  Wenn Sie andere als den Authentifizierungsdienst auswählen, behalten Benutzer und GroupObjectClass die Werte aus der zuvor ausgewählten Vorlage bei. Wenn der LDAP-Server nicht die gleichen Werte verwendet, kann der Vorgang fehlschlagen.

- **Ursache**

  Die Benutzer sind in OpenLDAP nicht richtig konfiguriert.

- **Korrekturmaßnahmen**

  Sie können dieses Problem mithilfe einer der folgenden Problemumgehungen manuell beheben.

  Wenn die Objektklasse und die Objektklasse der LDAP-Benutzer Benutzer Benutzer bzw. Gruppen sind, führen Sie die folgenden Schritte aus:

  a. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Setup** > **Authentifizierung**.

  b. Wählen Sie im Dropdown-Menü **Authentifizierungsdienst** die Option **Active Directory** aus, und wählen Sie dann **andere** aus.

  c. Füllen Sie die Textfelder aus. Wenn die Objektklasse und die Objektklasse des LDAP-Benutzers positixAccount bzw. positixGroup sind, führen Sie die folgenden Schritte aus:

  d. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Setup** > **Authentifizierung**.

  e. Wählen Sie im Dropdown-Menü **Authentifizierungsdienst** die Option **OpenLDAP** aus, und wählen Sie dann **andere** aus.

  f. Füllen Sie die Textfelder aus. Wenn die ersten beiden Problemumgehungen nicht gelten, rufen Sie den an `option-set` API, und legen Sie den fest `auth.ldap.userObjectClass` Und `auth.ldap.groupObjectClass` Optionen für die richtigen Werte.

Fehlerbehebung beim Zugriff auf CIFS-Freigaben

Sie können möglicherweise nicht auf CIFS-Freigaben zugreifen, wenn die Storage-Objekte, die diese Freigaben bereitstellen, nicht verfügbar sind. Sie sollten Verfügbarkeitsereignisse wie Volume Offline, Junction Path Offline oder SVM CIFS Server Down prüfen, die generiert werden, wenn diese Objekte nicht verfügbar sind.

Bevor Sie beginnen

Sie müssen die Rolle „Storage Administrator“ besitzen, um diese Aufgabe ausführen zu können.

Über diese Aufgabe

Wenn Sie eine entsprechende Warnung konfiguriert haben, werden Sie über eine E-Mail über das Verfügbarkeitsereignis benachrichtigt.

Schritte

1. Klicken Sie auf der Seite **Dashboards/Übersicht** auf das entsprechende Offline-Ereignis.

   Wenn Sie beispielsweise ein Ereignis Volume Offline erhalten, klicken Sie auf das **`Volume_name` Ereignis Volume Offline** im Verfügbarkeitsfenster im Bereich ungelöste Vorfälle und Risiken.

2. Klicken Sie auf der Seite **Event** Details auf **`Volume_name`** Im Feld * Quelle*.
3. Klicken Sie auf der Seite **Health/Volume** Details auf die Nummer, die CIFS Shares entspricht, im Fenster **Related Devices**.
4. Klicken Sie auf der Seite **Health/Storage Virtual Machine** Details auf die Registerkarte **CIFS Shares**.

   Sie können die Anzahl der betroffenen CIFS-Freigaben anzeigen.

Nachdem Sie fertig sind

Sie müssen die Fehler entweder mit dem OnCommand System Manager oder der ONTAP CLI beheben.

Bestimmte Sonderzeichen funktionieren nicht mit der Berichtssuche

- **Ausgabe**

  Die Verwendung der Sonderzeichen % und _ bei der Suche in einem Bericht führt zu einem Fehlschlagen des Vorgangs.

- **Korrekturmaßnahmen**

  Wenn Sie nach einer Zeichenfolge suchen, die % oder _ enthält, sollten Sie vor dem angegebenen Zeichen einen Doppelschrägstrich verwenden.

  Um beispielsweise einen String mit S_10 zu finden, müssen Sie S_10 eingeben.

Überwachung und Management der Cluster-Performance

Einführung in das Performance-Monitoring von OnCommand Unified Manager

OnCommand Unified Manager bietet Funktionen für das Performance-Monitoring und Ursachenanalyse für Systeme, auf denen NetApp ONTAP Software ausgeführt wird.

Unified Manager hilft Ihnen, Workloads zu identifizieren, die die Cluster-Komponenten überbeanspruchen, und die Performance anderer Workloads auf dem Cluster zu senken. Durch das Definieren von Richtlinien für Performance-Schwellenwerte können Sie auch Maximalwerte für bestimmte Performance-Zähler angeben, sodass Ereignisse bei Überschreitung des Schwellenwerts generiert werden. Unified Manager benachrichtigt Sie über diese Performance-Ereignisse, sodass Korrekturmaßnahmen ergriffen und die Performance wieder auf normalen Niveau des Betriebs wiederhergestellt werden kann. Sie können Ereignisse in der Benutzeroberfläche von Unified Manager anzeigen und analysieren.

Unified Manager überwacht die Performance zweier Workload-Typen:

- Benutzerdefinierte Workloads

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

- Systemdefinierte Workloads

  Diese Workloads bestehen aus interner Systemaktivität.

Funktionen für das Performance-Monitoring in Unified Manager

Unified Manager sammelt und analysiert Performance-Statistiken von Systemen, auf denen ONTAP Software ausgeführt wird. Es nutzt dynamische Performance-Schwellenwerte und benutzerdefinierte Performance-Schwellenwerte, um eine Vielzahl von Performance-Zähler über viele Cluster-Komponenten zu überwachen.

Eine hohe Reaktionszeit (Latenz) gibt an, dass das Storage-Objekt, beispielsweise ein Volume, langsamer als normal läuft. Dieses Problem weist außerdem darauf hin, dass die Performance für Client-Applikationen, die das Volume nutzen, gesunken ist. Unified Manager ermittelt die Storage-Komponente, in der das Performance-Problem liegt, und enthält eine Liste mit Vorschlägen, die Sie zur Behebung des Performance-Problems ergreifen können.

Unified Manager umfasst die folgenden Funktionen:

- Überwachung und Analyse der Workload-Performance-Statistiken eines Systems mit ONTAP Software
- Tracking von Performance-Zählern für Cluster, Nodes, Aggregate, Ports, SVMs Volumes, LUNs, NVMe-Namespaces und LIFs.
- Zeigt detaillierte Diagramme an, die Workload-Aktivitäten im Zeitverlauf darstellen, einschließlich IOPS (Vorgänge), MB/s (Durchsatz), Latenz (Reaktionszeit), Auslastung, Performance-Kapazität und Cache-Verhältnis.

- Ermöglicht die Erstellung benutzerdefinierter Performance-Schwellenwertrichtlinien, die Ereignisse auslösen und E-Mail-Alarme senden, wenn die Schwellenwerte nicht überschritten werden.
- Hier werden systemdefinierte Schwellenwerte und dynamische Performance-Schwellenwerte verwendet, die Informationen zu Ihrer Workload-Aktivität enthalten, um Performance-Probleme zu identifizieren und zu benachrichtigen.
- Ermittelt eindeutig die Clusterkomponente, die mit einem Konflikt in Konflikt steht.
- Identifiziert Workloads, die zu viel Cluster-Komponenten nutzen, und Workloads, deren Performance durch den gesteigerten Durchsatz beeinträchtigt wird

Unified Manager-Schnittstellen zum Management der Storage-Systemperformance

Es gibt zwei Benutzeroberflächen, die OnCommand Unified Manager für das Monitoring und die Behebung von Performance-Problemen im Storage bereitstellt: Die webbasierte Benutzeroberfläche und die Wartungskonsole.

Unified Manager Web-UI

Die Web-UI von Unified Manager ermöglicht Administratoren das Überwachen und Beheben von Performance-bezogenen Storage-Problemen.

In diesem Abschnitt werden einige gängige Workflows beschrieben, die ein Administrator zur Behebung von Problemen mit der Storage-Performance ausführen kann, die in der Weboberfläche von Unified Manager angezeigt werden.

Wartungskonsole

Die Wartungskonsole ermöglicht einem Administrator, Betriebssystemprobleme, Probleme mit dem Versionsaufrüstungs-, Benutzer-Zugriffsprobleme und Netzwerkprobleme im Zusammenhang mit dem Unified Manager Server selbst zu überwachen, zu diagnostizieren und zu beheben. Wenn die Web-UI von Unified Manager nicht verfügbar ist, stellt die Wartungskonsole die einzige Zugriffsmöglichkeit auf Unified Manager dar.

Dieser Abschnitt enthält eine Anleitung zum Zugriff auf die Wartungskonsole und zur Behebung von Problemen im Zusammenhang mit der Funktionsweise des Unified Manager-Servers.

Aktivitäten zur Cluster-Konfiguration und zur Datenerfassung für die Performance

Das Erfassungsintervall für *Cluster-Konfigurationsdaten* beträgt 15 Minuten. Beispielsweise dauert es nach dem Hinzufügen eines Clusters 15 Minuten, bis die Cluster-Details in der UI von Unified Manager angezeigt werden. Dieses Intervall gilt, wenn Sie die Änderungen auch auf einem Cluster vornehmen.

Wenn Sie beispielsweise einer SVM in einem Cluster zwei neue Volumes hinzufügen, werden diese neuen Objekte in der UI nach dem nächsten Abfrageintervall bis zu 15 Minuten angezeigt.

Unified Manager sammelt alle fünf Minuten aktuelle Performance-Statistiken_ von allen überwachten Clustern. Diese Daten werden analysiert, um Performance-Ereignisse und potenzielle Probleme zu identifizieren. Es speichert 30 Tage Verlaufsdaten zu fünf Minuten und 390 Tage historischer Performance-Daten von einer Stunde. So können Sie sehr granulare Performance-Details für den aktuellen Monat und allgemeine Performance-Trends für bis zu ein Jahr anzeigen.

Die Erfassungsumfragen werden um einige Minuten verschoben, sodass Daten aus jedem Cluster nicht gleichzeitig gesendet werden, was die Performance beeinträchtigen kann.

In der folgenden Tabelle werden die Erfassungsaktivitäten beschrieben, die Unified Manager durchführt:

Aktivität	Zeitintervall	Beschreibung
Performance-Statistikabfrage	Alle 5 Minuten	Erfassung von Performance-Daten in Echtzeit von jedem Cluster
Statistische Analyse	Alle 5 Minuten	Nach jeder Statistikabfrage vergleicht Unified Manager die erfassten Daten mit benutzerdefinierten, systemdefinierten und dynamischen Schwellenwerten. Wenn gegen Performance-Schwellenwerte Grenzwerte verstoßen wurde, generiert Unified Manager Ereignisse und sendet E-Mails an die angegebenen Benutzer, sofern hierfür konfiguriert.
Konfigurationsabfrage	Alle 15 Minuten	Erfasst detaillierte Inventarinformationen aus jedem Cluster, um alle Storage-Objekte (Nodes, SVMs, Volumes usw.) zu identifizieren
Zusammenfassung	Jede Stunde	Fasst die letzten 12 fünf-Minuten-Performance-Datensammlungen in einem Durchschnittswert von Stunden zusammen. Die Durchschnittswerte pro Stunde werden in einigen UI-Seiten verwendet und 390 Tage lang aufbewahrt.
Prognoseanalyse und Datenbeschneidung	Jeden Tag nach Mitternacht	Analysiert Cluster-Daten, um dynamische Schwellenwerte für Volume-Latenz und IOPS für die nächsten 24 Stunden festzulegen. Löscht alle fünf-Minuten-Performancedaten, die älter als 30 Tage sind, aus der Datenbank.

Aktivität	Zeitintervall	Beschreibung
Datenbeschnitt	Jeden Tag nach 2 Uhr	Löscht aus der Datenbank alle Ereignisse und dynamischen Schwellenwerte, die älter als 390 Tage sind.
Datenbeschnitt	Jeden Tag nach 3:30 Uhr	Löscht aus der Datenbank alle Leistungsdaten von einer Stunde, die älter als 390 Tage sind.

Was ist ein Data-Continuity-Erfassungszyklus

Durch einen Datenkontinuitätszyklus werden Performancedaten außerhalb des Echtzeit-Zyklus der Cluster-Performance-Erfassung abgerufen, der standardmäßig alle fünf Minuten ausgeführt wird. Datenkontinuitätssammlungen ermöglichen es Unified Manager, Lücken statistischer Daten zu schließen, die auftreten, wenn sie keine Echtzeitdaten erfassen konnten.

Die Datenkontinuitätssammlung wird nur auf Clustern unterstützt, die mit der Software ONTAP Version 8.3.1 oder höher installiert sind.

Unified Manager führt Datenkontinuität-Abfragen der historischen Performance-Daten durch, wenn die folgenden Ereignisse auftreten:

- Dem Unified Manager wird zunächst ein Cluster hinzugefügt.

  Unified Manager sammelt historische Performance-Daten für die letzten 15 Tage. So können Sie einige Stunden nach dem Hinzufügen von Performance-Informationen von zwei Wochen für ein Cluster anzeigen.

  Darüber hinaus werden systemdefinierte Schwellenwertereignisse für den vorherigen Zeitraum gemeldet, sofern vorhanden.

  ⓘ 15 Tage der historischen Volumen-Statistiken werden derzeit nicht gesammelt.

- Der aktuelle Erfassungszyklus für Performance-Daten ist nicht pünktlich abgeschlossen.

  Wenn die Echtzeit-Performance-Umfrage über den fünf-Minuten-Erfassungszeitraum hinausgeht, wird ein Datenkontinuitätssammlungszyklus eingeleitet, um die fehlenden Informationen zu erfassen. Ohne die Datenkontinuitätssammlung wird der nächste Erfassungszeitraum übersprungen.

- Unified Manager war für einen bestimmten Zeitraum nicht zugänglich und dann wieder online, wie in den folgenden Situationen:
  - Es wurde neu gestartet.
  - Sie wurde während eines Software-Upgrades oder beim Erstellen einer Sicherungsdatei heruntergefahren.
  - Ein Netzwerkausfall ist behoben.
- Ein Cluster war für einen Zeitraum nicht zugänglich und dann wieder online, wie in den folgenden Situationen:

- Ein Netzwerkausfall ist behoben.
- Eine langsame Wide Area Network-Verbindung verzögerte die normale Erfassung von Performancedaten.

Ein Datenerfassungszyklus kann maximal 24 Stunden historische Daten erfassen. Wenn Unified Manager länger als 24 Stunden ausfällt, wird auf den UI-Seiten eine Lücke in den Performance-Daten angezeigt.

Ein Datenerfassungszyklus und ein Datenerfassungszyklus in Echtzeit können nicht gleichzeitig ausgeführt werden. Der Datenerfassungszyklus muss vor Beginn der Performance-Datenerfassung in Echtzeit abgeschlossen sein. Wenn die Daten-Continuity-Sammlung länger als eine Stunde historische Daten erfasst werden muss, befindet sich oben im Performance Dashboard eine Bannermeldung für den Cluster.

Was bedeutet der Zeitstempel bei erfassten Daten und Ereignissen

Der Zeitstempel, der in den erfassten Systemzustand und Performance-Daten angezeigt wird oder der als Erkennungszeit für ein Ereignis angezeigt wird, basiert auf der ONTAP Cluster-Zeit, die an die im Webbrowser eingestellte Zeitzone angepasst wurde.

Es wird dringend empfohlen, einen NTP-Server (Network Time Protocol) zu verwenden, um die Zeit auf Unified Manager-Servern, ONTAP-Clustern und Webbrowsern zu synchronisieren.

Wenn Zeitstempel, die für ein bestimmtes Cluster nicht korrekt angezeigt werden, möchten Sie möglicherweise überprüfen, ob die Cluster-Zeit ordnungsgemäß festgelegt wurde.

Navigation in Performance-Workflows in der Unified Manager GUI

Die Unified Manager-Oberfläche bietet viele Seiten zum Sammeln und Anzeigen von Performance-Informationen. Über das linke Navigationsfenster navigieren Sie zu den Seiten der GUI, und Sie verwenden die Registerkarten und Links auf den Seiten, um Informationen anzuzeigen und zu konfigurieren.

Sie verwenden alle der folgenden Seiten, um Informationen zur Cluster-Performance zu überwachen und Fehler zu beheben:

- Dashboard-Seiten
- Inventarseiten für Storage-Objekte
- Landing Pages für Storage-Objekte (einschließlich Performance Explorer)
- Konfigurations- und Setup-Seiten
- Ereignisseiten

Auf einer Seite in Unified Manager wird möglicherweise eine große Menge an Informationen angezeigt. Um alle verfügbaren Informationen anzuzeigen, scrollen Sie immer zum Ende der Seite.

Melden Sie sich bei der UI an

Sie können sich über einen unterstützten Webbrowser bei der Benutzeroberfläche von

Unified Manager anmelden.

Bevor Sie beginnen

- Der Webbrowser muss die Mindestanforderungen erfüllen.

  Weitere Informationen finden Sie in der Interoperabilitäts-Matrix unter "mysupport.netapp.com/matrix" Für die vollständige Liste der unterstützten Browser-Versionen.

- Sie müssen die IP-Adresse oder URL des Unified Manager-Servers haben.

Über diese Aufgabe

Nach 24 Stunden Inaktivität werden Sie automatisch von der Sitzung abgemeldet.

Schritte

1. Geben Sie die URL in Ihren Webbrowser ein `URL` Ist die IP-Adresse oder der vollqualifizierte Domänenname (FQDN) des Unified Manager-Servers:
   - Für IPv4: `https://URL/`
   - Für IPv6: `https://[URL]/`Wenn der Server ein selbstsigniertes digitales Zertifikat verwendet, zeigt der Browser möglicherweise eine Warnung an, dass das Zertifikat nicht vertrauenswürdig ist. Sie können entweder das Risiko bestätigen, dass der Zugriff fortgesetzt wird, oder ein Zertifikat einer Zertifizierungsstelle (CA) installieren, das digitale Zertifikat für die Serverauthentifizierung unterzeichnet hat.
2. Geben Sie im Anmeldebildschirm Ihren Benutzernamen und Ihr Kennwort ein.

   Wenn die Anmeldung bei der Unified Manager-Benutzeroberfläche mit SAML-Authentifizierung geschützt ist, geben Sie Ihre Anmeldedaten anstelle der Login-Seite des Unified Manager auf der Anmeldeseite des Identitäts-Providers (IdP) ein.

   Die Seite Dashboards/Übersicht wird angezeigt.

   Wenn der Unified Manager-Server nicht initialisiert wird, wird in einem neuen Browser-Fenster der Assistent für die erste Erfahrung angezeigt. Sie müssen einen anfänglichen E-Mail-Empfänger eingeben, an den E-Mail-Benachrichtigungen gesendet werden, den SMTP-Server, der E-Mail-Kommunikation durchführt, und ob AutoSupport aktiviert ist, um Informationen über Ihre Unified Manager-Installation an den technischen Support zu senden. Nach Abschluss dieser Informationen wird die Unified Manager-Benutzeroberfläche angezeigt.

Grafische Oberfläche und Navigationspfade

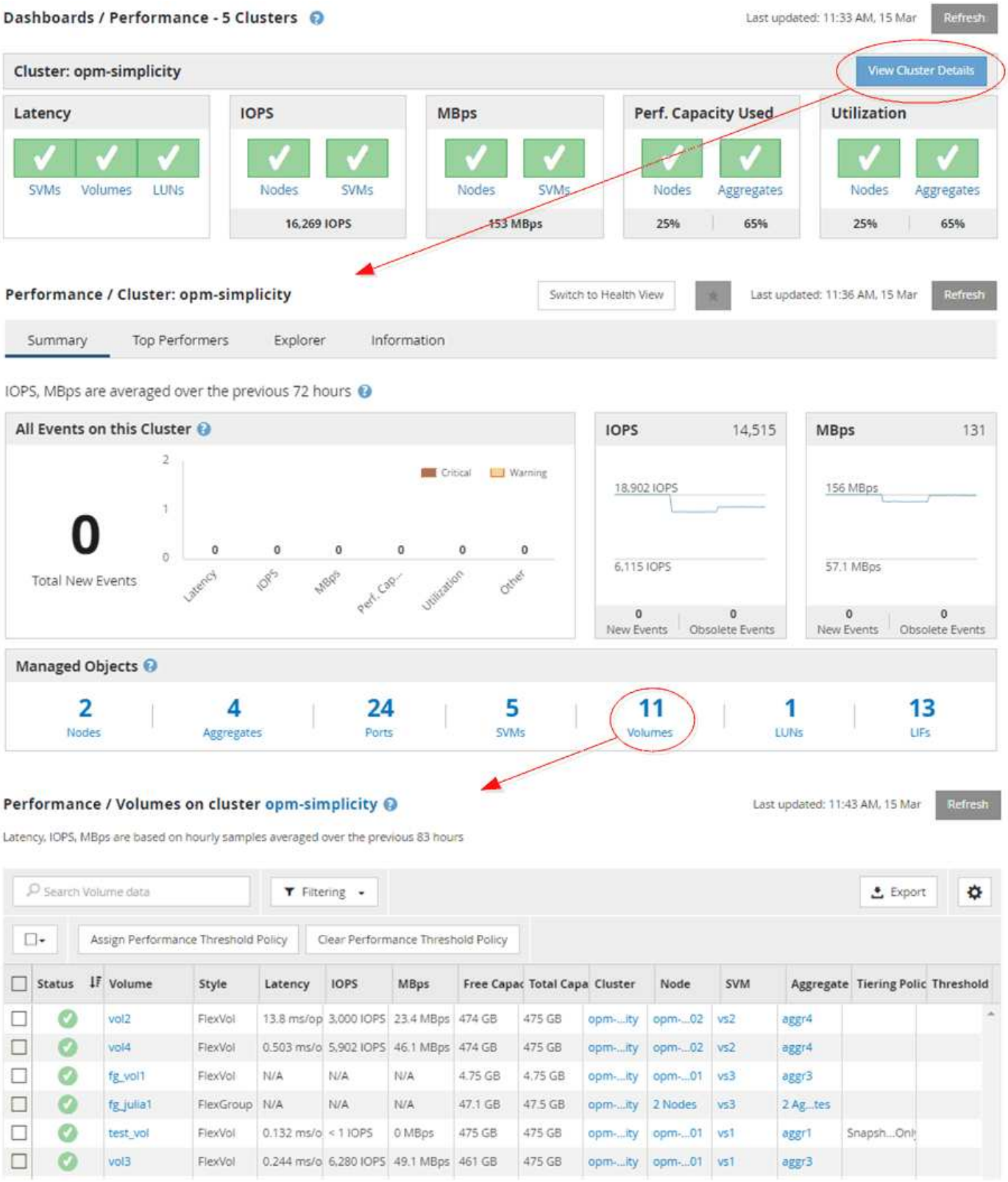
Unified Manager bietet große Flexibilität und ermöglicht die Ausführung mehrerer Aufgaben auf verschiedene Weise. Bei der Arbeit in Unified Manager gibt es viele Navigationspfade, die Sie entdecken werden. Obwohl nicht alle möglichen Kombinationen von Navigationen angezeigt werden können, sollten Sie mit ein paar der häufigsten Szenarien vertraut sein.

Überwachen Sie die Navigation von Cluster-Objekten

Mit Unified Manager lässt sich die Performance aller Objekte in jedem Cluster überwachen, der von Unified Manager gemanagt wird. Das Monitoring Ihrer Storage-Objekte bietet Ihnen einen Überblick über die Performance von Clustern und Objekten und umfasst das Performance-Ereignis-Monitoring. Sie können sich allgemeine Performance- und Ereignisse anzeigen lassen oder Details zu Objekt-Performance- und Performance-Ereignissen genauer untersuchen.

Dies ist ein Beispiel für viele mögliche Cluster-Objekt-Navigationen:

1. Geben Sie auf der Seite Dashboards/Leistung einen Cluster an, den Sie untersuchen möchten, und navigieren Sie zur Zielseite des ausgewählten Clusters.
2. Geben Sie auf der Seite „Performance/Cluster Summary“ das Cluster-Objekt an, das untersucht werden soll, und navigieren Sie zur Inventarseite des jeweiligen Objekts. In diesem Beispiel wird **Volumes** ausgewählt, um die Seite Performance/Volumes Inventory anzuzeigen.



Monitoring der Navigation zur Cluster-Performance

Mit Unified Manager lässt sich die Performance aller Cluster überwachen, die von Unified Manager gemanagt werden. Das Monitoring der Cluster bietet einen Überblick über die Cluster- und Objekt-Performance und umfasst das Performance-Ereignis-Monitoring. Sie können sich grundlegende Performance- und Ereignisse anzeigen lassen oder Details zu

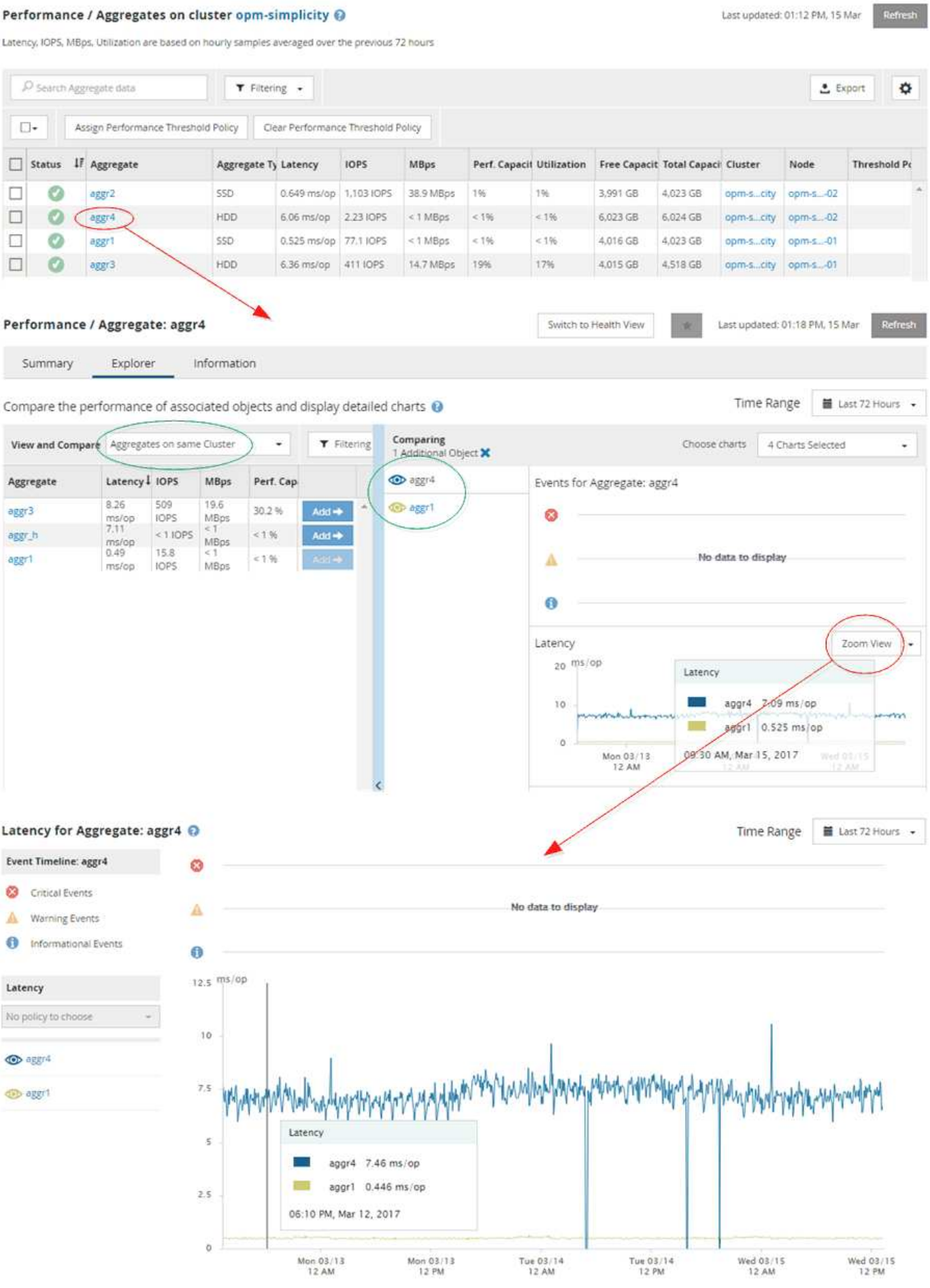
Cluster- und Objekt-Performance- und Performance-Ereignissen sowie deren Objekt-Performance genauer untersuchen.

Dies ist ein Beispiel für viele mögliche Navigationspfade zur Cluster-Performance:

1. Identifizieren Sie auf der Seite Dashboards/Leistung einen Cluster, den Sie untersuchen möchten, und klicken Sie auf **Cluster-Details anzeigen**, um zur Zielseite des ausgewählten Clusters zu navigieren.
2. Geben Sie auf der Seite „Performance/Cluster Summary“ den Objekttyp an, den Sie untersuchen möchten, und klicken Sie darauf, um die Seite „Object Inventory“ anzuzeigen.

   In diesem Beispiel ist **Aggregate** ausgewählt und zeigt die Bestandsseite zu Performance/Aggregaten an.
3. Identifizieren Sie auf der Seite „Performance/Aggregate“ das Aggregat, das Sie untersuchen möchten, und klicken Sie auf diesen Aggregatnamen, um zur Seite „Performance/Aggregate Explorer“ zu navigieren.
4. Wählen Sie optional im Menü Ansicht und Vergleich weitere Objekte aus, die mit diesem Aggregat verglichen werden sollen, und fügen Sie anschließend dem Vergleichsfenster eines der Objekte hinzu.

   Statistiken für beide Objekte werden in den Zählerdiagrammen zum Vergleich angezeigt.
5. Klicken Sie im Vergleichsanfenster rechts auf der Explorer-Seite auf **Zoom View** in einer der Zählerdiagramme, um Details zum Leistungsverlauf für dieses Aggregat anzuzeigen.


Performance / Aggregates on cluster opm-simplicity
Last updated: 01:12 PM, 15 Mar
Refresh
Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours
Search Aggregate data
Filtering
Export
Assign Performance Threshold Policy
Clear Performance Threshold Policy
Status
Aggregate
Aggregate Ty
Latency
IOPS
MBps
Perf. Capaci
Utilization
Free Capacit
Total Capaci
Cluster
Node
Threshold Pc
aggr2 SSD 0.649 ms/op 1,103 IOPS 38.9 MBps 1% 1% 3,991 GB 4,023 GB opm-s...city opm-s...-02
aggr4 HDD 6.06 ms/op 2.23 IOPS < 1 MBps < 1% < 1% 6,023 GB 6,024 GB opm-s...city opm-s...-02
aggr1 SSD 0.525 ms/op 77.1 IOPS < 1 MBps < 1% < 1% 4,016 GB 4,023 GB opm-s...city opm-s...-01
aggr3 HDD 6.36 ms/op 411 IOPS 14.7 MBps 19% 17% 4,015 GB 4,518 GB opm-s...city opm-s...-01
Performance / Aggregate: aggr4
Switch to Health View
Last updated: 01:18 PM, 15 Mar
Refresh
Summary
Explorer
Information
Compare the performance of associated objects and display detailed charts
Time Range
Last 72 Hours
View and Compare
Aggregates on same Cluster
Filtering
Comparing
1 Additional Object
Choose charts
4 Charts Selected
Aggregate
Latency
IOPS
MBps
Perf. Cap
aggr3 8.26 ms/op 509 IOPS 19.6 MBps 30.2 % Add
aggr_h 7.11 ms/op < 1 IOPS < 1 MBps < 1 % Add
aggr1 0.49 ms/op 15.8 IOPS < 1 MBps < 1 % Add
aggr4
aggr1
Events for Aggregate: aggr4
No data to display
Latency
Zoom View
20 ms/op
10
0
Latency
aggr4 7.09 ms/op
aggr1 0.525 ms/op
09:30 AM, Mar 15, 2017
Mon 03/13 12 AM
Latency for Aggregate: aggr4
Time Range
Last 72 Hours
Event Timeline: aggr4
Critical Events
Warning Events
Informational Events
No data to display
Latency
No policy to choose
aggr4
aggr1
12.5 ms/op
10
7.5
5
2.5
0
Latency
aggr4 7.46 ms/op
aggr1 0.446 ms/op
06:10 PM, Mar 12, 2017
Mon 03/13 12 AM
Mon 03/13 12 PM
Tue 03/14 12 AM
Tue 03/14 12 PM
Wed 03/15 12 AM
Wed 03/15 12 PM

Navigation zur Ereignisuntersuchung

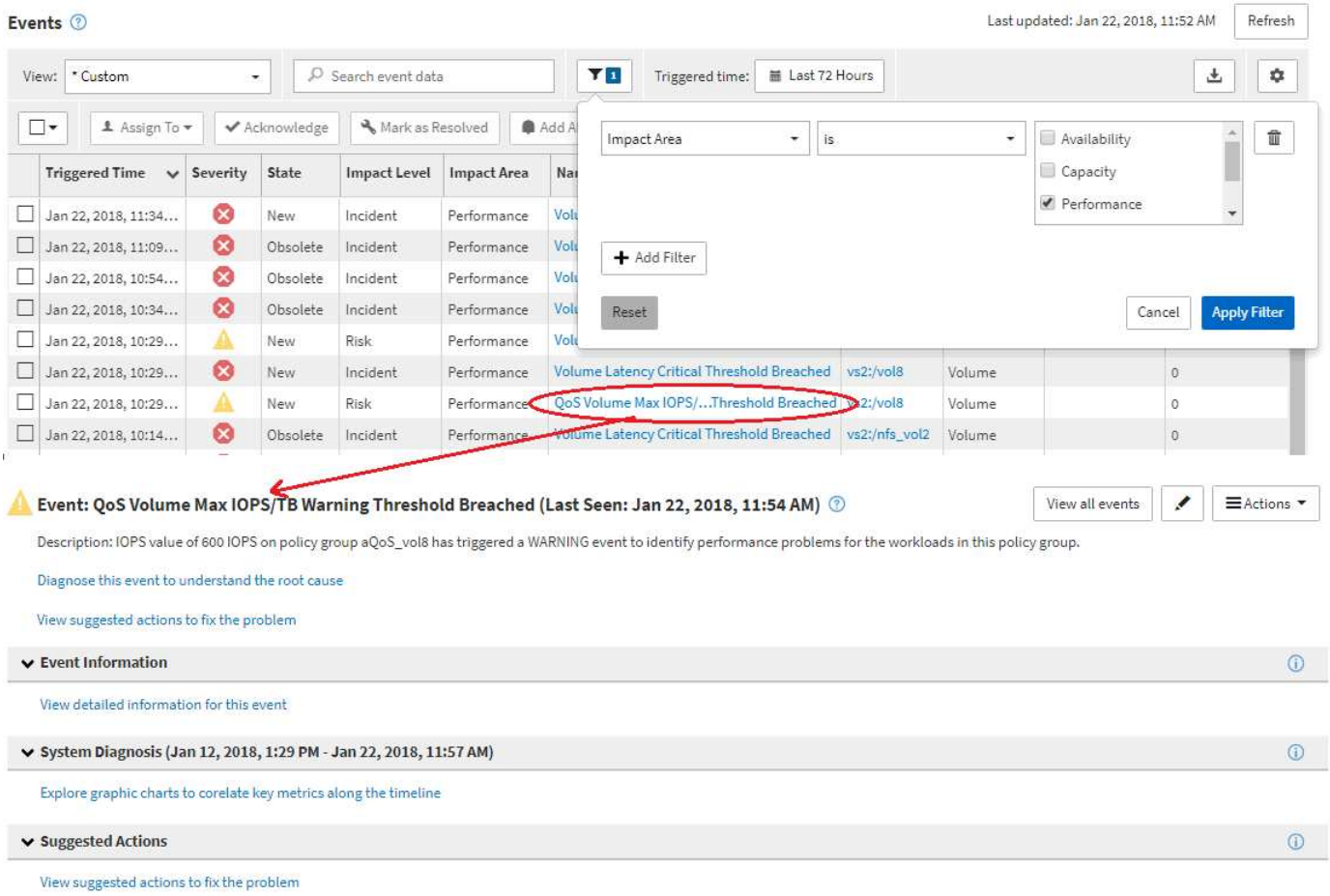
Auf den Seiten mit den Unified Manager Event-Details werden Performance-Ereignisse detailliert analysiert. Dies ist von Vorteil bei der Untersuchung von Performance-Ereignissen, bei der Fehlerbehebung und bei der Feinabstimmung der System-Performance.

Je nach Art des Performance-Ereignisses werden möglicherweise zwei Arten von Ereignis-Detailseiten angezeigt:

- Seite mit den Ereignisdetails für benutzerdefinierte und systemdefinierte Schwellenwertrichtlinienereignisse
- Seite mit Ereignisdetails für dynamische Schwellenwertrichtlinienereignisse

Dies ist ein Beispiel für eine Ereignisuntersuchung-Navigation.

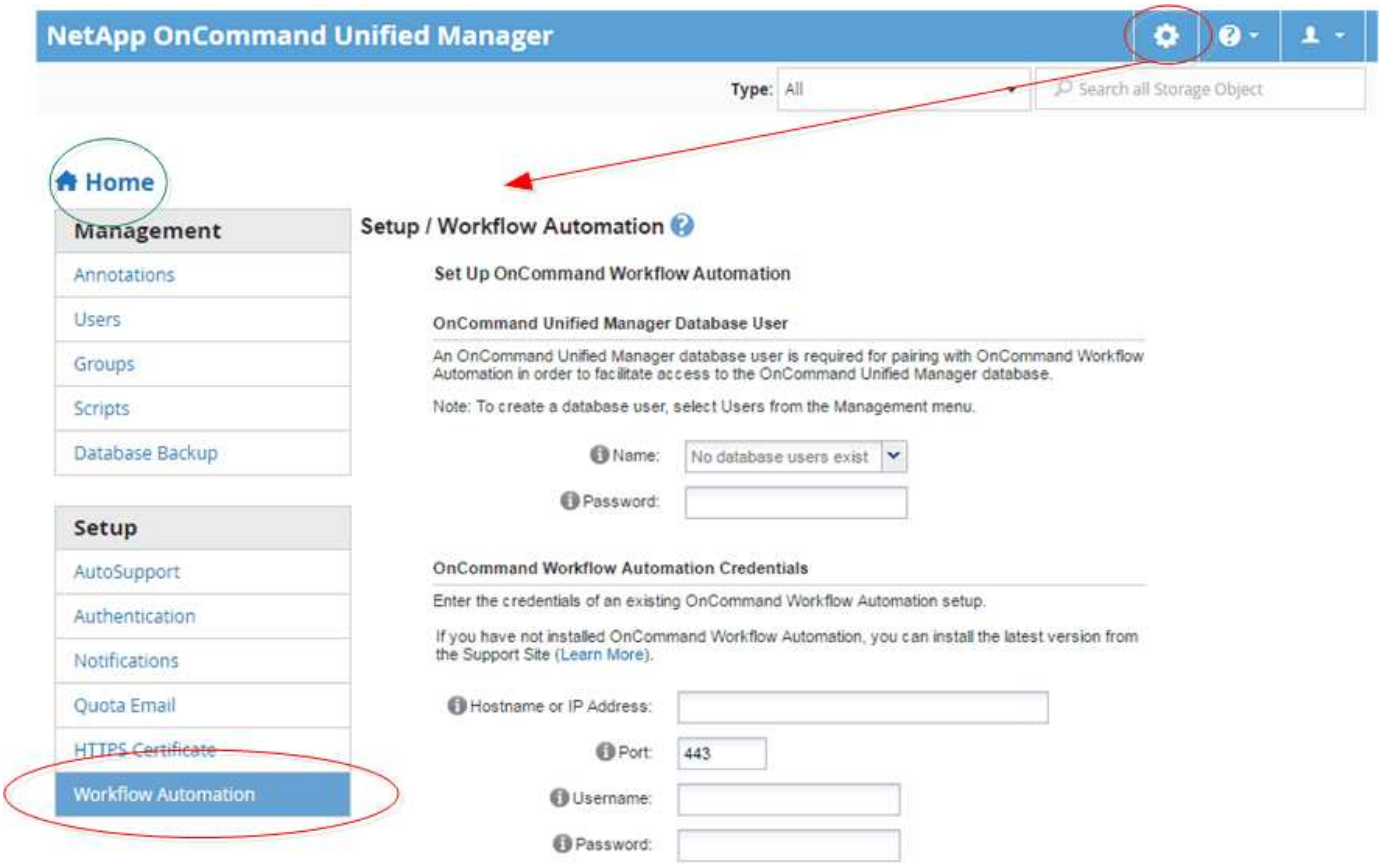
1. Klicken Sie im linken Navigationsbereich auf **Events**.
2. Klicken Sie auf der Seite Ereignisbestand auf die Schaltfläche Filter und wählen Sie im Bereich Auswirkungen die Option **Leistung** aus, um die Ereignisliste zu filtern.
3. Klicken Sie auf den Namen des Ereignisses, das Sie untersuchen möchten, und die Seite Ereignisdetails wird angezeigt.
4. Erweitern Sie alle Bereiche, z. B. vorgeschlagene Aktionen, um weitere Details zu dem Ereignis anzuzeigen, das Ihnen bei der Lösung des Problems helfen kann.



Navigation in der Unified Manager-Administration

Die Unified Manager-Administrationsfunktion ermöglicht das Management von Benutzern und Datenquellen. Sie können auch Setup-Aufgaben wie Authentifizierung, AutoSupport, E-Mail, HTTPS-Zertifikate, Netzwerke, Und NTP-Server über die Seite „Unified Manager Administration“.

Dies ist ein Beispiel für viele mögliche Administrationspfade. Gehen Sie wie folgt vor, um eine Verbindung zu einem Workflow Automation-Server hinzuzufügen oder zu entfernen:



Klicken Sie auf das Symbol **Home**, um zur Hauptnavigationsseite von Unified Manager zurückzukehren.

Suche nach Speicherobjekten

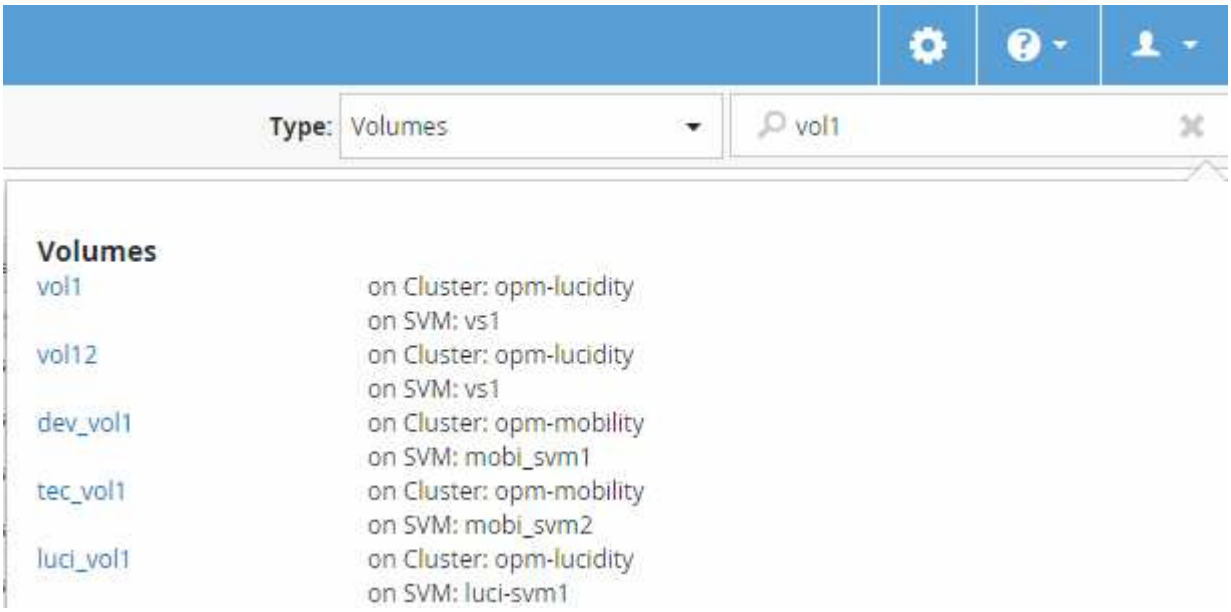
Um schnell auf ein bestimmtes Objekt zuzugreifen, können Sie das Feld **Alle Speicherobjekte durchsuchen** oben rechts in der Schnittstelle verwenden. Mit dieser Methode der globalen Suche über alle Objekte können Sie schnell bestimmte Objekte nach Typ finden. Die Suchergebnisse werden nach Speicherobjekttyp sortiert und Sie können sie über das Dropdown-Menü **Typ** filtern. Eine gültige Suche muss mindestens drei Zeichen enthalten.

Die globale Suche zeigt die Gesamtzahl der Ergebnisse an, aber nur die 20 besten Suchergebnisse sind verfügbar. Daher kann die globale Suchfunktion als Verknüpfungstool für die Suche nach bestimmten Elementen gedacht werden, wenn Sie die Elemente kennen, die Sie schnell finden möchten. Für vollständige

Suchergebnisse können Sie die Suche auf den Objektbestandsseiten und den zugehörigen Filterfunktionen verwenden.

Sie können auf das Dropdown-Feld **Typ** klicken und **Alle** auswählen, um gleichzeitig nach allen Objekten und Ereignissen zu suchen. Alternativ können Sie auf das Dropdown-Feld **Typ** klicken, um den Objekttyp anzugeben. Geben Sie eine beliebige Anzahl von Zeichen des Objekts oder Ereignisnamens in das Feld **Alle Speicherobjekte durchsuchen** ein, und drücken Sie dann **Enter** oder klicken Sie auf **Alle durchsuchen**, um die Suchergebnisse anzuzeigen, z. B.:

- Ereignisse: Leistungsereignis-IDs
- Cluster: Cluster-Namen
- Nodes: Node-Namen
- Aggregate: Aggregatnamen
- SVMs: SVM-Namen
- Volumes: Volume-Namen
- LUNs: LUN-Pfade



LIFs und Ports sind in der globalen Suchleiste nicht durchsuchbar.

In diesem Beispiel wurde im Dropdown-Feld **Typ** der Objekttyp Volume ausgewählt. Durch Eingabe von „`vol`“ in das Feld **Alle Speicherobjekte durchsuchen** wird eine Liste aller Volumes angezeigt, deren Namen diese Zeichen enthalten. Bei der Objektsuche können Sie auf ein beliebiges Suchergebnis klicken, um zur Seite Performance Explorer des entsprechenden Objekts zu navigieren. Bei der Suche nach Ereignissen wird durch Klicken auf ein Element im Suchergebnis die Seite Ereignisdetails aufgerufen.

Wenn in den Suchergebnissen mehrere Volumes mit demselben Namen angezeigt werden, werden der Name der zugehörigen Cluster und SVMs nicht angezeigt.

Filtern des Seiteninhalts zur Leistungsbestandsbestandsliste

Sie können Leistungsbestandsdaten in Unified Manager filtern, um Daten anhand bestimmter Kriterien schnell zu finden. Mithilfe der Filterung können Sie den Inhalt der

Seiten von Unified Manager einschränken, um nur die für Sie jeweils interessierten Ergebnisse anzuzeigen. Dies bietet eine sehr effiziente Methode, nur die Leistungsdaten anzuzeigen, an denen Sie interessiert sind.

Über diese Aufgabe

Verwenden Sie **Filterung**, um die Rasteransicht entsprechend Ihren Einstellungen anzupassen. Die verfügbaren Filteroptionen basieren auf dem Objekttyp, der im Raster angezeigt wird. Wenn aktuell Filter angewendet werden, wird links neben dem Filtersteuerelement ein Sternchen (*) angezeigt.

Es werden vier Filterparameter unterstützt.

Parameter	Validierung
Zeichenfolge (Text)	Die Operatoren sind **enthält** und **beginnt mit**.
Nummer	Die Betreiber sind **größer als** und **kleiner als**.
Ressource	Die Operatoren sind **Name enthält** und **Name beginnt mit**.
Status	Die Betreiber sind **ist** und **ist nicht**.

Für jeden Filter sind alle drei Felder erforderlich; die verfügbaren Filter spiegeln die filterbaren Spalten auf der aktuellen Seite wider. Es können maximal vier Filter angewendet werden. Gefilterte Ergebnisse basieren auf kombinierten Filterparametern. Gefilterte Ergebnisse gelten für alle Seiten in Ihrer gefilterten Suche und nicht nur für die aktuell angezeigte Seite.

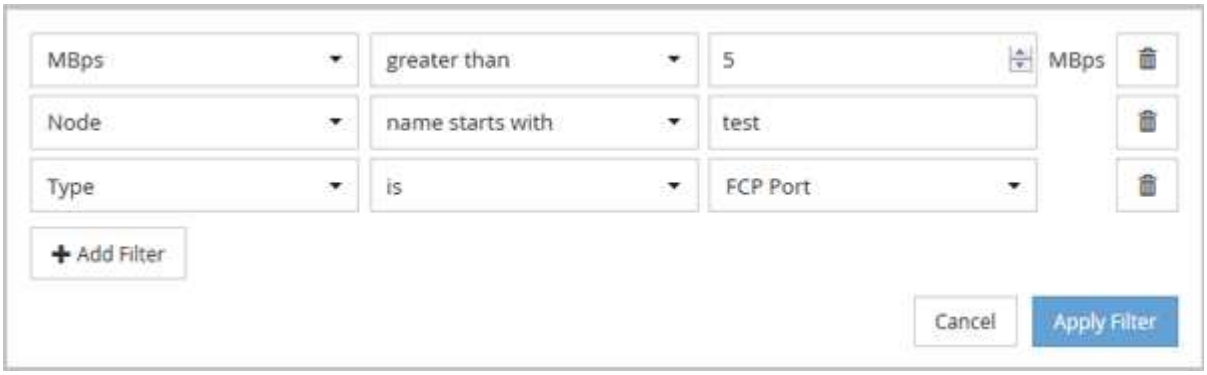
Sie können Filter über das Filterfenster hinzufügen.

1. Klicken Sie oben auf der Seite auf **Filtern**. Das Filterbedienfeld wird angezeigt.
2. Klicken Sie im Filterfenster auf die linke Dropdown-Liste und wählen Sie einen Objektnamen aus, z. B. *Cluster* oder einen Performance-Zähler.
3. Klicken Sie auf die Dropdown-Liste Mitte, und wählen Sie den booleschen Operator **Name enthält** oder **Name beginnt mit** aus, wenn die erste Auswahl ein Objektname war. Wenn es sich bei der ersten Auswahl um einen Leistungszähler handelte, wählen Sie **größer als** oder **kleiner als** aus. Wenn die erste Auswahl **Status** war, wählen Sie **ist** oder **ist nicht**.
4. Wenn für Ihre Suchkriterien ein numerischer Wert erforderlich ist, werden die nach-oben- und nach-unten-Pfeiltasten im Feld rechts angezeigt. Sie können auf die nach-oben- und nach-unten-Pfeiltasten klicken, um den gewünschten numerischen Wert anzuzeigen.
5. Geben Sie bei Bedarf Ihre nicht-numerischen Suchkriterien in das Textfeld rechts ein.
6. Um Filter hinzuzufügen, klicken Sie auf **Filter hinzufügen**. Es wird ein zusätzliches Filterfeld angezeigt. Führen Sie diesen Filter mithilfe des in den vorherigen Schritten beschriebenen Verfahrens aus. Beachten Sie, dass beim Hinzufügen Ihres vierten Filters die Schaltfläche **Filter hinzufügen** nicht mehr angezeigt wird.
7. Klicken Sie Auf **Filter Anwenden**. Die Filteroptionen werden auf das Raster angewendet, und ein Sternchen (*) wird in der Filterschaltfläche angezeigt.
8. Verwenden Sie den Filterbereich, um einzelne Filter zu entfernen, indem Sie auf das Papierkorb-Symbol rechts neben dem zu entfernenden Filter klicken.

9. Um alle Filter zu entfernen, klicken Sie unten im Filterfenster auf **Zurücksetzen**.

Beispiel für die Filterung

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



Nachdem Sie auf **Filter anwenden** geklickt haben, wird das Filterfenster geschlossen und wendet Ihre Filter an.

Zugriff auf OnCommand System Manager über die Unified Manager Schnittstelle

Wenn für die Fehlerbehebung Konfigurationsänderungen an einem Cluster erforderlich sind, können Sie die grafische Schnittstelle von System Manager anstelle der ONTAP Befehlszeilenschnittstelle verwenden. System Manager ist als Webservice in ONTAP enthalten, ist standardmäßig aktiviert und kann über einen Browser aufgerufen werden.

Bevor Sie beginnen

Sie müssen ein mit dem konfiguriertes Cluster-Benutzerkonto besitzen `admin` Rolle und der `http`, `ontapi`, und `console` Applikationstypen

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboards** > **Clusteransicht**.
2. Wählen Sie auf der Seite **Dashboards/Clusteransicht** den Cluster aus, den Sie verwalten möchten.

   Ein Überblick über den Monitoring-Status, die Kapazität und die Performance des Clusters wird angezeigt.

3. Klicken Sie auf das Symbol **System Manager**.

   Wenn das Cluster ein selbstsigniertes digitales Zertifikat verwendet, wird im Browser möglicherweise eine Warnung angezeigt, dass das Zertifikat nicht vertrauenswürdig ist. Sie können entweder das Risiko bestätigen, den Zugriff fortzusetzen, oder ein von der Zertifizierungsstelle signiertes digitales Zertifikat auf dem Cluster zur Server-Authentifizierung installieren.

4. Melden Sie sich mit den Anmeldedaten des Cluster-Administrators bei System Manager an.

   Wenn die Anmeldung bei der System Manager-Benutzeroberfläche mit SAML-Authentifizierung geschützt ist, geben Sie Ihre Anmeldedaten anstelle der System Manager-Anmeldeseite auf der Anmeldeseite des Identitäts-Providers (IdP) ein.

Hinzufügen zu und Entfernen von Speicherobjekten aus der Liste Favoriten

Sie können einer Favoritenliste Storage-Objekte hinzufügen, damit Sie diese Objekte im Hinblick auf Zustand, Kapazität und Performance überwachen können. Sie können den Objektstatus in der Favoritenliste verwenden, um Probleme zu ermitteln und zu beheben, bevor sie kritisch werden. Die Favoritenliste enthält außerdem den aktuellsten Überwachungsstatus eines Speicherobjekts. Sie können Speicherobjekte aus der Favoritenliste entfernen, wenn sie nicht mehr als Favorit markiert werden müssen.

Über diese Aufgabe

In der Favoritenliste können bis zu 20 Cluster, Nodes, Aggregate oder Volumes hinzugefügt werden. Wenn Sie der Liste „Favoriten“ einen Node hinzufügen, wird dieser als Cluster angezeigt.

Schritte

1. Rufen Sie die Seite **Details** des Speicherobjekts auf, das Sie als Favorit markieren möchten.
2. Klicken Sie auf das Sternsymbol ( ) Zum Hinzufügen des Speicherobjekts zur Favoritenliste.

Hinzufügen eines Aggregats zur Favoritenliste

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **Aggregate**.
2. Klicken Sie auf der Seite „Inventar/Aggregate“ auf das Aggregat, das Sie der Liste „Favoriten“ hinzufügen möchten.
3. Klicken Sie auf der Seite „Systemzustand/Aggregat-Details“ auf das STAR-Symbol ( ).

Nachdem Sie fertig sind

Um ein Speicherobjekt aus der Liste Favoriten zu entfernen, wechseln Sie zur Listenseite Favoriten, klicken Sie auf das Sternsymbol ( ) Auf der Objektkarte, die Sie entfernen möchten, und wählen Sie dann die Option **aus Favoriten entfernen**.

Lesezeichen häufig aufgerufene Produktseiten

Sie können häufig aufgerufene Produktseiten über die Unified Manager-Benutzeroberfläche als Lesezeichen hinzufügen. So können Sie schnell zu diesen Seiten zurückkehren. Wenn Sie die Seite später anzeigen, werden die neuesten Daten angezeigt.

Über diese Aufgabe

Sie können den Link (URL) auch auf die aktuelle Produktseite kopieren, sodass Sie ihn in eine E-Mail oder eine andere Anwendung einfügen können, um ihn mit anderen Personen zu teilen.

Schritte

1. Erstellen Sie ein Lesezeichen mit einem beliebigen Schritt, der benötigt wird, um eine Seite in Ihrem Browser zu markieren.

Der Link für die Seite wird mit Details über die Seite gespeichert, aber Sie können den Lesezeichentext anpassen, um die Seite zu identifizieren: Z. B. „`Unified Manager` Node: Node-01`“ oder „`Unified Manager Benutzerdefiniertes Schwellenwertereignis: IOPS Volume1“.

Lesezeichen für Ihre bevorzugten Hilfethemen

Auf der Registerkarte „Hilfe-Favoriten“ können Sie häufig verwendete Hilfethemen als Lesezeichen hinzufügen. Hilfe-Lesezeichen ermöglichen den schnellen Zugriff auf Ihre bevorzugten Themen.

Schritte

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

Allgemeines zu Performance-Ereignissen und Meldungen

Performance-Ereignisse sind Benachrichtigungen, die Unified Manager automatisch generiert, wenn eine vordefinierte Bedingung eintritt oder wenn ein Performance-Zählerwert einen Schwellenwert überschreitet. Ereignisse helfen Ihnen bei der Ermittlung von Performance-Problemen in den überwachten Clustern.

Sie können Benachrichtigungen so konfigurieren, dass E-Mail-Benachrichtigungen automatisch gesendet werden, wenn Performance-Ereignisse bestimmter Schweregrade auftreten.

Quellen von Leistungsereignissen

Performance-Ereignisse sind Probleme im Zusammenhang mit der Workload-Performance auf einem Cluster. Sie helfen dabei, Storage-Objekte mit langen Reaktionszeiten zu identifizieren, die auch als hohe Latenz bezeichnet werden. Zusammen mit anderen gleichzeitig aufgetretenen Gesundheitsereignissen können Sie die Probleme bestimmen, die die langsamen Reaktionszeiten verursacht oder dazu beigetragen haben.

Unified Manager erhält Leistungsereignisse aus den folgenden Quellen:

- **Benutzerdefinierte Richtlinienereignisse für Leistungsschwellenwerte**

  Leistungsprobleme basierend auf festgelegten benutzerdefinierten Schwellenwerten. Sie konfigurieren Richtlinien für Performance-Schwellenwerte für Storage-Objekte, wie z. B. Aggregate und Volumes, so dass Ereignisse generiert werden, wenn ein Schwellenwert für einen Performance-Zähler überschritten wurde.

  Sie müssen eine Performance-Schwellenwertrichtlinie definieren und sie einem Storage-Objekt zuweisen, um diese Ereignisse zu empfangen.

- **Systemdefinierte Leistungsschwellenwerte-Policy-Ereignisse**

  Performance-Probleme basierend auf Schwellenwerten, die systemdefiniert sind. Diese Schwellenwertrichtlinien sind in der Installation von Unified Manager enthalten, um allgemeine

Performance-Probleme zu beheben.

Diese Schwellenwertrichtlinien sind standardmäßig aktiviert und Sie können Ereignisse kurz nach dem Hinzufügen eines Clusters sehen.

- **Dynamische Leistungsschwellenwerte**

  Performance-Probleme, die auf Fehler oder Fehler in EINER IT-Infrastruktur zurückzuführen sind oder durch eine zu hohe Auslastung der Cluster-Ressourcen führen. Die Ursache dieser Ereignisse kann ein einfaches Problem sein, das sich über einen bestimmten Zeitraum selbst korrigiert oder durch eine Reparatur- oder Konfigurationsänderung behoben werden kann. Ein dynamisches Schwellenwertereignis gibt an, dass Volume-Workloads in einem ONTAP System aufgrund anderer Workloads mit hohen Anforderungen an gemeinsam genutzte Cluster-Komponenten nur langsam sind.

  Diese Schwellenwerte sind standardmäßig aktiviert, und bei Ihnen kann es Ereignisse nach drei Tagen nach dem Erfassen von Daten aus einem neuen Cluster geben.

Arten von Schweregrad für Performance-Ereignisse

Jedes Performance-Ereignis ist mit einem Schweregrad verknüpft, der Ihnen dabei hilft, die Ereignisse zu priorisieren, die unmittelbare Korrekturmaßnahmen erfordern.

- * Kritisch*

  Ein Performance-Ereignis, das zu einer Serviceunterbrechung führen kann, wenn keine Korrekturmaßnahmen sofort ergriffen werden.

  Kritische Ereignisse werden nur von benutzerdefinierten Schwellenwerten gesendet.

- **Warnung**

  Ein Performance-Zähler für ein Cluster-Objekt befindet sich außerhalb des normalen Bereichs und sollte überwacht werden, um sicherzustellen, dass es den kritischen Schweregrad nicht erreicht. Ereignisse dieses Schweregrades führen nicht zu einer Serviceunterbrechung und unmittelbare Korrekturmaßnahmen sind möglicherweise nicht erforderlich.

  Warnereignisse werden von benutzerdefinierten, systemdefinierten oder dynamischen Schwellenwerten gesendet.

- **Information**

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

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

Von Unified Manager erkannte Konfigurationsänderungen

Unified Manager überwacht Ihre Cluster auf Konfigurationsänderungen. So können Sie feststellen, ob eine Änderung zu einem Performance-Ereignis geführt oder beigetragen hat. Auf den Seiten des Performance Explorer wird ein Symbol für das

Änderungsereignis (angezeigt) Zur Angabe des Datums und der Uhrzeit, zu der die Änderung erkannt wurde.

Sie können die Performance-Diagramme auf den Seiten des Performance Explorers und auf der Seite Performance/Volume Details überprüfen, um festzustellen, ob sich das Änderungsereignis auf die Performance des ausgewählten Cluster-Objekts auswirkt. Wenn die Änderung zu oder um die gleiche Zeit wie ein Performance-Ereignis erkannt wurde, hat die Änderung möglicherweise zum Problem beigetragen, was dazu führte, dass die Ereigniswarnung ausgelöst wurde.

Unified Manager erkennt die folgenden Änderungsereignisse, die als Informationsereignisse kategorisiert sind:

- Ein Volume wird zwischen Aggregaten verschoben.

  Unified Manager erkennt, wenn eine Verschiebung gerade ausgeführt, abgeschlossen oder fehlgeschlagen ist. Wenn Unified Manager während einer Volume-Verschiebung ausfällt, erkennt er bei der Sicherung die Volume-Verschiebung und zeigt ein Änderungsereignis für ihn an.

- Der Durchsatz (MB/s oder IOPS) wird von einer QoS-Richtliniengruppe begrenzt, die eine oder mehrere überwachte Workload-Änderungen enthält.

  Das Ändern eines Richtliniengruppenlimits kann zu intermittierenden Latenzspitzen (Antwortzeit) führen, die auch Ereignisse für die Richtliniengruppe auslösen können. Die Latenz kehrt nach und nach wieder in den normalen Zustand zurück und alle durch diese Spitzen verursachten Ereignisse werden obsolet.

- Ein Node in einem HA-Paar übernimmt den Storage seines Partner-Nodes oder gibt ihn zurück.

  Unified Manager erkennt, wann der Takeover-, Teil- oder Giveback-Vorgang abgeschlossen wurde. Wenn der Takeover durch einen Panik- Knoten verursacht wird, erkennt Unified Manager das Ereignis nicht.

- Ein Upgrade oder Zurücksetzen von ONTAP wurde erfolgreich abgeschlossen.

  Die vorherige und die neue Version werden angezeigt.

Was passiert, wenn ein Ereignis empfangen wird

Wenn Unified Manager ein Ereignis empfängt, wird es auf der Seite Dashboards/Übersicht, auf den Registerkarten Zusammenfassung und Explorer der Seite Leistung/Cluster, auf der Seite Ereignisinventar und auf der objektspezifischen Bestandsseite (z. B. auf der Seite „Systemzustand/Volumes-Bestandsaufnahme“) angezeigt.

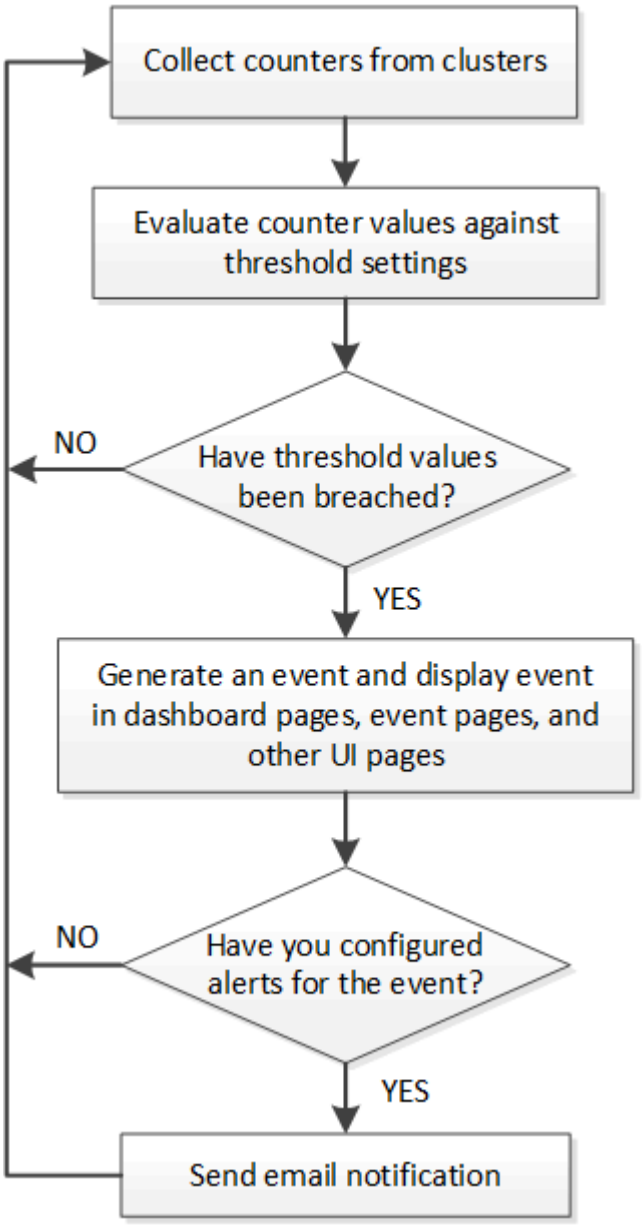
Wenn Unified Manager mehrere kontinuierliche Vorkommnisse derselben Clusterkomponente erkennt, werden alle Vorkommnisse als einzelnes Ereignis behandelt und nicht als separate Ereignisse. Die Dauer des Ereignisses wird erhöht, um anzugeben, dass das Ereignis noch aktiv ist.

Je nachdem, wie Sie Einstellungen auf der Seite Konfiguration/Warnmeldungen konfigurieren, können Sie andere Benutzer über diese Ereignisse benachrichtigen. Die Meldung bewirkt, dass folgende Aktionen ausgelöst werden:

- Eine E-Mail über das Ereignis kann an alle Unified Manager Administrator-Benutzer gesendet werden.
- Das Ereignis kann an weitere E-Mail-Empfänger gesendet werden.
- Ein SNMP-Trap kann an den Trap-Empfänger gesendet werden.

- Ein benutzerdefiniertes Skript kann ausgeführt werden, um eine Aktion auszuführen.

Dieser Workflow wird im folgenden Diagramm dargestellt.



Welche Informationen sind in einer Alarm-E-Mail enthalten

Die Warnmeldungen von Unified Manager liefern die Art des Ereignisses, den Schweregrad des Ereignisses, den Namen der Richtlinie, die gegen das Ereignis verstoßen wurde, und eine Beschreibung des Ereignisses. Die E-Mail-Nachricht enthält auch einen Hyperlink für jedes Ereignis, mit dem Sie die Detailseite für das Ereignis in der Benutzeroberfläche anzeigen können.

Alle Benutzer, die sich für den Erhalt von Benachrichtigungen angemeldet haben, erhalten Warnmeldungen per E-Mail.

Wenn sich ein Performance-Zähler oder Kapazitätswert während einer Inkassofrist groß ändert, kann es dazu führen, dass sowohl ein kritisches als auch ein Warnereignis gleichzeitig für dieselbe Schwellenwertrichtlinie

ausgelöst werden. In diesem Fall erhalten Sie möglicherweise eine E-Mail für das Warnereignis und eine für das kritische Ereignis. Dies liegt daran, dass Sie mit Unified Manager separat Warnmeldungen für Warnung und kritische Schwellenwertverletzungen erhalten.

Nach dem Upgrade auf Unified Manager 7.2 oder höher funktionieren Links zu Ereignissen und Warnmeldungen von E-Mails, die von älteren Versionen von Unified Manager gesendet wurden, aufgrund einer Änderung des Ereignisses und der Alarm-URLs nicht mehr.

Nachstehend finden Sie eine Beispiel-E-Mail für eine Warnmeldung:

From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from OnCommand Unified Manager: Thin-Provisioned Volume Space At Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1

Hinzufügen von Meldungen

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

Bevor Sie beginnen

- Sie müssen Benachrichtigungseinstellungen wie die Benutzer-E-Mail-Adresse, SMTP-Server und SNMP-Trap-Host konfiguriert haben, damit der Unified Manager-Server diese Einstellungen verwenden kann, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.

- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Meldung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie ein Skript basierend auf dem Ereignis ausführen möchten, müssen Sie das Skript mithilfe der Seite Management/Scripts zu Unified Manager hinzugefügt haben.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können eine Warnmeldung direkt auf der Seite Ereignisdetails erstellen, nachdem Sie ein Ereignis empfangen haben. Zusätzlich können Sie eine Warnung auf der Seite Konfiguration/Warnmeldungen erstellen, wie hier beschrieben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Alerting**.
2. Klicken Sie auf der Seite **Konfiguration/Alarmfunktionen** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
4. Klicken Sie auf **Ressourcen**, und wählen Sie die Ressourcen aus, die in die Warnung aufgenommen oder von ihr ausgeschlossen werden sollen.

   Sie können einen Filter festlegen, indem Sie im Feld **Name enthält** eine Textzeichenfolge angeben, um eine Gruppe von Ressourcen auszuwählen. Die Liste der verfügbaren Ressourcen zeigt auf der Grundlage der angegebenen Textzeichenfolge nur die Ressourcen an, die der Filterregel entsprechen. Die von Ihnen angegebene Textzeichenfolge ist die Groß-/Kleinschreibung.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschl- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschließregel, und die Warnung wird nicht für Ereignisse generiert, die sich auf die ausgeschlossene Ressource beziehen.

5. Klicken Sie auf **Events** und wählen Sie die Ereignisse basierend auf dem Ereignisnamen oder dem Schweregrad aus, für den Sie eine Warnung auslösen möchten.

   Um mehrere Ereignisse auszuwählen, drücken Sie die Strg-Taste, während Sie Ihre Auswahl treffen.

6. Klicken Sie auf **Actions**, und wählen Sie die Benutzer aus, die Sie benachrichtigen möchten, wählen Sie die Benachrichtigungshäufigkeit aus, wählen Sie aus, ob ein SNMP-Trap an den Trap-Empfänger gesendet wird, und weisen Sie ein Skript zu, das ausgeführt werden soll, wenn eine Warnung erzeugt wird.

   Wenn Sie die für den Benutzer angegebene E-Mail-Adresse ändern und die Warnmeldung zur Bearbeitung erneut öffnen, erscheint das Feld Name leer, da die geänderte E-Mail-Adresse dem zuvor ausgewählten Benutzer nicht mehr zugeordnet ist. Wenn Sie die E-Mail-Adresse des ausgewählten Benutzers auf der Seite Verwaltung/Benutzer geändert haben, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

   Sie können auch Benutzer über SNMP-Traps benachrichtigen.

7. Klicken Sie Auf **Speichern**.

Beispiel für das Hinzufügen einer Meldung

Dieses Beispiel zeigt, wie eine Warnung erstellt wird, die die folgenden Anforderungen erfüllt:

- Alarmname: HealthTest
- Ressourcen: Enthält alle Volumes, deren Name „`abc`“ enthält und schließt alle Volumes aus, deren Name „`xyz`“ enthält
- Ereignisse: Umfasst alle kritischen Systemzustandsereignisse
- Aktionen: Enthält “sample@domain.com”, ein Skript “Test”, und der Benutzer muss alle 15 Minuten benachrichtigt werden

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

1. Klicken Sie auf **Name** und geben Sie ein `HealthTest` Im Feld **Alarmname**.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
   a. Eingabe `abc` Im Feld **Name enthält** werden die Volumes angezeigt, deren Name „`abc`“ enthält.
   b. Wählen Sie im Bereich Verfügbare Ressourcen **<<All Volumes whose name contains 'abc'>>** aus, und verschieben Sie sie in den Bereich Ausgewählte Ressourcen.
   c. Klicken Sie auf **Ausschließe**, und geben Sie ein `xyz` Klicken Sie im Feld **Name enthält** auf **Hinzufügen**.
3. Klicken Sie auf **Events** und wählen Sie im Feld Ereignis Severity * die Option **kritisch** aus.
4. Wählen Sie im Bereich passende Ereignisse die Option * Alle kritischen Ereignisse* aus, und verschieben Sie sie in den Bereich Ausgewählte Ereignisse.
5. Klicken Sie auf **Aktionen** und geben Sie ein `sample@domain.com` Im Feld „Diese Benutzer benachrichtigen“.
6. Wählen Sie **alle 15 Minuten**, um den Benutzer alle 15 Minuten zu benachrichtigen.

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

Hinzufügen von Meldungen für Performance-Ereignisse

Sie können Benachrichtigungen für einzelne Performance-Ereignisse wie alle anderen Ereignisse, die Unified Manager empfangen hat, konfigurieren. Außerdem können Sie eine einzelne Benachrichtigung erstellen, wenn alle Performance-Ereignisse gleich behandelt werden sollen und E-Mails an dieselbe Person gesendet werden sollen, wenn kritische bzw. Warnereignisse ausgelöst werden.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Das folgende Beispiel zeigt, wie ein Ereignis für alle Ereignisse bezüglich kritischer Latenz, IOPS und MB/s erstellt wird. Sie können diese Methode verwenden, um Ereignisse aus allen Leistungszählern und für alle Warnungsereignisse auszuwählen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Alerting**.
2. Klicken Sie auf der Seite **Konfiguration/Alarmfunktionen** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
4. Wählen Sie auf der Seite **Ressourcen** keine Ressourcen aus.

   Da keine Ressourcen ausgewählt werden, wird die Warnmeldung auf alle Cluster, Aggregate, Volumes usw. angewendet, für die diese Ereignisse empfangen werden.

5. Klicken Sie auf **Events** und führen Sie die folgenden Aktionen aus:
   a. Wählen Sie in der Liste Ereignis Severity die Option **kritisch** aus.
   b. Geben Sie im Feld Ereignisname enthält ein `latency` Und klicken Sie dann auf den Pfeil, um alle übereinstimmenden Ereignisse auszuwählen.
   c. Geben Sie im Feld Ereignisname enthält ein `iops` Und klicken Sie dann auf den Pfeil, um alle übereinstimmenden Ereignisse auszuwählen.
   d. Geben Sie im Feld Ereignisname enthält ein `mbps` Und klicken Sie dann auf den Pfeil, um alle übereinstimmenden Ereignisse auszuwählen.
6. Klicken Sie auf **Aktionen** und wählen Sie dann den Namen des Benutzers aus, der die Benachrichtigung per E-Mail im Feld * Diese Benutzer benachrichtigen* erhält.
7. Konfigurieren Sie alle anderen Optionen auf dieser Seite für die Ausgabe von SNMP-Taps und die Ausführung eines Skripts.
8. Klicken Sie Auf **Speichern**.

Typen systemdefinierter Performance-Schwellenwerte

Unified Manager bietet einige standardmäßige Schwellenwertrichtlinien, die die Cluster-Performance überwachen und Ereignisse automatisch generieren. Diese Richtlinien sind standardmäßig aktiviert und erzeugen Warn- oder Informationsereignisse, wenn die überwachten Performance-Schwellenwerte nicht eingehalten werden.

Systemdefinierte Performance-Schwellenwerte sind auf Cloud Volumes ONTAP-, ONTAP Edge- oder ONTAP Select-Systemen nicht aktiviert.

Wenn Sie von einer systemdefinierten Performance-Schwellenwertrichtlinie unnötige Ereignisse erhalten, können Sie einzelne Richtlinien auf der Seite „Konfiguration/Ereignisse verwalten“ deaktivieren.

Richtlinien für Node-Schwellwerte

Die systemdefinierten Richtlinien für Node-Performance-Schwellenwerte werden standardmäßig jedem Node in den von Unified Manager überwachten Clustern zugewiesen:

- **Node-Ressourcen werden überausgelastet**

  Identifiziert Situationen, in denen ein einzelner Node über dem Grenzen seiner betrieblichen Effizienz arbeitet und so Workload-Latenzen potenziell beeinträchtigen kann. Dies ist ein Warnereignis.

  Bei Nodes, die mit ONTAP 8.3.x und früherer Software installiert sind, sucht dieser Vorgang nach Nodes, die mehr als 30 Minuten lang mehr als 85 % ihrer CPU- und RAM-Ressourcen (Auslastung der Nodes) nutzen.

  Bei Knoten, die mit der Software ONTAP 9.0 und höher installiert werden, sucht dieser Vorgang nach Nodes, die mehr als 30 Minuten lang mehr als 100 % ihrer Performance-Kapazität nutzen.

- **Node HA-Paar überausgelastet**

  Bestimmt, in welchen Fällen die Nodes in einem HA-Paar über den Grenzen der betrieblichen Effizienz des HA-Paars arbeiten. Dies ist ein Informationsereignis.

  Bei Nodes, die mit ONTAP 8.3.x und früherer Software installiert sind, wird dies durch einen Blick auf die CPU- und RAM-Nutzung für die beiden Nodes im HA-Paar erreicht. Wenn die kombinierte Node-Auslastung der beiden Nodes über 140 % für mehr als eine Stunde beträgt, wirkt sich ein Controller-Failover auf die Workload-Latenzen aus.

  Bei Nodes, die mit der Software ONTAP 9.0 und höher installiert sind, werden dabei die verwendeten Performance-Kapazität für die beiden Nodes im HA-Paar untersucht. Wenn die kombinierte Performance-Kapazität der beiden Nodes über 200 % für mehr als eine Stunde beträgt, wirkt sich ein Controller-Failover auf die Workload-Latenzen aus.

- **Node-Disk-Fragmentierung**

  Die Situation erkennt, dass eine Festplatte oder eine Festplatte in einem Aggregat fragmentiert ist, was die Services eines wichtigen Systems verlangsamt und die Workload-Latenzen auf einem Node potenziell beeinträchtigt.

  Hier werden bestimmte Lese- und Schreibverhältnisse über alle Aggregate auf einem Node hinweg betrachtet. Diese Richtlinie kann auch während der Resynchronisierung der SyncMirror ausgelöst werden oder wenn Fehler während des Scrub-Betriebs der Festplatte gefunden werden. Dies ist ein Warnereignis.

  > Die Richtlinie „`Node Disk Fragmentierung`“ analysiert rein HDD-basierte Aggregate; Flash Pool, SSD und FabricPool Aggregate werden nicht analysiert.

Aggregieren von Schwellenwertrichtlinien

Die vom System definierte Richtlinie für aggregierte Performance-Grenzwerte wird standardmäßig jedem Aggregat in den Clustern zugewiesen, das von Unified Manager überwacht wird.

- **Aggregat Festplatten überausgelastet**

  Die Situation erkennt, in denen ein Aggregat über den Grenzen seiner betrieblichen Effizienz arbeitet und so die Workload-Latenzen potenziell beeinträchtigt werden. Es identifiziert diese Situationen durch die Suche nach Aggregaten, bei denen die Festplatten im Aggregat mehr als 95% für mehr als 30 Minuten ausgelastet sind. Diese Multicondition-Richtlinie führt dann die folgende Analyse durch, um die Ursache des Problems zu ermitteln:

  - Wird eine Festplatte im Aggregat derzeit im Hintergrund gewartet?

Zu den Hintergrund-Wartungsaktivitäten, für die eine Festplatte möglicherweise benötigt wird, zählen die Festplattenrekonstruktion, der Festplattenscrub, die SyncMirror-Neusynchronisierung und das Reparität.

- Gibt es einen Kommunikationsengpass für den Fibre Channel Interconnect im Platten-Shelf?
- Gibt es zu wenig freien Platz im Aggregat? Ein Warnereignis wird für diese Richtlinie nur dann ausgegeben, wenn eine (oder mehrere) der drei untergeordneten Richtlinien ebenfalls als verletzt betrachtet wird. Ein Performance-Ereignis wird nicht ausgelöst, wenn nur die Festplatten im Aggregat mehr als 95 % ausgelastet sind.

Die Richtlinie „`Aggregate Disks Over-used`“ analysiert rein HDD-basierte Aggregate und Flash Pool (Hybrid) Aggregate, SSD- und FabricPool-Aggregate werden nicht analysiert.

QoS-Schwellenwertrichtlinien

Die systemdefinierten QoS-Performance-Schwellenwertrichtlinien werden jedem Workload mit einer konfigurierten ONTAP QoS-Richtlinie für einen maximalen Durchsatz (IOPS, IOPS/TB oder MB/s) zugewiesen. Unified Manager löst ein Ereignis aus, wenn der Workload-Durchsatzwert 15 % geringer ist als der konfigurierte QoS-Wert.

- **QoS max IOPS oder MB/s Schwellenwert**

  Identifiziert Volumes und LUNs, die ihre maximalen IOPS-Werte durch QoS oder Durchsatzwerte von MB/s überschritten haben und die eine Workload-Latenz beeinträchtigen. Dies ist ein Warnereignis.

  Wird einem einzelnen Workload einer Richtliniengruppe zugewiesen, so wird dies durch Workloads gesucht, die während jedes Erfassungszeitraums für die vorherige Stunde den in der zugewiesenen QoS-Richtliniengruppe definierten Maximaldurchsatz überschritten haben.

  Wenn mehrere Workloads eine einzelne QoS-Richtlinie gemeinsam nutzen, werden dazu die IOPS oder MB/s aller Workloads in der Richtlinie hinzugefügt und die Gesamtsumme im Vergleich zum Schwellenwert überprüft.

- **QoS Peak IOPS/TB oder IOPS/TB mit Block Size Schwellenwert**

  Identifiziert Volumes, die die adaptive QoS-Grenze für IOPS/TB-Durchsatz überschritten haben (oder IOPS/TB mit Blockgrößen-Limit) und die sich auf die Workload-Latenz auswirken. Dies ist ein Warnereignis.

  Dazu wird der in der adaptiven QoS-Richtlinie definierte IOPS-Spitzenwert pro TB in einen QoS-Maximalwert für IOPS basierend auf der Größe jedes Volumes konvertiert. Anschließend werden Volumes untersucht, die während jedes Performance-Erfassungszeitraums für die vorherige Stunde die maximalen IOPS-Werte für QoS überschritten haben.

  Diese Richtlinie wird nur auf Volumes angewendet, wenn das Cluster mit ONTAP 9.3 und höher installiert ist.

  Wurde in der anpassungsfähigen QoS-Richtlinie das Element „`Blockgröße`“ definiert, wird dieser Schwellenwert basierend auf der Größe jedes Volumes in einen QoS-Maximalwert umgewandelt. Dann sucht es nach Volumes, die die maximalen MB/s der QoS in jedem Performance-Erfassungszeitraum für die vorherige Stunde überschritten haben.

Diese Richtlinie wird nur auf Volumes angewendet, wenn das Cluster mit ONTAP 9.5 und höher installiert ist.

Verwalten von benutzerdefinierten Performance-Schwellenwerten

Mithilfe von Performance-Schwellenwertrichtlinien können Sie den Zeitpunkt bestimmen, an dem Unified Manager ein Ereignis generiert, um Systemadministratoren über Probleme zu informieren, die sich auf die Workload-Performance auswirken könnten. Diese Schwellenwertrichtlinien werden als „*user-defined* Performance Schwellenwerte“ bezeichnet.

Diese Version unterstützt benutzerdefinierte, systemdefinierte und dynamische Performance-Schwellenwerte. Bei dynamischen und systemdefinierten Performance-Schwellenwerten analysiert Unified Manager die Workload-Aktivität, um den entsprechenden Schwellwert zu ermitteln. Mit benutzerdefinierten Schwellenwerten können Sie die oberen Performance-Grenzen für viele Performance-Zähler und für viele Storage-Objekte definieren.

Systemdefinierte Performance-Schwellenwerte und dynamische Performance-Schwellenwerte werden von Unified Manager festgelegt und können nicht konfiguriert werden. Wenn Sie von einer systemdefinierten Performance-Schwellenwertrichtlinie unnötige Ereignisse erhalten, können Sie einzelne Richtlinien auf der Seite „Konfiguration/Ereignisse verwalten“ deaktivieren.

Funktionsweise benutzerdefinierter Richtlinien für Leistungsschwellenwerte

Sie legen für Storage-Objekte Richtlinien für Performance-Schwellenwerte fest (z. B. für Aggregate und Volumes), damit ein Ereignis an den Storage-Administrator gesendet werden kann, um den Administrator zu informieren, dass im Cluster ein Performance-Problem auftritt.

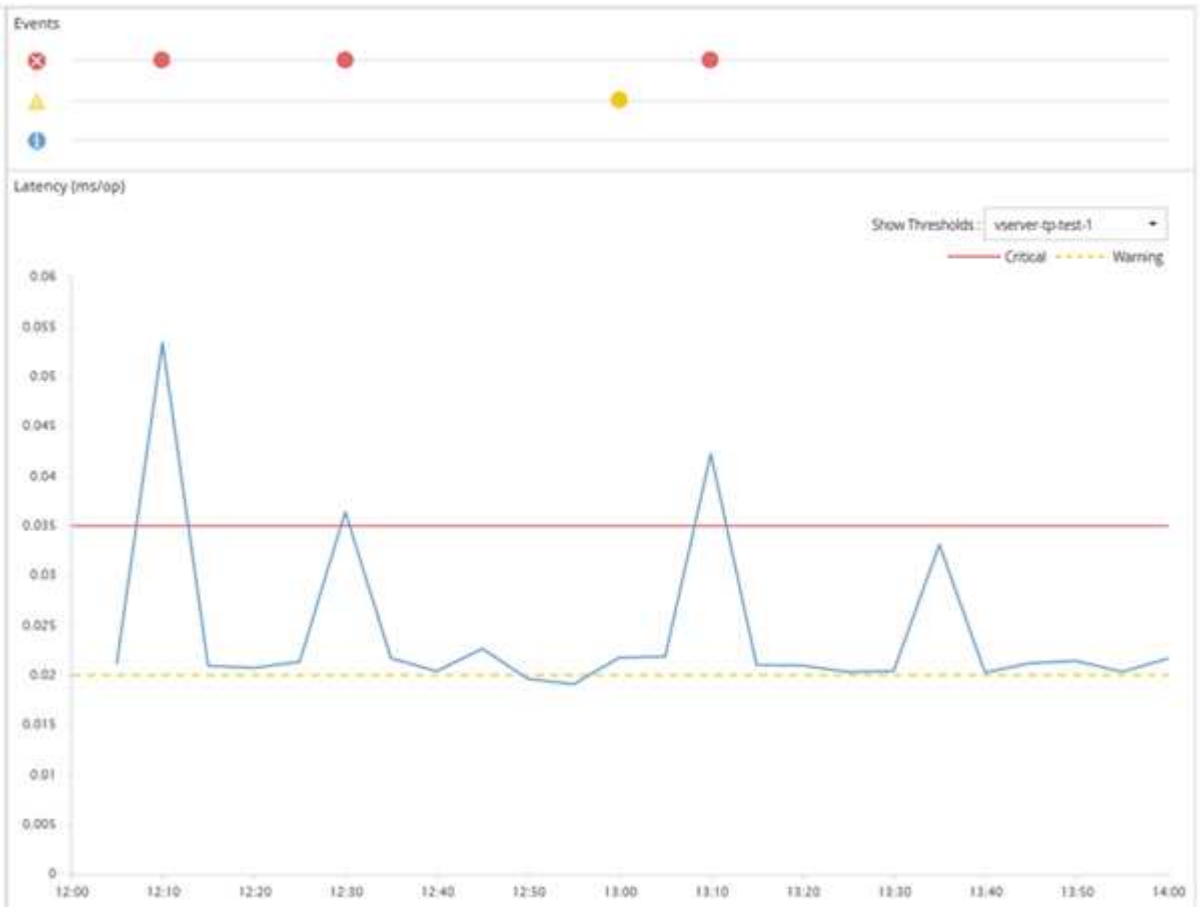
Sie erstellen eine Performance-Schwellenwertrichtlinie für ein Storage-Objekt durch:

- Auswählen eines Storage-Objekts
- Auswählen eines Performance-Zählers, der diesem Objekt zugeordnet ist
- Festlegen von Werten, die die oberen Grenzwerte des Performance-Zählers definieren, die als Warnung und kritische Situationen gelten
- Geben Sie einen Zeitraum an, der definiert, wie lange der Zähler den oberen Grenzwert überschreiten muss

Beispielsweise können Sie eine Performance-Schwellenwertrichtlinie für ein Volume festlegen, damit Sie bei jedem IOPS für dieses Volume 750 in 10 aufeinanderfolgenden Minuten eine wichtige Ereignisbenachrichtigung erhalten. Diese Schwellenwertrichtlinie kann auch festlegen, dass ein Warnereignis gesendet wird, wenn IOPS mehr als 500 Operationen pro Sekunde für 10 Minuten beträgt.

Der aktuelle Release bietet Schwellenwerte, die Ereignisse senden, wenn ein Zählerwert die Schwellenwerteinstellung überschreitet. Sie können keine Schwellenwerte festlegen, die Ereignisse senden, wenn ein Zählerwert unter eine Schwellenwerteinstellung fällt.

Hier wird ein Beispiel für ein Zählerdiagramm angezeigt, das angibt, dass ein Warnschwellenwert (gelbes Symbol) um 1:00 verletzt wurde und dass ein kritischer Schwellenwert (rotes Symbol) um 12:10, 12:30 und 1:10 Uhr verletzt wurde:



Für die angegebene Dauer muss eine Schwellenverletzung kontinuierlich auftreten. Wenn der Schwellenwert aus irgendeinem Grund unter die Grenzwerte fällt, wird eine spätere Verletzung als Beginn einer neuen Dauer betrachtet.

Durch einige Cluster-Objekte und Performance-Zähler können Sie eine kombinierte Schwellenwertrichtlinie erstellen, bei der zwei Performance-Zähler ihre Höchstgrenzen überschreiten müssen, bevor ein Ereignis generiert wird. Sie können beispielsweise anhand der folgenden Kriterien eine Schwellenwertrichtlinie erstellen:

Cluster-Objekt	Performance-Zähler	Warnschwellenwert	Kritischer Schwellenwert	Dauer
Datenmenge	Latenz	10 Millisekunden	20 Millisekunden	15 Minuten

Schwellenwertrichtlinien, die zwei Cluster-Objekte verwenden, führen dazu, dass ein Ereignis nur generiert wird, wenn beide Bedingungen nicht erfüllt sind. Beispiel anhand der in der Tabelle definierten Schwellwertrichtlinie:

Wenn Volume-Latenz durchschnittlich ist…	Und Festplatten-Auslastung aggregieren ist…	Dann…
15 Millisekunden	50 % erzielt	Es wird kein Ereignis gemeldet.

Wenn Volume-Latenz durchschnittlich ist…	Und Festplatten-Auslastung aggregieren ist…	Dann…
15 Millisekunden	75 % erzielt	Ein Warnereignis wird gemeldet.
25 Millisekunden	75 % erzielt	Ein Warnereignis wird gemeldet.
25 Millisekunden	90 % erzielt	Ein kritisches Ereignis wird gemeldet.

Was passiert, wenn eine Performance-Richtlinie nicht eingehalten wird

Wenn ein Zählerwert den definierten Performance-Schwellenwert für die in der Dauer angegebene Zeit überschreitet, wird der Schwellenwert überschritten und ein Ereignis wird gemeldet.

Das Ereignis veranlasst folgende Aktionen:

- Das Ereignis wird auf der Seite Performance Dashboard, der Seite Performance Cluster Summary, der Seite Events und der objektspezifischen Seite Performance Inventory angezeigt.
- (Optional) eine E-Mail-Benachrichtigung über das Ereignis kann an einen oder mehrere E-Mail-Empfänger gesendet werden, und ein SNMP-Trap kann an einen Trap-Empfänger gesendet werden.
- (Optional) Ein Skript kann ausgeführt werden, um Speicherobjekte automatisch zu ändern oder zu aktualisieren.

Die erste Aktion wird immer ausgeführt. Sie konfigurieren, ob die optionalen Aktionen auf der Seite Konfiguration/Warnmeldungen ausgeführt werden. Je nachdem, ob eine Warnung oder eine kritische Grenzwertrichtlinie nicht eingehalten wird, können Sie eindeutige Aktionen definieren.

Nach einer Richtlinienverletzung bei einem Performance-Schwellenwert für ein Storage-Objekt werden für diese Richtlinie keine weiteren Ereignisse generiert, bis der Zählerwert den Schwellenwert überschreitet und zu diesem Zeitpunkt wird die Dauer für dieses Limit zurückgesetzt. Während der Schwellenwert weiterhin überschritten wird, wird die Endzeit des Ereignisses kontinuierlich aktualisiert, sodass dieses Ereignis fortgesetzt wird.

Ein Schwellenwertereignis erfasst oder friert die Informationen in Bezug auf Schweregrad und Richtliniendefinition so ein, dass eindeutige Schwellenwertinformationen mit dem Ereignis angezeigt werden, auch wenn die Schwellenwertrichtlinie zukünftig geändert wird.

Welche Performance-Zähler können mithilfe von Schwellenwerten verfolgt werden

Einige allgemeine Performance-Zähler wie IOPS und MB/s können Schwellenwerte für alle Storage-Objekte festlegen. Es gibt andere Zähler, deren Schwellenwerte nur für bestimmte Speicherobjekte festgelegt werden können.

Verfügbare Performance-Zähler

Storage Objekt	Performance-Zähler	Beschreibung
Cluster	IOPS	Durchschnittliche Anzahl von ein-/Ausgabeoperationen, die das Cluster pro Sekunde verarbeitet.
MB/Sek.	Durchschnittliche Anzahl der Megabyte an Daten, die in diesen und von diesem Cluster pro Sekunde übertragen werden.	Knoten
IOPS	Durchschnittliche Anzahl der ein-/Ausgabevorgänge der Knoten verarbeitet pro Sekunde.	MB/Sek.
Durchschnittliche Anzahl der Megabyte an Daten, die in diesen Node pro Sekunde übertragen werden.	Latenz	Durchschnittliche Anzahl von Millisekunden, in denen der Node auf Applikationsanforderungen reagiert.
Auslastung	Durchschnittlicher Prozentsatz der CPU und des RAM des Node, der verwendet wird.	Verwendete Performance-Kapazität
Durchschnittlicher Prozentsatz der Performance-Kapazität, die vom Node verbraucht wird.	Verwendete Performance-Kapazität – Übernahme	Durchschnittlicher Prozentsatz der Performance-Kapazität, die vom Node verbraucht wird, sowie die Performance-Kapazität des Partner-Nodes.
Aggregat	IOPS	Durchschnittliche Anzahl der ein-/Ausgabevorgänge die aggregierten Prozesse pro Sekunde.
MB/Sek.	Durchschnittliche Anzahl der Megabyte an Daten, die in dieses Aggregat pro Sekunde übertragen werden.	Latenz
Durchschnittliche Anzahl von Millisekunden, die das Aggregat zur Reaktion auf Applikationsanforderungen benötigt.	Auslastung	Durchschnittlicher Prozentsatz der verwendeten Festplatten des Aggregats.
Verwendete Performance-Kapazität	Durchschnittlicher Prozentsatz der Performance-Kapazität, die vom Aggregat verbraucht wird.	Storage Virtual Machine (SVM)

Storage Objekt	Performance-Zähler	Beschreibung
IOPS	Durchschnittliche Anzahl von ein-/Ausgabevorgängen, die die SVM in einer Sekunde verarbeitet	MB/Sek.
Durchschnittliche Anzahl der in und von dieser SVM pro Sekunde übertragenen Megabyte.	Latenz	Durchschnittliche Anzahl von Millisekunden, die SVM zur Beantwortung von Applikationsanforderungen benötigt.
Datenmenge	IOPS	Durchschnittliche Anzahl der ein-/Ausgabevorgänge die Volume-Prozesse pro Sekunde.
MB/Sek.	Durchschnittliche Anzahl der Megabyte an Daten, die in dieses Volume pro Sekunde übertragen werden.	Latenz
Durchschnittliche Anzahl von Millisekunden, die das Volume zur Beantwortung von Applikationsanforderungen benötigt.	Cache-fehlsverhältnis	Durchschnittlicher Prozentsatz von Leseanforderungen von Client-Applikationen, die vom Volume zurückgegeben werden, anstatt vom Cache zurückgegeben zu werden.
LUN	IOPS	Durchschnittliche Anzahl der ein-/Ausgabevorgänge, die das LUN pro Sekunde verarbeitet.
MB/Sek.	Durchschnittliche Anzahl der Megabyte an Daten, die in diese LUN pro Sekunde übertragen werden.	Latenz
Durchschnittliche Anzahl von Millisekunden, die die LUN benötigt, um auf Applikationsanforderungen zu reagieren.	Namespace	IOPS
Durchschnittliche Anzahl der ein-/Ausgabevorgänge, die der Namespace pro Sekunde verarbeitet.	MB/Sek.	Durchschnittliche Anzahl der Megabyte an Daten, die in diesen Namespace pro Sekunde übertragen werden.

Storage Objekt	Performance-Zähler	Beschreibung
Latenz	Durchschnittliche Anzahl von Millisekunden, in denen der Namespace auf Applikationsanforderungen reagiert.	Port
Bandbreitenauslastung	Durchschnittlicher Prozentsatz der verfügbaren Bandbreite des Ports, die verwendet wird.	MB/Sek.
Durchschnittliche Anzahl der Megabyte an Daten, die in diesen Port pro Sekunde übertragen werden.	Logische Schnittstelle (LIF)	MB/Sek.

Daten zur Performance-Kapazität sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.

Welche Objekte und Zähler können in Schwellwertrichtlinien für Kombinationen verwendet werden

Nur einige Leistungsindikatoren können in Kombinationsrichtlinien kombiniert werden. Wenn primäre und sekundäre Performance-Zähler angegeben werden, müssen beide Performance-Zähler ihre Höchstgrenzen überschreiten, bevor ein Ereignis generiert wird.

Primäres Speicherobjekt und Zähler	Sekundäres Storage Objekt und Zähler
Volume-Latenz	Volume IOPS
Volumen-Mbps	Aggregatauslastung
Verwendete Aggregat-Performance-Kapazität	Node-Auslastung
Verwendete Node-Performance-Kapazität	Verwendete Node-Performance-Kapazität – Übernahme
LUN-Latenz	LUN IOPS
LUN MBit/Sek.	Aggregatauslastung
Verwendete Aggregat-Performance-Kapazität	Node-Auslastung
Verwendete Node-Performance-Kapazität	Verwendete Node-Performance-Kapazität – Übernahme

Wenn eine Richtlinie für eine Volume-Kombination auf ein FlexGroup Volume anstatt auf ein FlexVol Volume angewendet wird, können nur die Attribute „`Volume IOPS`“ und „`Volume Mbps`“ als sekundärer Zähler ausgewählt werden. Wenn die Schwellenwertrichtlinie eines der Node- oder Aggregatattribute enthält, wird die Richtlinie nicht auf das FlexGroup Volume angewendet. Die hier vorliegende Fehlermeldung wird veröffentlicht. Der Grund dafür ist, dass FlexGroup Volumes auf mehr als einem Node oder Aggregat vorhanden sein können.

Benutzerdefinierte Richtlinien für Leistungsschwellenwerte werden erstellt

Sie erstellen Performance-Schwellenwertrichtlinien für Storage-Objekte, damit Benachrichtigungen gesendet werden, wenn ein Performance-Zähler einen bestimmten Wert überschreitet. Die Ereignisbenachrichtigung identifiziert, dass ein Performance-Problem auf dem Cluster auftritt.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Sie erstellen Richtlinien für Leistungsschwellenwerte, indem Sie die Schwellenwerte auf der Seite Schwellenwertrichtlinie erstellen eingeben. Sie können neue Richtlinien erstellen, indem Sie alle Richtlinienwerte auf dieser Seite definieren, oder Sie können eine Kopie einer vorhandenen Richtlinie erstellen und die Werte in der Kopie ändern (genannt *Cloning*).

Gültige Schwellenwerte sind 0.001 bis 10,000,000 für Zahlen, 0.001-100 für Prozentsätze und 0.001-200 für Performance-Kapazität verwendet Prozentwerte.

Der aktuelle Release bietet Schwellenwerte, die Ereignisse senden, wenn ein Zählerwert die Schwellenwerteinstellung überschreitet. Sie können keine Schwellenwerte festlegen, die Ereignisse senden, wenn ein Zählerwert unter eine Schwellenwerteinstellung fällt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Konfiguration** > **Leistungsschwellenwerte**.

   Die Seite Konfiguration/Leistungsschwellenwerte wird angezeigt.

2. Je nachdem, ob Sie eine neue Richtlinie erstellen möchten oder eine ähnliche Richtlinie klonen und die geklonte Version ändern möchten, klicken Sie auf die entsprechende Schaltfläche.

An…	Klicken Sie Auf…
Erstellen Sie eine neue Richtlinie	**Erstellen**
Vorhandene Richtlinie klonen	Wählen Sie eine vorhandene Richtlinie aus, und klicken Sie auf **Clone**

   Die Seite Schwellenwertrichtlinie erstellen oder Schwellenwertrichtlinie klonen wird angezeigt.

3. Definieren Sie die Schwellenwertrichtlinie, indem Sie die Performance-Zählerschwellenwerte angeben, die

für bestimmte Storage-Objekte festgelegt werden sollen:

a. Wählen Sie den Speicherobjekttyp aus, und geben Sie einen Namen und eine Beschreibung für die Richtlinie an.
b. Wählen Sie den zu verfollenden Leistungszähler aus und geben Sie die Grenzwerte an, die Warnungs- und kritische Ereignisse definieren.

   Sie müssen mindestens eine Warnung oder einen kritischen Grenzwert definieren. Sie müssen nicht beide Arten von Limits definieren.

c. Wählen Sie ggf. einen sekundären Leistungsindikenzähler aus und geben Sie die Grenzwerte für Warnungs- und kritische Ereignisse an.

   Zum Einbeziehen eines sekundären Zählers müssen beide Zähler die Grenzwerte überschreiten, bevor der Schwellenwert überschritten wird und ein Ereignis gemeldet wird. Es können nur bestimmte Objekte und Zähler anhand einer Kombinationsrichtlinie konfiguriert werden.

d. Wählen Sie die Dauer aus, für die die Grenzwerte für ein zu sendes Ereignis überschritten werden müssen.

Beim Klonen einer vorhandenen Richtlinie müssen Sie einen neuen Namen für die Richtlinie eingeben.

4. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

   Sie gelangen wieder zur Seite Konfigurations-/Performance-Schwellenwerte. Eine Erfolgsmeldung oben auf der Seite bestätigt, dass die Schwellenwertrichtlinie erstellt wurde und einen Link zur Inventarseite für diesen Objekttyp enthält, damit Sie die neue Richtlinie sofort auf Speicherobjekte anwenden können.

Nachdem Sie fertig sind

Wenn Sie die neue Schwellenwertrichtlinie zu diesem Zeitpunkt auf Speicherobjekte anwenden möchten, können Sie auf den Link **Gehe zu Object_type now** klicken, um zur Inventarseite zu gelangen.

Zuweisen von Richtlinien zu Performance-Schwellenwerten zu Storage-Objekten

Sie weisen einem Storage-Objekt eine benutzerdefinierte Performance-Schwellenwertrichtlinie zu, damit Unified Manager ein Ereignis meldet, wenn der Wert des Performance-Zählers die Richtlinieneinstellung überschreitet.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Die Richtlinie für Performance-Schwellenwerte oder -Richtlinien, die Sie auf das Objekt anwenden möchten, müssen vorhanden sein.

Über diese Aufgabe

Sie können nur eine Performance-Richtlinie gleichzeitig auf ein Objekt oder eine Gruppe von Objekten anwenden.

Sie können jedem Storage-Objekt maximal drei Schwellenwertrichtlinien zuweisen. Wenn bei der Zuweisung von Richtlinien zu mehreren Objekten bereits die maximale Anzahl an Richtlinien zugewiesen ist, führt Unified Manager die folgenden Aktionen durch:

- Wendet die Richtlinie auf alle ausgewählten Objekte an, die ihr Maximum nicht erreicht haben
- Ignoriert die Objekte, die die maximale Anzahl von Richtlinien erreicht haben
- Zeigt eine Meldung an, dass die Richtlinie nicht allen Objekten zugewiesen wurde

Wenn zudem einige Objekte den in der Schwellenwertrichtlinie verfolgten Zähler nicht unterstützen, wird die Richtlinie nicht auf das Objekt angewendet. Wenn Sie beispielsweise eine Schwellenwertrichtlinie „`Performance Capacity used`“ erstellen und sie dann einem Node zuweisen, der über keine ONTAP 9.0 oder höher installierte Software verfügt, wird die Richtlinie nicht auf diesen Node angewendet.

Schritte

1. Wählen Sie auf der Seite „Performance Inventory“ eines beliebigen Storage-Objekts das Objekt oder die Objekte aus, denen Sie eine Schwellenwertrichtlinie zuweisen möchten:

So weisen Sie Schwellenwerte zu…	Klicken Sie Auf…
Ein einzelnes Objekt	Das Kontrollkästchen links neben dem Objekt.
Mehrere Objekte	Das Kontrollkästchen links von jedem Objekt.
Alle Objekte auf der Seite	Der Dropdown-Feld, und wählen Sie **Wählen Sie alle Objekte auf dieser Seite** aus.
Alle Objekte desselben Typs	Der Dropdown-Feld, und wählen Sie **Alle Objekte auswählen**.

   Mithilfe der Sortier- und Filterfunktion können Sie die Objektliste auf der Bestandsseite verfeinern, um die Anwendung von Schwellenwertrichtlinien auf viele Objekte zu erleichtern.

2. Treffen Sie Ihre Auswahl und klicken Sie dann auf **Richtlinie für Leistungsschwellenwert zuweisen**.

   Die Seite „Grenzwertrichtlinie zuweisen“ wird angezeigt und zeigt eine Liste von Schwellenwertrichtlinien an, die für diesen spezifischen Typ von Speicherobjekt vorhanden sind.

3. Klicken Sie auf die einzelnen Richtlinien, um die Details zu den Einstellungen für den Leistungsschwellenwert anzuzeigen, um zu überprüfen, ob Sie die richtige Schwellenwertrichtlinie ausgewählt haben.
4. Klicken Sie nach Auswahl der entsprechenden Schwellenwertrichtlinie auf **Richtlinie zuweisen**.

   Eine Erfolgsmeldung oben auf der Seite bestätigt, dass die Schwellenwertrichtlinie dem Objekt oder den Objekten zugewiesen wurde und stellt einen Link zur Seite Alerting bereit, sodass Sie die Warnungseinstellungen für dieses Objekt und die Richtlinie konfigurieren können.

Nachdem Sie fertig sind

Wenn Sie Benachrichtigungen über E-Mail oder als SNMP-Trap senden möchten, um Sie darüber zu informieren, dass ein bestimmtes Leistungsereignis generiert wurde, müssen Sie die Alarmeinstellungen auf der Seite Konfiguration/Alarmauslösung konfigurieren.

Anzeigen von Richtlinien für Performance-Schwellenwerte

Sie können alle derzeit definierten Performance-Schwellenwertrichtlinien auf der Seite Konfiguration/Performance-Schwellenwerte anzeigen.

Über diese Aufgabe

Die Liste der Schwellenwertrichtlinien wird alphabetisch nach Richtlinienname sortiert und umfasst Richtlinien für alle Arten von Storage-Objekten. Sie können auf eine Spaltenüberschrift klicken, um die Richtlinien nach dieser Spalte zu sortieren. Wenn Sie nach einer bestimmten Richtlinie suchen, können Sie mithilfe der Filter- und Suchmechanismen die Liste der Schwellenwertrichtlinien, die in der Bestandsliste angezeigt werden, verfeinern.

Sie können den Mauszeiger über den Richtliniennamen und den Bedingungsnamen bewegen, um die Konfigurationsdetails der Richtlinie anzuzeigen. Zusätzlich können Sie mithilfe der bereitgestellten Schaltflächen benutzerdefinierte Schwellenwertrichtlinien erstellen, klonen, bearbeiten und löschen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Konfiguration** > **Leistungsschwellenwerte**.

   Die Seite Konfiguration/Leistungsschwellenwerte wird angezeigt.

Bearbeiten benutzerdefinierter Richtlinien für Leistungsschwellenwerte

Sie können die Schwellenwerteinstellungen für vorhandene Performance-Schwellenwertrichtlinien bearbeiten. Dies kann nützlich sein, wenn Sie feststellen, dass Sie zu viele oder zu wenige Warnmeldungen für bestimmte Schwellwerte erhalten.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Sie können den Richtliniennamen oder den Typ des Storage-Objekts, das für vorhandene Schwellenwertrichtlinien überwacht wird, nicht ändern.

Schritte

1. Wählen Sie im linken Navigationsbereich **Konfiguration** > **Leistungsschwellenwerte**.

   Die Seite Konfigurations-/Leistungsschwellenwerte wird angezeigt.

2. Wählen Sie die Schwellenwertrichtlinie aus, die Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

   Die Seite „Schwellenwertrichtlinie bearbeiten“ wird angezeigt.

3. Nehmen Sie Ihre Änderungen an der Schwellenwertrichtlinie vor und klicken Sie auf **Speichern**.

   Sie gelangen wieder zur Seite Konfigurations-/Performance-Schwellenwerte.

Ergebnisse

Nachdem sie gespeichert wurden, werden Änderungen sofort für alle Speicherobjekte aktualisiert, die die Richtlinie verwenden.

Nachdem Sie fertig sind

Je nach Art der Änderungen, die Sie an der Richtlinie vorgenommen haben, sollten Sie möglicherweise die für die Objekte konfigurierten Warnungseinstellungen überprüfen, die die Richtlinie auf der Seite Konfiguration/Alarmauslösung verwenden.

Entfernen von Richtlinien für Performance-Schwellenwerte aus Storage-Objekten

Sie können eine benutzerdefinierte Performance-Schwellenwertrichtlinie aus einem Storage-Objekt entfernen, wenn Unified Manager den Wert des Performance-Zählers nicht mehr überwachen soll.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Sie können jeweils nur eine Richtlinie aus einem ausgewählten Objekt entfernen.

Sie können eine Schwellenwertrichtlinie aus mehreren Speicherobjekten entfernen, indem Sie mehr als ein Objekt in der Liste auswählen.

Schritte

1. Wählen Sie auf der Seite **Inventory** eines Speicherobjekts ein oder mehrere Objekte aus, auf denen mindestens eine Richtlinie für Leistungsschwellenwerte angewendet wurde.

So löschen Sie Schwellenwerte aus…	Tun Sie das…
Ein einzelnes Objekt	Aktivieren Sie das Kontrollkästchen links neben dem Objekt.
Mehrere Objekte	Aktivieren Sie das Kontrollkästchen links neben jedem Objekt.
Alle Objekte auf der Seite	Klicken Sie Auf Und wählen Sie **Wählen Sie alle Objekte auf dieser Seite** aus.
Alle Objekte desselben Typs	Klicken Sie Auf Und wählen Sie **Alle Objekte auswählen**.

2. Klicken Sie Auf **Richtlinie Für Leistungsschwellenwert Löschen**.

   Auf der Seite Schwellenwertrichtlinie löschen wird eine Liste mit Schwellenwertrichtlinien angezeigt, die den Speicherobjekten derzeit zugewiesen sind.

3. Wählen Sie die Schwellenwertrichtlinie aus, die Sie aus den Objekten entfernen möchten, und klicken Sie auf **Richtlinie löschen**.

   Wenn Sie eine Schwellenwertrichtlinie auswählen, werden die Details der Richtlinie angezeigt, damit Sie bestätigen können, dass Sie die entsprechende Richtlinie ausgewählt haben.

Was passiert, wenn eine Performance-Schwellenwertrichtlinie geändert wird

Wenn Sie den Zählerwert oder die Dauer einer vorhandenen Richtlinie für den Performance-Schwellenwert anpassen, wird die Richtlinienänderung auf alle Storage-Objekte angewendet, die die Richtlinie verwenden. Die neue Einstellung erfolgt sofort und Unified Manager beginnt, die Performance-Zählerwerte mit den neuen Schwellenwerten für alle neu erfassten Performance-Daten zu vergleichen.

Falls für Objekte, die die geänderte Schwellenwertrichtlinie verwenden, aktive Ereignisse vorhanden sind, werden die Ereignisse als veraltet markiert, und die Schwellenwertrichtlinie beginnt, den Zähler als neu definierte Schwellenwertrichtlinie zu überwachen.

Wenn Sie den Zähler anzeigen, auf dem der Schwellenwert in der Detailansicht Zählerdiagramme angewendet wurde, spiegeln die kritischen und Warnschwellenwerte die aktuellen Schwellenwerteinstellungen wider. Die ursprünglichen Schwellwerteinstellungen werden auf dieser Seite nicht angezeigt, auch wenn Sie historische Daten anzeigen, wenn die alte Schwellenwerteinstellung wirksam war.

> Da ältere Schwellenwerteinstellungen nicht in der detaillierten Ansicht der Zählerdiagramme angezeigt werden, werden möglicherweise historische Ereignisse unter den aktuellen Schwellenwerten angezeigt.

Was passiert mit Performance-Schwellenwertrichtlinien, wenn ein Objekt verschoben wird

Da Performance-Schwellenwertrichtlinien Storage-Objekten zugewiesen werden. Wenn Sie ein Objekt verschieben, bleiben alle zugewiesenen Schwellenwertrichtlinien nach Abschluss der Verschiebung mit dem Objekt verbunden. Wenn Sie beispielsweise ein Volume oder eine LUN zu einem anderen Aggregat verschieben, sind die Schwellenwertrichtlinien weiterhin für das Volume oder die LUN auf dem neuen Aggregat aktiv.

Wenn für die Schwellenwertrichtlinie eine sekundäre Zählerbedingung (eine Kombinationsrichtlinie) besteht – z. B. wenn einem Aggregat oder einem Node eine zusätzliche Bedingung zugewiesen ist – wird die sekundäre Zählerbedingung auf das neue Aggregat bzw. den Node angewendet, auf das das Volume oder die LUN verschoben wurde.

Falls für Objekte, die die geänderte Schwellenwertrichtlinie verwenden, neue aktive Ereignisse vorhanden sind, werden die Ereignisse als veraltet markiert und die Schwellenwertrichtlinie beginnt, den Zähler als neu definierte Schwellenwertrichtlinie zu überwachen.

Ein Vorgang zum Verschieben eines Volumes führt dazu, dass ONTAP ein Informationseränderungsereignis sendet. Auf der Seite „Performance Explorer“ und auf der Seite „Performance/Volume Details“ wird ein Symbol für das Änderungsereignis angezeigt, um die Uhrzeit anzugeben, zu der der Vorgang abgeschlossen wurde.

Wenn Sie ein Objekt in ein anderes Cluster verschieben, wird die benutzerdefinierte Schwellenwertrichtlinie aus dem Objekt entfernt. Falls erforderlich, müssen Sie dem Objekt nach Abschluss des Verschiebevorgangs eine Schwellenwertrichtlinie zuweisen. Dynamische und systemdefinierte Schwellenwertrichtlinien werden jedoch nach dem Verschieben in ein neues Cluster automatisch auf ein Objekt angewendet.

Schwellenwertrichtlinien-Funktionalität während HA Takeover und Giveback

Wenn ein Takeover- oder Giveback-Vorgang in einer Hochverfügbarkeits-(HA-)Konfiguration durchgeführt werden, behalten Objekte, die von einem Node auf den anderen Node verschoben werden, ihre Schwellenwertrichtlinien auf dieselbe Weise wie bei der manuellen Verschiebung bei. Da Unified Manager alle 15 Minuten nach Änderungen der Cluster-Konfiguration sucht, werden die Auswirkungen der Umschaltung auf den neuen Node erst nach der nächsten Abfrage der Cluster-Konfiguration identifiziert.

Wenn sowohl ein Takeover- als auch ein Giveback-Vorgang innerhalb des Erfassungszeitraums von 15 Minuten Konfigurationsänderungen durchgeführt werden, werden die Performance-Statistiken von einem Node zu einem anderen Node verschoben.

Schwellenwertrichtlinien während der Aggregatverschiebung

Wenn Sie ein Aggregat mithilfe von von von einem Node zu einem anderen Node verschieben `aggregate relocation start` Der Befehl wird sowohl für alle Objekte als auch für kombinierte Schwellwerte beibehalten und der Node-Teil der Schwellenwertrichtlinie wird auf den neuen Node angewendet.

Schwellenwertrichtlinien während der MetroCluster Umschaltung

Objekte, die in einer MetroCluster-Konfiguration von einem Cluster zu einem anderen Cluster verschoben werden, behalten ihre benutzerdefinierten Richtlinieneinstellungen nicht bei. Bei Bedarf können Sie Schwellenwertrichtlinien für die Volumes und LUNs anwenden, die zum Partner-Cluster verschoben wurden. Nachdem ein Objekt zurück in das ursprüngliche Cluster verschoben wurde, wird die benutzerdefinierte Schwellenwertrichtlinie automatisch neu angewendet.

Volume-Verhalten während des Umschalens und Zurück

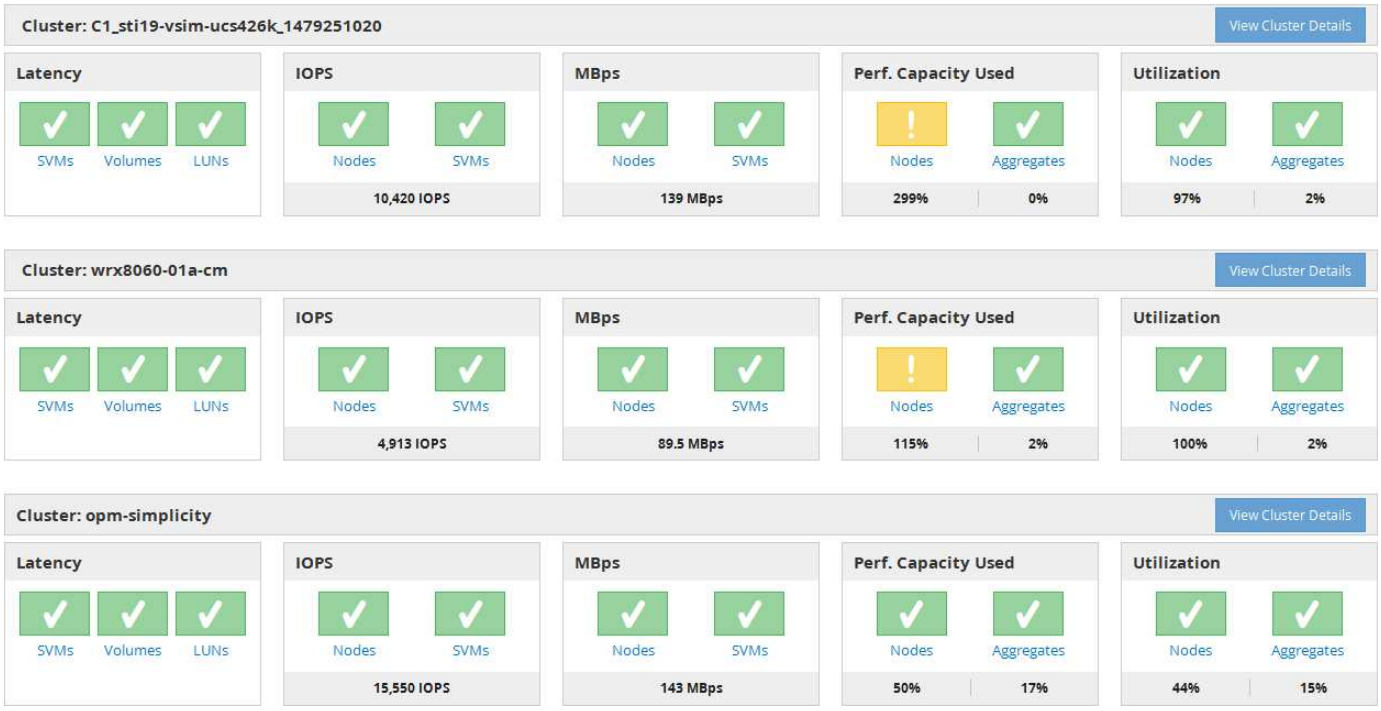
Monitoring der Cluster-Performance über das Performance-Dashboard

Das Performance-Dashboard von OnCommand System Manager zeigt den Performance-Status aller Cluster an, die von dieser Instanz von Unified Manager überwacht werden. So können Sie die allgemeine Performance der gemanagten Cluster beurteilen und alle erkannten Ereignisse schnell erfassen, lokalisieren oder zur Lösung zuweisen.

Allgemeines zum Performance-Dashboard

Das Unified Manager Performance Dashboard bietet einen allgemeinen Überblick über den Performance-Status aller Cluster, die in Ihrer Umgebung überwacht werden. Cluster, die Performance-Probleme haben, werden oben auf der Seite nach Schweregrad geordnet. Die Informationen auf dem Dashboard werden automatisch zu jedem fünf-Minuten-Zeitraum der Performance-Erfassung aktualisiert.

Das folgende Bild zeigt ein Beispiel eines Unified Manager Performance-Dashboards für die Überwachung von zwei Clustern:



Die Statussymbole, die die Storage-Objekte darstellen, können den folgenden Status aufweisen und vom höchsten Schweregrad bis den niedrigsten Schweregrad sortiert sein:

- Kritisch (): Ein oder mehrere neue kritische Performanceereignisse wurden für das Objekt gemeldet.
- Warnung (): Für das Objekt wurden mindestens ein neues Warnungsleistungsereignis gemeldet.
- Normal (): Für das Objekt wurden keine neuen Performanceereignisse gemeldet.

Die Farbe gibt an, ob neue Ereignisse für das Objekt vorhanden sind. Ereignisse, die nicht mehr aktiv sind, die als veraltete Ereignisse bezeichnet werden, haben keinen Einfluss auf die Farbe des Symbols.

Cluster-Performance-Zähler

Für jedes Cluster werden die folgenden Performance-Kategorien angezeigt:

- Latenz

  Zeigt, wie schnell das Cluster auf Client-Applikationsanforderungen reagiert, in Millisekunden pro Vorgang.

- IOPS

  Zeigt die Betriebsgeschwindigkeit des Clusters unter der Anzahl der ein-/Ausgabevorgänge pro Sekunde an.

- MB/Sek.

  Zeigt an, wie viele Daten in das und aus dem Cluster in Megabyte pro Sekunde übertragen werden.

- Verwendete Performance-Kapazität

Zeigt, ob Nodes oder Aggregate die verfügbare Performance-Kapazität überbeanspruchen.

- Auslastung

  Zeigt, ob die Ressourcen auf beliebigen Nodes oder Aggregaten überlastet sind.

Um die Performance Ihres Clusters und Ihrer Storage-Objekte zu analysieren, können Sie eine der folgenden Aktionen durchführen:

- Sie können auf **Cluster-Details anzeigen** klicken, um die Cluster-Startseite anzuzeigen. Dort werden detaillierte Performance- und Ereignisinformationen für die ausgewählten Cluster- und Speicherobjekte angezeigt.
- Sie können auf eines der roten oder gelben Statussymbole eines Objekts klicken, um die Inventarseite für dieses Objekt anzuzeigen. Dort können Sie Details zum Speicherobjekt anzeigen.

  Beispielsweise wird durch Klicken auf ein Volume-Symbol die Seite „Performance/Volume-Inventar“ mit einer Liste aller Volumes im ausgewählten Cluster angezeigt, die nach der schlechtesten Performance bis zur besten Performance sortiert ist.

Performance Dashboard – Banner-Meldungen und Beschreibungen

Unified Manager zeigt möglicherweise Cluster-Banner-Meldungen auf dem Performance Dashboard an, um Sie über Statusprobleme für ein bestimmtes Cluster zu benachrichtigen.

Bannernachricht	Beschreibung	Auflösung
`No performance data is being collected from cluster cluster_name. Restart Unified Manager to correct this issue.`	Der Unified Manager Erfassungsservice wurde angehalten, und keine Performance-Daten werden von allen Clustern erfasst.	Starten Sie Unified Manager neu, um dieses Problem zu beheben. Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den technischen Support.
`More than x hour(s) of historical data is being collected from cluster cluster_name. Current data collections will start after all historical data is collected.`	Derzeit wird ein Datenkontinuitätssammlung ausgeführt, um Performance-Daten außerhalb des Echtzeit-Cluster Performance-Erfassungszyklus abzurufen.	Es ist keine Aktion erforderlich. Aktuelle Performance-Daten werden nach Abschluss des Datenerfassungs-Zyklus erfasst. Ein Datenerfassungszyklus wird ausgeführt, wenn ein neues Cluster hinzugefügt wird oder Unified Manager aktuelle Performance-Daten aus einem bestimmten Grund nicht erfasst hat.

Ändern des Erfassungsintervalls der Performance-Statistiken

Das Standard-Erfassungsintervall für Performance-Statistiken beträgt 5 Minuten. Sie können dieses Intervall auf 10 oder 15 Minuten ändern, wenn Sie feststellen, dass Sammlungen von großen Clustern nicht innerhalb der Standardzeit abgeschlossen

werden. Diese Einstellung wirkt sich auf die Erfassung der Statistiken aus allen Clustern aus, die diese Instanz von Unified Manager überwacht.

Bevor Sie beginnen

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

Über diese Aufgabe

Das Problem der Performance-Statistiken-Sammlungen, die nicht rechtzeitig beenden, wird durch die Banner-Meldungen angezeigt `Unable to consistently collect from cluster <cluster_name>` Oder `Data collection is taking too long on cluster <cluster_name>`.

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

> Wenn Sie diesen Wert ab der Standardeinstellung von 5 Minuten ändern, kann sich dies auf die Anzahl und Häufigkeit von Performance-Ereignissen auswirken, die Unified Manager meldet. So werden z. B. durch systemdefinierte Performance-Schwellenwerte Ereignisse ausgelöst, wenn die Richtlinie 30 Minuten lang überschritten wird. Bei der Verwendung von 5-minütigen Sammlungen muss die Richtlinie für sechs aufeinanderfolgende Sammlungen überschritten werden. Bei 15-minütigen Sammlungen muss die Richtlinie nur für zwei Sammelzeiträume überschritten werden.

Eine Meldung am Ende der Seite „Cluster Data Sources“ zeigt das aktuelle Intervall zur Erfassung statistischer Daten an.

Schritte

1. Loggen Sie sich mit SSH als Wartungsbenutzer beim Unified Manager Host ein.

   Die Eingabeaufforderungen für die Unified ManagerMaintenance-Konsole werden angezeigt.

2. Geben Sie die Nummer der Menüoption **Konfiguration des Leistungsintervalls** ein, und drücken Sie dann die Eingabetaste.
3. Geben Sie bei der entsprechenden Aufforderung das Wartungs-Benutzerpasswort erneut ein.
4. Geben Sie die Nummer für das neue Abfrageintervall ein, das Sie einstellen möchten, und drücken Sie dann die Eingabetaste.

Nachdem Sie fertig sind

Wenn Sie das Einfassungsintervall von Unified Manager auf 10 oder 15 Minuten geändert haben und eine aktuelle Verbindung zu einem externen Datenanbieter (z. B. Graphite) besteht, müssen Sie das Übertragungsintervall des Datenanbieters so ändern, dass es dem Erfassungsintervall von Unified Manager entspricht oder größer ist.

Monitoring der Cluster-Performance über die Startseite des Performance Cluster

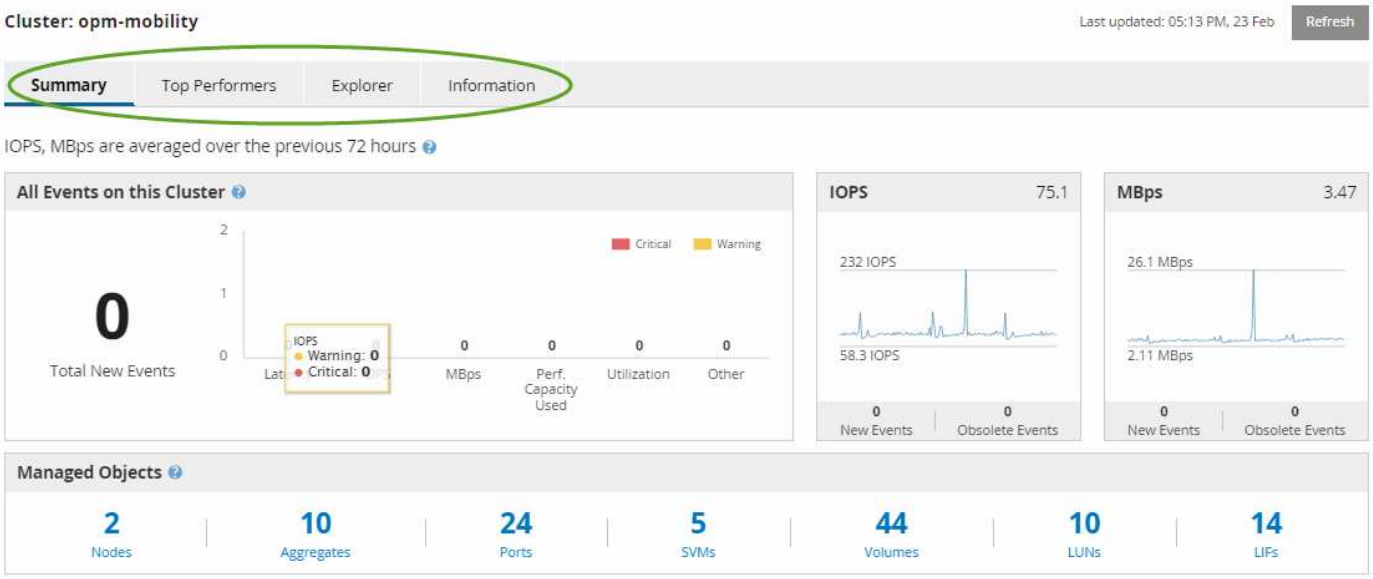
Auf der Seite „Performance Cluster Landing“ wird der Performance-Status eines

ausgewählten Clusters angezeigt, der von einer Instanz von Unified Manager überwacht wird. Auf dieser Seite können Sie die allgemeine Performance eines bestimmten Clusters bewerten und schnell alle erkannten Cluster-spezifischen Ereignisse bemerken, lokalisieren oder zur Behebung zuweisen.

Informationen zur Landing Page des Performance Cluster

Die Seite „Performance Cluster Landing“ bietet eine grundlegende Performance-Übersicht über ein ausgewähltes Cluster und legt den Performance-Status der 10 wichtigsten Objekte im Cluster fest. Leistungsprobleme werden oben auf der Seite im Bereich „Alle Ereignisse auf diesem Cluster“ angezeigt.

Die Performance Cluster Landing Page bietet eine allgemeine Übersicht über jedes Cluster, das von einer Instanz von Unified Manager gemanagt wird. Auf dieser Seite erhalten Sie Informationen zu Ereignissen und der Performance sowie Informationen zur Überwachung und Fehlerbehebung der Cluster. Das folgende Bild zeigt ein Beispiel der „Performance Cluster Landing Page“ für den Cluster mit dem Namen „opm-Mobility“:



Die Ereignisanzahl auf der Seite „Cluster Summary“ entspricht möglicherweise nicht der Ereignisanzahl auf der Seite „Performance Event Inventory“. Dies liegt daran, dass auf der Seite „Cluster Summary“ jeweils ein Ereignis in den Bars für Latenz und Auslastung angezeigt werden kann, wenn gegen eine Kombinationsrichtlinie ein Schwellenwert überschritten wurde, während auf der Seite „Performance Event Inventory“ nur ein Ereignis angezeigt wird, wenn die Kombinationsrichtlinie nicht eingehalten wurde.

Wenn ein Cluster aus dem Management durch Unified Manager entfernt wurde, wird rechts neben dem Cluster-Namen oben auf der Seite der Status **removed** angezeigt.

Landing Page für Performance Cluster

Auf der Seite „Performance Cluster Landing“ wird der Performance-Status eines ausgewählten Clusters angezeigt. Auf der Seite können Sie alle Details zu jedem Performance-Zähler für die Storage-Objekte im ausgewählten Cluster abrufen.

Klicken Sie auf die Schaltfläche **Favoriten** ( ) Um dieses Objekt zu Ihrer Liste der bevorzugten

Speicherobjekte hinzuzufügen. Eine blaue Taste ( ) Zeigt an, dass dieses Objekt bereits ein Favorit ist.

Die Landing Page für Performance Cluster enthält vier Registerkarten, die die Cluster-Details in vier Informationsbereiche trennen:

- Übersichtsseite
  - Bereich Cluster-Ereignisse
  - Bereich „Managed Objects“
- Seite „Top Performers“
- Explorer-Seite
- Informationsseite

Performance Cluster Summary

Die Seite Performance Cluster Summary bietet eine Zusammenfassung der aktiven Ereignisse, IOPS Performance und MB/s für ein Cluster. Diese Seite enthält auch die Gesamtzahl der Storage-Objekte im Cluster.

Teilfenster „Cluster-Performance“-Ereignisse

Im Teilfenster Cluster Performance-Ereignisse werden Performance-Statistiken und alle aktiven Ereignisse für das Cluster angezeigt. Dies ist am hilfreichsten, wenn es um das Monitoring der Cluster und aller Cluster-bezogenen Performance und Ereignisse geht.

Alle Ereignisse in diesem Clusterfenster

Im Teilfenster „Alle Ereignisse“ in diesem Teilfenster „Cluster“ werden alle aktiven Cluster-Performance-Ereignisse der letzten 72 Stunden angezeigt. Die Gesamtzahl der aktiven Ereignisse wird ganz links angezeigt. Diese Zahl stellt die Summe aller neuen und bestätigten Ereignisse für alle Speicherobjekte in diesem Cluster dar. Sie können auf den Link „Aktive Ereignisse insgesamt“ klicken, um zur Seite „Ereignisbestand“ zu navigieren, die gefiltert wird, um diese Ereignisse anzuzeigen.

Im Balkendiagramm für aktive Ereignisse insgesamt für das Cluster wird die Gesamtzahl der aktiven kritischen und Warnereignisse angezeigt:

- Latenz (insgesamt für Nodes, Aggregate, SVMs, Volumes, LUNs, Und Namespaces)
- IOPS (insgesamt für Cluster, Nodes, Aggregate, SVMs, Volumes, LUNs und Namespaces)
- MB/s (insgesamt für Cluster, Nodes, Aggregate, SVMs, Volumes, LUNs, Namespaces, Ports und LIFs)
- Verwendete Performance-Kapazität (insgesamt für Nodes und Aggregate)
- Auslastung (insgesamt für Nodes, Aggregate und Ports)
- Sonstiges (Cache-Miss-Verhältnis für Volumes)

Die Liste enthält aktive Performanceereignisse, die aus benutzerdefinierten Schwellenwertrichtlinien, systemdefinierten Schwellenwertrichtlinien und dynamischen Schwellenwerten ausgelöst werden.

Diagrammdaten (vertikale Zählerbalken) werden rot (angezeigt) Für kritische Ereignisse, und gelb ( ) Für Warnereignisse. Positionieren Sie den Cursor über jede vertikale Zählerleiste, um den tatsächlichen Typ und die Anzahl der Ereignisse anzuzeigen. Sie können auf **Aktualisieren** klicken, um die Daten des Zählerfelds zu aktualisieren.

Sie können kritische Ereignisse und Warnereignisse im Leistungsdiagramm für aktive Ereignisse anzeigen oder ausblenden, indem Sie in der Legende auf die Symbole **kritisch** und **Warnung** klicken. Wenn Sie bestimmte Ereignistypen ausblenden, werden die Legende-Symbole grau angezeigt.

Thekenabdeckungen

Die Zählerfelder zeigen Cluster-Aktivitäten und Performance-Ereignisse der letzten 72 Stunden an und umfassen die folgenden Zähler:

- **IOPS-Zählerpanel**

  IOPS gibt die Betriebsgeschwindigkeit des Clusters in der Anzahl der ein-/Ausgabevorgänge pro Sekunde an. Dieses Zählerfeld bietet eine allgemeine Übersicht über den IOPS-Zustand des Clusters im vorherigen Zeitraum von 72 Stunden. Sie können den Mauszeiger über die Trendkurve positionieren, um den IOPS-Wert für einen bestimmten Zeitpunkt anzuzeigen.

- **MB/s-Zähler-Panel**

  MB/s gibt an, wie viele Daten in Megabyte pro Sekunde an und aus dem Cluster übertragen wurden. Dieses Zählerfeld bietet eine allgemeine Übersicht über den Zustand des Clusters im Vergleich mit dem vorherigen 72-Stunden-Zeitraum. Sie können den Cursor über die Trendlinie des Diagramms positionieren, um den Mbps-Wert für eine bestimmte Zeit anzuzeigen.

Die Zahl oben rechts im Diagramm im grauen Balken ist der Durchschnittswert aus dem letzten 72-Stunden-Zeitraum. Die Zahlen unten und oben im Trendliniendiagramm sind die Mindest- und Höchstwerte der letzten 72 Stunden. Der graue Balken unterhalb des Diagramms enthält die Anzahl der aktiven (neuen und bestätigten) Ereignisse und der veralteten Ereignisse aus dem Zeitraum der letzten 72 Stunden.

Die Zählerfelder enthalten zwei Arten von Ereignissen:

- * Aktiv*

  Zeigt an, dass das Leistungsereignis aktuell aktiv ist (neu oder bestätigt). Das Problem, das das Ereignis verursacht hat, wurde nicht selbst behoben oder wurde nicht behoben. Der Performance-Zähler für das Storage-Objekt bleibt über dem Performance-Schwellenwert.

- **Veraltet**

  Zeigt an, dass das Ereignis nicht mehr aktiv ist. Das Problem, das das Ereignis verursacht hat, hat sich selbst korrigiert oder wurde behoben. Der Performance-Zähler für das Storage-Objekt liegt nicht mehr über dem Performance-Schwellenwert.

Bei **Active Events** können Sie Ihren Cursor über das Ereignissymbol positionieren und auf die Ereignisnummer klicken, um die entsprechende Seite mit den Ereignisdetails zu verlinken. Wenn es mehrere Ereignisse gibt, können Sie auf **Alle Ereignisse anzeigen** klicken, um die Seite „Ereignisbestand“ anzuzeigen, die gefiltert wird, um alle Ereignisse für den ausgewählten Zählertyp des Objekts anzuzeigen.

Bereich „Managed Objects“

Der Fensterbereich verwaltete Objekte auf der Registerkarte Performance-Übersicht bietet eine Übersicht über die Speicherobjekttypen und -Zählungen für das Cluster. In diesem Teilfenster können Sie den Status der Objekte in jedem Cluster verfolgen.

Die Anzahl der verwalteten Objekte ist die Anzahl der Point-in-Time-Daten vom letzten Erfassungszeitraum.

Neue Objekte werden in 15-Minuten-Intervallen entdeckt.

Durch Klicken auf die verknüpfte Nummer eines Objekttyps wird die Seite „Objekt-Performance-Bestandsaufnahme“ für diesen Objekttyp angezeigt. Die Seite „Objektbestandsliste“ wird gefiltert, um nur die Objekte auf diesem Cluster anzuzeigen.

Die verwalteten Objekte sind:

- **Knoten**

  Ein physisches System in einem Cluster

- **Aggregate**

  Ein Satz aus mehreren redundanten Array von unabhängigen Festplatten (RAID)-Gruppen, die als eine einzige Einheit zur Sicherung und Bereitstellung gemanagt werden können.

- **Ports**

  Ein physischer Verbindungspunkt auf Knoten, der zur Verbindung mit anderen Geräten im Netzwerk verwendet wird.

- **SVMs**

  Eine virtuelle Maschine, die Netzwerkzugriff über eindeutige Netzwerkadressen ermöglicht. Eine SVM kann Daten aus einem anderen Namespace bereitstellen und kann vom Rest des Clusters getrennt verwaltet werden.

- **Bände**

  Eine logische Einheit, die über ein oder mehrere der unterstützten Zugriffsprotokolle zugängliche Benutzerdaten enthält. Die Zählung umfasst sowohl FlexVol Volumes als auch FlexGroup Volumes. Es umfasst keine FlexGroup Komponenten oder Infinite Volumes.

- **LUNs**

  Der Bezeichner einer logischen Fibre Channel (FC)-Einheit oder einer logischen iSCSI-Einheit. Eine logische Einheit entspricht in der Regel einem Speichervolumen und wird innerhalb eines Computerbetriebssystems als Gerät dargestellt.

- **LIFs**

  Eine logische Netzwerkschnittstelle, die einen Netzwerkzugriffspunkt für einen Node darstellt. Die Anzahl umfasst alle LIF-Typen.

Seite „Top Performers“

Auf der Seite „Top Performers“ werden die Speicherobjekte angezeigt, die je nach dem ausgewählten Performance-Zähler die höchste oder niedrigste Performance haben. Beispielsweise können Sie in der Kategorie SVMs die SVMs mit den höchsten IOPS, mit der höchsten Latenz oder mit den niedrigsten MB/s anzeigen. Diese Seite wird auch angezeigt, wenn einer der Top-Performer aktive Performanceereignisse hat (Neu oder bestätigt).

Auf der Seite Top Performers werden maximal 10 Objekte angezeigt. Das Volume-Objekt umfasst sowohl FlexVol Volumes als auch FlexGroup Volumes. Es umfasst keine FlexGroup Komponenten oder Infinite Volumes.

- **Zeitbereich**

  Sie können einen Zeitbereich für die Anzeige der Top-Performer auswählen. Der ausgewählte Zeitbereich gilt für alle Speicherobjekte. Verfügbare Zeitbereiche:

  - Letzte Stunde
  - Letzte 24 Stunden
  - Letzte 72 Stunden (Standard)
  - Letzte 7 Tage

- **Metrisch**

  Klicken Sie auf das Menü **metrisch**, um einen anderen Zähler auszuwählen. Zähleroptionen sind nur dem Objekttyp zugeordnet. Verfügbare Zähler für das Objekt **Volumes** sind beispielsweise **Latenz**, **IOPS** und **Mbps**. Durch Ändern des Zählers werden die Plattendaten basierend auf dem ausgewählten Zähler mit den Top-Performern neu geladen.

  Verfügbare Zähler:

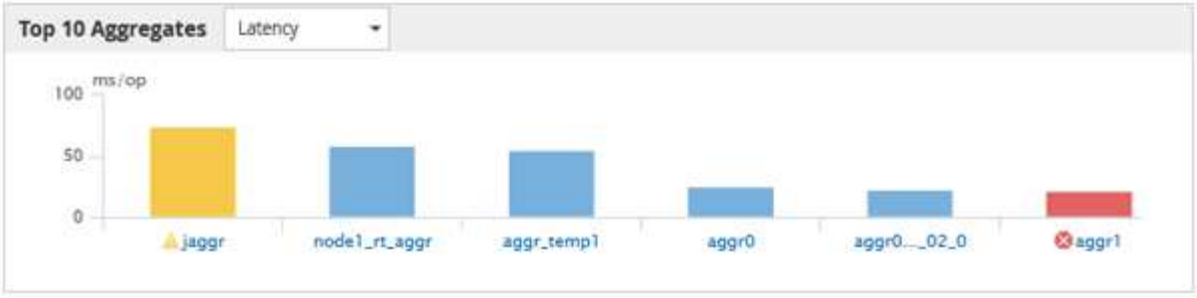
  - Latenz
  - IOPS
  - MB/Sek.
  - Verwendete Performance-Kapazität (für Nodes und Aggregate)
  - Auslastung (für Nodes und Aggregate)

- * Sortieren*

  Klicken Sie auf das Menü **Sortieren**, um eine aufsteigende oder absteigende Sortierung für das ausgewählte Objekt und den ausgewählten Zähler auszuwählen. Die Optionen sind **höchste bis niedrigste** und **niedrigste bis höchste**. Bei diesen Optionen werden die Objekte mit höchster Performance oder mit geringster Performance angezeigt.

- **Counter Bar**

  Der Zählerbalken im Diagramm zeigt die Performance-Statistiken für jedes Objekt an, die als Balken für dieses Objekt dargestellt sind. Die Balkendiagramme sind farbcodiert. Wenn der Zähler keinen Performance-Schwellenwert überschreitet, wird der Zählerbalken in blau angezeigt. Wenn eine Schwellenverletzung aktiv ist (ein neues oder quited Event), wird der Balken in der Farbe für das Ereignis angezeigt: Warnereignisse werden in Gelb (angezeigt), und kritische Ereignisse werden in rot ( ). Schwellenverletzungen werden zudem durch Symbole für die Schweregrade für Warn- und kritische Ereignisse angezeigt.



Die X-Achse zeigt für jedes Diagramm die besten Interpreten für den ausgewählten Objekttyp an. Die Y-Achse zeigt die Einheiten an, die für den ausgewählten Zähler gelten. Wenn Sie unter jedem vertikalen Balkendiagramm auf den Objektnamen klicken, werden Sie zur Seite Performance Landing für das ausgewählte Objekt navigieren.

- **Severity Ereignisanzeige**

  Das Symbol **Severity Event** wird links neben einem Objektnamen für den aktiven kritischen (angezeigt ⊗) Oder Warnung (⚠) Ereignisse in den Grafiken der Top-Performer. Klicken Sie zum Anzeigen auf das Symbol * Severity Event*:

  - **Ein Event**

    Navigiert zur Seite mit den Veranstaltungsdetails für dieses Ereignis.

  - * Zwei oder mehr Veranstaltungen*

    Navigiert zur Seite „Ereignisbestand“, die gefiltert wird, um alle Ereignisse für das ausgewählte Objekt anzuzeigen.

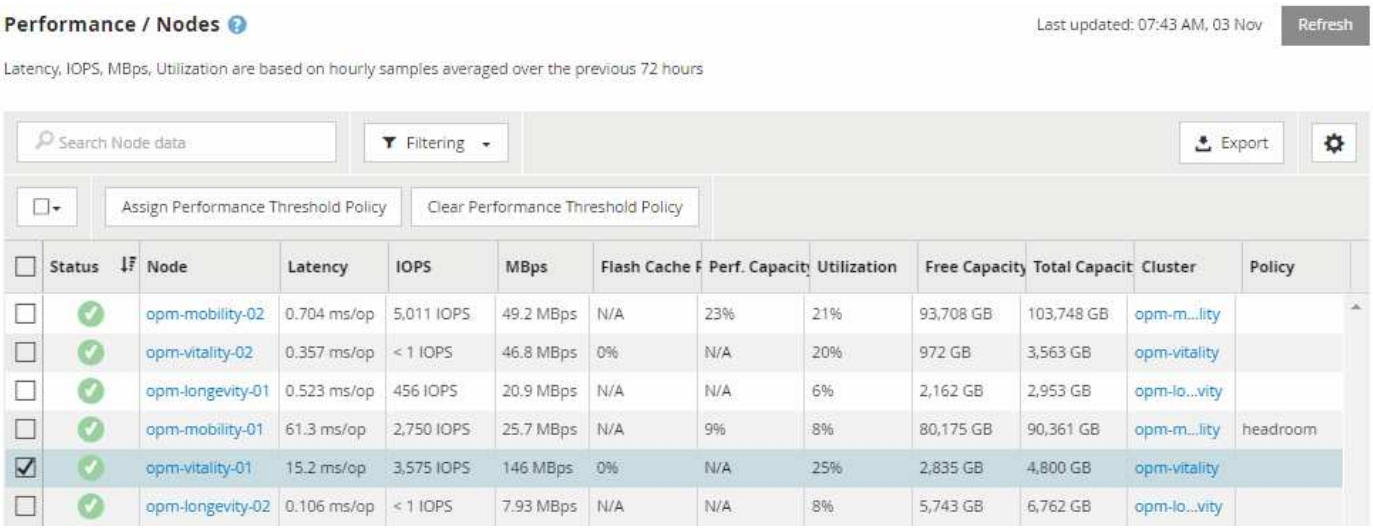
- **Export-Taste**

  Erstellt ein `.csv` Datei, die die in der Zählerleiste angezeigten Daten enthält. Sie können die Datei für das einzelne Cluster erstellen, das Sie anzeigen, oder für alle Cluster im Datacenter.

Überwachung der Performance mithilfe der Seiten „Performance Inventory“ (Performance-Bestandsaufnahme

Auf den Objektbestands-Performance-Seiten werden Performance-Informationen, Performance-Ereignisse und Objektzustand für alle Objekte innerhalb einer Objekttyp-Kategorie angezeigt. Dadurch erhalten Sie einen schnellen Überblick über den Performance-Status jedes Objekts in einem Cluster, beispielsweise für alle Nodes oder alle Volumes.

Die Seiten für die Objektbestandsleistung bieten einen allgemeinen Überblick über den Objektstatus, sodass Sie die Gesamtleistung aller Objekte bewerten und Objektleistungsdaten vergleichen können. Sie können den Inhalt der Objektbestandsseiten durch Suchen, Sortieren und Filtern verfeinern. Dies ist insbesondere beim Monitoring und Management der Objekt-Performance von Vorteil, da Objekte mit Performance-Problemen schnell lokalisiert und der Fehlerbehebungsprozess gestartet werden kann.



Standardmäßig werden Objekte auf den Seiten des Performance-Inventars nach Wichtigkeit der Objektleistung sortiert. Objekte mit neuen kritischen Performance-Ereignissen werden zuerst aufgeführt, Objekte mit Warnmeldungen werden an zweiter Stelle aufgeführt. Dies bietet eine unmittelbare visuelle Darstellung von Problemen, die behoben werden müssen. Alle Performance-Daten basieren auf einem Durchschnitt von 72 Stunden.

Sie können einfach von der Seite „Objektbestandsleistung“ zu einer Seite mit Objektdetails navigieren, indem Sie in der Spalte Objektname auf den Objektnamen klicken. Beispielsweise klicken Sie auf der Seite Performance/Nodes Inventory in der Spalte **Nodes** auf ein Node-Objekt. Die Seite Objektdetails enthält detaillierte Informationen und Details zum ausgewählten Objekt, einschließlich eines Gegenübers aktiver Ereignisse.

Objektüberwachung mithilfe der Bestandsseiten des Performance-Objekts

Über die Seiten zum Performance-Objektbestand können Sie die Objekt-Performance basierend auf den Werten bestimmter Performance-Zähler oder auf der Grundlage von Performance-Ereignissen überwachen. Dies ist vorteilhaft, da durch die Identifizierung von Objekten mit Performance-Ereignissen die Ursache von Cluster-Performance-Problemen untersucht werden kann.

Auf den Seiten des Performance-Objektbestands werden die zugeordneten Zähler, zugeordnete Objekte und Performance-Schwellenwertrichtlinien für alle Objekte in allen Clustern angezeigt. Auf diesen Seiten können Sie außerdem Richtlinien für Leistungsschwellenwerte auf Objekte anwenden. Sie können die Seite anhand einer beliebigen Spalte sortieren und alle Objektnamen oder -Daten durchsuchen.

Sie können Daten von diesen Seiten in kommagetrennte Werte exportieren (`.csv`) Datei mit der Schaltfläche **Exportieren** und dann die exportierten Daten zum Erstellen von Berichten verwenden.

Inhalt der Seite zur Leistungsbestandsliste wird verfeinert

Die Inventarseiten für Performance-Objekte enthalten Tools, mit denen Sie Inhalte aus Objektbeständen verfeinern können, damit Sie bestimmte Daten schnell und einfach auffinden können.

Die Informationen auf den Seiten zum Bestand von Performance-Objekten können umfangreich sein und häufig über mehrere Seiten hinweg erfasst werden. Diese umfassenden Daten eignen sich hervorragend für

das Monitoring, die Nachverfolgung und die Performance. Das Auffinden bestimmter Daten erfordert jedoch Tools, mit denen Sie die gesuchten Daten schnell finden. Daher enthalten die Seiten für den Bestand von Performance-Objekten Funktionen zum Suchen, Sortieren und Filtern. Darüber hinaus können Suchen und Filtern zusammenarbeiten, um Ihre Ergebnisse weiter einzugrenzen.

Suchen auf den Seiten „Objektbestandsleistung“

Sie können Zeichenfolgen auf den Seiten „Objektbestandsleistung“ suchen. Verwenden Sie das Feld **Suche** oben rechts auf der Seite, um Daten anhand des Objektnamens oder des Richtliniennamens schnell zu finden. So lassen sich entweder spezifische Objekte und zugehörige Daten schnell finden oder Richtlinien schnell finden und zugehörige Richtlinienobjektdaten anzeigen.

Schritte

1. Führen Sie je nach Ihren Suchanforderungen eine der folgenden Optionen durch:

So finden Sie das:	Geben Sie dies ein…
Zu einem bestimmten Objekt	Der Objektname in das Feld * Suchen* und klicken Sie auf **Suchen**. Das Objekt, nach dem Sie gesucht haben, und die zugehörigen Daten werden angezeigt.
Eine benutzerdefinierte Richtlinie für Leistungsschwellenwerte	Der Name der Richtlinie ganz oder teilweise in das Feld **Suche** und klicken Sie auf **Suchen**. Die Objekte, die der von Ihnen gesuchten Richtlinie zugeordnet sind, werden angezeigt.

Sortieren auf den Seiten „Objektbestandsleistung“

Sie können alle Daten auf den Seiten „Objektbestandsleistung“ nach jeder Spalte in aufsteigender oder absteigender Reihenfolge sortieren. So können Sie schnell Objektbestandsdaten finden, was bei der Überprüfung der Leistung oder beim Beginn eines Fehlerbehebungsprozesses hilfreich ist.

Über diese Aufgabe

Die ausgewählte Spalte für die Sortierung wird durch einen markierten Spaltenüberschrift und ein Pfeilsymbol angezeigt, das die Sortierrichtung rechts neben dem Namen angibt. Ein nach-oben-Pfeil zeigt eine aufsteigende Reihenfolge an; ein Pfeil nach unten zeigt die absteigende Reihenfolge an. Die Standard-Sortierreihenfolge ist durch **Status** (Ereignis-Kritikalität) in absteigender Reihenfolge, wobei die wichtigsten Performanceereignisse zuerst aufgelistet werden.

Schritte

1. Sie können auf einen Spaltennamen klicken, um die Sortierreihenfolge der Spalte in aufsteigender oder absteigender Reihenfolge zu ändern.

   Der Inhalt der Seite „Objektbestandsleistung“ wird auf der Grundlage der ausgewählten Spalte in aufsteigender oder absteigender Reihenfolge sortiert.

Filtern von Daten auf den Seiten „Objektbestandsleistung“

Sie können Daten auf den Seiten „Objektbestandsleistung“ filtern, um Daten anhand bestimmter Kriterien schnell zu finden. Mithilfe der Filterung können Sie den Inhalt der Seiten „Objektbestandsleistung“ eingrenzen, um nur die von Ihnen angegebenen Ergebnisse anzuzeigen. Dies bietet eine sehr effiziente Methode, nur die Leistungsdaten anzuzeigen, an denen Sie interessiert sind.

Über diese Aufgabe

Über das Filterfeld können Sie die Rasteransicht entsprechend Ihren Einstellungen anpassen. Verfügbare Filteroptionen basieren auf dem in der Tabelle angezeigten korrelierten Objekttyp. Wenn aktuell Filter angewendet werden, wird links neben dem Filtersteuerelement ein Sternchen (*) angezeigt.

Es werden vier Filterparameter unterstützt.

Parameter	Validierung
Zeichenfolge (Text)	Die Operatoren sind **enthält** und **beginnt mit**.
Nummer	Die Betreiber sind **größer als** und **kleiner als**.
Ressource	Die Operatoren sind **Name enthält** und **Name beginnt mit**.
Status	Die Betreiber sind **ist** und **ist nicht**.

Für jeden Filter sind alle drei Felder erforderlich; die verfügbaren Filter spiegeln die filterbaren Spalten auf der aktuellen Seite wider. Es können maximal vier Filter angewendet werden. Gefilterte Ergebnisse basieren auf kombinierten Filterparametern. Gefilterte Ergebnisse gelten für alle Seiten in Ihrer gefilterten Suche und nicht nur für die aktuell angezeigte Seite.

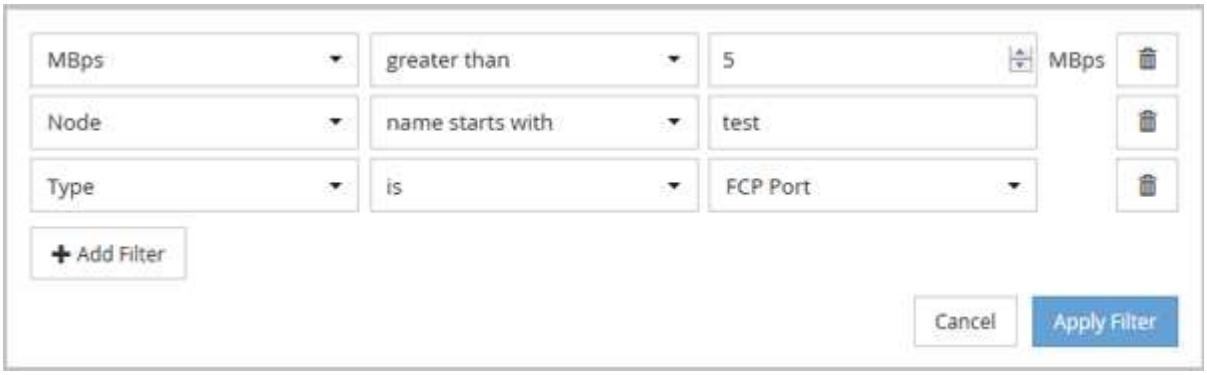
Sie können Filter über das Filterfenster hinzufügen.

1. Klicken Sie oben auf der Seite auf **Filtern**. Das Filterbedienfeld wird angezeigt.
2. Klicken Sie im Filterfenster auf die linke Dropdown-Liste und wählen Sie einen Objektnamen aus, z. B. *Cluster* oder einen Performance-Zähler.
3. Klicken Sie auf die Dropdown-Liste Mitte, und wählen Sie den booleschen Operator **Name enthält** oder **Name beginnt mit** aus, wenn die erste Auswahl ein Objektname war. Wenn es sich bei der ersten Auswahl um einen Leistungszähler handelte, wählen Sie **größer als** oder **kleiner als** aus. Wenn die erste Auswahl **Status** war, wählen Sie **ist** oder **ist nicht**.
4. Wenn für Ihre Suchkriterien ein numerischer Wert erforderlich ist, werden die nach-oben- und nach-unten-Pfeiltasten im Feld rechts angezeigt. Sie können auf die nach-oben- und nach-unten-Pfeiltasten klicken, um den gewünschten numerischen Wert anzuzeigen.
5. Geben Sie bei Bedarf Ihre nicht-numerischen Suchkriterien in das Textfeld rechts ein.
6. Um Filter hinzuzufügen, klicken Sie auf **Filter hinzufügen**. Es wird ein zusätzliches Filterfeld angezeigt. Führen Sie diesen Filter mithilfe des in den vorherigen Schritten beschriebenen Verfahrens aus. Beachten Sie, dass beim Hinzufügen Ihres vierten Filters die Schaltfläche **Filter hinzufügen** nicht mehr angezeigt wird.

7. Klicken Sie Auf **Filter Anwenden**. Die Filteroptionen werden auf das Raster angewendet, und ein Sternchen (*) wird in der Filterschaltfläche angezeigt.
8. Verwenden Sie den Filterbereich, um einzelne Filter zu entfernen, indem Sie auf das Papierkorb-Symbol rechts neben dem zu entfernenden Filter klicken.
9. Um alle Filter zu entfernen, klicken Sie unten im Filterfenster auf **Zurücksetzen**.

Beispiel für die Filterung

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



Nachdem Sie auf **Filter anwenden** geklickt haben, wird das Filterfenster geschlossen und wendet Ihre Filter an.

Analyse der Empfehlungen von Unified Manager für das Tiering von Daten in die Cloud

Auf der Seite „Performance/Volumes Inventory“ werden Informationen zur Größe der auf dem inaktiven (kalten) Volume gespeicherten Benutzerdaten angezeigt. In einigen Fällen erkennt Unified Manager bestimmte Volumes, die durch das Tiering inaktiver Daten auf das Cloud-Tier (Cloud-Provider oder StorageGRID) eines FabricPool-fähigen Aggregats profitieren würden.

FabricPool wurde in ONTAP 9.2 eingeführt. Wenn Sie eine Version der ONTAP Software vor 9.2 verwenden, ist für Unified Manager die Empfehlung für Tiering-Daten ein Upgrade der ONTAP Software erforderlich. Darüber hinaus der `auto` die tiering-Richtlinie wurde in ONTAP 9.4 eingeführt, wenn man also empfiehlt, den zu verwenden `auto` die tiering-Richtlinie muss auf ONTAP 9.4 oder höher aktualisiert werden.

Die folgenden drei Felder zum Inventarbereich von Performance/Volumes enthalten Informationen darüber, ob Sie die Festplattenauslastung Ihres Storage-Systems verbessern und Speicherplatz auf dem Performance-Tier einsparen können, indem Sie inaktive Daten auf die Cloud-Tier verschieben.

- **Tiering-Richtlinie**

  Die Tiering-Richtlinie legt fest, ob die Daten auf dem Volume auf der Performance-Tier verbleiben oder ob

einige der Daten von der Performance-Tier in die Cloud-Tier verschoben werden.

Der Wert in diesem Feld gibt die Tiering-Richtlinie an, die auf das Volume gesetzt ist, auch wenn sich das Volume derzeit nicht auf einem FabricPool Aggregat befindet. Die Tiering-Richtlinie tritt nur in Kraft, wenn das Volume auf einem FabricPool Aggregat ist.

- **Kalte Daten**

  Die kalten Daten zeigen die Größe der auf dem inaktiven (kalten) Volume gespeicherten Benutzerdaten an.

  Ein Wert wird hier nur angezeigt, wenn ONTAP 9.4 oder höher verwendet wird, da es erfordert, dass das Aggregat, auf dem das Volume bereitgestellt wird, über das verfügt `inactive data reporting` Parameter auf gesetzt `enabled`, Und dass die Mindestzahl der Kühltage Schwelle erreicht worden ist (für Volumen, die die verwenden `snapshot-only` Oder `auto` tiering-Richtlinie). Andernfalls wird der Wert als „`N/A`“ aufgeführt.

- * Cloud-Empfehlung*

  Nachdem genügend Informationen über die Datenaktivität auf dem Volume erfasst wurden, kann Unified Manager feststellen, dass keine Aktionen erforderlich sind oder dass Sie Speicherplatz auf der Performance-Tier einsparen können, indem Sie inaktive Daten per Tiering auf das Cloud-Tier verschieben.

> Das Feld „kalte Daten“ wird alle 15 Minuten aktualisiert. Das Feld „Cloud Empfehlung“ wird jedoch alle 7 Tage aktualisiert, wenn die Analyse der kalten Daten auf dem Volume durchgeführt wird. Daher kann die genaue Menge der kalten Daten zwischen den Feldern abweichen. Das Feld Cloud Recommendation zeigt das Datum an, an dem die Analyse ausgeführt wurde.

Wenn die Meldung inaktiver Daten aktiviert ist, zeigt das Feld „kalte Daten“ die genaue Menge inaktiver Daten an. Ohne die Funktion zur Berichterstellung inaktiver Daten bestimmt Unified Manager mithilfe von Performance-Statistiken, ob Daten auf einem Volume inaktiv sind. Die Menge der inaktiven Daten wird in diesem Fall nicht im Feld „kalte Daten“ angezeigt, aber es wird angezeigt, wenn Sie den Mauszeiger über das Wort **Tier** bewegen, um die Cloud-Empfehlung anzuzeigen.

Folgende Cloud-Empfehlungen werden angezeigt:

- **Lernen**. Es wurden nicht genügend Daten gesammelt, um eine Empfehlung zu treffen.
- **Stufe**. Die Analyse hat festgestellt, dass das Volume inaktive (kalte) Daten enthält und dass Sie das Volume so konfigurieren sollten, dass diese Daten in das Cloud-Tier verschoben werden. In einigen Fällen muss hierfür unter Umständen zunächst das Volume in ein FabricPool-fähiges Aggregat verschoben werden. In anderen Fällen, in denen sich das Volume bereits auf einem FabricPool Aggregat befindet, müssen Sie nur die Tiering-Richtlinie ändern.
- **Keine Aktion**. Entweder das Volume verfügt über wenige inaktive Daten. Das Volume ist bereits auf die Tiering-Richtlinie „`Auto`“ für ein FabricPool Aggregat festgelegt, oder das Volume ist ein Datensicherungs-Volume. Dieser Wert wird auch angezeigt, wenn das Volume offline ist oder wenn es in einer MetroCluster-Konfiguration verwendet wird.

Zum Verschieben eines Volumes oder zum Ändern der Tiering-Richtlinie für Volumes oder der Einstellungen für die Berichterstellung für inaktive Daten für das Aggregat verwenden Sie OnCommand System Manager, ONTAP CLI-Befehle oder eine Kombination dieser Tools.

Wenn Sie mit der Rolle „OnCommand Administrator“ oder „Storage Administrator“ bei Unified Manager angemeldet sind, ist der Link „Volume konfigurieren“ in der Cloud-Empfehlung verfügbar, wenn Sie den

Mauszeiger über das Wort „Tier*“ bewegen. Klicken Sie auf diese Schaltfläche, um die Seite Volumes in System Manager zu öffnen, um die empfohlene Änderung vorzunehmen.

Überwachung der Leistung mit den Seiten des Performance Explorers

Auf den Seiten des Performance-Explorers werden ausführliche Informationen über die Performance jedes Objekts in einem Cluster angezeigt. Die Seite bietet eine detaillierte Ansicht der Performance aller Cluster-Objekte, sodass Sie die Performance-Daten bestimmter Objekte über verschiedene Zeiträume auswählen und vergleichen können.

Sie können auch die Gesamtleistung aller Objekte beurteilen und Objekt-Performance-Daten in einem Side-by-Side-Format vergleichen.

Wird ein Objekt nicht mehr von Unified Manager verwaltet, wird rechts neben dem Objektnamen oben auf der Seite Performance Explorer der Status **entfernt** angezeigt.

Allgemeines zum Root-Objekt

Das Root-Objekt ist die Basis, mit der andere Objektvergleiche erstellt werden. So lassen sich Daten von anderen Objekten mit dem Root-Objekt anzeigen und vergleichen. So wird eine Performance-Datenanalyse bereitgestellt, mit der Fehler behoben und die Objekt-Performance verbessert werden kann.

Der Name des Stammobjekts wird oben im Fenster „Vergleichen“ angezeigt. Unter dem Root-Objekt werden zusätzliche Objekte angezeigt. Obwohl die Anzahl der zusätzlichen Objekte, die Sie dem Vergleichbereich hinzufügen können, nicht begrenzt ist, ist nur ein Root-Objekt zulässig. Die Daten für das Root-Objekt werden automatisch in den Diagrammen im Bereich Counter Charts angezeigt.

Das Root-Objekt kann nicht geändert werden. Es ist immer auf die Objektseite eingestellt, die Sie anzeigen. Wenn Sie beispielsweise die Seite Volume Performance Explorer von Volume1 öffnen, ist Volume1 das Root-Objekt und kann nicht geändert werden. Wenn Sie einen Vergleich mit einem anderen Root-Objekt durchführen möchten, müssen Sie auf den Link für ein Objekt klicken und seine Landing Page öffnen.

Ereignisse und Schwellenwerte werden nur für Root-Objekte angezeigt.

Filter anwenden, um die Liste der korrelierten Objekte im Raster zu reduzieren

Durch Filtern können Sie eine kleinere, besser definierte Untergruppe von Objekten im Raster anzeigen. Wenn Sie beispielsweise 25 Volumes in der Tabelle haben, können Sie durch Filtern nur die Volumes anzeigen, die einen Durchsatz von weniger als 90 MB/s oder eine Latenz größer als 1 ms/op. Haben

Festlegen eines Zeitbereichs für korrelierte Objekte

Mit der Auswahl für den Zeitbereich auf der Seite Performance Explorer können Sie den Zeitbereich für den Vergleich von Objektdaten festlegen. Wenn Sie einen Zeitbereich angeben, wird der Inhalt der Seiten des Performance Explorers verfeinert, um nur die Objektdaten innerhalb des von Ihnen angegebenen Zeitbereichs anzuzeigen.

Über diese Aufgabe

Durch die Feinjustierung des Zeitbereichs können nur die Leistungsdaten angezeigt werden, für die Sie sich interessieren. Sie können einen vordefinierten Zeitbereich auswählen oder einen benutzerdefinierten Zeitbereich angeben. Der Standardzeitbereich liegt bei den vorangegangenen 72 Stunden.

Auswählen eines vordefinierten Zeitbereichs

Die Auswahl eines vordefinierten Zeitbereichs stellt eine schnelle und effiziente Möglichkeit dar, die Datenausgabe bei der Anzeige von Cluster-Objekt-Performance-Daten anzupassen und zu fokussieren. Bei der Auswahl eines vordefinierten Zeitbereichs stehen Daten für bis zu 13 Monate zur Verfügung.

Schritte

1. Klicken Sie oben rechts auf der Seite **Performance Explorer** auf **Zeitbereich**.
2. Wählen Sie auf der rechten Seite des Bedienfelds **Zeitbereich Auswahl** einen vordefinierten Zeitbereich aus.
3. Klicken Sie Auf **Bereich Anwenden**.

Festlegen eines benutzerdefinierten Zeitbereichs

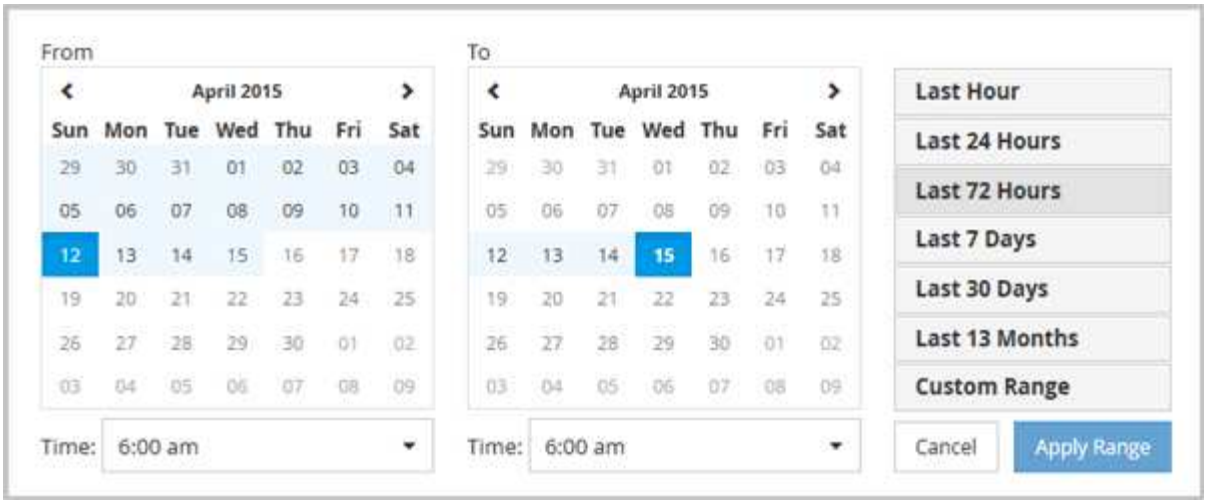
Auf der Seite „Performance Explorer“ können Sie den Datums- und Zeitbereich für Ihre Leistungsdaten angeben. Die Angabe eines benutzerdefinierten Zeitbereichs bietet größere Flexibilität als die Verwendung vordefinierter Zeitbereiche bei der Raffination von Cluster-Objektdaten.

Über diese Aufgabe

Sie können einen Zeitbereich zwischen einer Stunde und 390 Tagen auswählen. 13 Monate sind 390 Tage, weil jeder Monat als 30 Tage gezählt wird. Wenn Sie einen Datums- und Zeitbereich angeben, erhalten Sie weitere Details, mit denen Sie bestimmte Performanceereignisse oder eine Reihe von Ereignissen vergrößern können. Durch das Festlegen eines Zeitbereichs lassen sich auch potenzielle Leistungsprobleme beheben, da durch das Festlegen eines Datums- und Zeitbereichs die Daten des Performance-Ereignisses detaillierter dargestellt werden. Verwenden Sie das Steuerelement **Zeitbereich**, um vordefinierte Datums- und Zeitbereiche auszuwählen, oder geben Sie Ihren eigenen benutzerdefinierten Datums- und Zeitbereich von bis zu 390 Tagen an. Die Schaltflächen für vordefinierte Zeitbereiche variieren von **Letzte Stunde** bis **Letzte 13 Monate**.

Wenn Sie die Option **Letzte 13 Monate** wählen oder einen benutzerdefinierten Datumsbereich größer als 30 Tage angeben, wird ein Dialogfeld angezeigt, in dem Sie darauf hingewiesen werden, dass die Leistungsdaten für einen Zeitraum von mehr als 30 Tagen mit stündlichen Durchschnittswerten und nicht mit einer 5-minütigen Datenabfrage gespeichert werden. Daher kann es zu einem Verlust der visuellen Granularität bei Timeline kommen. Wenn Sie im Dialogfeld auf die Option **nicht wieder anzeigen** klicken, wird die Meldung nicht angezeigt, wenn Sie die Option **Letzte 13 Monate** wählen oder einen benutzerdefinierten Datumsbereich von mehr als 30 Tagen angeben. Die Übersichtsdaten gelten auch für einen kleineren Zeitbereich, wenn der Zeitbereich ein Datum/Uhrzeit enthält, das mehr als 30 Tage von heute entfernt ist.

Bei der Auswahl eines Zeitbereichs (benutzerdefiniert oder vordefiniert) basieren Zeitbereiche von 30 Tagen oder weniger auf 5-Minuten-Intervalldatenproben. Zeitbereiche, die größer als 30 Tage sind, basieren auf einer Stunde Intervalldatenproben.



1. Klicken Sie auf das Dropdown-Feld **Zeitbereich**, und das Fenster Zeitbereich wird angezeigt.
2. Um einen vordefinierten Zeitbereich auszuwählen, klicken Sie rechts neben dem Fenster **Zeitbereich** auf eine der Schaltflächen **Letzte…**. Bei der Auswahl eines vordefinierten Zeitbereichs stehen Daten für bis zu 13 Monate zur Verfügung. Die von Ihnen ausgewählte Schaltfläche für den vordefinierten Zeitbereich wird hervorgehoben, und die entsprechenden Tage und Zeiten werden in den Kalendern und Zeitauswahlschaltern angezeigt.
3. Um einen benutzerdefinierten Datumsbereich auszuwählen, klicken Sie links im Kalender **von** auf das Startdatum. Klicken Sie auf **<** oder **>**, um im Kalender vorwärts oder rückwärts zu navigieren. Um das Enddatum anzugeben, klicken Sie rechts im Kalender **bis** auf ein Datum. Beachten Sie, dass das Standard-Enddatum heute ist, es sei denn, Sie geben ein anderes Enddatum an. Die Schaltfläche **benutzerdefinierter Bereich** rechts neben dem Fenster Zeitbereich wird hervorgehoben, was darauf hinweist, dass Sie einen benutzerdefinierten Datumsbereich ausgewählt haben.
4. Um einen benutzerdefinierten Zeitbereich auszuwählen, klicken Sie unter dem Kalender **von** auf das Steuerelement **Uhrzeit** und wählen die Startzeit aus. Um die Endzeit festzulegen, klicken Sie rechts unter dem **bis**-Kalender auf das Steuerelement **Zeit** und wählen die Endzeit aus. Die Schaltfläche **benutzerdefinierter Bereich** rechts neben dem Fenster Zeitbereich wird hervorgehoben, was darauf hinweist, dass Sie einen benutzerdefinierten Zeitbereich ausgewählt haben.
5. Optional können Sie die Start- und Endzeiten festlegen, wenn Sie einen vordefinierten Datumsbereich auswählen. Wählen Sie den zuvor beschriebenen vordefinierten Datumsbereich aus, und wählen Sie dann die Start- und Endzeiten wie zuvor beschrieben aus. Die ausgewählten Daten werden in den Kalendern markiert, Ihre festgelegten Start- und Endzeiten werden in den Steuerelementen **Zeit** angezeigt und die Schaltfläche **benutzerdefinierter Bereich** ist markiert.
6. Klicken Sie nach Auswahl des Datums- und Zeitbereichs auf **Bereich anwenden**. Die Leistungsstatistiken für diesen Zeitbereich werden in den Diagrammen und in der Zeitleiste „Ereignisse“ angezeigt.

Definieren der Liste der korrelierten Objekte für die Vergleichgrafiken

Im Bereich Zählerdiagramm können Sie eine Liste der korrelierten Objekte für Daten- und Leistungsvergleich definieren. Wenn beispielsweise bei Ihrer Storage Virtual Machine (SVM) ein Performance-Problem auftritt, können Sie alle Volumes in der SVM vergleichen, um das mögliche Problem zu identifizieren.

Über diese Aufgabe

Sie können ein beliebiges Objekt aus dem Raster der korrelierten Objekte den Fenstern „Vergleichen“ und „Zählerdiagramm“ hinzufügen. So können Sie Daten mehrerer Objekte und das Root-Objekt anzeigen und

vergleichen. Sie können Objekte in das Raster der korrelierten Objekte hinzufügen und aus diesem entfernen. Das Root-Objekt im Vergleichsfenster kann jedoch nicht entfernt werden.

> Das Hinzufügen vieler Objekte zum Vergleichspfenster kann sich negativ auf die Performance auswirken. Um die Leistung zu erhalten, sollten Sie eine begrenzte Anzahl von Diagrammen für den Datenvergleich auswählen.

Schritte

1. Suchen Sie im Objektraster das Objekt, das Sie hinzufügen möchten, und klicken Sie auf die Schaltfläche **Hinzufügen**.

   Die Schaltfläche **Hinzufügen** wird grau, und das Objekt wird der Liste der zusätzlichen Objekte im Fenster Vergleich hinzugefügt. Die Daten des Objekts werden den Diagrammen in den Zähldiagrammen hinzugefügt. Die Farbe des Augensymbols des Objekts ( ) Passt die Farbe der Trend-Zeile des Objekts in den Diagrammen an.

2. Daten für ausgewählte Objekte ausblenden oder anzeigen:

Hier…	Führen Sie diese Aktion durch…
Ausgewähltes Objekt ausblenden	Klicken Sie auf das Augensymbol des ausgewählten Objekts ( ) Im Vergleichfenster. Die Objektdaten sind ausgeblendet, und das Augensymbol für das Objekt wird grau.
Ein ausgeblendtes Objekt anzeigen	Klicken Sie im Vergleichfenster auf das graue Augensymbol des ausgewählten Objekts. Das Augensymbol kehrt in seine ursprüngliche Farbe zurück, und die Objektdaten werden wieder in die Diagramme im Bereich Counter Charts eingefügt.

3. Ausgewählte Objekte aus dem Fensterbereich **Comparing** entfernen:

Hier…	Führen Sie diese Aktion durch…
Ausgewähltes Objekt entfernen	Bewegen Sie den Mauszeiger über den Namen des ausgewählten Objekts im Vergleichenfenster, um die Schaltfläche Objekt entfernen (**X**) anzuzeigen, und klicken Sie dann auf die Schaltfläche. Das Objekt wird aus dem Teilfenster „Vergleichen“ entfernt und seine Daten werden aus den Zählerdiagrammen gelöscht.
Alle ausgewählten Objekte entfernen	Klicken Sie auf die Schaltfläche Alle Objekte entfernen (**X**) oben im Fenster vergleichen. Alle ausgewählten Objekte und ihre Daten werden entfernt, wobei nur das Root-Objekt übrig bleibt.

Allgemeines zu Zählerdiagrammen

Diagramme im Fensterbereich Zählerdiagramme ermöglichen das Anzeigen und Vergleichen von Performancedaten für das Root-Objekt und für Objekte, die Sie aus dem Raster der korrelierten Objekte hinzugefügt haben. Auf diese Weise können Sie Performance-Trends besser verstehen und Performance-Probleme isolieren und lösen.

Standardmäßig werden Zählerdiagramme angezeigt, sind Ereignisse, Latenz, IOPS und MB/s. Optionale Diagramme, die angezeigt werden können, sind Auslastung, verwendete Performance-Kapazität, verfügbare IOPS, IOPS/TB und das Verhältnis „Cache Miss“. Zusätzlich können Sie festlegen, dass sich Gesamtwerte oder Aufbruchwerte für die verwendeten Latenzdiagramme, IOPS, MB/s und Performance-Kapazitäten anzeigen lassen.

Der Performance Explorer zeigt bestimmte Zählerdiagramme standardmäßig an, ob das Speicherobjekt sie alle unterstützt oder nicht. Wenn ein Zähler nicht unterstützt wird, ist das Zählerdiagramm leer und die Meldung `Not applicable for <object>` Wird angezeigt.

Die Diagramme zeigen Leistungstrends für das Root-Objekt und für alle Objekte an, die Sie im Vergleichsanfenster ausgewählt haben. Die Daten in den einzelnen Karten sind wie folgt angeordnet:

- **X-Achse**

  Zeigt den angegebenen Zeitraum an. Wenn Sie keinen Zeitbereich angegeben haben, ist die Standardeinstellung der vorhergehenden 72-Stunden-Periode.

- **Y-Achse**

  Zeigt Zählereinheiten an, die für das ausgewählte Objekt oder Objekte eindeutig sind.

Trendlinienfarben entsprechen der Farbe des Objektnamens, die im vergleichenden Fensterbereich angezeigt wird. Sie können den Cursor auf einer beliebigen Trendlinie über einen Punkt positionieren, um Details zu Zeit und Wert für diesen Punkt anzuzeigen.

Wenn Sie einen bestimmten Zeitraum innerhalb eines Diagramms untersuchen möchten, können Sie eine der folgenden Methoden verwenden:

- Mit der Schaltfläche **<** können Sie den Bereich Counter Charts erweitern, um die Breite der Seite zu erweitern.
- Verwenden Sie den Cursor (wenn er zu einer Lupe übergeht), um einen Teil des Zeitrahmens im Diagramm auszuwählen, um diesen Bereich zu fokussieren und zu vergrößern. Sie können auf „Diagramm zurücksetzen“ klicken, um das Diagramm auf den Standardzeitraum zurückzusetzen.
- Verwenden Sie die Taste **Zoom View**, um ein großes Einzelcounter-Diagramm anzuzeigen, das erweiterte Details und Schwellenwertanzeigen enthält.

Gelegentlich werden Lücken in den Trendlinien angezeigt. Defizite bedeuten, dass entweder Unified Manager Performancedaten aus dem Storage-System sammeln konnte, oder dass Unified Manager möglicherweise nicht verfügbar war.

Arten von Performance-Zählerdiagrammen

Es gibt Standard-Performance-Diagramme, in denen die Zählerwerte für das

ausgewählte Speicherobjekt angezeigt werden. In jedem der Counter-Diagramme werden die Gesamtwerte angezeigt, die in Lese-, Schreib- und andere Kategorien unterteilt sind. Darüber hinaus zeigen einige Counter-Diagramme zusätzliche Details an, wenn das Diagramm in der Zoom-Ansicht angezeigt wird.

In der folgenden Tabelle sind die verfügbaren Performance-Zählerdiagramme aufgeführt.

Verfügbare Diagramme	Diagrammbeschreibung
Veranstaltungen	Zeigt kritische, Fehler-, Warn- und Informationsereignisse an, die mit den statistischen Diagrammen für das Root-Objekt korreliert sind. Zusätzlich zu den Performance-Ereignissen werden Systemzustandsereignisse angezeigt, um einen vollständigen Überblick über die Gründe zu geben, warum die Performance beeinträchtigt werden könnte.
Latenz Insgesamt	Anzahl der Millisekunden, die erforderlich sind, um auf Applikationsanforderungen zu reagieren. Beachten Sie, dass die durchschnittlichen Latenzwerte I/O-gewichtet sind.
Latenz - Aufschlüsselung	Dieselben Informationen, die in der Latenzzeit gesamt angezeigt werden, jedoch mit getrennten Performance-Daten in Lese-, Schreib- und sonstige Latenz.die Diagrammoption gilt nur, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume, eine LUN ist. Oder Namespace.
Latenz – Cluster-Komponenten	Dieselben Informationen, die in Latenz-Summe angezeigt werden, jedoch mit den Performance-Daten getrennt nach Cluster-Komponente in Latenz.Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volume ist.
IOPS – gesamt	Anzahl der pro Sekunde verarbeiteten ein-/Ausgabevorgänge.
IOPS – Aufschlüsselung	Die gleichen Informationen, die auf dem IOPS-Wert insgesamt angezeigt werden, jedoch mit getrennten Performance-Daten in Lese-, Schreib- und sonstige IOPS. Bei Anzeige in der Zoom-Ansicht zeigt das Diagramm Volumes die minimalen und maximalen Durchsatzwerte der QoS an, sofern diese in ONTAP konfiguriert sind. Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume, eine LUN, Oder Namespace.

Verfügbare Diagramme	Diagrammbeschreibung
IOPS – Protokolle	Die gleichen Informationen, die unter IOPS insgesamt angezeigt werden, aber die Performance-Daten werden in individuelle Diagramme für den Datenverkehr mit CIFS-, NFS-, FCP-, NVMe- und iSCSI-Protokollen unterteilt. Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt eine SVM ist.
IOPS/TB – gesamt	Anzahl der pro Sekunde verarbeiteten ein-/Ausgabevorgänge, basierend auf dem gesamten Speicherplatz, der vom Workload in Terabyte verbraucht wird. Dieser Zähler, auch I/O-Dichte genannt, misst die Performance mit einer bestimmten Menge an Storage-Kapazität.bei Anzeige in der Zoom-Ansicht zeigt das Diagramm Volumes QoS erwartet und Spitzendurchsatzwerte an, falls es in ONTAP konfiguriert ist. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volume ist.
MB/s – Gesamt	Anzahl der Megabyte an Daten, die in das Objekt und vom Objekt pro Sekunde übertragen werden.
Mbps - Aufschlüsselung	Dieselben Informationen, die im Diagramm MB/s angezeigt werden, jedoch mit Trennung der MB/s-Daten in Festplattenlesevorgänge, Flash Cache Lese-, Schreib- und andere MB/s.bei Anzeige in der Ansicht Zoom zeigt das Volume-Diagramm QoS-Maximaldurchsatz an, sofern es in ONTAP konfiguriert ist. Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume, eine LUN, Oder Namespace. Flash Cache-Daten werden nur für Nodes und nur angezeigt, wenn ein Flash Cache Modul im Node installiert ist.
Genutzte Performance-Kapazität – Insgesamt	Prozentsatz der Performance-Kapazität, die vom Node oder Aggregat verbraucht wird Daten zur Performance-Kapazität sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.

Verfügbare Diagramme	Diagrammbeschreibung
Genutzte Performance-Kapazität – Aufschlüsselung	Die verwendete Performance-Kapazität ist in Benutzerprotokolle und Systembackground-Prozesse unterteilt. Darüber hinaus wird die Menge der freien Performance-Kapazität dargestellt.
Verfügbare IOPS – gesamt	Anzahl der ein-/Ausgabevorgänge pro Sekunde, die derzeit für dieses Objekt verfügbar sind (frei). Diese Zahl ergibt sich aus der Subtraktion der derzeit verwendeten IOPS von den IOPS-Gesamtwerten, die Unified Manager berechnet, die das Objekt ausführen kann. Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt ein Knoten oder Aggregat ist. Verfügbare IOPS-Daten sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.
Auslastung – Gesamt	Verfügbarer Prozentsatz der verfügbaren Ressource des Objekts, das verwendet wird. Die Auslastung zeigt Node-Auslastung für Nodes, Festplattenauslastung für Aggregate und die Bandbreitenauslastung für Ports an. Diese Diagrammoption gilt nur, wenn es sich um ein Node, Aggregat oder Port handelt.
Cache-Miss-Verhältnis - Gesamt	Prozentsatz von Leseanforderungen von Client-Applikationen, die von der Festplatte zurückgegeben werden, anstatt vom Cache zurückgegeben zu werden. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volume ist.

Auswählen der anzuzeigenden Leistungsdiagramme

In der Dropdown-Liste Diagramme auswählen können Sie die Arten von Performance-Zählerdiagrammen auswählen, die im Bereich Counter Charts angezeigt werden sollen. So können Sie basierend auf Ihren Performance-Anforderungen bestimmte Daten und Zähler anzeigen.

Schritte

1. Klicken Sie im Fensterbereich **Counter Charts** auf die Dropdown-Liste **Diagramme auswählen**.
2. Diagramme hinzufügen oder entfernen:

An…	Tun Sie das…
Einzelne Diagramme hinzufügen oder entfernen	Aktivieren Sie die Kontrollkästchen neben den Diagrammen, die Sie anzeigen oder ausblenden möchten
Alle Diagramme hinzufügen	Klicken Sie Auf **Alle Auswählen**
Alle Diagramme entfernen	Klicken Sie Auf **Auswahl Aufheben**

Ihre Diagrammauswahl wird im Bereich Counter Charts angezeigt. Beachten Sie, dass beim Hinzufügen von Diagrammen die neuen Diagramme in den Bereich Counter Charts eingefügt werden, um mit der Reihenfolge der Diagramme zu übereinstimmen, die in der Dropdown-Liste Choose Charts aufgeführt sind. Wenn Sie weitere Diagramme auswählen, muss möglicherweise ein zusätzliches Scrollen durchgeführt werden.

Erweitern des Fensterbereichs Counter Charts

Sie können das Fenster Zählerdiagramme so erweitern, dass die Diagramme größer und lesbarer sind.

Über diese Aufgabe

Nachdem Sie die Vergleichsobjekte und den Zeitbereich für Zähler definiert haben, können Sie einen größeren Counter Charts-Bereich anzeigen. Sie verwenden die **<**-Schaltfläche in der Mitte des Performance Explorer-Fensters, um das Fenster zu erweitern.

Schritte

1. Erweitern oder verkleinern Sie das Fenster **Counter Charts**.

An…	Tun Sie das…
Erweitern Sie das Fenster Counter Charts, um die Breite der Seite anzupassen	Klicken Sie auf die Schaltfläche **<**
Verkleinern Sie das Fenster Counter Charts auf die rechte Hälfte der Seite	Klicken Sie auf die Schaltfläche **>**

Ändern des Fokus der Zählerdiagramme auf einen kürzeren Zeitraum

Mit der Maus können Sie den Zeitbereich reduzieren, um sich auf einen bestimmten Zeitraum im Bereich Zählerdiagramm oder im Fenster Zoomansicht der Zählerdiagramme zu konzentrieren. So sehen Sie eine granularere und mikroskopische Ansicht aller Teile der Zeitachse von Performance-Daten, Ereignissen und Schwellenwerten.

Bevor Sie beginnen

Der Cursor muss in eine Lupe geändert werden, um anzuzeigen, dass diese Funktion aktiv ist.

> Bei Verwendung dieser Funktion, die die Zeitleiste so ändert, dass Werte angezeigt werden, die der detaillierteren Anzeige entsprechen, ändert sich der Zeit- und Datumsbereich im Auswahlfeld **Zeitbereich** nicht von den ursprünglichen Werten für das Diagramm.

Schritte

1. Um einen bestimmten Zeitraum anzuzeigen, klicken Sie auf die Lupe und ziehen Sie die Maus, um den Bereich hervorzuheben, den Sie im Detail sehen möchten.

   Die Zählerwerte für den ausgewählten Zeitraum füllen das Zählerdiagramm aus.

2. Um zum ursprünglichen Zeitabschnitt zurückzukehren, der im Auswahlfeld **Zeitbereich** festgelegt wurde, klicken Sie auf die Schaltfläche **Diagrammzoom zurücksetzen**.

   Das Zählerdiagramm wird im Originalzustand angezeigt.

Anzeigen von Ereignisdetails in der Ereigniszeitleiste

Sie können alle Ereignisse und ihre zugehörigen Details im Fenster „Zeitleiste für Ereignisse“ des Performance Explorers anzeigen. Dies ist eine schnelle und effiziente Methode zur Anzeige aller Zustand- und Performance-Ereignisse, die sich während eines bestimmten Zeitbereichs auf dem Root-Objekt auftraten, die bei der Fehlerbehebung von Performance-Problemen hilfreich sein können.

Über diese Aufgabe

Im Bereich Ereigniszeitleiste werden kritische Ereignisse, Fehler, Warnungen und Informationsereignisse angezeigt, die während des ausgewählten Zeitbereichs auf dem Root-Objekt aufgetreten sind. Jeder Schweregrad eines Ereignisses hat seine eigene Zeitachse. Einzelne oder mehrere Ereignisse werden durch einen Ereignispunkt in der Zeitleiste dargestellt. Sie können den Cursor über einen Ereignispunkt positionieren, um die Ereignisdetails anzuzeigen. Um die visuelle Granularität mehrerer Ereignisse zu erhöhen, kann der Zeitbereich verkürzt werden. Dadurch werden mehrere Ereignisse in einzelne Ereignisse verteilt, sodass Sie jedes Ereignis einzeln anzeigen und untersuchen können.

Jeder Punkt des Performance-Ereignisses in der Ereignisleiste wird vertikal mit einer entsprechenden Spitze in den Zählerdiagrammen-Trendlinien, die unter der Ereigniszeitleiste angezeigt werden, angeordnet. Dies bietet eine direkte visuelle Korrelation zwischen Ereignissen und Gesamtleistung. Systemzustandsereignisse werden auch in der Zeitleiste angezeigt, jedoch entsprechen diese Arten von Ereignissen nicht unbedingt einer Spitze in einem der Performance-Diagramme.

Schritte

1. Positionieren Sie den Cursor im Fensterbereich **Ereignisleiste** über einen Ereignispunkt in einer Zeitleiste, um eine Zusammenfassung des Ereignisses oder der Ereignisse an diesem Punkt anzuzeigen.

   In einem Popup-Dialogfeld werden Informationen zu den Ereignistypen, zu Datum und Uhrzeit des Ereignisses, zum Status und zur Dauer des Ereignisses angezeigt.

2. Vollständige Ereignisdetails für ein oder mehrere Ereignisse anzeigen:

Hier…	Klicken Sie hier…
Zeigen Sie Details zu einem einzelnen Event an	**Ereignisdetails anzeigen** im Popup-Dialog.
Zeigen Sie Details für mehrere Ereignisse an	**Ereignisdetails anzeigen** im Popup-Dialog. Durch Klicken auf ein einzelnes Ereignis im Dialogfeld mehrere Ereignisse wird die entsprechende Seite Ereignisdetails angezeigt.

Zählerdiagramme Ansicht „Zoom“

Die Zählerdiagramme bieten eine Zoom-Ansicht, mit der Sie Leistungsdetails über den angegebenen Zeitraum vergrößern können. So lassen sich Performance-Details und Ereignisse wesentlich granularer anzeigen, was bei der Behebung von Performance-Problemen von Vorteil ist.

Wenn in der Zoom-Ansicht angezeigt wird, bieten einige der Abbruchdiagramme zusätzliche Informationen, die angezeigt werden, wenn sich das Diagramm nicht in der Zoom-Ansicht befindet. So werden beispielsweise im Aufschlüsselung der IOPS, IOPS/TB und MB/s auf den Seiten der Zoom-Ansicht QoS-Richtlinienwerte für Volumes und LUNs angezeigt, wenn sie in ONTAP festgelegt wurden.

Bei systemdefinierten Performance-Schwellenwerten stehen nur die Richtlinien „`Node-Ressourcen überausgelastet`“ und „`QoS Throughput Limit Inered`“ in der Liste **Policies** zur Verfügung. Die anderen systemdefinierten Schwellwertrichtlinien stehen derzeit nicht zur Verfügung.

Anzeigen der Zoom-Ansicht der Zählerdiagramme

Die Zoom-Ansicht der Zählerdiagramme bietet eine feinere Detailebene für das ausgewählte Zählerdiagramm und die zugehörige Zeitleiste. Dadurch werden die Daten der Zählerdiagramme vergrößert, sodass Sie einen schärfereren Überblick über Performanceereignisse und deren zugrunde liegende Ursachen haben können.

Über diese Aufgabe

Sie können die Zoom-Ansicht der Zählerdiagramme für jedes Zählerdiagramm anzeigen.

Schritte

1. Klicken Sie auf **Zoom View**, um das ausgewählte Diagramm zu öffnen ein neues Browser-Fenster.
2. Wenn Sie ein Diagramm anzeigen und dann auf **Zoom View** klicken, wird das Diagramm in Zoom View angezeigt. Wenn Sie die Ansichtsoption ändern möchten, können Sie in der Zoom-Ansicht **Gesamt** auswählen.

Festlegen des Zeitbereichs in der Zoom-Ansicht

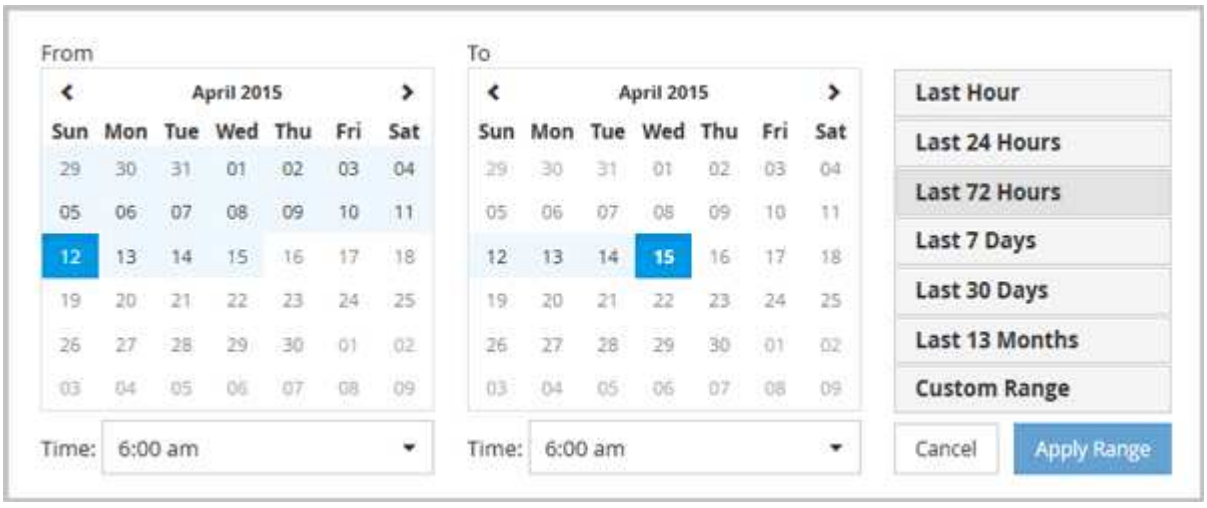
Mit dem Steuerelement **Zeitbereich** im Fenster Zähldiagramme Zoom-Ansicht können Sie einen Datums- und Zeitbereich für das ausgewählte Diagramm festlegen. So können Sie bestimmte Daten schnell auf Basis eines voreingestellten Zeitbereichs oder eines eigenen benutzerdefinierten Zeitbereichs finden.

Über diese Aufgabe

Sie können einen Zeitbereich zwischen einer Stunde und 390 Tagen auswählen. 13 Monate sind 390 Tage, weil jeder Monat als 30 Tage gezählt wird. Wenn Sie einen Datums- und Zeitbereich angeben, erhalten Sie weitere Details, mit denen Sie bestimmte Performanceereignisse oder eine Reihe von Ereignissen vergrößern können. Durch das Festlegen eines Zeitbereichs lassen sich auch potenzielle Leistungsprobleme beheben, da durch das Festlegen eines Datums- und Zeitbereichs die Daten des Performance-Ereignisses detaillierter dargestellt werden. Verwenden Sie das Steuerelement **Zeitbereich**, um vordefinierte Datums- und Zeitbereiche auszuwählen, oder geben Sie Ihren eigenen benutzerdefinierten Datums- und Zeitbereich von bis zu 390 Tagen an. Die Schaltflächen für vordefinierte Zeitbereiche variieren von **Letzte Stunde** bis **Letzte 13 Monate**.

Wenn Sie die Option **Letzte 13 Monate** wählen oder einen benutzerdefinierten Datumsbereich größer als 30 Tage angeben, wird ein Dialogfeld angezeigt, in dem Sie darauf hingewiesen werden, dass die Leistungsdaten für einen Zeitraum von mehr als 30 Tagen mit stündlichen Durchschnittswerten und nicht mit einer 5-minütigen Datenabfrage gespeichert werden. Daher kann es zu einem Verlust der visuellen Granularität bei Timeline kommen. Wenn Sie im Dialogfeld auf die Option **nicht wieder anzeigen** klicken, wird die Meldung nicht angezeigt, wenn Sie die Option **Letzte 13 Monate** wählen oder einen benutzerdefinierten Datumsbereich von mehr als 30 Tagen angeben. Die Übersichtsdaten gelten auch für einen kleineren Zeitbereich, wenn der Zeitbereich ein Datum/Uhrzeit enthält, das mehr als 30 Tage von heute entfernt ist.

Bei der Auswahl eines Zeitbereichs (benutzerdefiniert oder vordefiniert) basieren Zeitbereiche von 30 Tagen oder weniger auf 5-Minuten-Intervalldatenproben. Zeitbereiche, die größer als 30 Tage sind, basieren auf einer Stunde Intervalldatenproben.



1. Klicken Sie auf das Dropdown-Feld **Zeitbereich**, und das Fenster Zeitbereich wird angezeigt.
2. Um einen vordefinierten Zeitbereich auszuwählen, klicken Sie rechts neben dem Fenster **Zeitbereich** auf eine der Schaltflächen **Letzte…**. Bei der Auswahl eines vordefinierten Zeitbereichs stehen Daten für bis zu 13 Monate zur Verfügung. Die von Ihnen ausgewählte Schaltfläche für den vordefinierten Zeitbereich wird hervorgehoben, und die entsprechenden Tage und Zeiten werden in den Kalendern und Zeitauswahlschaltern angezeigt.

3. Um einen benutzerdefinierten Datumsbereich auszuwählen, klicken Sie links im Kalender **von** auf das Startdatum. Klicken Sie auf **<** oder **>**, um im Kalender vorwärts oder rückwärts zu navigieren. Um das Enddatum anzugeben, klicken Sie rechts im Kalender **bis** auf ein Datum. Beachten Sie, dass das Standard-Enddatum heute ist, es sei denn, Sie geben ein anderes Enddatum an. Die Schaltfläche **benutzerdefinierter Bereich** rechts neben dem Fenster Zeitbereich wird hervorgehoben, was darauf hinweist, dass Sie einen benutzerdefinierten Datumsbereich ausgewählt haben.
4. Um einen benutzerdefinierten Zeitbereich auszuwählen, klicken Sie unter dem Kalender **von** auf das Steuerelement **Uhrzeit** und wählen die Startzeit aus. Um die Endzeit festzulegen, klicken Sie rechts unter dem **bis**-Kalender auf das Steuerelement **Zeit** und wählen die Endzeit aus. Die Schaltfläche **benutzerdefinierter Bereich** rechts neben dem Fenster Zeitbereich wird hervorgehoben, was darauf hinweist, dass Sie einen benutzerdefinierten Zeitbereich ausgewählt haben.
5. Optional können Sie die Start- und Endzeiten festlegen, wenn Sie einen vordefinierten Datumsbereich auswählen. Wählen Sie den zuvor beschriebenen vordefinierten Datumsbereich aus, und wählen Sie dann die Start- und Endzeiten wie zuvor beschrieben aus. Die ausgewählten Daten werden in den Kalendern markiert, Ihre festgelegten Start- und Endzeiten werden in den Steuerelementen **Zeit** angezeigt und die Schaltfläche **benutzerdefinierter Bereich** ist markiert.
6. Klicken Sie nach Auswahl des Datums- und Zeitbereichs auf **Bereich anwenden**. Die Leistungsstatistiken für diesen Zeitbereich werden in den Diagrammen und in der Zeitleiste „Ereignisse“ angezeigt.

Auswählen von Leistungsschwellenwerten in der Zoom-Ansicht der Zählerdiagramme

Das Anwenden von Schwellenwerten in der Zoom-Ansicht von Zählerdiagrammen bietet eine detaillierte Ansicht der Vorkommen von Performance-Schwellenwerten. Auf diese Weise können Sie Schwellenwerte anwenden oder entfernen und die Ergebnisse sofort anzeigen. Dies kann bei der Entscheidung hilfreich sein, ob die Fehlerbehebung Ihr nächster Schritt sein sollte.

Über diese Aufgabe

Durch Auswahl von Schwellenwerten in der Zoom-Ansicht für Zählerdiagramme können Sie präzise Daten zu Ereignissen mit Leistungsschwellenwerten anzeigen. Sie können jeden Schwellenwert anwenden, der im Bereich **Richtlinien** der Zoom-Ansicht der Zählerdiagramme angezeigt wird.

Es kann jeweils nur eine Richtlinie auf das Objekt in der Zoom-Ansicht der Zählerdiagramme angewendet werden.

Schritte

1. Wählen Sie das aus oder heben Sie die Auswahl auf Das ist einer Richtlinie zugeordnet.

   Der ausgewählte Schwellenwert wird auf die Zoom-Ansicht der Zählerdiagramme angewendet. Kritische Schwellenwerte werden als rote Linie angezeigt. Warnschwellenwerte werden als gelbe Linie angezeigt.

Anzeige der minimalen und maximalen Einstellungen für Workload-QoS

In den Performance Explorer-Diagrammen können Sie die durch ONTAP definierten Quality of Service (QoS)-Richtlinieneinstellungen auf einem Volume oder einer LUN anzeigen. Die Einstellung für den maximalen Durchsatz begrenzt die Auswirkungen konkurrierender Workloads auf die Systemressourcen. Eine Einstellung für den Durchsatz stellt sicher, dass ein wichtiger Workload das Mindestdurchsatz erfüllt,

unabhängig von der Nachfrage durch konkurrierende Workloads.

Über diese Aufgabe

QoS-Durchsatz „minimum“ und „maximum“ IOPS- und MB/s-Einstellungen werden in den Zählerdiagrammen nur angezeigt, wenn sie in ONTAP konfiguriert wurden. Durchsatzminimum-Einstellungen sind nur auf Systemen mit ONTAP 9.2 oder neuer Software, nur auf AFF Systemen verfügbar. Diese Einstellungen lassen sich derzeit nur für IOPS festlegen.

Adaptive QoS-Richtlinien sind ab ONTAP 9.3 verfügbar und werden mit IOPS/TB statt IOPS ausgedrückt. Durch diese Richtlinien wird der QoS-Richtlinienwert automatisch auf Basis der Volume-Größe pro Workload angepasst. Auf diese Weise bleibt das Verhältnis von IOPS zu Terabyte erhalten, wenn sich das Volume ändert. Sie können eine anpassungsfähige QoS-Richtliniengruppe nur auf Volumes anwenden. Die QoS-Terminologie „erwarted“ und „Peak“ werden für anpassungsfähige QoS-Richtlinien statt der minimalen und maximalen Größe verwendet.

Unified Manager generiert Warnereignisse bei Verletzungen der QoS-Richtlinien, wenn der Workload-Durchsatz die festgelegte Richtlinieneinstellung für QoS während jeder Performance-Einsammlung in der vorherigen Stunde überschritten hat. Der Workload-Durchsatz kann den QoS-Schwellenwert für nur einen kurzen Zeitraum während des jeweiligen Erfassungszeitraums überschreiten. Unified Manager zeigt jedoch den „average“-Durchsatz während des Erfassungszeitraums auf dem Diagramm an. Aus diesem Grund werden QoS-Ereignisse angezeigt, während der Durchsatz für einen Workload möglicherweise nicht den in der Tabelle aufgeführten Richtlinienschwellenwert überschritten hat.

Schritte

1. Führen Sie auf der Seite **Performance Explorer** für das ausgewählte Volume oder die ausgewählte LUN die folgenden Aktionen durch, um die QoS-Decken- und Bodeneinstellungen anzuzeigen:

Ihr Ziel ist	Tun Sie das…
IOPS-Obergrenze anzeigen (max. QoS)	Klicken Sie im Diagramm IOPS Total oder Breakdown auf **Zoom View**.
Anzeige der MB/s-Obergrenze (QoS max.)	Klicken Sie im Diagramm MB/s Total oder Breakdown auf **Zoom View**.
IOPS-Bereich anzeigen (QoS-Min.)	Klicken Sie im Diagramm IOPS Total oder Breakdown auf **Zoom View**.
Anzeige der IOPS/TB-Obergrenze (QoS-Spitzenwert)	Klicken Sie bei Volumes im Diagramm IOPS/TB auf **Zoom View**.
Anzeige des IOPS/TB-Bodens (QoS erwartet)	Klicken Sie bei Volumes im Diagramm IOPS/TB auf **Zoom View**.

   Die gestrichelte horizontale Linie gibt den in ONTAP festgelegten maximalen oder minimalen Durchsatzwert an. Sie können auch anzeigen, wann Änderungen an den QoS-Werten implementiert wurden.

2. Um die spezifischen Werte für IOPS und MB/s im Vergleich zur QoS-Einstellung anzuzeigen, bewegen Sie den Cursor in den Diagrammbereich, um das Popup-Fenster anzuzeigen.

Nachdem Sie fertig sind

Wenn bei bestimmten Volumes oder LUNs eine sehr hohe IOPS oder MB/s vorhanden ist und die Systemressourcen besonders stark belastet werden, können Sie mit System Manager oder der ONTAP CLI die QoS-Einstellungen so anpassen, dass diese Workloads sich nicht auf die Performance anderer Workloads auswirken.

Weitere Informationen zum Anpassen der QoS-Einstellungen finden Sie im Power Guide *ONTAP 9 zur Leistungsüberwachung*.

"ONTAP 9 Leistungsüberwachung – Stromversorgungshandbuch"

Wie verschiedene Arten von QoS-Richtlinien in Unified Manager angezeigt werden

Sie können die von ONTAP definierten Richtlinieneinstellungen für die Quality of Service (QoS) anzeigen, die auf ein Volume oder eine LUN angewendet wurden. Diese Einstellungen finden Sie in den Diagrammen zu IOPS/TB und MB/s im Performance Explorer. Die in den Diagrammen angezeigten Informationen unterscheiden sich je nach QoS-Richtlinie, die auf den Workload angewendet wurde.

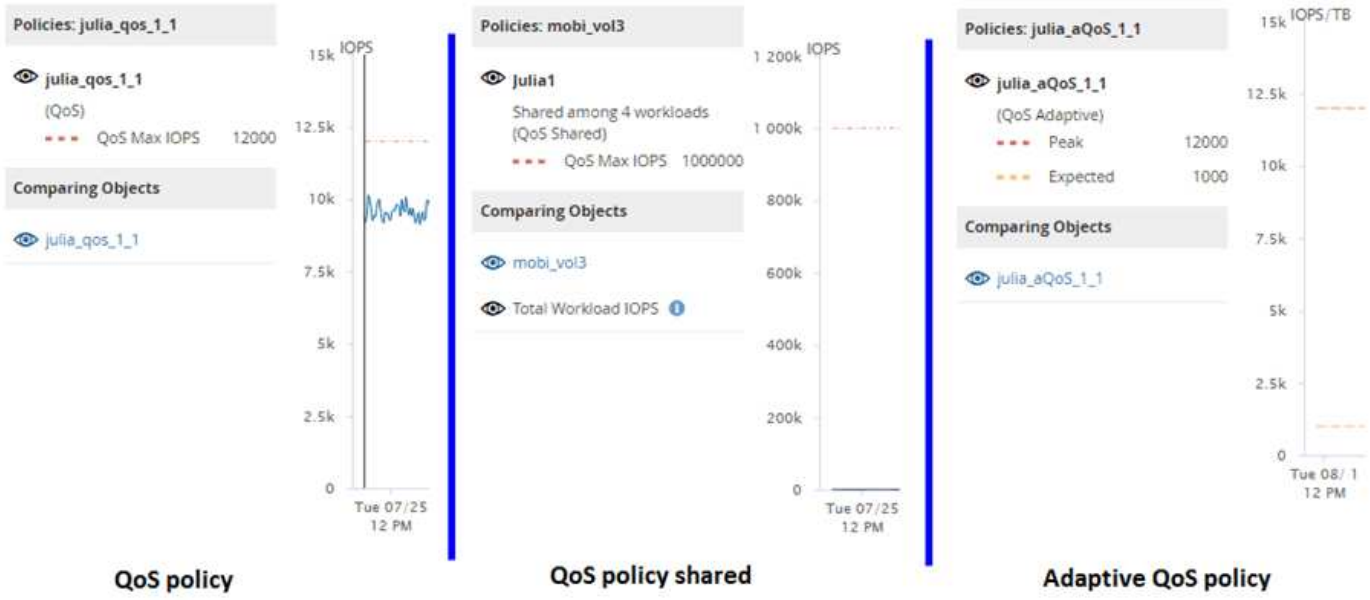
Eine Einstellung für den Durchsatz „`ceiling`“ definiert den maximalen Durchsatz, den der Workload verbrauchen kann, und begrenzt somit die Auswirkungen auf konkurrierende Workloads für Systemressourcen. Durch eine Einstellung für den Durchsatz „`Boden`“ wird der Mindestdurchsatz definiert, der für den Workload verfügbar sein muss, damit ein wichtiger Workload die Mindestdurchsatz-Ziele erfüllt, unabhängig von der Nachfrage durch konkurrierende Workloads.

Gemeinsame und nicht gemeinsam genutzte QoS-Richtlinien für IOPS und MB/s definieren Boden und Decke mit den Begriffen „`minimum`“ und „`maximum`“. Adaptive QoS-Richtlinien für IOPS/TB, die mit ONTAP 9.3 eingeführt wurden, definieren Boden und Obergrenze mit den Begriffen „`erwarted`“ und „`Peak`“.

Mit ONTAP können Sie diese zwei Arten von QoS-Richtlinien erstellen, abhängig davon, wie sie auf Workloads angewendet werden, gibt es in den Performance-Diagrammen drei Arten, die QoS-Richtlinie angezeigt wird.

Art der Richtlinie	Funktionalität	Anzeige in der Unified Manager-Schnittstelle
QoS-Richtlinien für gemeinsame Workloads, die einem einzelnen Workload zugewiesen sind oder QoS-Richtlinien, die nicht gemeinsam genutzt werden, die einem einzelnen Workload oder mehreren Workloads zugewiesen sind	Jeder Workload kann die angegebene Durchsatzeinstellung belegen	Zeigt „`(QoS)`“ an.
QoS-Richtlinien für gemeinsame Nutzung, die mehreren Workloads zugewiesen sind	Alle Workloads teilen sich die angegebene Durchsatzeinstellung	Zeigt „`(QoS Shared)`“ an.
Anpassungsfähige QoS-Richtlinie, die einem einzelnen oder mehreren Workloads zugewiesen ist	Jeder Workload kann die angegebene Durchsatzeinstellung belegen	Zeigt „`(QoS Adaptive)`“ an

Die folgende Abbildung zeigt ein Beispiel dafür, wie die drei Optionen in den Zählerdiagrammen angezeigt werden.



Wenn eine normale QoS-Richtlinie, die in IOPS definiert wurde, im IOPS/TB-Diagramm für einen Workload angezeigt wird, konvertiert ONTAP den IOPS-Wert in einen IOPS/TB-Wert, und Unified Manager zeigt diese Richtlinie im IOPS/TB-Diagramm zusammen mit dem Text „`QoS", definiert in IOPS`“ an.

Wenn eine in IOPS/TB definierte anpassungsfähige QoS-Richtlinie im IOPS-Diagramm für einen Workload angezeigt wird, konvertiert ONTAP den IOPS/TB-Wert in einen IOPS-Wert und Unified Manager zeigt diese Richtlinie im IOPS-Diagramm zusammen mit dem Text „`QoS Adaptive, Definiert in IOPS/Used TB`" oder „`QoS Adaptive, definiert in IOPS/zugewiesenen TB`“, abhängig davon, wie die Einstellung für die IOPS-Spitzenzuweisung konfiguriert ist. Wenn die Zuweisungseinstellung auf „`Alered-space`“ festgelegt ist, wird der IOPS-Spitzenwert basierend auf der Größe des Volumes berechnet. Wenn die Zuweisungseinstellung auf „`used-space`“ festgelegt ist, wird die IOPS-Spitzenauslastung basierend auf der im Volume gespeicherten Datenmenge unter Berücksichtigung der Storage-Effizienz berechnet.

Das IOPS/TB-Diagramm zeigt Performance-Daten nur dann an, wenn die logische Kapazität, die vom Volume verwendet wird, größer als oder gleich 1 TB ist. In der Tabelle werden Lücken angezeigt, wenn die genutzte Kapazität während des ausgewählten Zeitrahmens unter 1 TB fällt.

Anzeigen der Volume-Latenz nach Clusterkomponente

Sie können detaillierte Latenzinformationen zu einem Volume mithilfe der Seite Performance/Volume Explorer anzeigen. Das Zählerdiagramm „Latenz“ zeigt die gesamte Latenz auf dem Volume an, und das Diagramm „Latenz – Aufschlüsselung der Zähler“ ist hilfreich, um die Auswirkungen der Lese- und Schreiblatenz auf das Volume zu ermitteln.

Über diese Aufgabe

Außerdem zeigt das Diagramm Latenz – Cluster-Komponenten einen detaillierten Vergleich der Latenz der einzelnen Cluster-Komponenten an, um zu ermitteln, wie jede Komponente zu der gesamten Latenz auf dem Volume beiträgt. Die folgenden Cluster-Komponenten werden angezeigt:

- Netzwerk
- QoS-Richtlinie
- Netzwerkverarbeitung
- Cluster Interconnect
- Datenverarbeitung
- Aggregatvorgänge
- MetroCluster-Ressourcen
- Cloud-Latenz
- Sync SnapMirror

Schritte

1. Wählen Sie auf der Seite **Performance/Volume Explorer** für Ihr ausgewähltes Volume im Latenzdiagramm im Dropdown-Menü die Option **Cluster Components** aus.

   Das Diagramm Latenz – Cluster-Komponenten wird angezeigt.

2. Um eine größere Version des Diagramms anzuzeigen, wählen Sie **Zoom-Ansicht**.

   Das Vergleichsdiagramm für die Cluster-Komponente wird angezeigt. Sie können den Vergleich einschränken, indem Sie die Auswahl aufheben oder auswählen Der jeder Cluster-Komponente zugeordnet ist.

3. Um die spezifischen Werte anzuzeigen, bewegen Sie den Cursor in den Diagrammbereich, um das Popup-Fenster anzuzeigen.

Anzeigen von SVM-IOPS-Traffic nach Protokoll

Sie können detaillierte IOPS-Informationen für eine SVM über die Seite „Performance/SVM Explorer“ anzeigen. Das Zählerdiagramm „IOPS – Zählerdiagramm“ zeigt die gesamte IOPS-Auslastung auf der SVM. Das Zählerdiagramm „IOPS – Aufschlüsselung Sie dient zur Ermittlung der Auswirkungen von Lese-, Schreib- und anderen IOPS auf die SVM.

Über diese Aufgabe

Außerdem zeigt das Diagramm „IOPS – Protokolle“ einen detaillierten Vergleich des IOPS-Datenverkehrs für jedes auf der SVM zu verwendenden Protokoll. Folgende Protokolle sind verfügbar:

- CIFS
- NFS
- FCP
- ISCSI
- NVMe

Schritte

1. Wählen Sie auf der Seite **Performance/SVM Explorer** für Ihre ausgewählte SVM aus dem IOPS-Diagramm im Dropdown-Menü die Option **Protokolle** aus.

   Das Diagramm IOPS – Protokolle wird angezeigt.

2. Um eine größere Version des Diagramms anzuzeigen, wählen Sie **Zoom-Ansicht**.

   Das erweiterte IOPS-Protokoll-Vergleichstabelle wird angezeigt. Sie können den Vergleich einschränken, indem Sie die Auswahl aufheben oder auswählen Dies ist mit einem Protokoll verbunden.

3. Um die spezifischen Werte anzuzeigen, bewegen Sie den Cursor in den Diagrammbereich eines der beiden Diagramme, um das Popup-Fenster anzuzeigen.

Anzeigen der Latenzdiagramme von Volumes und LUNs zur Überprüfung der Performance-Garantie

Sie können die Volumes und LUNs, die Sie für das Programm „`Performance Guarantee`“ abonniert haben, anzeigen, um zu überprüfen, dass die Latenz den Wert nicht überschritten hat, den Sie garantiert haben.

Über diese Aufgabe

Die Garantie für Latenz-Performance beträgt eine Millisekunde pro Operation, der nicht überschritten werden sollte. Er basiert auf einem stündlichen Durchschnitt und nicht auf dem Standardzeitraum der Performance-Erfassung in fünf Minuten.

Schritte

1. Wählen Sie auf der Seite **Performance Volumes** oder **Performance LUNs** Inventory den gewünschten Datenträger oder LUN aus.
2. Wählen Sie auf der Seite **Performance Explorer** für das ausgewählte Volumen oder die ausgewählte LUN aus dem Auswahlfeld **Statistik in** aus.

   Die horizontale Linie im Latenzdiagramm zeigt eine reibungslosere Linie, da die 5-Minuten-Sammlungen durch den Durchschnitt pro Stunde ersetzt werden.

3. Wenn Sie andere Volumes auf demselben Aggregat haben, die unter der Performance-Garantie liegen, können Sie diese Volumes hinzufügen, um den Latenzwert im gleichen Diagramm anzuzeigen.

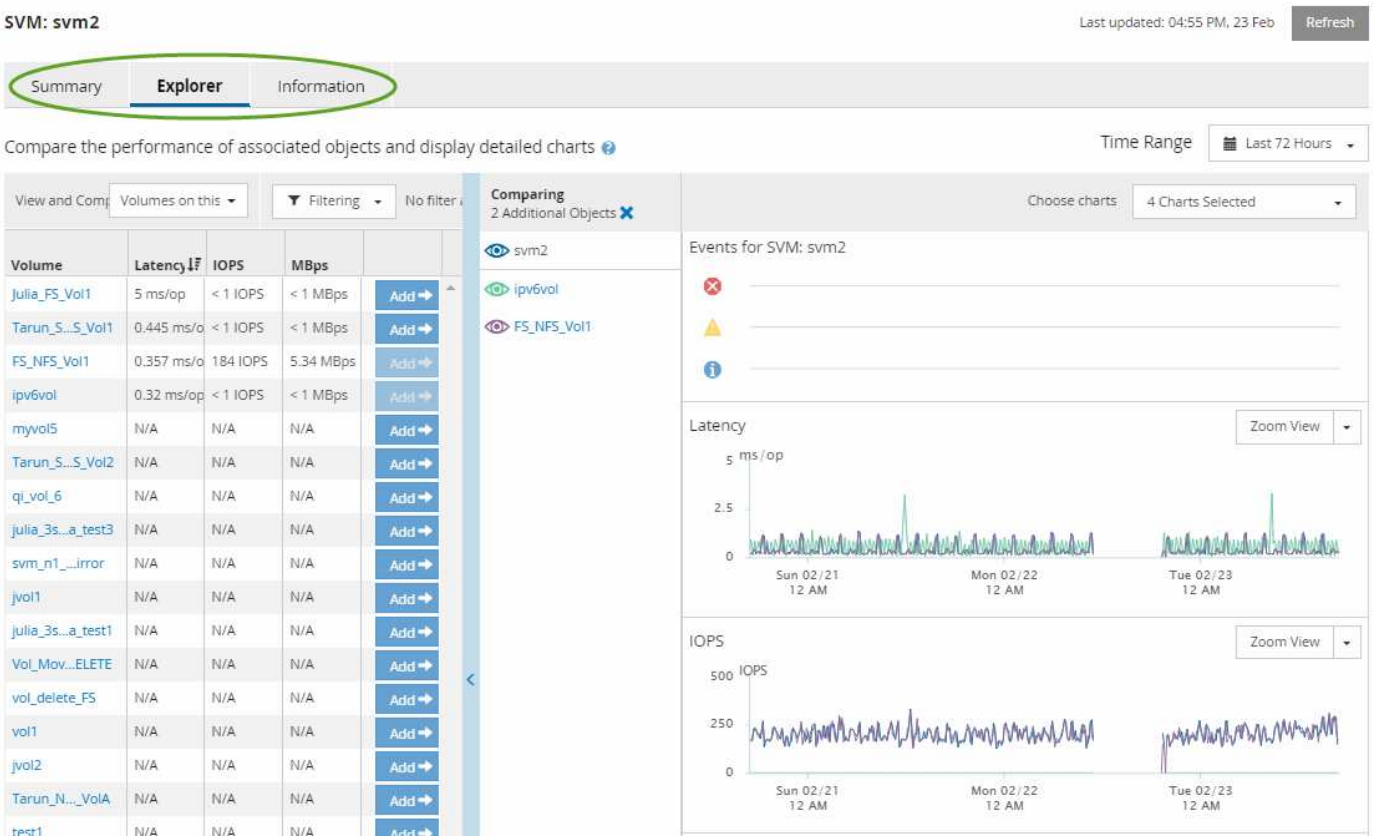
Komponenten der ObjektLanding-Pages

Auf den Seiten „Objekt-Landing“ werden Details zu allen kritischen, Warn- und Informationsereignissen angezeigt. Sie bieten eine detaillierte Ansicht der Performance aller Cluster-Objekte, sodass Sie einzelne Objekte über verschiedene Zeiträume auswählen und vergleichen können.

Auf den Seiten „Objekt-Landing“ können Sie die Gesamtleistung aller Objekte untersuchen und die Performance-Daten des Objekts im nebeneinander liegenden Format vergleichen. Dies ist bei der Leistungsbeurteilung und bei der Fehlersuche von Ereignissen von Vorteil.

Die Daten, die in den Zusammenfassungsfeldern des Zählers und in den Zählerdiagrammen angezeigt werden, basieren auf einem fünfminütigen Abtastintervall. Die Daten, die im Objektbestandsraster links auf der Seite angezeigt werden, basieren auf einem einstündigen Probenahmeintervall.

Die folgende Abbildung zeigt ein Beispiel für eine Landing Page des Objekts, auf der die Explorer-Informationen angezeigt werden:



Abhängig vom angezeigten Storage-Objekt kann auf der Objekt-Landing-Page die folgenden Registerkarten enthalten, die Performance-Daten zum Objekt liefern:

- Zusammenfassung

  Zeigt drei oder vier Zählerdiagramme an, die die Ereignisse und die Leistung pro Objekt für den vorangegangenen 72-Stunden-Zeitraum enthalten, einschließlich einer Trendlinie, die die hohen und niedrigen Werte in diesem Zeitraum anzeigt.

- Explorer

  Zeigt ein Raster von Storage-Objekten an, die mit dem aktuellen Objekt verknüpft sind. So können Sie die Performance-Werte des aktuellen Objekts mit den zugehörigen Objekten vergleichen. Diese Registerkarte enthält bis zu elf Zählerdiagramme und eine Zeitbereichauswahl, mit der Sie eine Vielzahl von Vergleichen durchführen können.

- Informationsdaten

  Zeigt Werte für nicht-Performance-Konfigurationsattribute am Storage-Objekt an, einschließlich der installierten Version der ONTAP Software, des HA-Partnernamens und der Anzahl der Ports und LIFs.

- Erstklassige Performance

  Für Cluster: Zeigt die Storage-Objekte an, die basierend auf dem von Ihnen ausgewählten Performance-Zähler die höchste Performance oder die niedrigste Performance haben.

- Failover-Planung

  Für Nodes: Zeigt die Schätzung der Performance-Auswirkungen auf einen Node an, wenn der HA-Partner des Node ausfällt.

- Details

  Für Volumes: Zeigt detaillierte Performance-Statistiken für alle I/O-Aktivitäten und Vorgänge für den ausgewählten Volume-Workload an. Diese Registerkarte ist für FlexVol Volumes, FlexGroup Volumes und Komponenten von FlexGroups verfügbar.

Übersichtsseite

Auf der Seite Zusammenfassung werden Zählerdiagramme angezeigt, die Details zu den Ereignissen und der Performance pro Objekt für den vorangegangenen 72-Stunden-Zeitraum enthalten. Diese Daten werden nicht automatisch aktualisiert, sondern sind zum letzten Laden der Seite aktuell. Die Diagramme auf der Übersichtsseite beantworten die Frage *muss ich weiter suchen?*

Diagramme und Zählerstatistiken

Die Übersichtsdiagramme bieten einen schnellen, umfassenden Überblick über die letzten 72 Stunden und helfen Ihnen, mögliche Probleme zu identifizieren, für die weitere Untersuchungen erforderlich sind.

Die Zählerstatistiken der Übersichtsseite werden in Diagrammen angezeigt.

Sie können den Cursor in einem Diagramm über die Trendlinie positionieren, um die Zählerwerte für einen bestimmten Zeitpunkt anzuzeigen. In den Übersichtsdiagrammen wird außerdem die Gesamtzahl der aktiven kritischen und Warnereignisse für die letzten 72 Stunden für die folgenden Zähler angezeigt:

- **Latenz**

  Durchschnittliche Reaktionszeit aller I/O-Anforderungen, in Millisekunden pro Vorgang ausgedrückt

  Wird für alle Objekttypen angezeigt.

- **IOPS**

  Durchschnittliche Betriebsgeschwindigkeit, ausgedrückt in ein-/Ausgabeoperationen pro Sekunde

  Wird für alle Objekttypen angezeigt.

- **Mbps**

  Durchschnittlicher Durchsatz: In Megabyte pro Sekunde ausgedrückt

  Wird für alle Objekttypen angezeigt.

- **Verwendete Leistungskapazität**

Prozentsatz der Performance-Kapazität, die von einem Node oder Aggregat verbraucht wird

Nur für Nodes und Aggregate angezeigt Dieses Diagramm wird nur angezeigt, wenn Sie ONTAP 9.0 oder höher verwenden.

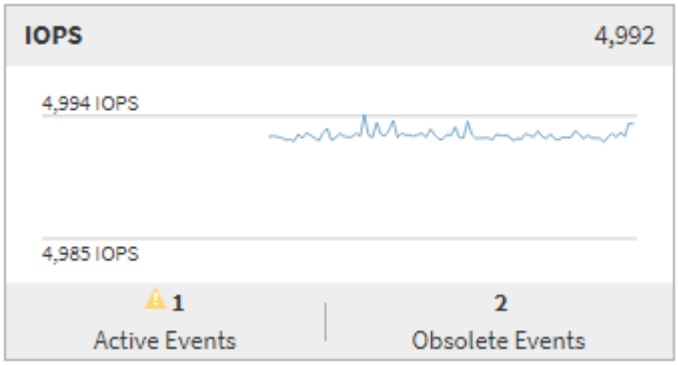
- **Nutzung**

  Prozentsatz der Objektauslastung für Nodes und Aggregate oder Bandbreitenauslastung für Ports.

  Nur für Nodes, Aggregate und Ports angezeigt

Wenn Sie den Mauszeiger über die Ereignisanzahl für aktive Ereignisse positionieren, werden Typ und Anzahl der Ereignisse angezeigt. Kritische Ereignisse werden rot (■), und Warnereignisse werden in gelb (■).

Die Zahl oben rechts im Diagramm im grauen Balken ist der Durchschnittswert aus dem letzten 72-Stunden-Zeitraum. Die Zahlen unten und oben im Trendliniendiagramm sind die Mindest- und Höchstwerte der letzten 72 Stunden. Der graue Balken unterhalb des Diagramms enthält die Anzahl der aktiven (neuen und bestätigten) Ereignisse und der veralteten Ereignisse aus dem Zeitraum der letzten 72 Stunden.



- **Latenzzähler-Diagramm**

  Das Latenzzähler-Diagramm bietet einen allgemeinen Überblick über die Objektlatenz für den vorherigen 72-Stunden-Zeitraum. Die Latenz bezeichnet die durchschnittliche Reaktionszeit aller I/O-Anfragen. Sie wird in Millisekunden pro Vorgang ausgedrückt, die Servicezeit, die Wartezeit oder beides, während ein Datenpaket oder ein Block in der betrachten Cluster-Storage-Komponente zu finden ist.

  Oben (Zählerwert): die Zahl in der Kopfzeile zeigt den Durchschnitt für den vorangegangenen 72-Stunden-Zeitraum an.

  Mitte (Performance-Diagramm): die Zahl unten im Diagramm zeigt die niedrigste Latenz an, und die Zahl oben im Diagramm zeigt die höchste Latenz für den letzten 72-Stunden-Zeitraum an. Positionieren Sie den Mauszeiger über die Trendkurve, um den Latenzwert für einen bestimmten Zeitraum anzuzeigen.

  Bottom (Ereignisse): im Pop-up-Fenster werden die Details der Ereignisse angezeigt. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinformationen“ zu navigieren, um vollständige Ereignisdetails anzuzeigen.

- **IOPS-Zählerdiagramm**

  Das IOPS-Zählerdiagramm bietet eine allgemeine Übersicht über den Objekt-IOPS-Zustand des vorherigen Zeitraums von 72 Stunden. IOPS gibt die Geschwindigkeit des Storage-Systems in der Anzahl der ein-/Ausgabe-Vorgänge pro Sekunde an.

Oben (Zählerwert): die Zahl in der Kopfzeile zeigt den Durchschnitt für den vorangegangenen 72-Stunden-Zeitraum an.

Mitte (Performance-Diagramm): die Zahl unten im Diagramm zeigt die niedrigsten IOPS an, und die Zahl oben im Diagramm zeigt die höchsten IOPS für den Zeitraum von 72 Stunden an. Positionieren Sie den Mauszeiger über die Trendkurve, um den IOPS-Wert für einen bestimmten Zeitpunkt anzuzeigen.

Bottom (Ereignisse): im Pop-up-Fenster werden die Details der Ereignisse angezeigt. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinformationen“ zu navigieren, um vollständige Ereignisdetails anzuzeigen.

- **MB/s-Zählerdiagramm**

  Das MB/s-Zählerdiagramm zeigt die Performance des Objekts im MB/s an und zeigt an, wie viele Daten in Megabyte pro Sekunde an und vom Objekt übertragen wurden. Das MB/s-Zählerdiagramm bietet eine allgemeine Übersicht über den Zustand des Objekts im Hinblick auf den Zustand der vorherigen 72-Stunden-Periode.

  Oben (Zählerwert): die Zahl in der Kopfzeile zeigt die durchschnittliche Anzahl von Mbps für den vorangegangenen 72-Stunden-Zeitraum an.

  Mitte (Leistungsdiagramm): der Wert unten im Diagramm zeigt die niedrigste Anzahl von Mbit/s an, und der Wert oben im Diagramm zeigt die höchste Anzahl von Mbit/s für den vorangegangenen 72-Stunden-Zeitraum an. Positionieren Sie den Cursor über die Trendlinie des Diagramms, um den Wert für MB/s für eine bestimmte Zeit anzuzeigen.

  Bottom (Ereignisse): im Pop-up-Fenster werden die Details der Ereignisse angezeigt. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinformationen“ zu navigieren, um vollständige Ereignisdetails anzuzeigen.

- **Leistungskapazität verwendetes Zählerdiagramm**

  Das Zählerdiagramm mit der verwendeten Performance-Kapazität zeigt den Prozentsatz der Performance-Kapazität an, die vom Objekt verbraucht wird.

  Oben (Zählerwert): die Zahl im Header zeigt die durchschnittliche Nutzleistung für den vorangegangenen 72-Stunden-Zeitraum an.

  Mittel (Leistungsdiagramm): der Wert unten im Diagramm zeigt den am wenigsten genutzten Prozentsatz der Performance-Kapazität an, und der Wert oben im Diagramm zeigt den am höchsten verwendeten Prozentsatz der Performance-Kapazität für den Zeitraum von 72 Stunden an. Positionieren Sie den Cursor über die Trendkurve, um den für eine bestimmte Zeit verwendeten Performance-Kapazitätswert anzuzeigen.

  Bottom (Ereignisse): im Pop-up-Fenster werden die Details der Ereignisse angezeigt. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinformationen“ zu navigieren, um vollständige Ereignisdetails anzuzeigen.

- **Auslastungszähler-Diagramm**

  Das Zählerdiagramm mit der Auslastung zeigt den Prozentsatz der Objektauslastung an. Das Zählerdiagramm mit der Auslastung bietet einen allgemeinen Überblick über den Prozentsatz der Objekt- oder Bandbreitenauslastung des vorhergehenden Zeitraums von 72 Stunden.

  Oben (Zählerwert): die Zahl in der Kopfzeile zeigt den durchschnittlichen Auslastungsgrad für den vorangegangenen 72-Stunden-Zeitraum an.

Mitte (Leistungsdiagramm): der Wert unten im Diagramm zeigt den niedrigsten Prozentsatz der Auslastung an, und der Wert oben im Diagramm zeigt den höchsten Auslastungsgrad für den vorangegangenen 72-Stunden-Zeitraum an. Positionieren Sie den Cursor über die Trendkurve, um den Nutzungswert für eine bestimmte Zeit anzuzeigen.

Bottom (Ereignisse): im Pop-up-Fenster werden die Details der Ereignisse angezeigt. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinformationen“ zu navigieren, um vollständige Ereignisdetails anzuzeigen.

Veranstaltungen

In der Ereignishistorie-Tabelle werden, sofern zutreffend, die letzten Ereignisse aufgelistet, die auf diesem Objekt aufgetreten sind. Durch Klicken auf den Ereignisnamen werden Details des Ereignisses auf der Seite Ereignisdetails angezeigt.

Komponenten der Seite Performance Explorer

Auf der Seite „Performance Explorer“ können Sie die Performance ähnlicher Objekte in einem Cluster vergleichen, z. B. aller Volumes in einem Cluster. Dies ist von Vorteil bei der Fehlerbehebung von Performance-Ereignissen und bei der Feinabstimmung der Objekt-Performance. Sie können auch Objekte mit dem Root-Objekt vergleichen, dem Basisobjekt, mit dem andere Objektvergleiche erstellt werden.

Klicken Sie auf die Schaltfläche **Favoriten** ( ) Um dieses Objekt zu Ihrer Liste der bevorzugten Speicherobjekte hinzuzufügen. Eine blaue Taste ( ) Zeigt an, dass dieses Objekt bereits ein Favorit ist.

Klicken Sie auf die Schaltfläche **zur Integritätsansicht wechseln**, um die Seite Integritätsdetails für dieses Objekt anzuzeigen. In einigen Fällen können Sie wichtige Informationen über die Speicherkonfigurationseinstellungen für dieses Objekt erhalten, die bei der Fehlerbehebung hilfreich sein können.

Auf der Seite Performance Explorer werden eine Liste der Cluster-Objekte und ihre Performance-Daten angezeigt. Auf dieser Seite werden alle Clusterobjekte des gleichen Typs (z. B. Volumes und ihre objektspezifischen Performance-Statistiken) in einem tabellarischen Format angezeigt. Diese Ansicht bietet einen effizienten Überblick über die Cluster-Objekt-Performance.

Wenn „N/A“ in einer beliebigen Zelle der Tabelle angezeigt wird, bedeutet dies, dass kein Wert für diesen Zähler verfügbar ist, da zu diesem Zeitpunkt kein I/O für dieses Objekt vorhanden ist.

Die Seite Performance Explorer enthält die folgenden Komponenten:

- **Zeitbereich**

  Ermöglicht die Auswahl eines Zeitbereichs für die Objektdaten.

  Sie können einen vordefinierten Bereich auswählen oder Ihren eigenen benutzerdefinierten Zeitbereich festlegen.

- **Anzeigen und Vergleichen**

  Ermöglicht die Auswahl, welcher Typ des korrelierten Objekts in der Tabelle angezeigt wird.

  Die verfügbaren Optionen hängen vom Root-Objekttyp und dessen verfügbaren Daten ab. Sie können auf

die Dropdown-Liste Anzeigen und Vergleichen klicken, um einen Objekttyp auszuwählen. Der ausgewählte Objekttyp wird in der Liste angezeigt.

- **Filterung**

  Hiermit können Sie die Menge der einbezogenen Daten auf der Grundlage Ihrer Präferenzen eingrenzen.

  Sie können Filter erstellen, die auf die Objektdaten angewendet werden, z. B. IOPS über 4. Sie können bis zu vier gleichzeitige Filter hinzufügen.

- * Vergleich*

  Zeigt eine Liste der Objekte an, die Sie zum Vergleich mit dem Stammobjekt ausgewählt haben.

  Die Daten für die Objekte im vergleichenden Fensterbereich werden in den Zählerdiagrammen angezeigt.

- **Statistik In** Anzeigen

  Bei Volume und LUNs können Sie auswählen, ob die Statistiken nach jedem Erfassungszyklus angezeigt werden (Standardeinstellung 5 Minuten), oder ob die Statistiken als stündlicher Durchschnitt angezeigt werden. Durch diese Funktionalität können Sie das Latenzdiagramm zur Unterstützung des NetApp „`Performance Guarantee`“-Programms anzeigen.

- **Counter Charts**

  Zeigt graphengraphierte Daten für jede Objektleistungkategorie an.

  Normalerweise werden standardmäßig nur drei oder vier Diagramme angezeigt. Mit der Komponente Diagramm auswählen können Sie zusätzliche Diagramme anzeigen oder bestimmte Diagramme ausblenden. Sie können auch auswählen, ob Sie die Ereigniszeitleiste ein- oder ausblenden möchten.

- **Zeitleiste Für Veranstaltungen**

  Zeigt die Performance- und Integritätsereignisse an, die in der Zeitbereich-Komponente in der von Ihnen ausgewählten Zeitachse auftreten.

Performance-Management mithilfe von Performance-Kapazität und verfügbaren IOPS-Informationen

Performance Capacity zeigt an, wie viel Durchsatz eine Ressource erhalten kann, ohne die nützliche Performance dieser Ressource zu überschreiten. Wenn Sie die Nutzung vorhandener Performance-Zähler verwenden, ist die Performance-Kapazität der Punkt, an dem Sie die maximale Auslastung eines Node oder Aggregats erhalten, bevor die Latenz zu einem Problem wird.

Unified Manager sammelt Performance-Kapazitätsstatistiken von Nodes und Aggregaten in jedem Cluster. *Performance-Kapazität verwendet* ist der Prozentsatz der derzeit genutzten Performance-Kapazität und *Performance Capacity free* ist der Prozentsatz der noch verfügbaren Performance-Kapazität.

Während die freie Performance-Kapazität einen Prozentsatz der noch verfügbaren Ressource bietet, gibt Ihnen *verfügbare IOPS* die Anzahl an IOPS an, die der Ressource hinzugefügt werden können, bevor sie die maximale Performance-Kapazität erreicht. Mithilfe dieser Kennzahl können Sie sicherstellen, dass Sie Workloads mit einer vorab festgelegten Anzahl von IOPS zu einer Ressource hinzufügen können.

Das Monitoring der Informationen zur Performance-Kapazität bietet folgende Vorteile:

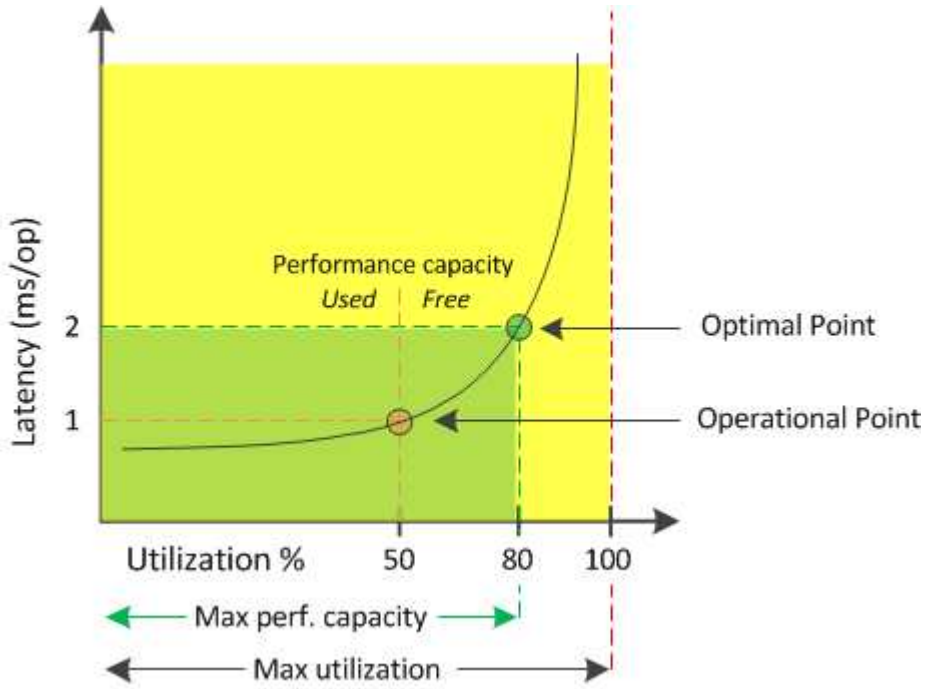
- Hilft bei der Workflow-Bereitstellung und beim Lastausgleich.
- Hilft Ihnen, eine Überlastung eines Knotens zu verhindern oder seine Ressourcen über den optimalen Punkt hinaus zu schieben, wodurch die Fehlerbehebung verringert wird.
- Präzisere Bestimmung, bei denen möglicherweise zusätzliche Storage-Geräte erforderlich sind

Welche Performance-Kapazität wird verwendet

Mit dem verwendeten Zähler für die Performance-Kapazität können Sie ermitteln, ob die Performance eines Node oder Aggregats an einem Punkt anliegt, an dem sich die Performance bei einer Workload-Steigerung verschlechtern kann. Es kann Ihnen auch zeigen, ob ein Node oder Aggregat derzeit zu bestimmten Zeiten überlastet ist. Die Verwendung der Performance-Kapazität ähnelt der Auslastung, allerdings bietet die vorherige Appliance einen besseren Einblick in die verfügbaren Performance-Funktionen in einer physischen Ressource für einen bestimmten Workload.

Daten zur Performance-Kapazität sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.

Die optimale genutzte Performance-Kapazität ist der Punkt, an dem ein Node oder Aggregat optimale Auslastung und Latenz (Reaktionszeit) bietet und effizient eingesetzt wird. In der folgenden Abbildung ist eine Beispiellatenz im Vergleich zur Auslastungskurve gezeigt für ein Aggregat.



In diesem Beispiel weist der_Operationspunkt_ darauf hin, dass das Aggregat derzeit bei einer Auslastung von 50 % und einer Latenz von 1.0 ms/op. Arbeitet Basierend auf den vom Aggregat erfassten Statistiken stellt Unified Manager fest, dass für dieses Aggregat zusätzliche Performance-Kapazität verfügbar ist. In diesem Beispiel wird der *optimale Punkt* als Punkt identifiziert, an dem das Aggregat bei einer Auslastung von 80 % und einer Latenz von 2.0 ms/op. Liegt Somit können Sie diesem Aggregat auch mehr Volumes und LUNs hinzufügen, sodass Ihre Systeme effizienter genutzt werden.

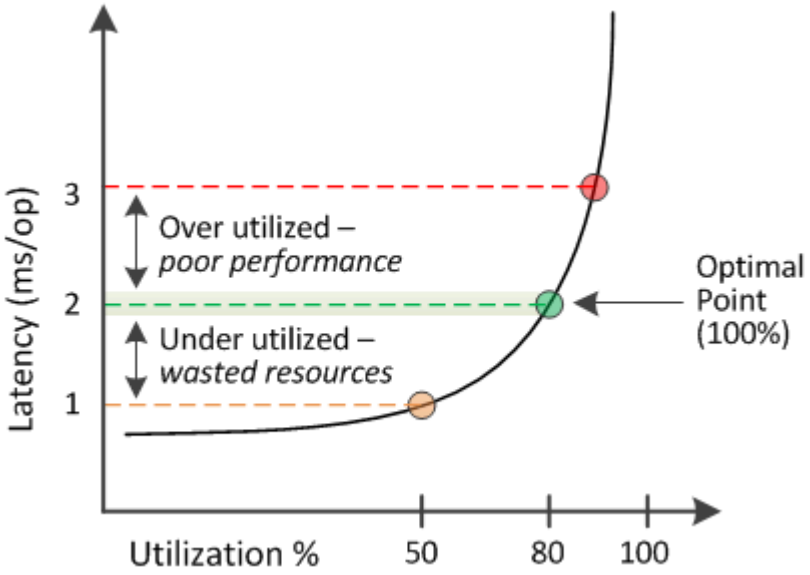
Der verwendete Zähler für die Performance-Kapazität soll eine größere Zahl sein als der Zähler „`Auslastung`“, da die Performance-Kapazität die Auswirkungen auf die Latenz hinzufügt. Wenn beispielsweise ein Node oder Aggregat zu 70 % genutzt wird, kann der Wert für die Performance-Kapazität je nach Latenzwert im Bereich von 80 % bis 100 % liegen.

In einigen Fällen kann der Auslastungszähler jedoch höher auf der Seite Dashboards/Leistung sein. Dies ist normal, da das Dashboard die aktuellen Zählerwerte zu jedem Erfassungszeitraum aktualisiert. Es werden die Durchschnittswerte über einen Zeitraum nicht angezeigt, wie die anderen Seiten in der Benutzeroberfläche von Unified Manager. Der verwendete Zähler für die Performance-Kapazität dient am besten als Indikator für die über einen Zeitraum gemittelte Performance, während der Auslastungszähler am besten zur Ermittlung der unmittelbaren Nutzung einer Ressource genutzt wird.

Was der Wert der verwendeten Performance-Kapazität bedeutet

Der von Performance genutzte Wert hilft Ihnen dabei, die Nodes und Aggregate zu identifizieren, die derzeit zu stark ausgelastet sind oder nicht ausgelastet sind. Auf diese Weise können Sie Workloads neu verteilen, um die Effizienz der Storage-Ressourcen zu steigern.

Die folgende Abbildung zeigt die Latenz im Vergleich zur Auslastungskurve einer Ressource und identifiziert mit farbigen Punkten drei Bereiche, in denen sich der aktuelle betriebliche Punkt befinden könnte.



- Ein Prozentsatz der genutzten Performance-Kapazität gleich 100 ist am optimalen Punkt.

  Die Ressourcen werden jetzt effizient genutzt.

- Ein Prozentsatz an Performance, der höher als 100 ist, bedeutet, dass der Node oder das Aggregat zu stark ausgelastet ist und dass Workloads eine suboptimale Performance erhalten.

  Der Ressource sollten keine neuen Workloads hinzugefügt werden, die bestehende Workloads müssen eventuell neu verteilt werden.

- Ein Prozentsatz an Performance-Kapazität unter 100 zeigt an, dass der Node oder das Aggregat nicht ausgelastet ist und dass die Ressourcen nicht effizient genutzt werden.

  Der Ressource können weitere Workloads hinzugefügt werden.

Im Gegensatz zur Auslastung kann die genutzte Performance-Kapazität über 100 % liegen. Es gibt keinen maximalen Prozentsatz, aber Ressourcen werden in der Regel zwischen 110 % und 140 % liegen, wenn sie überausgelastet sind. Höhere Prozentsätze deuten auf eine Ressource mit schwerwiegenden Problemen hin.

Was verfügbar ist, ist IOPS

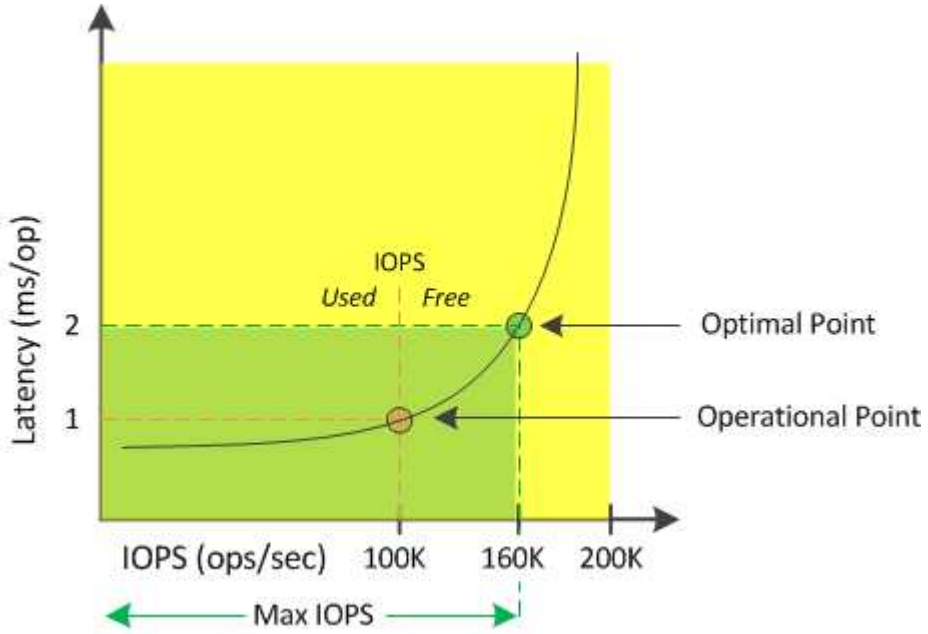
Der verfügbare IOPS-Zähler ermittelt die verbleibende Anzahl an IOPS, die einem Node oder Aggregat hinzugefügt werden kann, bevor die Ressource ihr Limit erreicht. Die gesamten IOPS, die ein Node bereitstellen kann, basieren auf den physischen Eigenschaften des Node, beispielsweise auf der Anzahl der CPUs, der CPU-Geschwindigkeit und dem RAM-Umfang. Die gesamten IOPS, die ein Aggregat bereitstellen kann, basieren auf den physischen Eigenschaften der Festplatten, zum Beispiel auf einer SATA-, SAS- oder SSD-Festplatte.

Während der freie Zähler für Performance-Kapazität den Prozentsatz einer noch verfügbaren Ressource angibt, liefert der verfügbare IOPS-Zähler genau die Anzahl der IOPS (Workloads) für eine Ressource, bevor sie die maximale Performance-Kapazität erreicht.

Wenn Sie beispielsweise zwei Storage-Systeme FAS2520 und FAS8060 nutzen, erhalten Sie bei einem Performance-Kapazitätswert von 30 % auch freie Performance-Kapazität. Dieser Wert bietet jedoch keine Übersicht darüber, wie viele Workloads auf diesen Nodes implementiert werden können. Der verfügbare IOPS-Zähler zeigt möglicherweise, dass bei der FAS8060 500 verfügbare IOPS verfügbar sind, bei der FAS2520 jedoch nur 100 verfügbare IOPS.

Verfügbare IOPS-Daten sind nur verfügbar, wenn die Nodes in einem Cluster mit der Software ONTAP 9.0 oder höher installiert sind.

Die folgende Abbildung zeigt eine Beispiellatenz im Vergleich zur IOPS-Kurve für einen Node.



Die maximale Anzahl an IOPS, die eine Ressource liefern kann, ist die Anzahl der IOPS, wenn der Zähler für die Performance-Kapazität bei 100 % liegt (der optimale Punkt). Der Betriebspunkt identifiziert, dass der Node

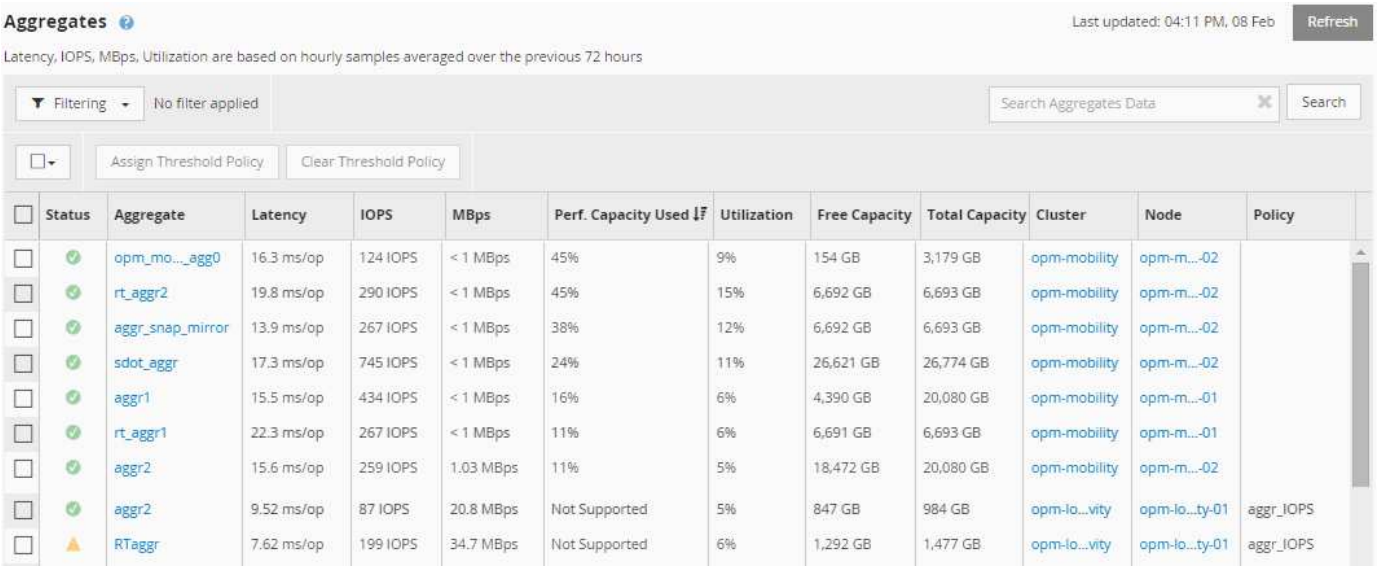
derzeit bei 100.000 IOPS mit einer Latenz von 1.0 ms/op arbeitet Auf der Grundlage der vom Node erfassten Statistiken ermittelt Unified Manager, dass die maximalen IOPS für den Node 160.000 beträgt, was bedeutet, dass 60.000 freie oder verfügbare IOPS vorhanden sind. Daher können Sie diesem Node weitere Workloads hinzufügen, sodass die Systeme effizienter genutzt werden.

Wenn die Ressource minimale Benutzeraktivitäten hat, wird der verfügbare IOPS-Wert unter Annahme eines allgemeinen Workloads auf Grundlage von etwa 4,500 IOPS pro CPU-Kern berechnet. Das liegt daran, dass Unified Manager nicht über die Daten verfügt, um die Eigenschaften des Workloads, der bereitgestellt werden soll, exakt abzuschätzen.

Anzeigen der verwendeten Werte für die Node- und Aggregat-Performance

Sie können die verwendeten Werte für die Performance-Kapazität für alle Nodes oder für alle Aggregate in einem Cluster überwachen oder Details für einen einzelnen Node oder Aggregat anzeigen.

Die verwendeten Werte für die Performance-Kapazität werden auf der Seite Performance Dashboard, auf den Seiten Performance Inventory, Top Performers, Create Threshold Policy, auf den Seiten Performance Explorer und in Detaildiagrammen angezeigt. Beispielsweise enthält die Seite „Performance/Aggregate Inventory“ eine Spalte „Perf“. Kapazität zur Anzeige des verwendeten Werts für die Performance-Kapazität aller Aggregate.



Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS
	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS

Der Status „`N/A`“ wird angezeigt, wenn Nodes nicht mit der Software ONTAP 9.0 oder höher installiert wurden.

Durch das Monitoring des verwendeten Zählers für die Performance-Kapazität können Sie Folgendes identifizieren:

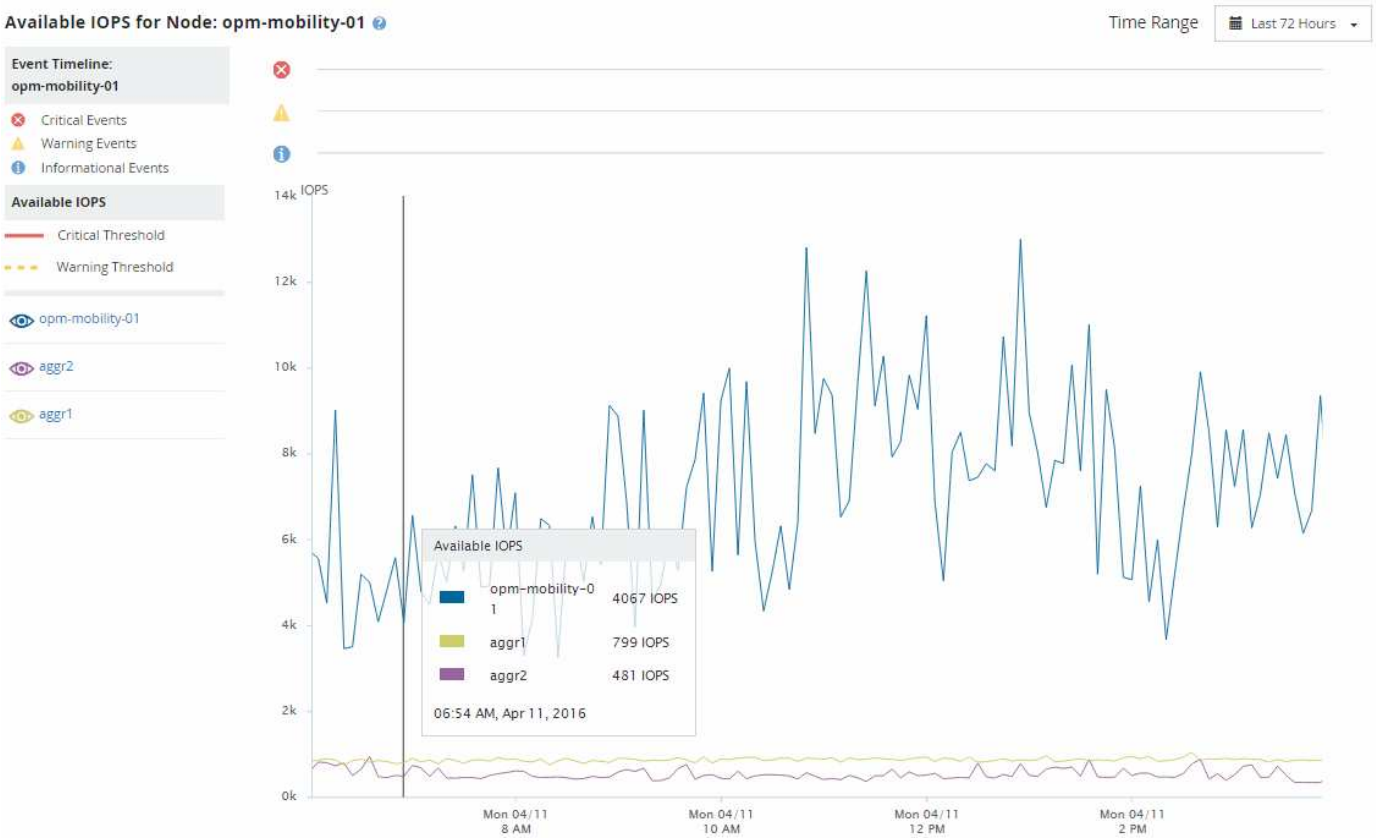
- Unabhängig davon, ob Nodes oder Aggregate auf jedem Cluster einen hohen Wert an Performance-Kapazität aufweisen
- Gibt an, ob Nodes oder Aggregate auf beliebigen Clustern über Ereignisse mit aktiver Performance-Kapazität verfügen
- Die Nodes und Aggregate verfügen über die in einem Cluster genutzte Kapazität mit der höchsten und niedrigsten Performance
- Zählerwerte im Bereich Latenz und Auslastung in Verbindung mit Nodes oder Aggregaten mit hohen Werten im Bereich der Performance-Kapazität

- Auswirkungen auf die verwendete Performance-Kapazität für Nodes in einem HA-Paar auf einen Node, wenn einer der Nodes ausfällt
- Die am stärksten ausgelasteten Volumes und LUNs auf einem Aggregat mit hoher Performance-Kapazität

Anzeigen der verfügbaren IOPS-Werte für Node und Aggregat

Sie können die verfügbaren IOPS-Werte für alle Nodes und alle Aggregate in einem Cluster überwachen. Alternativ können Sie Details zu einem einzelnen Node oder Aggregat anzeigen.

Verfügbare IOPS-Werte werden in den Performance Explorer-Seitendiagrammen angezeigt. Wenn Sie beispielsweise einen Node auf der Seite „Performance/Node Explorer“ anzeigen, können Sie das Zählerdiagramm „`verfügbare IOPS`“ in der Liste auswählen, damit Sie die verfügbaren IOPS-Werte für mehrere Aggregate auf diesem Node vergleichen können.



Durch das Monitoring des verfügbaren IOPS-Zählers können Sie Folgendes identifizieren:

- Die Nodes oder Aggregate mit den höchsten verfügbaren IOPS-Werten unterstützen Sie bei der Entscheidung, wo zukünftige Workloads implementiert werden können.
- Die Nodes oder Aggregate mit den kleinsten verfügbaren IOPS-Werten, um die zu überwachenden Ressourcen auf potenzielle künftige Performance-Probleme zu identifizieren.
- Die am stärksten ausgelasteten Volumes und LUNs auf einem Aggregat mit kleinem verfügbaren IOPS-Wert.

Anzeigen von Zählerdiagrammen zur Performance-Kapazität zur Erkennung von Problemen

Auf der Seite „Performance Explorer“ können Sie die verwendeten Performance-Kapazitäten für Nodes und Aggregate anzeigen. Damit können Sie detaillierte Performance-Kapazitätsdaten für die ausgewählten Nodes und Aggregate für einen bestimmten Zeitraum anzeigen.

Über diese Aufgabe

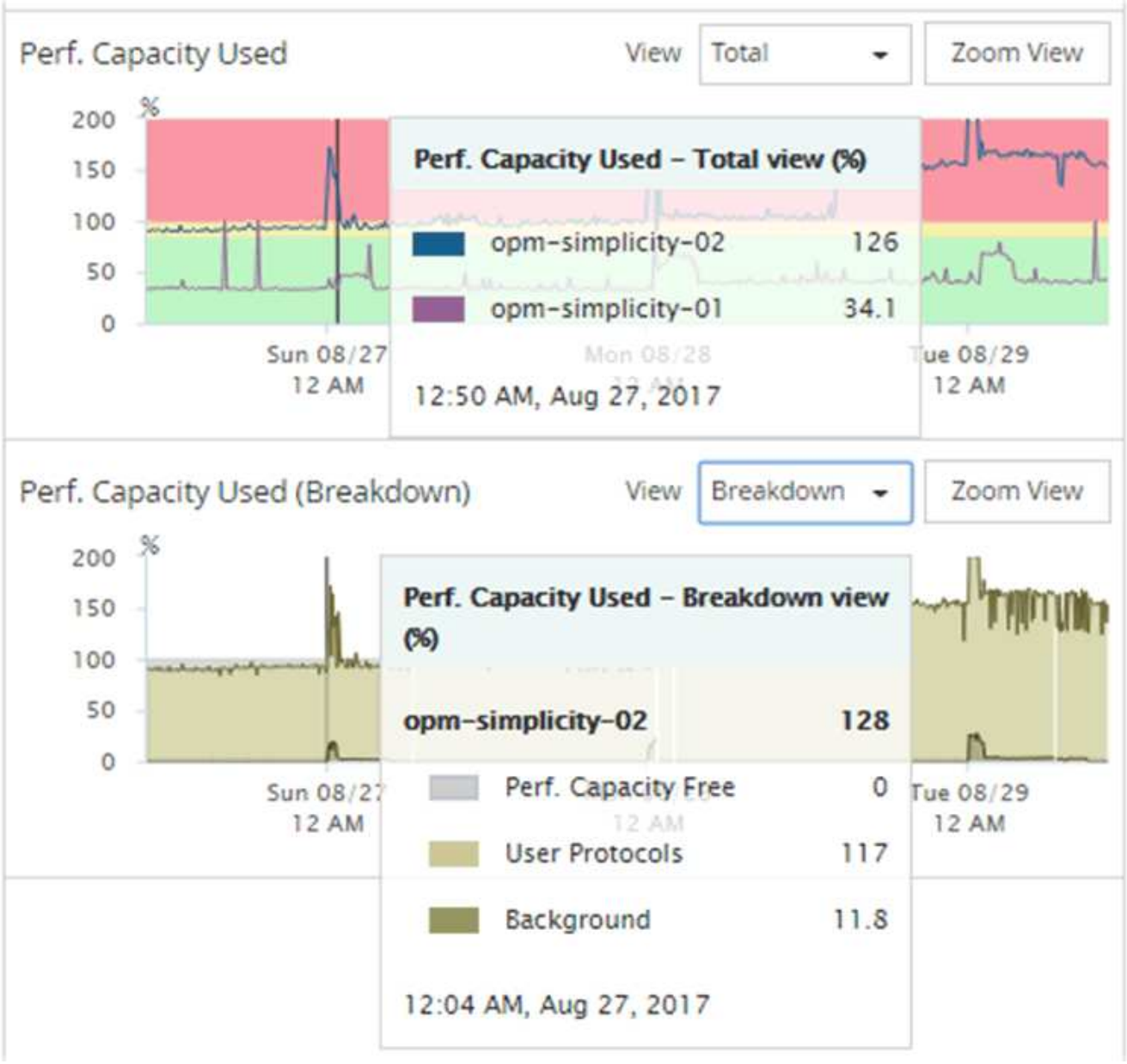
Das Standard-Zählerdiagramm zeigt die Werte der verwendeten Performance-Kapazität für die ausgewählten Nodes oder Aggregate an. Das Counter Chart Breakdown zeigt die Werte für die Gesamtkapazität des Root-Objekts an, das basierend auf Benutzerprotokollen und Hintergrundsystemprozessen in die Nutzung unterteilt ist. Darüber hinaus wird die Menge der freien Performance-Kapazität dargestellt.

Da einige Hintergrundaktivitäten zu System- und Datenmanagement als Benutzer-Workloads identifiziert und als Benutzerprotokolle kategorisiert werden, erscheint der Prozentsatz der Benutzerprotokolle künstlich hoch, wenn diese Prozesse ausgeführt werden. Diese Prozesse laufen normalerweise um Mitternacht, wenn die Cluster-Nutzung gering ist. Wenn bei der Durchführung von Benutzerprotokollen um Mitternacht eine Spitze sichtbar ist, überprüfen Sie, ob Cluster-Backup-Jobs oder andere Hintergrundaktivitäten zu diesem Zeitpunkt konfiguriert wurden.

Schritte

1. Wählen Sie die **Explorer** Registerkarte von einem Knoten oder Aggregat * Landing* Seite.
2. Klicken Sie im Fenster **Counter Charts** auf **Choose Charts** und wählen Sie dann die Option *Perf. Diagramm „verwendete Kapazität“.
3. Blättern Sie nach unten, bis Sie das Diagramm anzeigen können.

   Die Farben des Standarddiagramms zeigen an, wenn sich das Objekt im optimalen Bereich (gelb) befindet, wenn das Objekt nicht ausgelastet ist (grün) und wenn das Objekt überausgelastet ist (rot). Das Diagramm zeigt detaillierte Performance-Kapazitätsdetails nur für das Root-Objekt.



4. Wenn Sie eine Karte in einem vollen Format anzeigen möchten, klicken Sie auf **Zoom View**.

   Auf diese Weise können Sie mehrere Zählerdiagramme in einem separaten Fenster öffnen, um die genutzte Performance-Kapazität mit IOPS- oder MB/s-Werten im gleichen Zeitraum zu vergleichen.

Performance-Kapazität nutzte Schwellenwertbedingungen für die Performance

Sie können benutzerdefinierte Performance-Schwellenwertrichtlinien erstellen, damit Ereignisse ausgelöst werden, wenn der für einen Node oder ein Aggregat genutzte Performance-Wert die festgelegte Einstellung für den verwendeten Schwellenwert für die Performance-Kapazität überschreitet.

Außerdem können Nodes mit einem Schwellenwert von „`Performance Capacity used Takeover`“ konfiguriert werden. Diese Schwellenwertrichtlinie gibt die für beide Nodes verwendeten Performance-Statistiken in einem HA-Paar an und ermittelt, ob einem der beiden Nodes genügend Kapazität fehlen würde, wenn der andere Node ausfällt. Da der Workload während des Failover` Kombination der Workloads der

beiden Partner-Nodes ist, kann die gleiche Performance-Kapazität, die für eine Übernahme verwendet wird, auf beide Nodes angewendet werden.

> Die genutzte Performance-Kapazität entspricht der Leistung im Allgemeinen den Nodes. Ist der Node-übergreifende Datenverkehr jedoch über seinen Failover-Partner für einen der Nodes vorgesehen, kann die Gesamt-Performance, die bei der Ausführung aller Workloads auf einem Partner-Node verwendet wird, auf einem anderen Partner-Node geringfügig anders sein – je nachdem, welcher Node ausgefallen ist.

Die verwendeten Performance-Kapazitäten können auch als sekundäre Performance-Schwellenwerteinstellungen verwendet werden, um bei der Definition von Schwellenwerten für LUNs und Volumes eine kombinierte Schwellenwertrichtlinie zu erstellen. Die verwendete Performance-Kapazität wird auf das Aggregat oder den Node angewendet, auf dem sich das Volume oder die LUN befindet. Sie können beispielsweise anhand der folgenden Kriterien eine kombinierte Schwellenwertrichtlinie erstellen:

Storage Objekt	Performance-Zähler	Warnschwellenwert	Kritischer Schwellenwert	Dauer
Datenmenge	Latenz	15 ms/OP	25 ms/OP	20 Minuten

Aufgrund von Grenzwertrichtlinien wird ein Ereignis nur erzeugt, wenn beide Bedingungen während der gesamten Dauer nicht erfüllt werden.

Verwenden der Performance-Kapazität, die zum Managen der Performance verwendet wird

In der Regel möchten Unternehmen mit einer Performance-Kapazität von unter 100 Prozent betreiben, um die Ressourcen effizient zu nutzen und gleichzeitig zusätzliche Performance-Kapazitäten zu reservieren, um Spitzenlasten zu erzielen. Anhand von Schwellenwertrichtlinien kann angepasst werden, wenn Warnmeldungen gesendet werden, um hohe Werte für die verwendete Kapazität zu erreichen.

Sie können bestimmte Ziele basierend auf Ihren Performance-Anforderungen festlegen. So könnten Finanzdienstleister mehr Performance-Kapazität reservieren, um eine zeitnahe Ausführung von Transaktionen zu gewährleisten. Diese Unternehmen möchten möglicherweise Schwellenwerte für die verwendete Performance-Kapazität im Bereich von 70-80 Prozent festlegen. Produzierende Unternehmen mit geringeren Margen können sich für weniger Performance-Kapazität entscheiden, wenn sie bereit sind, Performance zu riskieren, um DIE IT-Kosten besser zu managen. Diese Unternehmen können Grenzwerte für die verwendete Performance-Kapazität im Bereich von 85-95 Prozent festlegen.

Wenn der verwendete Wert für die Performance-Kapazität den in einer benutzerdefinierten Schwellenwertrichtlinie festgelegten Prozentsatz überschreitet, sendet Unified Manager eine Alarm-E-Mail und fügt das Ereignis zur Seite „Ereignisbestand“ hinzu. Auf diese Weise lassen sich potenzielle Probleme verwalten, bevor sie die Performance beeinträchtigen. Diese Ereignisse können auch als Indikatoren verwendet werden, an denen Sie Workloads und Änderungen innerhalb Ihrer Nodes und Aggregate vornehmen müssen.

Verstehen und Verwenden der Seite Node Failover Planning

Die Seite „Performance/Node Failover Planning“ schätzt die Auswirkungen auf die Performance eines Node, wenn der hochverfügbare Partner-Node des Node ausfällt. Die

Schätzungen von Unified Manager beruhen auf der historischen Performance von Nodes im HA-Paar.

Die Schätzung der Auswirkungen auf die Performance bei einem Failover hilft Ihnen, die folgenden Szenarien zu planen:

- Wenn ein Failover die geschätzte Performance des übernehmenden Node immer wieder auf ein nicht akzeptables Niveau verschlechtert, können Sie Korrekturmaßnahmen ergreifen, um die Performance-Beeinträchtigung aufgrund eines Failover zu verringern.
- Vor dem Initiieren eines manuellen Failover zur Durchführung von Hardwarewartungsaufgaben können Sie einschätzen, welche Auswirkungen der Failover auf die Performance des Takeover-Nodes hat, um den optimalen Zeitpunkt für die Durchführung der Aufgabe zu bestimmen.

Verwenden der Seite Knoten-Failover-Planung, um Korrekturmaßnahmen zu ermitteln

Basierend auf den Informationen, die auf der Seite „Performance/Node Failover Planning“ angezeigt werden, können Sie Maßnahmen ergreifen, um sicherzustellen, dass ein Failover nicht dazu führt, dass die Performance eines HA-Paars unter eine akzeptable Ebene fällt.

Um beispielsweise die geschätzten Performance-Auswirkungen eines Failover zu verringern, können Sie einige Volumes oder LUNs von einem Node im HA-Paar auf andere Nodes im Cluster verschieben. So wird sichergestellt, dass der primäre Node nach einem Failover weiterhin eine akzeptable Performance liefern kann.

Komponenten der Seite Knoten-Failover-Planung

Die Komponenten der Seite Performance/Node Failover Planning werden in einem Raster und im Fenster Comparing angezeigt. In diesen Abschnitten können Sie die Auswirkungen eines Node-Failovers auf die Performance des Takeover-Nodes bewerten.

Das Raster der Performance-Statistiken

Auf der Seite „Performance/Node-Failover-Planung“ wird ein Raster mit Statistiken zu Latenz, IOPS, Auslastung und Performance-Kapazität angezeigt.

> Die IOPS-Werte, die auf dieser Seite und auf der Seite „Performance/Node Performance Explorer“ angezeigt werden, sind möglicherweise nicht dieselben.

Im Raster ist jedem Node eine der folgenden Rollen zugewiesen:

- Primär

  Der Node, der beim Ausfall des Partners für den HA-Partner übernimmt. Das Root-Objekt ist immer der primäre Node.

- Partner

  Der Node, der im Failover-Szenario ausfällt.

- Geschätzte Übernahme

  Das gleiche wie der primäre Knoten. Für diesen Node angezeigte Performance-Statistiken zeigen die Performance des Takeover-Node, nachdem der ausgefallene Partner übernommen wurde.

> Obwohl der Workload des Takeover-Node den kombinierten Workloads beider Nodes nach einem Failover entspricht, wurden die Statistiken für den geschätzten Takeover-Node nicht als Summe der Statistiken des primären Nodes und des Partner-Nodes angezeigt. Wenn zum Beispiel die Latenz des primären Node 2 ms/op beträgt und die Latenz des Partnerknotens 3 ms/op beträgt, kann der geschätzte Übernahmeknoten eine Latenz von 4 ms/op haben Dieser Wert ist eine Berechnung, die Unified Manager durchführt.

Sie können auf den Namen des Partner-Knotens klicken, wenn er das Root-Objekt werden soll. Nachdem die Seite Performance/Node Performance Explorer angezeigt wurde, können Sie auf die Registerkarte **Failover Planning** klicken, um zu sehen, wie sich die Leistung in diesem Ausfallszenario ändert. Wenn beispielsweise Node1 der primäre Node und Node2 der Partner-Node ist, können Sie auf Node2 klicken, um ihn zum primären Node zu machen. Auf diese Weise sehen Sie, wie sich die geschätzte Performance je nach dem Ausfall des Node ändert.

Teilfenster „Vergleichen“

In der folgenden Liste werden die im Teilfenster „Vergleich“ angezeigten Komponenten standardmäßig beschrieben:

- **Veranstaltungsdiagramme**

  Sie werden im gleichen Format wie auf der Seite Performance/Node Performance Explorer angezeigt. Sie beziehen sich nur auf den primären Node.

- **Counter-Charts**

  Sie zeigen historische Statistiken für den im Raster angezeigten Performance-Zähler an. In jedem Diagramm wird im Diagramm für den geschätzten Takeover-Node die geschätzte Performance angezeigt, wenn ein Failover zu einem bestimmten Zeitpunkt aufgetreten ist.

  Angenommen, das Auslastungsdiagramm zeigt 73 % des Node Estimated Takeover um 11:00 Uhr an Am 8. Februar. Wenn zu diesem Zeitpunkt ein Failover aufgetreten wäre, hätte die Auslastung des Takeover-Nodes 73 % betragen.

  Anhand der historischen Statistiken finden Sie den optimalen Zeitpunkt für das Initiieren eines Failover und minimieren so das Risiko einer Überlastung des Takeover-Nodes. Sie können einen Failover nur zu Zeiten planen, in denen die prognostizierte Performance des Takeover-Node akzeptabel ist.

Standardmäßig werden Statistiken sowohl für das Root-Objekt als auch für den Partner-Node im Teilfenster „Vergleichen“ angezeigt. Anders als auf der Seite Performance/Node Performance Explorer zeigt diese Seite nicht die Schaltfläche **Hinzufügen** an, um Objekte zum Statistikvergleich hinzuzufügen.

Sie können das vergleichende Fenster auf die gleiche Weise anpassen wie auf der Seite Performance/Node Performance Explorer. Die folgende Liste zeigt Beispiele zur Anpassung der Diagramme:

- Klicken Sie auf einen Node-Namen, um die Statistiken des Node in den Zählerdiagrammen anzuzeigen oder zu verbergen.
- Klicken Sie auf **Zoom-Ansicht**, um ein detailliertes Diagramm für einen bestimmten Zähler in einem neuen

Fenster anzuzeigen.

Verwenden einer Schwellenwertrichtlinie auf der Seite Knoten-Failover-Planung

Sie können eine Node-Schwellenwertrichtlinie erstellen, sodass Sie auf der Seite „Performance/Node Failover Planning“ eine Benachrichtigung erhalten können, wenn ein potenzieller Failover die Performance des Takeover-Node auf ein inakzeptables Maß verschlechtert.

Die vom System definierte Performance-Schwellenwertrichtlinie „`Node HA-Paar Overused`“ erzeugt ein Warnereignis, wenn der Schwellenwert für sechs aufeinanderfolgende Erfassungszeiträume (30 Minuten) überschritten wird. Der Schwellenwert ist dann nicht erreicht, wenn die kombinierte Performance-Kapazität, die von den Nodes in einem HA-Paar genutzt wird, 200 % überschreitet.

Das Ereignis der vom System definierten Schwellenwertrichtlinie gibt Ihnen Warnungen vor, dass ein Failover dazu führt, dass die Latenz des Takeover-Node auf ein inakzeptables Maß erhöht wird. Wenn ein Ereignis, das von dieser Richtlinie für einen bestimmten Node generiert wird, angezeigt wird, können Sie zur Seite Performance/Node-Failover-Planung für diesen Node wechseln, um den prognostizierten Latenzwert aufgrund eines Failover anzuzeigen.

Zusätzlich zur Nutzung dieser systemdefinierten Schwellenwertrichtlinie können Sie unter Verwendung des Zählers „`Performance Capacity Used - Takeover`“ Schwellenwertrichtlinien erstellen und die Richtlinie dann auf ausgewählte Nodes anwenden. Wenn Sie einen Schwellenwert von weniger als 200 % angeben, erhalten Sie ein Ereignis, bevor der Schwellenwert für die vom System definierte Richtlinie nicht erreicht wird. Sie können auch den Mindestzeitraum angeben, für den der Schwellenwert auf weniger als 30 Minuten überschritten wird, wenn Sie benachrichtigt werden möchten, bevor das vom System definierte Richtlinienereignis generiert wird.

Sie können beispielsweise eine Schwellenwertrichtlinie zur Generierung eines Warnungsereignisses definieren, wenn die kombinierte Performance-Kapazität der Nodes in einem HA-Paar mehr als 10 Minuten lang 175 % überschreitet. Sie können diese Richtlinie auf Node1 und Node2 anwenden, die ein HA-Paar bilden. Nachdem Sie eine Warnmeldung für Node1 oder Node2 erhalten haben, können Sie die Seite Performance/Node-Failover-Planung für diesen Node anzeigen, um die geschätzten Performance-Auswirkungen auf den Takeover-Node einzuschätzen. Sie können Korrekturmaßnahmen ergreifen, um bei einem Failover einen Überlastung des Takeover-Node zu vermeiden. Wenn Sie Maßnahmen ergreifen, wenn die kombinierte Performance-Kapazität, die von den Nodes verwendet wird, unter 200 % liegt, erreicht die Latenz des Ersatz-Node nicht ein inakzeptables Maß, selbst wenn in diesem Zeitraum ein Failover stattfindet.

Verwenden des Leistungsdiagramms zur verwendeten Kapazität zur Failover-Planung

Das Diagramm „Detailed Performance Capacity Used – Breakdown“ zeigt die für den primären Knoten und den Partner-Knoten verwendete Performance-Kapazität an. Er zeigt außerdem die Menge der freien Performance-Kapazität auf dem geschätzten Takeover-Node an. Anhand dieser Informationen können Sie ermitteln, ob bei einem Ausfall des Partner-Node möglicherweise ein Performance-Problem auftritt.

Über diese Aufgabe

Neben der Anzeige der Gesamt-Performance-Kapazität, die für die Nodes verwendet wird, unterteilt das Diagramm die Werte für jeden Knoten in Benutzerprotokolle und Hintergrundprozesse.

- Benutzerprotokolle sind die I/O-Vorgänge von Benutzerapplikationen auf und vom Cluster.
- Hintergrundprozesse sind interne Systemprozesse, die mit Storage-Effizienz, Datenreplizierung und Systemzustand verknüpft sind.

Mit dieser zusätzlichen Detailebene können Sie ermitteln, ob ein Performance-Problem auf Benutzerapplikationsaktivitäten oder auf System-Prozessen im Hintergrund verursacht wird, wie Deduplizierung, RAID rekonstruieren, Festplatte Schrubben und SnapMirror Kopien.

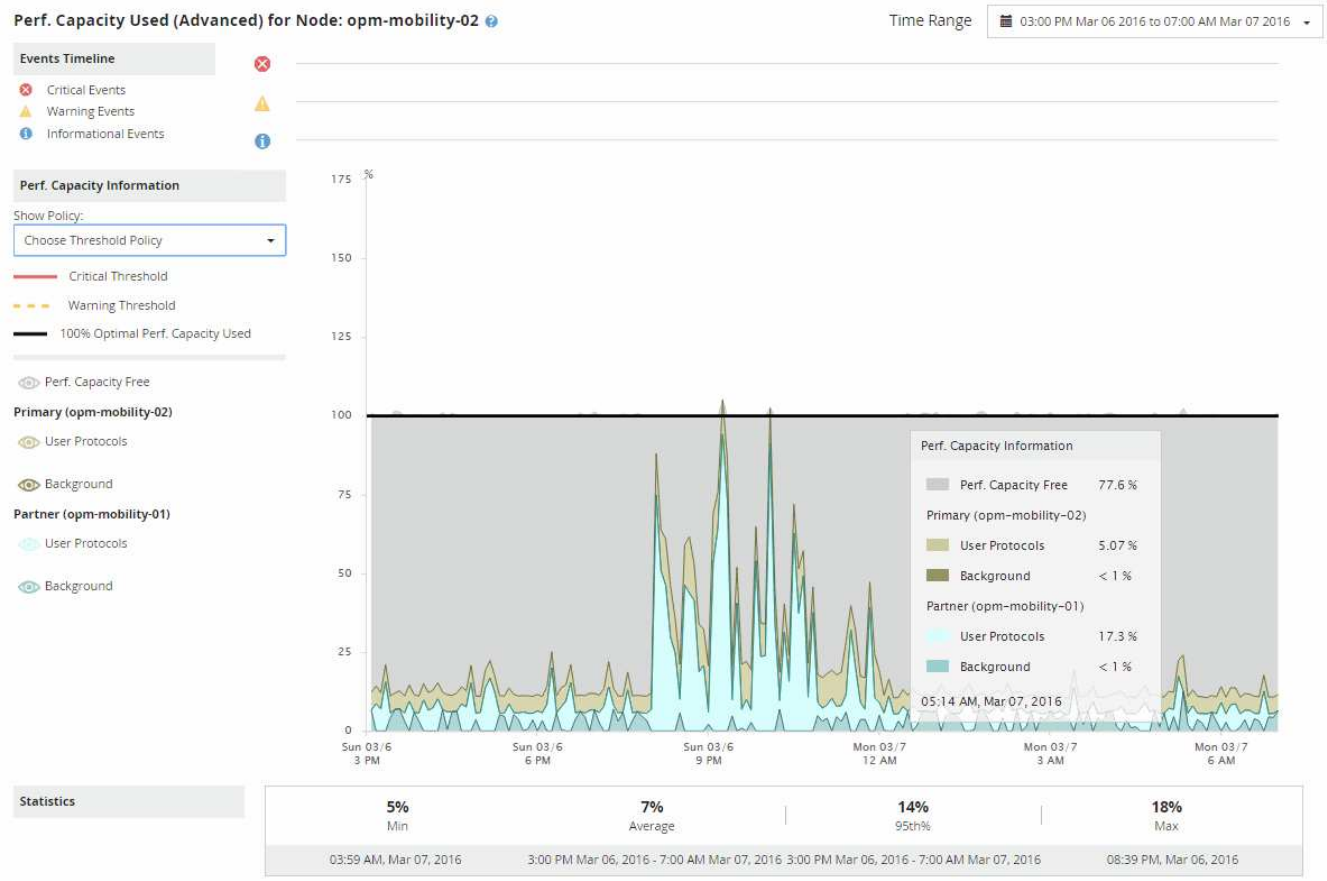
Schritte

1. Wechseln Sie zur Seite **Leistung/Knoten-Failover-Planung** für den Knoten, der als Geschätzter Übernahmeknoten dient.
2. Wählen Sie im Auswahlfeld **Zeitbereich** den Zeitraum aus, für den die historischen Statistiken im Zählerraster und in den Zählerdiagrammen angezeigt werden.

   Die Zählerdiagramme mit den Statistiken für den primären Node, den Partner-Node und den geschätzten Takeover-Node werden angezeigt.

3. Wählen Sie aus der Liste **Choose Charts** die Option **Perf. Verwendete Kapazität**.
4. Im **Perf. Verwendete Kapazität** Diagramm, wählen Sie **Breakdown** und klicken Sie auf **Zoom View**.

   Das detaillierte Diagramm für Perf. Die verwendete Kapazität wird angezeigt.



5. Bewegen Sie den Cursor über das detaillierte Diagramm, um die Informationen zur verwendeten Performance-Kapazität im Popup-Fenster anzuzeigen.

   Die Perf. Der freie Prozentsatz der Kapazität ist die am geschätzten Takeover-Node verfügbare

Performance-Kapazität. Es zeigt an, wie viel Performance-Kapazität nach einem Failover auf dem Takeover-Node übrig ist. Wenn der Wert 0 % beträgt, erhöht ein Failover die Latenz auf ein inakzeptables Level auf dem Takeover-Node.

6. Ziehen Sie Korrekturmaßnahmen in Betracht, um einen freien Prozentsatz bei niedriger Performance-Kapazität zu vermeiden.

   Wenn Sie einen Failover für eine Node-Wartung initiieren möchten, wählen Sie eine Zeit zum Fehlschlagen des Partner-Node aus, wenn der freie Prozentsatz der Performance-Kapazität nicht bei 0 ist.

Erfassung von Daten und Monitoring der Workload-Performance

Unified Manager erfasst und analysiert Workload-Aktivitäten alle 5 Minuten, um Performance-Ereignisse zu identifizieren und Konfigurationsänderungen alle 15 Minuten zu erkennen. Es werden maximal 30 Tage 5 vergangener Performance- und Ereignisdaten aufbewahrt. Anhand dieser Daten wird der erwartete Bereich für alle überwachten Workloads prognostiziert.

> In diesem Kapitel wird beschrieben, wie dynamische Schwellenwerte funktionieren und wie sie zur Überwachung der Workload-Performance eingesetzt werden. Dieses Kapitel gilt nicht für Statistiken oder Ereignisse, die durch benutzerdefinierte oder systemdefinierte Leistungsschwellenwerte entstehen.

Unified Manager muss die Workload-Aktivität mindestens 3 Tage lang sammeln, bevor sie mit der Analyse beginnen kann. Vor dem erwarteten Bereich für I/O-Reaktionszeiten und Vorgänge kann auf der Seite Performance/Volume Details und auf der Seite Event Details angezeigt werden. Während diese Aktivität erfasst wird, werden im erwarteten Bereich nicht alle Änderungen angezeigt, die von der Workload-Aktivität auftreten. Nach der Erfassung von 3 Tagen Aktivität passt Unified Manager den erwarteten Bereich alle 24 Stunden um 12:00 Uhr an, um Workload-Aktivitätsänderungen zu berücksichtigen und einen präziseren Leistungsschwellenwert festzulegen.

In den ersten 4 Tagen, an denen Unified Manager ein Volume überwacht, werden die Diagramme auf der Seite Performance/Volume Details nicht den erwarteten Bereich für dieses Volume angezeigt, wenn mehr als 24 Stunden seit der letzten Datenerfassung vergangen sind. Ereignisse, die vor der letzten Sammlung erkannt wurden, sind weiterhin verfügbar.

> Bei der Sommerzeit (Sommerzeit) wird die Systemzeit geändert, wodurch der erwartete Bereich der Performance-Statistiken für überwachte Workloads verändert wird. Unified Manager beginnt sofort mit der Korrektur des erwarteten Bereichs, der ungefähr 15 Tage dauert. In dieser Zeit können Sie Unified Manager weiterhin verwenden. Da Unified Manager jedoch den erwarteten Bereich zum Erkennen von Ereignissen verwendet, sind einige Ereignisse möglicherweise nicht korrekt. Ereignisse, die vor der Zeitänderung erkannt wurden, werden nicht beeinträchtigt. Wenn Sie die Zeit auf einem Cluster oder auf einem Unified Manager-Server zu einem früheren Zeitpunkt manuell ändern, wirkt sich dies auch auf die Ergebnisse der Ereignisanalyse aus.

Arten von Workloads, die von Unified Manager überwacht werden

Mit Unified Manager lässt sich die Performance von zwei Workload-Typen überwachen: Benutzerdefiniert und systemdefiniert.

- ***benutzerdefinierte Workloads***

  Der I/O-Durchsatz von Applikationen zum Cluster. Dies sind Prozesse, die an Lese- und Schreibanfragen beteiligt sind. Ein FlexVol Volume oder FlexGroup Volume ist ein benutzerdefinierter Workload.

  > Unified Manager überwacht nur die Workload-Aktivität auf dem Cluster. Er überwacht nicht die Applikationen, Clients oder Pfade zwischen den Applikationen und dem Cluster.

  Wenn eine oder mehrere der folgenden Optionen für einen Workload zutrifft, kann er nicht von Unified Manager überwacht werden:

  - Es handelt sich um eine Kopie der Datensicherung (DP) im schreibgeschützten Modus. (Beachten Sie, dass bei Verwendung von ONTAP 8.3 und höher DP-Volumes für vom Benutzer erzeugten Datenverkehr überwacht werden.)
  - Es handelt sich um ein Infinite Volume.
  - Ein offline-Datenklon.
  - Es handelt sich um ein gespiegeltes Volume in einer MetroCluster-Konfiguration.

- ***systemdefinierte Workloads***

  Zu den internen Prozessen, die mit Storage-Effizienz, Datenreplizierung und Systemzustand verbunden sind, gehören:

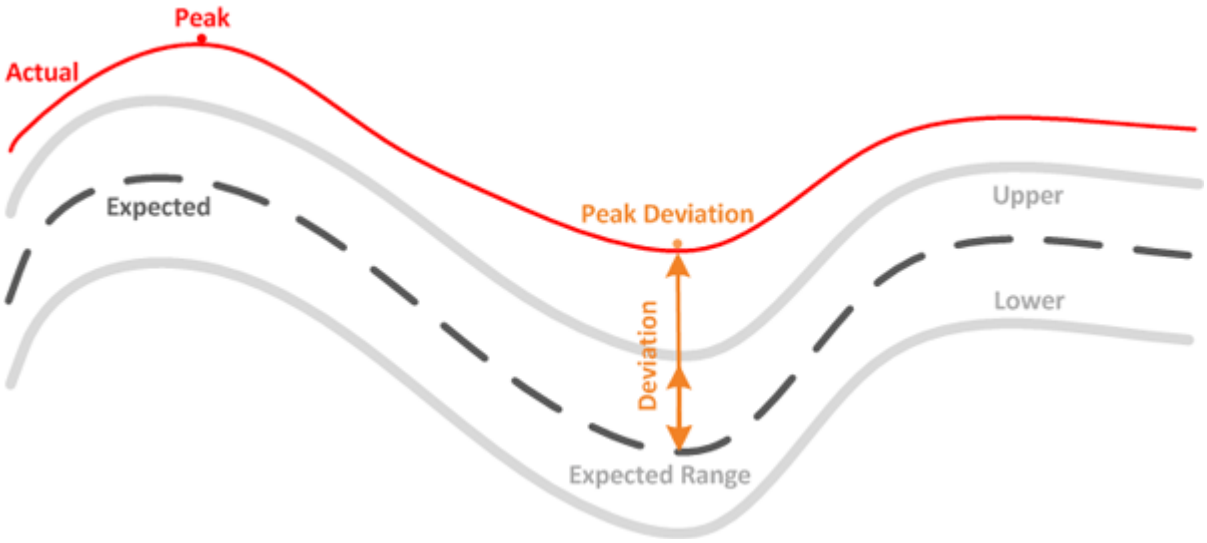
  - Storage-Effizienz, z. B. Deduplizierung
  - Der Zustand der Festplatte, einschließlich RAID-Rekonstruktion, Disk-Schrubben usw.
  - Datenreplizierung, z. B. SnapMirror Kopien
  - Management-Aktivitäten
  - Systemzustand des File-Systems, der verschiedene WAFL-Aktivitäten umfasst
  - Filesystem-Scanner, z. B. WAFL-Scan
  - Copy-Offload, z. B. Verlagerung von Storage-Effizienzvorgängen von VMware Hosts
  - Systemzustand, wie z. B. das Verschieben von Volumes, die Datenkomprimierung usw.
  - Nicht überwachte Volumes

Performance-Daten für systemdefinierte Workloads werden nur in der GUI angezeigt, wenn die von diesen Workloads verwendete Cluster-Komponente mit Konflikten belegt ist. Sie können beispielsweise nicht nach dem Namen eines systemdefinierten Workloads suchen, um dessen Performance-Daten in der GUI anzuzeigen. Wenn mehrere systemdefinierte Workloads desselben Typs angezeigt werden, wird dem Workload-Namen ein Buchstabe angehängt. Das Schreiben ist für die Verwendung durch das Supportpersonal bestimmt.

Messwerte für die Workload-Performance

Unified Manager misst die Performance von Workloads auf einem Cluster basierend auf historischen und erwarteten statistischen Werten, die den erwarteten Wertebereich für die Workloads bilden. Es vergleicht die tatsächlichen statistischen Workload-Werte mit dem erwarteten Bereich, um zu ermitteln, ob die Workload-Performance zu hoch oder zu niedrig ist. Ein Workload, der nicht den erwarteten Leistung entspricht, löst einen Performance-Ereignisbericht aus, damit Sie benachrichtigt werden.

In der folgenden Abbildung stellt der tatsächliche Wert in Rot die tatsächlichen Performance-Statistiken im Zeitrahmen dar. Der tatsächliche Wert hat den Leistungsschwellenwert überschritten, der die oberen Grenzen des erwarteten Bereichs darstellt. Der Peak ist der höchste ist-Wert im Zeitrahmen. Die Abweichung misst die Änderung zwischen den erwarteten Werten und den ist-Werten, während die Peak-Abweichung die größte Änderung zwischen den erwarteten Werten und den ist-Werten angibt.



In der folgenden Tabelle sind die Messwerte zur Workload-Performance aufgeführt.

Messung	Beschreibung
Aktivität	Der Prozentsatz des QoS-Limits, der von den Workloads in der Richtliniengruppe verwendet wird Wenn Unified Manager eine Änderung an einer Richtliniengruppe erkennt, z. B. das Hinzufügen oder Entfernen eines Volumes oder das Ändern des QoS-Limits, kann der tatsächliche und erwartete Wert 100 % des festgelegten Grenzwerts überschreiten. Wenn ein Wert 100 % des festgelegten Grenzwerts überschreitet, wird er als >100 % angezeigt. Wenn ein Wert kleiner als 1 % des festgelegten Grenzwerts ist, wird er als <1 % angezeigt.
Tatsächlich	Der messbare Performance-Wert zu einem bestimmten Zeitpunkt für einen bestimmten Workload.

Messung	Beschreibung
Abweichung	Die Änderung zwischen den erwarteten Werten und den ist-Werten. Es ist das Verhältnis des ist-Wertes minus dem erwarteten Wert zum oberen Wert des erwarteten Bereichs minus dem erwarteten Wert. Ein negativer Abweichungswert zeigt, dass die Workload-Performance niedriger ist als erwartet, während ein positiver Abweichungswert darauf hinweist, dass die Workload-Performance höher ist als erwartet. Wenn die erwarteten Werte und der ist-Wert sehr gering sind, z.B. in den Hundertstel oder Tausendstel eines Prozentwerts, wird in der Abweichung N/A angezeigt
Erwartet	Die erwarteten Werte basieren auf der Analyse historischer Performance-Daten für einen bestimmten Workload. Unified Manager analysiert diese statistischen Werte, um den erwarteten Wertebereich zu bestimmen.
Erwarteter Bereich	Der erwartete Wertebereich ist eine Prognose oder Vorhersage dessen, was die oberen und unteren Leistungswerte zu einem bestimmten Zeitpunkt erwartet werden. Bei der Workload-Latenz bilden die oberen Werte den Performance-Schwellenwert. Wenn der tatsächliche Wert den Performance-Schwellenwert überschreitet, löst Unified Manager eine Warnmeldung im Rahmen des Performance-Ereignisses aus.
Spitze	Der maximale Wert, der über einen Zeitraum gemessen wird.
Maximale Abweichung	Der maximale Abweichungswert, der über einen Zeitraum gemessen wird.
Warteschlangentiefe	Die Anzahl der ausstehenden I/O-Anfragen, die an der Interconnect-Komponente warten.

Messung	Beschreibung
Auslastung	Für die Netzwerkverarbeitung, Datenverarbeitung und aggregierte Komponenten ist der prozentuale Anteil der Auslastung während eines bestimmten Zeitraums an den Workload-Vorgängen beschäftigt. Beispielsweise der prozentuale Anteil der Zeit, die für die Netzwerkverarbeitung oder Datenverarbeitung erforderlich ist, um eine I/O-Anfrage zu bearbeiten, oder an ein Aggregat, um eine Lese- oder Schreibanforderung zu erfüllen.
Schreibdurchsatz	Der Schreibdurchsatz in Megabyte pro Sekunde (MB/s), von Workloads in einem lokalen Cluster zum Partner-Cluster in einer MetroCluster-Konfiguration.

Der erwartete Leistungsbereich

Der erwartete Wertebereich ist eine Prognose oder Vorhersage dessen, was die oberen und unteren Leistungswerte zu einem bestimmten Zeitpunkt erwartet werden. Bei der Workload-Latenz bilden die oberen Werte den Performance-Schwellenwert. Wenn der tatsächliche Wert den Performance-Schwellenwert überschreitet, löst Unified Manager eine Warnmeldung im Rahmen des Performance-Ereignisses aus.

Beispiel: Während der regulären Geschäftszeiten zwischen 9:00 Uhr Bis 5:00 Uhr checken die meisten Mitarbeiter ihre E-Mail-Adresse möglicherweise zwischen 9:00 Uhr ein Und 10:30 Uhr Der erhöhte Bedarf an E-Mail-Servern bedeutet eine Zunahme der Workload-Aktivitäten im Back-End Storage während dieser Zeit. Mitarbeiter können von ihren E-Mail-Clients langsame Reaktionszeiten feststellen.

Während der Mittagspause zwischen 12:00 Uhr Und 13:00 Uhr Und am Ende des Arbeitstages nach 5:00 Uhr werden die meisten Mitarbeiter wahrscheinlich von ihren Computern weg. Der Bedarf an E-Mail-Servern sinkt in der Regel, wodurch auch der Bedarf an Back-End Storage sinkt. Alternativ können geplante Workload-Operationen wie Storage-Backups oder Virus-Scans nach 5:00 Uhr geplant werden Und erhöhen Sie die Aktivität im Back-End Storage.

Über mehrere Tage bestimmt der Anstieg und die Abnahme der Workload-Aktivität den erwarteten Aktivitätsbereich, wobei die Workloads über- und Untergrenzen verteilt sind. Wenn sich die tatsächlichen Workload-Aktivitäten für ein Objekt außerhalb der oberen oder unteren Grenzen befinden und für einen bestimmten Zeitraum außerhalb der Grenzen liegen, kann dies darauf hindeuten, dass das Objekt überlastet oder nicht ausgelastet ist.

Wie sich der erwartete Bereich bildet

Unified Manager muss mindestens 3 Tage Workload-Aktivität sammeln, bevor sie mit der Analyse beginnen kann. Anschließend kann der erwartete Bereich für I/O-Reaktionszeiten und Vorgänge auf der GUI angezeigt werden. Die erforderliche Mindesterfassung berücksichtigt nicht alle Änderungen, die von der Workload-Aktivität durchgeführt werden. Nach der Erfassung der ersten 3 Tage der Aktivität passt Unified Manager den erwarteten Bereich alle 24 Stunden um 12:00 Uhr an, um Änderungen der Workload-Aktivität widerzuspiegeln und einen genaueren Leistungsschwellenwert festzulegen.

Bei der Sommerzeit (Sommerzeit) wird die Systemzeit geändert, wodurch der erwartete Bereich der Performance-Statistiken für überwachte Workloads verändert wird. Unified Manager beginnt sofort mit der Korrektur des erwarteten Bereichs, der ungefähr 15 Tage dauert. In dieser Zeit können Sie Unified Manager weiterhin verwenden. Da Unified Manager jedoch den erwarteten Bereich zum Erkennen von Ereignissen verwendet, sind einige Ereignisse möglicherweise nicht korrekt. Ereignisse, die vor der Zeitänderung erkannt wurden, werden nicht beeinträchtigt. Wenn Sie die Zeit auf einem Cluster oder auf einem Unified Manager-Server zu einem früheren Zeitpunkt manuell ändern, wirkt sich dies auch auf die Ergebnisse der Ereignisanalyse aus.

Wie der erwartete Bereich bei der Leistungsanalyse verwendet wird

Unified Manager verwendet den erwarteten Bereich, um die typischen Aktivitäten der I/O-Latenz (Reaktionszeit) und der IOPS (Vorgänge) für überwachte Workloads darzustellen. Er benachrichtigt Sie, wenn die tatsächliche Latenz für einen Workload über dem oberen Bereich des erwarteten Bereichs liegt. Dadurch wird ein Performance-Ereignis ausgelöst, sodass Sie das Performance-Problem analysieren und Korrekturmaßnahmen ergreifen können.

Der erwartete Bereich legt die Performance-Baseline für den Workload fest. Im Laufe der Zeit lernt Unified Manager aus früheren Performance-Messungen, um die erwartete Performance und Aktivitätslevel für den Workload zu prognostizieren. Die obere Grenze des erwarteten Bereichs bestimmt den Leistungsschwellenwert. Unified Manager verwendet die Basiskapazität, um zu ermitteln, ob die tatsächliche Latenz oder der tatsächliche Betrieb über einem Schwellenwert oder außerhalb des erwarteten Bereichs liegt. Der Vergleich der ist-Werte mit den erwarteten Werten erstellt ein Performance-Profil für den Workload.

Wenn die tatsächliche Latenz für einen Workload den Performance-Schwellenwert überschreitet, aufgrund von Konflikten bei einer Cluster-Komponente, ist die Latenz hoch, und der Workload arbeitet langsamer als erwartet. Die Performance anderer Workloads, die dieselben Cluster-Komponenten nutzen, ist möglicherweise auch langsamer als erwartet.

Unified Manager analysiert das Schwellenwertüberschreitereignis und legt fest, ob es sich bei der Aktivität um ein Performance-Ereignis handelt. Wenn die hohe Workload-Aktivität über einen langen Zeitraum, z. B. mehrere Stunden, konsistent bleibt, berücksichtigt Unified Manager die Aktivität als „Normal“ und passt den erwarteten Bereich dynamisch an, um den neuen Performance-Schwellenwert zu bilden.

Einige Workloads weisen möglicherweise durchgängig niedrige Aktivitäten auf, bei denen der erwartete Bereich des Betriebs oder der Latenz im Laufe der Zeit keine hohen Änderungsraten aufweisen. Um die Anzahl der Ereignismeldungen zu minimieren, löst Unified Manager während der Analyse von Performance-Ereignissen ein Ereignis nur für Volumes mit niedriger Aktivität aus, deren Vorgänge und Latenzen erheblich höher sind als erwartet.

In diesem Beispiel weist die Latenz für ein Volume einen erwarteten Bereich auf, in Grau, von 0 Millisekunden pro Vorgang (ms/op) bei dem niedrigsten und 5 ms/op bei dem höchsten Wert auf. Wird die tatsächliche Latenz blau auf 10 ms/op plötzlich erhöht, weil der Netzwerk-Traffic oder die Konflikte einer Cluster-Komponente zeitweise zu hoch sind, liegt sie über dem erwarteten Bereich und hat den Performance-

Schwellenwert überschritten.

Wenn der Netzwerk-Traffic gesunken ist oder die Cluster-Komponente keine Konflikte mehr aufweist, wird die Latenz innerhalb des erwarteten Bereichs zurückgegeben. Wenn die Latenz für einen langen Zeitraum bei oder über 10 ms/op bleibt, müssen Sie möglicherweise Korrekturmaßnahmen ergreifen, um das Ereignis zu beheben.

Unified Manager verwendet Workload-Latenz zur Identifizierung von Performance-Problemen

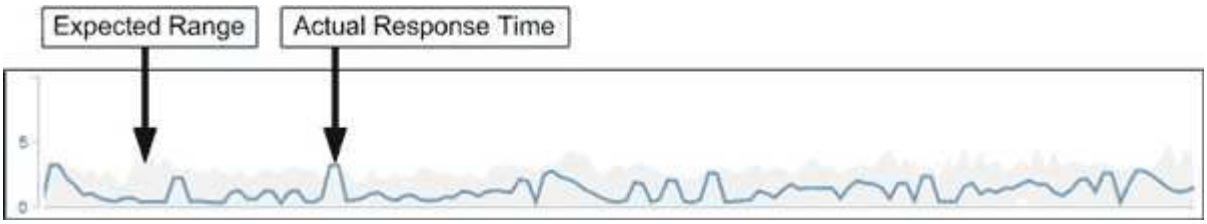
Die Workload-Latenz (Reaktionszeit) ist die Zeit, die ein Volume auf einem Cluster benötigt, um auf I/O-Anforderungen von Client-Applikationen zu reagieren. Unified Manager verwendet die Latenz, um Performance-Ereignisse zu erkennen und zu benachrichtigen.

Eine hohe Latenz bedeutet, dass Anfragen von Applikationen auf Volumes eines Clusters länger dauern als üblich. Die Ursache für die hohe Latenz könnte sich auf dem Cluster selbst befinden, aufgrund von Konflikten bei einer oder mehreren Cluster-Komponenten. Hohe Latenzzeiten könnten auch auf Probleme außerhalb des Clusters zurückzuführen sein, beispielsweise Netzwerkengpässe, Probleme mit dem Client, der die Applikationen hostet, oder Probleme mit den Applikationen selbst.

Unified Manager überwacht nur die Workload-Aktivität auf dem Cluster. Er überwacht nicht die Applikationen, Clients oder Pfade zwischen den Applikationen und dem Cluster.

Operationen im Cluster, z. B. die Erstellung von Backups oder die Durchführung von Deduplizierung, die die Anforderungen von Clusterkomponenten erhöhen, die für andere Workloads gemeinsam genutzt werden, können ebenfalls zu einer hohen Latenz beitragen. Wenn die tatsächliche Latenz den Performance-Schwellenwert des erwarteten Bereichs überschreitet, analysiert Unified Manager das Ereignis, um zu ermitteln, ob es sich um ein Performance-Ereignis handelt, das Sie möglicherweise beheben müssen. Die Latenz wird in Millisekunden pro Vorgang (ms/op) gemessen.

Auf der Seite Performance/Volume Details können Sie sich eine Analyse der Latenzstatistiken anzeigen lassen, um zu ermitteln, wie die Aktivitäten einzelner Prozesse wie Lese- und Schreibanfragen mit den Latenzstatistiken insgesamt verglichen werden. Der Vergleich hilft Ihnen dabei zu ermitteln, welche Vorgänge die höchste Aktivität haben oder ob bestimmte Vorgänge anormale Aktivitäten haben, die sich auf die Latenz eines Volumes auswirken. Bei der Analyse von Performance-Ereignissen können Sie mithilfe der Latenzstatistiken feststellen, ob ein Ereignis durch ein Problem auf dem Cluster verursacht wurde. Sie können auch die spezifischen Workload-Aktivitäten oder Cluster-Komponenten ermitteln, die am Ereignis beteiligt sind.



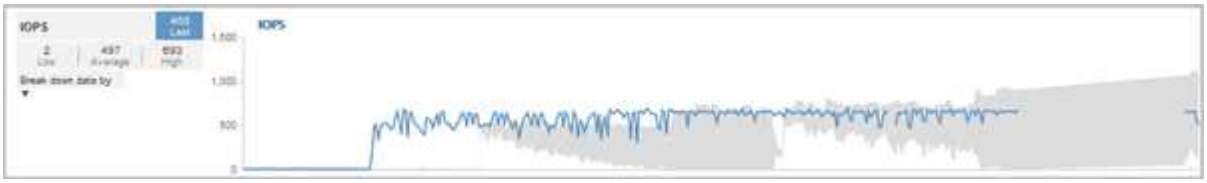
Dieses Beispiel zeigt das Latenzdiagramm auf der Seite Performance/Volume-Details. Die tatsächliche Reaktionszeit (Latenz) ist eine blaue Linie, und der erwartete Bereich ist grau.

In der blauen Zeile kann es zu Lücken kommen, wenn Unified Manager keine Daten erfassen konnte. Dies kann eintreten, da das Cluster oder Volume nicht erreichbar war, Unified Manager während dieser Zeit ausgeschaltet wurde oder die Sammlung länger als den 5-Minuten-Erfassungszeitraum nahm.

Einfluss von Cluster-Vorgängen auf die Workload-Latenz

Operationen (IOPS) stellen die Aktivität aller benutzerdefinierten und systemdefinierten Workloads auf einem Cluster dar. Die IOPS-Statistiken helfen Ihnen bei der Bestimmung, ob Cluster-Prozesse, z. B. Backups oder Deduplizierungsvorgänge, Auswirkungen auf die Workload-Latenz (Reaktionszeit) haben oder ein Performance-Ereignis verursacht haben oder dazu beigetragen haben.

Bei der Analyse von Performance-Ereignissen können Sie mithilfe der IOPS-Statistiken feststellen, ob ein Performance-Ereignis durch ein Problem auf dem Cluster verursacht wurde. Ermitteln Sie die spezifischen Workload-Aktivitäten, die möglicherweise zum Performance-Event beigetragen haben. Die IOPS werden in Operationen pro Sekunde (OPs/Sek.) gemessen.



Dieses Beispiel zeigt das IOPS-Diagramm auf der Seite „Performance/Volume Details“. Die tatsächlichen Statistiken für den Betrieb sind eine blaue Linie und der erwartete Bereich von Statistiken zum Betrieb ist grau.

In manchen Fällen, in denen ein Cluster überlastet ist, wird möglicherweise von Unified Manager die Meldung angezeigt `Data collection is taking too long on Cluster cluster_name`. Das bedeutet, dass für die Analyse von Unified Manager nicht genügend Statistiken erfasst wurden. Sie müssen die Ressourcen, die das Cluster verwendet, verringern, um Statistiken erfassen zu können.

Performance Monitoring von MetroCluster-Konfigurationen

Unified Manager ermöglicht das Monitoring des Schreibdurchsatzes zwischen Clustern in einer MetroCluster-Konfiguration, um Workloads mit einem hohen Schreibdurchsatz zu identifizieren. Falls diese hochperformanten Workloads dazu führen, dass andere Volumes auf dem lokalen Cluster hohe I/O-Reaktionszeiten aufweisen, löst Unified Manager Performance-Ereignisse aus, um Sie zu benachrichtigen.

Wenn ein lokales Cluster in einer MetroCluster-Konfiguration seine Daten auf sein Partner-Cluster spiegelt, werden die Daten in den NVRAM geschrieben und dann über die Interswitch-Links (ISLs) auf die Remote-Aggregate übertragen. Unified Manager analysiert den NVRAM, um die Workloads zu identifizieren, deren hoher Schreibdurchsatz den NVRAM übernutzt und so den NVRAM-Konflikt verursacht.

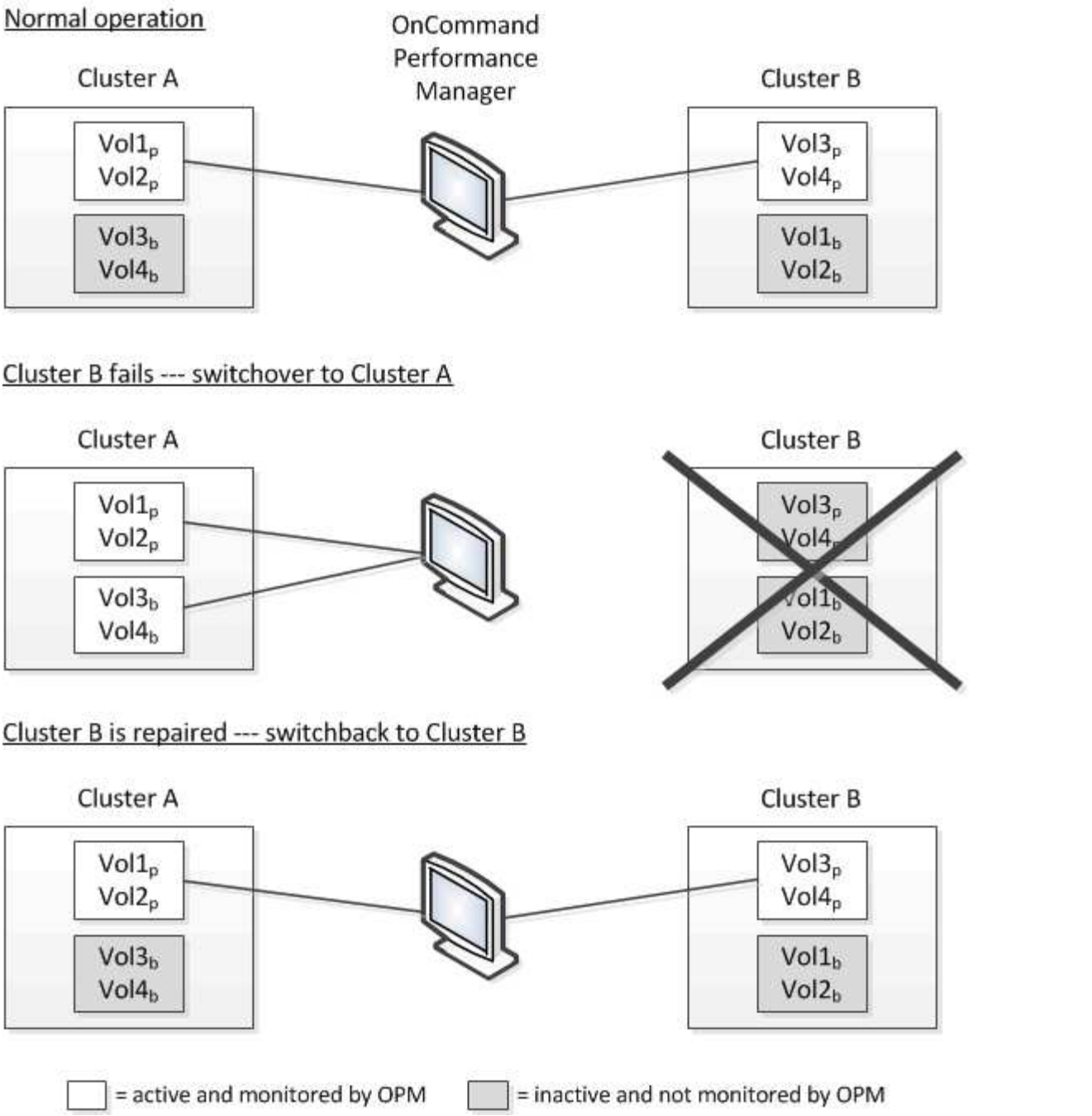
Workloads, deren Abweichung in der Reaktionszeit den Performance-Schwellenwert überschritten hat, werden als „*Opfern*“ bezeichnet. Workloads, deren Abweichung beim Schreibdurchsatz zum NVRAM höher ist als üblich, was zu den Engpässen führt, werden als *bullies* bezeichnet. Da nur Schreibanforderungen zum Partner-Cluster gespiegelt werden, analysiert Unified Manager nicht den Lesedurchsatz.

Unified Manager behandelt die Cluster in einer MetroCluster Konfiguration als einzelne Cluster. Es unterscheidet nicht zwischen Clustern, die Partner sind oder den Schreibdurchsatz von jedem Cluster korrelieren.

Volume-Verhalten während des Umschalens und Zurück

Ereignisse, die ein Switchover oder einen Switchover auslösen, bewirken, dass aktive Volumes von einem Cluster zu einem anderen Cluster in der Disaster-Recovery-Gruppe verschoben werden. Die Volumes auf dem Cluster, die aktiv waren und Clients Daten bereitstellen, werden angehalten, und die Volumes auf dem anderen Cluster sind aktiviert, und mit der Bereitstellung von Daten beginnen Sie. Unified Manager überwacht nur die Volumes, die aktiv sind und ausgeführt werden.

Da Volumes von einem Cluster zum anderen verschoben werden, wird empfohlen, beide Cluster zu überwachen. Eine einzige Instanz von Unified Manager kann beide Cluster in einer MetroCluster-Konfiguration überwachen. Manchmal erfordert die Entfernung zwischen den beiden Standorten jedoch zwei Unified Manager-Instanzen, um beide Cluster zu überwachen. Die folgende Abbildung zeigt eine einzelne Instanz von Unified Manager:



Die Volumes mit p in ihren Namen geben die primären Volumes an, und die Volumes mit b in ihren Namen sind durch SnapMirror erstellte gespiegelte Backup-Volumes.

Im Normalbetrieb:

- Cluster A verfügt über zwei aktive Volumes: Vol1p und Vol2p.
- Cluster B verfügt über 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 aktiven Volume (Statistiken, Ereignisse usw.) werden von Unified Manager erfasst. Die Statistiken zu Vol1p und Vol2p werden von Cluster A gesammelt, und die Statistiken von Vol3p und Vol4p werden von Cluster B gesammelt

Nach einem katastrophalen Ausfall verursacht eine Umschaltung aktiver Volumes von Cluster B zu Cluster A:

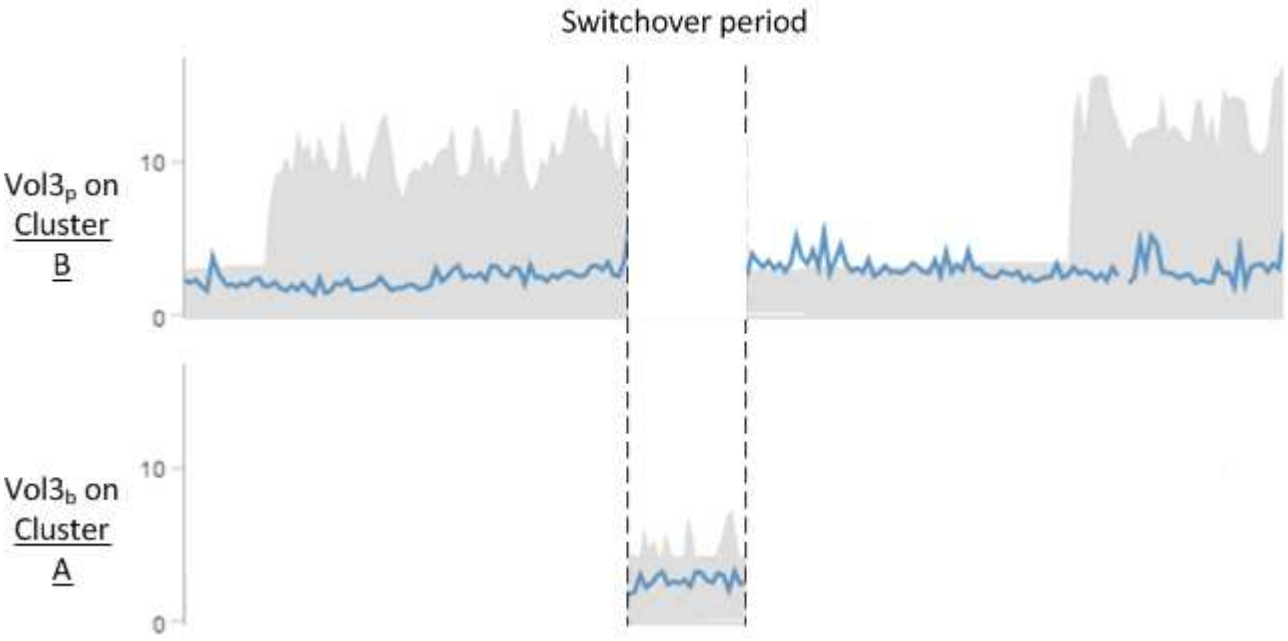
- Cluster A verfügt über vier aktive Volumes: Vol1p, Vol2p, Vol3b und Vol4b.
- Cluster B hat vier inaktive Volumes: Vol3p, Vol4p, Vol1b und Vol2b.

Wie im normalen Betrieb werden Informationen zu den aktiven Volumes von Unified Manager erfasst. Aber in diesem Fall werden die Statistiken zu Vol1p und Vol2p von Cluster A gesammelt, und die Statistiken Vol3b und Vol4b werden auch von Cluster A gesammelt

Beachten Sie, dass Vol3p und Vol3b nicht die gleichen Volumes sind, weil sie auf verschiedenen Clustern sind. Die Informationen im Unified Manager für Vol3p sind nicht identisch mit Vol3b:

- Während der Umstellung auf Cluster A sind Vol3p-Statistiken und -Ereignisse nicht sichtbar.
- Bei der ersten Umschaltung sieht Vol3b wie ein neues Volume ohne historische Informationen aus.

Wenn Cluster B repariert wird und ein Switchback durchgeführt wird, ist Vol3p wieder für Cluster B aktiv. Dies enthält die historischen Statistiken und eine Lücke zwischen den Statistiken für den Zeitraum während der Umschaltung. Vol3b kann von Cluster A nicht angezeigt werden, bis eine weitere Umschaltung erfolgt:



- MetroCluster Volumes, die inaktiv sind, z. B. Vol3b auf Cluster A nach dem Wechsel zurück, werden mit der Meldung „`Dieses Volume wurde gelöscht`“ identifiziert. Das Volume wird nicht tatsächlich gelöscht, es wird jedoch derzeit nicht von Unified Manager überwacht, da es sich nicht um das aktive Volume handelt.
- Wenn ein einziger Unified Manager beide Cluster in einer MetroCluster Konfiguration überwacht, liefert die Volume-Suche Informationen, unabhängig davon, welches Volume zu diesem Zeitpunkt aktiv ist. Eine Suche nach „`VOL3`“ gibt beispielsweise Statistiken und Ereignisse für Vol3b auf Cluster A zurück, wenn eine Umschaltung stattgefunden hat und VOL3 auf Cluster A aktiv ist

Was sind Performance-Ereignisse

Performance-Ereignisse sind Störungen im Zusammenhang mit der Workload-

Performance auf einem Cluster. Die Sie bei der Ermittlung von Workloads mit langsamen Reaktionszeiten unterstützen. Zusammen mit gleichzeitig aufgetretenen Gesundheitsereignissen können Sie die Probleme bestimmen, die die langsamen Reaktionszeiten verursacht oder dazu beigetragen haben.

Wenn Unified Manager mehrere Vorkommen derselben Clusterkomponente erkennt, werden alle Vorkommen als einzelnes Ereignis und nicht als separate Ereignisse behandelt.

Performance-Ereignisanalyse und -Benachrichtigung

Bei Performance-Ereignissen werden Sie über Probleme mit der I/O-Performance bei einem Volume-Workload informiert, die durch Konflikte bei einer Cluster-Komponente verursacht wurden. Unified Manager analysiert das Ereignis, um alle betroffenen Workloads zu ermitteln, die Komponente mit Konflikten zu identifizieren und ob das Ereignis weiterhin ein Problem ist, das Sie möglicherweise beheben müssen.

Unified Manager überwacht die I/O-Latenz (Reaktionszeit) und IOPS (Vorgänge) für Volumes auf einem Cluster. Wenn beispielsweise andere Workloads eine Cluster-Komponente zu hoch nutzen, liegt der Konflikt bei der Komponente und kann nicht auf einer optimalen Ebene Performance erbringen, um die Workload-Anforderungen zu erfüllen. Die Performance anderer Workloads, die dieselbe Komponente verwenden, kann beeinträchtigt werden und die Latenz steigt. Wenn die Latenz den Performance-Schwellenwert überschreitet, löst Unified Manager ein Performance-Ereignis aus und sendet eine E-Mail-Benachrichtigung, um Sie zu benachrichtigen.

Ereignisanalyse

Unified Manager führt die folgenden Analysen anhand der Performance-Statistiken der letzten 15 Tage durch, um die Opfer-Workloads, problematische Workloads und die an einem Ereignis beteiligte Cluster-Komponente zu identifizieren:

- Identifiziert Opfer-Workloads, deren Latenz den Performance-Schwellenwert überschritten hat; dies ist die obere Grenze des erwarteten Bereichs:
  - Bei Volumes auf HDD oder Flash Pool (hybride) Aggregaten werden Ereignisse nur ausgelöst, wenn die Latenz mehr als 5 Millisekunden (ms) beträgt und die IOPS mehr als 10 Operationen pro Sekunde (OPs/s) sind.
  - Bei Volumes auf reinen SSD-Aggregaten oder FabricPool (Composite)-Aggregaten werden Ereignisse nur ausgelöst, wenn die Latenz größer als 1 ms ist und die IOPS mehr als 100 OPs/s beträgt
- Identifiziert Konflikte bei der Cluster-Komponente.

> Wenn die Latenz der Opfer-Workloads am Cluster Interconnect größer als 1 ms ist, behandelt Unified Manager dies als erheblich und löst ein Ereignis für den Cluster Interconnect aus.

- Ermittelt die problematischer Workloads, die die Cluster-Komponente überbeanspruchen und sie verursachen, dass sie unkonflikte aufweisen.
- Ordnen Sie die betroffenen Workloads auf Grundlage ihrer Umlenkungen in der Auslastung oder Aktivität einer Cluster-Komponente an, um zu ermitteln, welche „Verursacher“ die höchste Nutzungsänderung der Cluster-Komponente aufweisen und welche Opfer am meisten davon betroffen sind.

Ein Ereignis kann nur für einen kurzen Moment eintreten und sich dann selbst korrigieren, nachdem die

verwendete Komponente keine Konflikte mehr hat. Ein kontinuierliches Ereignis: Eine erneute Auftreten für dieselbe Cluster-Komponente innerhalb eines Intervalls von fünf Minuten, bleibt im aktiven Status. Für kontinuierliche Ereignisse löst Unified Manager eine Warnmeldung aus, nachdem dasselbe Ereignis in zwei aufeinanderfolgenden Analyseintervallen erkannt wurde. Ereignisse, die ungelöst bleiben, die einen Status von neu haben, können unterschiedliche Beschreibungsmeldungen bei den an der Ereignisänderung beteiligten Workloads anzeigen.

Wenn ein Ereignis gelöst ist, bleibt es in Unified Manager als Teil der Aufzeichnung bisheriger Performance-Probleme für ein Volume verfügbar. Jedes Ereignis verfügt über eine eindeutige ID, mit der der Ereignistyp und die beteiligten Volumes, Cluster und Cluster-Komponenten identifiziert werden.

Ein einzelnes Volume kann gleichzeitig an mehreren Ereignissen beteiligt sein.

Ereignisstatus

Ereignisse können einen der folgenden Status haben:

- * Aktiv*

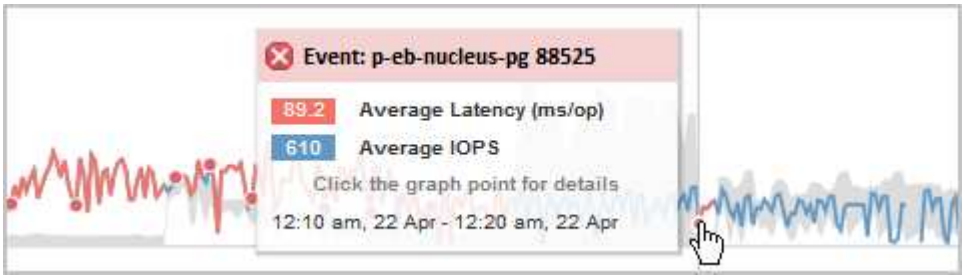
  Zeigt an, dass das Leistungsereignis aktuell aktiv ist (neu oder bestätigt). Das Problem, das das Ereignis verursacht hat, wurde nicht selbst behoben oder wurde nicht behoben. Der Performance-Zähler für das Storage-Objekt bleibt über dem Performance-Schwellenwert.

- **Veraltet**

  Zeigt an, dass das Ereignis nicht mehr aktiv ist. Das Problem, das das Ereignis verursacht hat, hat sich selbst korrigiert oder wurde behoben. Der Performance-Zähler für das Storage-Objekt liegt nicht mehr über dem Performance-Schwellenwert.

Ereignisbenachrichtigung

Die Ereignisalarme werden auf der Seite Dashboards/Übersicht, Dashboards/Leistung, Performance/Volume Details angezeigt und an angegebene E-Mail-Adressen gesendet. Sie können ausführliche Analyseinformationen zu einem Ereignis anzeigen und auf der Seite „Veranstaltungsdetails“ Vorschläge zu seiner Behebung erhalten.



In diesem Beispiel wird ein Ereignis durch einen roten Punkt (angezeigt) Auf der Latenzkarte auf der Seite Performance/Volume Details. Wenn Sie den Mauszeiger über den roten Punkt bewegen, wird ein Popup-Fenster mit weiteren Details zu dem Ereignis und Optionen zur Analyse angezeigt.

Interaktion mit Ereignissen

Auf der Seite Performance/Volume Details können Sie mit Ereignissen wie folgt interagieren:

- Wenn Sie den Mauszeiger über einen roten Punkt bewegen, wird eine Meldung angezeigt, die die Ereignis-ID zusammen mit der Latenz, der Anzahl der Operationen pro Sekunde und dem Datum und der

Zeit, zu der das Ereignis erkannt wurde, anzeigt.

Wenn für den gleichen Zeitraum mehrere Ereignisse vorliegen, wird in der Meldung die Anzahl der Ereignisse zusammen mit der durchschnittlichen Latenz und der durchschnittlichen Anzahl von Operationen pro Sekunde für das Volume angezeigt.

- Durch Klicken auf ein einzelnes Ereignis wird ein Dialogfeld angezeigt, das ausführlichere Informationen zu dem Ereignis enthält, einschließlich der involvierten Cluster-Komponenten, ähnlich dem Abschnitt „Zusammenfassung“ auf der Seite „Ereignisdetails“.

  Die Komponente in Konflikt ist eingekreist und rot hervorgehoben. Sie können entweder auf die Ereignis-ID oder **vollständige Analyse anzeigen** klicken, um die vollständige Analyse auf der Seite Ereignisdetails anzuzeigen. Wenn mehrere Ereignisse für den gleichen Zeitraum vorhanden sind, werden im Dialogfeld Details zu den drei letzten Ereignissen angezeigt. Sie können auf eine Ereignis-ID klicken, um die Ereignisanalyse auf der Seite Ereignisdetails anzuzeigen. Wenn mehr als drei Ereignisse für den gleichen Zeitraum vorhanden sind, wird das Dialogfeld durch Klicken auf den roten Punkt nicht angezeigt.

Wie Unified Manager die Auswirkungen auf die Performance eines Ereignisses ermittelt

Unified Manager verwendet für einen Workload die Abweichung von Aktivität, Auslastung, Schreibdurchsatz, Auslastung der Clusterkomponente oder der I/O-Latenz (Reaktionszeit), um den Einfluss auf die Workload-Performance zu ermitteln. Anhand dieser Informationen wird festgelegt, welche Rolle der jeweilige Workload im Ereignis spielt und wie sie auf der Seite „Ereignisdetails“ aufgelistet werden.

Unified Manager vergleicht die zuletzt analysierten Werte für einen Workload mit dem erwarteten Wertebereich. Die Differenz zwischen den zuletzt analysierten Werten und dem erwarteten Wertebereich identifiziert die Workloads, deren Performance am stärksten von dem Ereignis beeinflusst wurde.

Nehmen Sie beispielsweise an, dass ein Cluster zwei Workloads enthält: Workload A und Workload B. Der erwartete Bereich für den Workload A beträgt 5-10 Millisekunden pro Operation (ms/op) und seine tatsächliche Latenz beträgt normalerweise etwa 7 ms/op Der erwartete Bereich für Workload B beträgt 10-20 ms/op, seine tatsächliche Latenz beträgt normalerweise etwa 15 ms/op Beide Workloads liegen deutlich innerhalb des erwarteten Latenzbereichs. Aufgrund von Konflikten im Cluster erhöht sich die Latenz beider Workloads auf 40 ms/op, indem der Performance-Schwellenwert überschritten wird. Dies ist die obere Grenze des erwarteten Bereichs und das Auslösen von Ereignissen. Die Latenzabweichung von den erwarteten Werten bis zu den Werten über dem Performance-Schwellenwert für Workload A liegt bei rund 33 ms/op, die Abweichung für Workload B liegt bei etwa 25 ms/op Die Latenz beider Workloads liegt bei 40 ms/op, doch bei Workload A hatten die größeren Auswirkungen auf die Performance, da die höhere Latenzabweichung bei 33 ms/op

Auf der Seite „Ereignisdetails“ im Abschnitt „Systemdiagnose“ können Sie Workloads nach deren Abweichung bei Aktivität, Auslastung oder Durchsatz für eine Cluster-Komponente sortieren. Sie können Workloads auch nach Latenz sortieren. Wenn Sie eine Sortieroption auswählen, analysiert Unified Manager die Abweichungen von Aktivität, Auslastung, Durchsatz oder Latenz, da das Ereignis anhand der erwarteten Werte erkannt wurde, um die Sortierreihenfolge des Workloads zu bestimmen. Für die Latenz die roten Punkte (🔴) Geben Sie einen Performance-Schwellenwert an, der durch einen Opfer-Workload und die daraus folgende Auswirkung auf die Latenz übergeht. Jeder rote Punkt weist ein höheres Maß an Latenzabweichungen auf. So können Sie die betroffenen Workloads identifizieren, deren Latenz sich am stärksten auf ein Ereignis auswirkt.

Cluster-Komponenten und warum sie über Konflikte verfügen können

Sie können Probleme mit der Cluster-Performance identifizieren, wenn ein Konflikt zwischen einer Cluster-Komponente besteht. Die Performance von Volume-Workloads,

die die Komponente nutzen, wird langsamer. Dadurch wird die Reaktionszeit (Latenz) für Client-Anforderungen erhöht und ein Ereignis in Unified Manager ausgelöst.

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

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

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

- **Netzwerk**

  Zeigt die Wartezeit von I/O-Anfragen durch iSCSI-Protokolle oder Fibre Channel-Protokollen (FC) des Clusters an. Die Wartezeit liegt darin, auf die Transaktionen „iSCSI Ready to Transfer“ (R2T) oder „FCP Transfer Ready“ (XFER_RDY) zu warten, bis der Cluster auf eine I/O-Anforderung antworten kann. Wenn die Netzwerkkomponente unter einem Konflikt steht, bedeutet dies, dass hohe Wartezeiten auf der Protokollebene des Blocks die Latenz eines oder mehrerer Workloads beeinflussen.

- * Netzwerkverarbeitung*

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

- **QoS-Richtlinie**

  Steht für die Storage-Richtliniengruppe für Quality of Service (QoS), der Mitglied des Workloads ist Wenn die Richtliniengruppe Konflikte hat, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch das festgelegte Durchsatzlimit gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- * Cluster Interconnect*

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

- **Datenverarbeitung**

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

- **MetroCluster Ressourcen**

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

- **Aggregate oder SSD Aggregate Ops**

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

- **Cloud-Latenz**

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

- **Sync SnapMirror**

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

Rollen von Workloads, die an einem Performance-Ereignis beteiligt sind

Unified Manager verwendet Rollen, um die Beteiligung eines Workloads bei einem Performance-Ereignis zu ermitteln. Zu den Rollen gehören Opfer, Bullies und Haie. Ein benutzerdefiniertes Workload kann gleichzeitig Opfer, Bully und Haifisch sein.

Rolle	Beschreibung
Opfer	Ein benutzerdefiniertes Workload, dessen Performance aufgrund anderer Workloads, sogenannte „Verursacher“, stark gesunken ist, die eine Cluster-Komponente überlasten. Es werden nur benutzerdefinierte Workloads als „Opfer“ identifiziert. Unified Manager ermittelt anhand der Latenzabweichung von Opfer-Workloads, bei der die tatsächliche Latenz während eines Ereignisses deutlich größer geworden ist als der erwartete Latenzbereich.
Bully	Ein benutzerdefiniertes oder systemdefiniertes Workload, dessen Überprovisionierung einer Cluster-Komponente die Performance anderer Workloads, genannt „Opfern“, abnimmt. Unified Manager identifiziert problematische Workloads basierend auf der abweichenden Nutzung einer Cluster-Komponente, wobei die tatsächliche Nutzung während eines Ereignisses deutlich größer ist als der erwartete Nutzungsumfang.
Hai	Einen benutzerdefinierten Workload mit der höchsten Auslastung einer Cluster-Komponente im Vergleich zu allen an einem Ereignis beteiligten Workloads. Unified Manager identifiziert Haifisch-Workloads auf der Grundlage ihrer Verwendung einer Clusterkomponente bei einem Ereignis.

Workloads auf einem Cluster können viele der Cluster-Komponenten gemeinsam nutzen, z. B. Storage-Aggregate und die CPU für Netzwerk und Datenverarbeitung. Wenn ein Workload, z. B. ein Volume, seine Nutzung einer Cluster-Komponente so erhöht, dass die Komponente die Workload-Anforderungen nicht effizient erfüllen kann, hat die Komponente Konflikte. Der Workload, der eine Cluster-Komponente übernutzt, ist ein problematischer Bestandteil. Die anderen Workloads, die diese Komponenten gemeinsam nutzen und deren Performance durch die Täter beeinträchtigt wird, sind Opfer. Aktivitäten systemdefinierter Workloads wie Deduplizierung oder Snapshot Kopien können sich auch in „`bullying`“ eskalieren.

Wenn Unified Manager ein Ereignis erkennt, werden alle betroffenen Workloads und Cluster-Komponenten identifiziert, einschließlich der problematische Workloads, die das Ereignis verursacht haben, der Clusterkomponente, die Konflikte verursacht hat, und der Opfer-Workloads, deren Performance aufgrund der gesteigerten Aktivitäten als Folge problematischer Workloads gesunken ist.

Wenn Unified Manager die problematische Workloads nicht identifizieren kann, werden nur bei den betroffenen Workloads und der betroffenen Cluster-Komponente ein Alarm ausgegeben.

Unified Manager erkennt Workloads, die Opfer problematischer Workloads sind, und ermittelt zudem, ob dieselben Workloads problematische Workloads werden. Ein Workload kann für sich selbst eine problematische sein. Ein so leistungsstarker Workload, der durch eine Richtliniengruppenbeschränkung gedrosselt wird, führt beispielsweise dazu, dass alle Workloads in der Richtliniengruppe gedrosselt werden – auch selbst. Ein Workload, der ein problematischer oder Opfer in einem laufenden Performance-Ereignis ist, kann seine Rolle ändern oder nicht mehr Teilnehmer des Ereignisses sein. Auf der Seite Performance/Volume

Details in der Tabelle Ereignisliste wird das Datum und die Uhrzeit der Rollenänderung angezeigt, wenn das ausgewählte Volume seine Teilnehmerrolle ändert.

Analyse der Workload-Performance

Mit Unified Manager lässt sich die I/O-Performance von Volume-Workloads auf Clustern überwachen und analysieren. Sie können ermitteln, ob ein Performance-Problem im Cluster liegt und ob der Storage das Problem ist.

Dieses Kapitel beschreibt die Analyse der Workload-Performance mithilfe der Seite „Performance/Volume Details“ und der Seite „Ereignisdetails“.

Ermitteln, ob ein Workload ein Performance-Problem aufweist

Sie können mit Unified Manager feststellen, ob ein festgestellter Performance-Ereignis tatsächlich durch ein Performance-Problem auf dem Cluster verursacht wurde. Das Ereignis konnte beispielsweise zu einem Spitzenwert bei der Aktivität geführt haben, der die Reaktionszeit steigerte, aber jetzt ist die Reaktionszeit wieder auf das übliche Niveau zurückgekehrt.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den Namen des Volumes oder der zugehörigen LUN identifiziert haben, die Sie analysieren möchten.
- Unified Manager muss Performance-Statistiken vom Cluster mindestens fünf Tage gesammelt und analysiert haben.

Über diese Aufgabe

Wenn Sie die Seite „Ereignisdetails“ aufrufen, können Sie auf den Namenslink für ein Volume klicken, um direkt zur Seite „Performance/Volume Details“ zu gelangen.

Schritte

1. Geben Sie in der **Search**-Leiste mindestens die ersten drei Zeichen des Volume-Namens ein.

   Der Name des Volume wird in den Suchergebnissen angezeigt.

2. Klicken Sie auf den Namen des Volumes.

   Das Volume wird auf der Seite Performance/Volume Details angezeigt.

3. Klicken Sie im **Historic Data**-Diagramm auf **5d**, um die letzten fünf Tage historischer Daten anzuzeigen.
4. Lesen Sie das **Latenz**-Diagramm, um die folgenden Fragen zu beantworten:
   - Gibt es neue Performance-Ereignisse?
   - Gibt es historische Performance-Ereignisse, die darauf hindeuten, dass in der Vergangenheit Probleme mit dem Volume aufgetreten sind?

- Gibt es Spitzen in der Reaktionszeit, auch wenn sich die Spitzen innerhalb des erwarteten Bereichs befinden?
- Gab es Konfigurationsänderungen auf dem Cluster, die sich möglicherweise auf die Performance auswirken? Wenn bei der Antwortzeit des Volumes keine Performance-Ereignisse, Spitzenlasten oder kürzlich geänderte Konfigurationen angezeigt werden, die sich möglicherweise auf die Reaktionszeit auswirken, können Sie das durch das Cluster verursachte Performance-Problem ausschließen.

Untersuchung einer vermuteten langsamen Reaktionszeit für einen Workload

Sie können mit Unified Manager ermitteln, ob die Operationen im Cluster möglicherweise zur langsamen Reaktionszeit (Latenz) für einen Volume-Workload beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den Namen des Volumes oder der zugehörigen LUN identifiziert haben, die Sie analysieren möchten.
- Unified Manager muss Performance-Statistiken vom Cluster mindestens fünf Tage gesammelt und analysiert haben.

Über diese Aufgabe

Wenn Sie die Seite „Ereignisdetails“ aufrufen, können Sie auf den Namen eines Volumes klicken, um direkt zur Seite „Performance/Volume Details“ zu gelangen.

Schritte

1. Geben Sie in der **Search**-Leiste den Namen des Volumens ein.

   Der Name des Volume wird in den Suchergebnissen angezeigt.

2. Klicken Sie auf den Namen des Volumes.

   Das Volume wird auf der Seite Performance/Volume Details angezeigt.

3. Klicken Sie auf der Historischen Datenkarte auf **5d**, um die letzten fünf Tage historischer Daten anzuzeigen.
4. Lesen Sie das **IOPS** Diagramm, um die folgenden Fragen zu beantworten:
   - Gibt es dramatische Spitzen in der Aktivität?
   - Gibt es dramatische Tropfen in der Aktivität?
   - Gibt es anormale Änderungen im Betriebsmuster? Wenn der Betrieb keine dramatischen Spitzen oder Aktivitätsspitzen anzeigt und während dieser Zeit keine Änderungen an der Cluster-Konfiguration vorgenommen wurden, kann der Storage-Administrator bestätigen, dass andere Workloads die Volume-Performance nicht beeinträchtigt haben.
5. Wählen Sie im Menü **break down Data by** unter **IOPS** die Option **reads/writes/other** aus.
6. Klicken Sie Auf **Absenden**.

   Das Diagramm Lese-/Schreibvorgänge/Sonstiges wird unter dem IOPS-Diagramm angezeigt.

7. Prüfen Sie das Diagramm * Lese-/Schreibvorgänge/anderes*, um dramatische Spitzen oder Abfälle in der

Menge der Lese- oder Schreibvorgänge für das Volume zu identifizieren.

Wenn keine drastischen Spitzen oder Abfälle bei Lese- oder Schreibvorgängen vorliegen, kann der Storage-Administrator bestätigen, dass die I/O-Vorgänge im Cluster normal ausgeführt werden. Möglicherweise liegen Leistungsprobleme im Netzwerk oder den verbundenen Clients vor.

Trends der I/O-Reaktionszeit bei Cluster-Komponenten erkennen

Mit Unified Manager können Sie die Performance-Trends für alle überwachten Clusterkomponenten für einen Volume Workload anzeigen. Im Laufe der Zeit können Sie sehen, welche Komponenten die höchste Auslastung haben, ob Lese- oder Schreibanfragen die höchste Auslastung haben und wie sich die Auslastung auf die Reaktionszeit des Workloads ausgewirkt hat.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den Namen des Volumes oder der zugehörigen LUN, die Sie analysieren möchten, identifiziert haben.
- Um Performance-Statistiken von 30 Tagen anzuzeigen, muss Unified Manager mindestens 30 Tage Performance-Statistik aus dem Cluster gesammelt und analysiert haben.

Über diese Aufgabe

Anhand der Ermittlung der Performance-Trends für die Cluster-Komponenten kann der Administrator entscheiden, ob der Cluster überlastet oder nicht ausgelastet ist.

Wenn Sie die Seite „Ereignisdetails“ aufrufen, können Sie auf den Namen eines Volumes klicken, um direkt zur Seite „Performance/Volume Details“ zu gelangen.

Schritte

1. Geben Sie in der **Search**-Leiste den Namen des Volumens ein.

   Der Name des Volume wird in den Suchergebnissen angezeigt.

2. Klicken Sie auf den Namen des Volumes.

   Das Volume wird auf der Seite Performance/Volume Details angezeigt.

3. Klicken Sie auf dem Historischen Datendiagramm auf **30d**, um die letzten 30 Tage historischer Daten anzuzeigen.
4. Klicken Sie auf **Aufbrechen von Daten durch**.
5. Wählen Sie unter **Latenz Cluster-Komponenten** und **Lese-/Schreib-Latenz** aus.
6. Klicken Sie Auf **Absenden**.

   Beide Diagramme werden unter dem Latenzdiagramm angezeigt.

7. Sehen Sie sich das Diagramm * Cluster Components* an.

   Das Diagramm unterteilt die Gesamtantwortzeit nach Cluster-Komponente. Die Reaktionszeit im Aggregat

ist die höchste.

8. Vergleichen Sie das Diagramm **Cluster Components** mit dem Diagramm **Latenz**.

   Das Latenzdiagramm zeigt Spitzen in der gesamten Reaktionszeit, die mit den Spitzen in der Reaktionszeit des Aggregats abgeglichen werden. Am Ende des 30-Tage-Zeitrahmens, in dem die Leistungsschwelle überschritten wurde, gibt es einige wenige.

9. Prüfen Sie das Diagramm * Lese-/Schreib-Latenz*.

   Das Diagramm zeigt eine höhere Reaktionszeit bei Schreibanfragen als Leseanforderungen, was darauf hinweist, dass die Client-Anwendungen länger als gewöhnlich warten, um ihre Schreibanforderungen zu erfüllen.

10. Vergleichen Sie das Diagramm * Lese-/Schreib-Latenz* mit dem Diagramm * Latenz*.

    Die Spitzen bei der gesamten Antwortzeit, die auf das Aggregat im Diagramm „Cluster-Komponenten“ abgestimmt sind, werden auch auf die Schreibvorgänge im Latenzdiagramm für Lese-/Schreibvorgänge ausgerichtet. Der Administrator muss entscheiden, ob die Client-Applikationen, die den Workload verwenden, berücksichtigt werden müssen oder ob das Aggregat zu viel genutzt wird.

Analyse der Performance-Verbesserungen, die durch die Verschiebung eines Volumes erzielt wurden

Mit Unified Manager können Sie die Auswirkungen einer Verschiebung eines Volumes auf die Latenz (Reaktionszeit) anderer Volumes auf dem Cluster untersuchen. Durch die Verschiebung eines hochperformanten Volumes zu einem weniger ausgelasteten Aggregat oder eines Aggregats mit aktiviertem Flash-Storage kann das Volume effizienter ausgeführt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen den Namen des Volumes oder der zugehörigen LUN identifiziert haben, die Sie analysieren möchten.
- Unified Manager muss sieben Tage Daten erfasst und analysiert haben.

Über diese Aufgabe

Unified Manager bestimmt, wann ein Volume zwischen Aggregaten verschoben wird. Es kann erkennen, wann die Volume-Verschiebung stattfindet, abgeschlossen ist oder fehlgeschlagen ist. Auf der Seite Performance/Volume Details wird für jeden Status der Volume-Verschiebung ein Änderungssymbol angezeigt. Anhand dieses Symbols können Sie feststellen, wann ein Verschiebevorgang stattgefunden hat, und Sie können feststellen, ob dieser zu einem Performance-Ereignis beigetragen hat.

Wenn Sie die Seite „Ereignisdetails“ aufrufen, können Sie auf den Namen eines Volumes klicken, um direkt zur Seite „Performance/Volume Details“ zu wechseln.

Schritte

1. Geben Sie in der **Search**-Leiste den Namen des Volumens ein.

2. Klicken Sie auf den Namen des Volumes.

   Das Volume wird auf der Seite Performance/Volume Details angezeigt.

3. Passen Sie im Diagramm * Historic Data* die Schieberegler an, um die Aktivität der letzten Arbeitswoche anzuzeigen.
4. Analysieren Sie das **Latenz**-Diagramm und das **IOPS**-Diagramm, um zu sehen, wie sich das Volumen in den letzten Tagen abspielte.

   Angenommen, Sie stellen fest, dass ein konsistentes Muster sehr hoher durchschnittlicher Antwortzeiten von über 42 Millisekunden pro Betrieb (ms/OP) mit Performance-Ereignissen jeden Tag der Woche fällt und entscheiden, das Volume in ein weniger beschäftigtes Aggregat zu verschieben, um die Performance zu verbessern. Mit OnCommand System Manager kann das Volume zu einem Aggregat mit aktiviertem Flash Pool verschoben werden, um die Performance zu steigern. Etwa eine Stunde nach Abschluss der Volume-Verschiebung können Sie zu Unified Manager zurückkehren, um zu bestätigen, dass der Vorgang erfolgreich abgeschlossen wurde und sich die Latenz verbessert hat.

5. Wenn die Seite **Performance/Volume Details** nicht angezeigt wird, suchen Sie nach dem gewünschten Volume.
6. Klicken Sie im **Historic Data**-Diagramm auf **1d**, um die Aktivität vom letzten Tag, einige Stunden seit der Volumenbewegung, anzuzeigen.

   Im unteren Bereich der Seite in der Zeile Ereignisse Zeit wird ein Symbol für das Ereignis ändern ( ) Wird angezeigt, um die Zeit anzugeben, die der Vorgang der Volumenbewegung abgeschlossen wurde. Eine schwarze, vertikale Linie wird auch vom Änderungssymbol in das Latenzdiagramm angezeigt.

7. Zeigen Sie mit dem Cursor auf das Symbol Ereignis ändern, um Details zum Ereignis in der **Ereignisliste** anzuzeigen.

   Da das Volume zu einem Aggregat mit aktiviertem Flash Pool verschoben wurde, sehen Sie die Änderung bei Lese- und Schreib-I/O in den Cache.

8. Wählen Sie im Menü * Data by* unter **Mbps** die Option **Cache HIT Ratio** aus.

   Das Diagramm „Cache-Trefferverhältnis“ zeigt Statistiken zu den Lese- und Schreibvorgängen im Cache an.

   Das Volume wurde erfolgreich in ein Aggregat mit weniger Auslastung verschoben und das Änderungsereignis wird in der Ereignisliste rechts hervorgehoben. Die durchschnittliche Latenz sank deutlich von über 42 ms/op auf rund 24 ms/op Die derzeitige Latenz beträgt ca. 1.5 ms/op Im Cache-Trefferverhältnis-Diagramm liegt die Menge der erfolgreichen Lese- und Schreibvorgänge in den Cache jetzt bei 100 %, da sich das Volume jetzt auf einem Aggregat mit aktiviertem Flash Pool befindet.

So verschieben Sie ein FlexVol Volume

Wenn Sie wissen, wie das Verschieben eines FlexVol Volumes funktioniert, können Sie feststellen, ob die Verschiebung eines Volumes Service Level Agreements erfüllt und ermitteln, wo sich die Volume-Verschiebung befindet.

FlexVol Volumes werden von einem Aggregat oder Node zu einem anderen innerhalb derselben Storage Virtual Machine (SVM) verschoben. Durch eine Volume-Verschiebung wird der Client-Zugriff während der Verschiebung nicht unterbrochen.

Verschieben eines Volumes erfolgt in mehreren Phasen:

- Ein neues Volume wird auf dem Zielaggregat erstellt.
- Die Daten aus dem ursprünglichen Volume werden auf das neue Volume kopiert.

  Während dieser Zeit ist das ursprüngliche Volume intakt und für Clients verfügbar.

- Am Ende des Verschiebevorgangs wird der Client-Zugriff vorübergehend gesperrt.

  Während dieser Zeit führt das System eine endgültige Replikation vom Quell-Volume zum Ziel-Volume durch, tauscht die Identitäten der Quell- und Ziel-Volumes aus und ändert das Ziel-Volume in das Quell-Volume.

- Nach Abschluss der Verschiebung wird der Client-Datenverkehr zum neuen Quell-Volume weitergeleitet und der Client-Zugriff wird fortgesetzt.

Die Verschiebung wird für den Client-Zugriff nicht unterbrochen, da die Zeit, in der der Client-Zugriff gesperrt ist, bevor Clients eine Unterbrechung oder eine Unterbrechung bemerken. Der Client-Zugriff ist standardmäßig für 35 Sekunden gesperrt. Falls der Vorgang zur Verschiebung des Volumes nicht zum Zeitpunkt des Abzugriffs abgeschlossen werden kann, bricht das System diese letzte Phase der Verschiebung des Volumes ab und erlaubt den Client-Zugriff. Das System versucht standardmäßig dreimal die letzte Phase. Nach dem dritten Versuch wartet das System eine Stunde, bevor es erneut versucht wird, die letzte Phasenfolge zu versuchen. Das System führt die letzte Phase der Verschiebung des Volumes aus, bis die Volume-Verschiebung abgeschlossen ist.

Seite Performance/Volume Details

Diese Seite enthält detaillierte Performance-Statistiken für alle I/O-Aktivitäten und Vorgänge für das ausgewählte FlexVol Volume, das FlexGroup Volume oder den FlexGroup-Komponenten-Workload. Sie können einen bestimmten Zeitrahmen auswählen, in dem die Statistiken und Ereignisse für das Volume angezeigt werden sollen. Die Ereignisse identifizieren Performance-Ereignisse und Änderungen, die sich auf die I/O-Performance auswirken können.

Historisches Diagramm

Zeigt die historischen Leistungsanalyse-Daten für das ausgewählte Volume an. Sie können auf die Schieberegler klicken und ziehen, um einen Zeitrahmen festzulegen. Die Schieberegler erhöhen und reduzieren das Zeitfenster. Die Daten außerhalb des Zeitrahmenfensters sind ausgegraut. Mit dem Schieberegler unten im Diagramm können Sie das Zeitfenster über die historischen Daten verschieben. Die gesamte Seite, einschließlich der angezeigten Diagramme und Ereignisse, gibt die Daten wieder, die im Zeitfenster verfügbar sind. Unified Manager speichert auf dieser Seite maximal 30 Tage historische Daten.

Wenn Sie auf dem historischen Datendiagramm je nach Bildschirmauflösung einen Zeitrahmen von mehr als einem Tag auswählen, werden in den Diagrammen die maximalen Werte für Reaktionszeit und IOPS über die Anzahl der Tage hinweg angezeigt.

Optionen

- **Zeitauswahl**

  Gibt den Zeitbereich an, über den die Volume-Performance-Statistiken für die gesamte Seite angezeigt

werden sollen. Sie können 1 Tag (**1d**) bis 30 Tage (**30d**) anklicken oder auf **Benutzerdefiniert** klicken, um einen benutzerdefinierten Bereich auszuwählen. Für einen benutzerdefinierten Bereich können Sie ein Anfang- und Enddatum auswählen und dann auf **Aktualisieren** klicken, um die gesamte Seite zu aktualisieren.

> Wenn Sie auf der Seite Ereignisdetails auf die Seite Performance/Volume Details zugreifen, indem Sie auf den Namenslink eines Volumes klicken, wird standardmäßig automatisch ein Zeitbereich, z. B. 1 Tag oder 5 Tage vor dem aktuellen Tag, ausgewählt. Wenn Sie den Schieberegler im historischen Datendiagramm verschieben, ändert sich der Zeitbereich in einen benutzerdefinierten Bereich, aber die Auswahl **Benutzerdefiniert** Zeit ist nicht ausgewählt. Die Standardzeitauswahl bleibt ausgewählt.

- **Brechen Sie die Daten nach** auf

  Enthält eine Liste von Diagrammen, die Sie zur Seite „Performance/Volume-Details“ hinzufügen können, um detailliertere Performance-Statistiken für das ausgewählte Volume anzuzeigen.

In den Aufschlüsselung der Daten werden Performance-Statistiken angezeigt

Sie können die Diagramme verwenden, um Performance-Trends für ein Volume anzuzeigen. Sie können auch Statistiken für Lese- und Schreibvorgänge, Netzwerkprotokollaktivitäten, die Auswirkungen einer QoS-Richtliniengruppendrosselung auf Latenz, das Verhältnis von Lese- und Schreibzugriffen auf Cache Storage, die von einem Workload verwendete Cluster-CPU-Gesamtzeit und bestimmte Cluster-Komponenten anzeigen.

Diese Ansichten zeigen Statistiken von maximal 30 Tagen vom aktuellen Tag an. Wenn Sie im historischen Datendiagramm je nach Bildschirmauflösung einen Zeitrahmen von mehr als einem Tag auswählen, werden in den Diagrammen die maximalen Werte für Latenz und IOPS über die Anzahl der Tage hinweg angezeigt.

> Sie können das Kontrollkästchen * Alle auswählen* verwenden, um alle aufgeführten Diagrammoptionen auszuwählen oder zu deaktivieren.

- **Latenz**

  In den folgenden Diagrammen werden Informationen zur Latenz oder Reaktionszeit für den ausgewählten Workload detailliert aufgeführt:

  - **Clusterkomponenten**

    Zeigt ein Diagramm der Zeit an, die für jede Cluster-Komponente verwendet wurde, die vom ausgewählten Volume verwendet wurde.

    Das Diagramm hilft Ihnen, die Auswirkung auf die Latenz für jede Komponente in Verbindung mit der gesamten Latenz zu bestimmen. Sie können das Kontrollkästchen neben jeder Komponente verwenden, um das Diagramm anzuzeigen und auszublenden.

    Bei QoS-Richtliniengruppen werden Daten nur für benutzerdefinierte Richtliniengruppen angezeigt. Nullen werden für systemdefinierte Richtliniengruppen angezeigt, z. B. für Standardrichtliniengruppen.

  - **Lese-/Schreib-Latenz**

Zeigt ein Diagramm der Latenzen der erfolgreichen Lese- und Schreibanforderungen vom ausgewählten Volume-Workload im ausgewählten Zeitrahmen an.

Schreibanforderungen sind eine orangefarbene Zeile und Leseanforderungen sind eine blaue Zeile. Die Anforderungen sind spezifisch hinsichtlich der Latenz für den ausgewählten Volume-Workload und nicht für alle Workloads im Cluster.

Die Lese- und Schreib-Statistiken ergeben möglicherweise nicht immer die im Latenzdiagramm angezeigten Statistiken zur gesamten Latenz. Das erwartete Verhalten hängt davon ab, wie Unified Manager Statistiken zu Lese- und Schreibvorgängen für einen Workload sammelt und analysiert.

- **Policy Group Impact**

  Zeigt ein Diagramm des prozentualen Anteils der Latenz für den ausgewählten Volume-Workload an, der durch das Durchsatzlimit seiner QoS-Richtliniengruppe beeinträchtigt wird.

  Wenn der Workload gedrosselt wird, zeigt der Prozentsatz an, wie sehr die Drosselung zu einem bestimmten Zeitpunkt zur Latenz beigetragen hat. Die Prozentwerte geben die Drosselung an:

  - 0% = keine Drosselung
  - > 0% = Drosselung
  - > 20% = kritische Drosselung Wenn der Cluster mehr Arbeit erledigen kann, können Sie die Drosselung durch Erhöhung des Richtliniengruppenlimits verringern. Eine andere Option ist es, den Workload in ein weniger stark ausgelasteten Aggregat zu verschieben.

  Das Diagramm wird nur für Workloads in einer benutzerdefinierten QoS-Richtliniengruppe mit einem festgelegten Durchsatzlimit angezeigt. Sie wird nicht angezeigt, ob sich die Workloads in einer von dem System definierten Richtliniengruppe befinden, z. B. in der Standardrichtliniengruppe, oder in einer Richtliniengruppe, die kein QoS-Limit hat. Bei einer QoS-Richtliniengruppe können Sie den Mauszeiger auf den Namen der Richtliniengruppe zeigen, um ihr Durchsatzlimit und das letzte Mal anzuzeigen. Wenn die Richtliniengruppe geändert wurde, bevor das zugehörige Cluster zu Unified Manager hinzugefügt wurde, handelt es sich bei der letzten geänderten Zeit um das Datum und die Uhrzeit, zu der Unified Manager das Cluster zum ersten Mal entdeckte.

- **IOPS**

  Die folgenden Diagramme zeigen die IOPS-Daten für den ausgewählten Workload an:

  - **Lesen/Schreiben/Sonstiges**

    Zeigt ein Diagramm an, das die Anzahl der Lese- und Schreib-IOPS und anderer IOPS pro Sekunde im ausgewählten Zeitrahmen anzeigt.

  Andere IOPS sind Protokollaktivitäten, die vom Client initiiert werden und keine Lese- oder Schreibvorgänge sind. In einer NFS-Umgebung könnten dies beispielsweise Metadatenvorgänge wie getattr, setattr oder fsstat sein. In einer CIFS-Umgebung könnte es sich um Attributsuchen, Verzeichnislisten oder Virenschutzprüfungen handeln. Schreib-IOPS sind eine orangefarbene Linie und Leseanforderungen sind eine blaue Linie. Die Anforderungen sind spezifisch für alle Vorgänge des ausgewählten Volume-Workloads und nicht für alle Vorgänge im Cluster.

- **Mbps**

Die folgenden Diagramme zeigen die Durchsatzdaten für den ausgewählten Workload an:

- **Cache Trefferquote**

  Zeigt ein Diagramm des prozentualen Anteils der Leseanforderungen von Client-Applikationen an, die über den Cache im ausgewählten Zeitrahmen zufrieden sind.

  Der Cache könnte sich auf Flash Cache-Karten oder Solid State-Laufwerken (SSDs) in Flash Pool Aggregaten befinden. Ein Cache-Treffer in Blau ist ein aus dem Cache gelesener Treffer. Ein Cache-Treffer in orange ist ein Lesevorgang von einer Festplatte im Aggregat. Die Anforderungen sind spezifisch für den ausgewählten Volume-Workload, nicht jedoch für alle Workloads im Cluster.

Ausführlichere Informationen zur Volume-Cache-Nutzung können Sie auf den Integritätsseiten von Unified Manager und in OnCommand System Manager anzeigen.

- **Komponenten**

Die folgenden Diagramme zeigen die Daten nach Clusterkomponenten, die vom ausgewählten Workload verwendet werden:

- **Cluster CPU-Zeit**

  Zeigt ein Diagramm der CPU-Nutzungszeit in ms für alle Nodes im Cluster an, die vom ausgewählten Workload verwendet werden.

  Das Diagramm zeigt die kombinierte CPU-Nutzungszeit für die Netzwerkverarbeitung und Datenverarbeitung an. Auch die CPU-Zeit für systemdefinierte Workloads, die dem ausgewählten Workload zugewiesen sind und dieselben Nodes für die Datenverarbeitung nutzen, ist inbegriffen. Anhand der Tabelle können Sie ermitteln, ob der Workload ein hoher Verbrauch der CPU-Ressourcen auf dem Cluster darstellt. Mithilfe des Diagramms können Sie auch zusammen mit dem Latenzdiagramm für Lese-/Schreibvorgänge unter dem Latenzdiagramm oder dem Diagramm „Lese-/Schreibvorgänge/anderes“ unter dem IOPS-Diagramm festlegen, wie Änderungen an der Workload-Aktivität im Laufe der Zeit die Cluster-CPU-Auslastung beeinträchtigen.

- * Datenträgernutzung*

  Zeigt ein Diagramm an, das den Prozentsatz der Auslastung auf den Datenfestplatten im Storage-Aggregat im ausgewählten Zeitrahmen anzeigt.

Die Auslastung schließt nur Lese- und Schreibanfragen der Festplatte aus dem ausgewählten Volume-Workload ein. Lesezugriffe aus dem Cache sind nicht enthalten. Die Auslastung ist spezifisch für den ausgewählten Volume Workload, nicht für alle Workloads auf den Festplatten. Wenn ein überwachtes Volume an einer Volume-Verschiebung beteiligt ist, beziehen sich die Auslastungswerte in diesem Diagramm auf das Zielaggregat, zu dem das Volume verschoben wurde.

Darstellung der Performance-Daten

Unified Manager verwendet Diagramme oder Diagramme, um Ihnen Volume-Performance-Statistiken und Ereignisse über einen bestimmten Zeitraum anzuzeigen.

Mithilfe der Diagramme können Sie den Zeitbereich anpassen, für den Daten angezeigt werden sollen. Die Daten werden mit dem Zeitrahmen auf der horizontalen Achse des Diagramms und den Zählern auf der vertikalen Achse angezeigt, wobei Punktintervalle entlang der Diagrammlinien angezeigt werden. Die vertikale Achse ist dynamisch; die Werte passen sich an die Spitzen der erwarteten oder tatsächlichen Werte an.

Auswählen von Zeitrahmens

Auf der Seite Performance/Volume Details können Sie im Historic Data Chart einen Zeitrahmen für alle Diagramme auf der Seite auswählen. Die schaltflächen 1d, 5d, 10d und 30d geben 1 Tag bis 30 Tage (1 Monat) an und mit der Schaltfläche **Benutzerdefiniert** können Sie einen benutzerdefinierten Zeitbereich innerhalb dieser 30 Tage festlegen. Jeder Punkt in einem Diagramm entspricht einem Erfassungsintervall von 5 Minuten, und es werden maximal 30 Tage historische Performance-Daten aufbewahrt. Beachten Sie, dass Intervalle auch Netzwerkverzögerungen und andere Anomalien berücksichtigen.

In diesem Beispiel hat das Historic Data Chart einen Zeitrahmen auf den Anfang und das Ende des Monats März eingestellt. Im ausgewählten Zeitrahmen sind alle historischen Daten vor März ausgegraut.

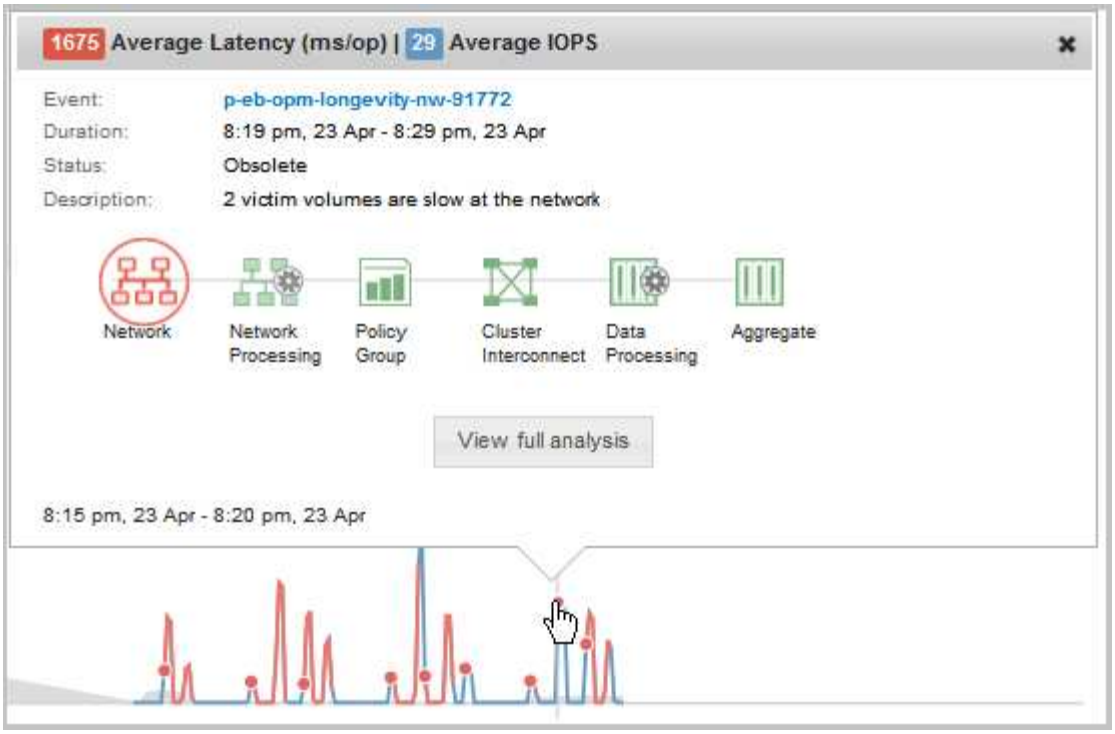
Anzeigen von Datenpunktinformationen

Um die Informationen zu Datenpunkten in einem Diagramm anzuzeigen, können Sie den Cursor über einen bestimmten Punkt im Diagramm positionieren, und ein Popup-Feld zeigt die Werte-, Datums- und Zeitinformationen an.

Wenn Sie in diesem Beispiel den Mauszeiger über das IOPS-Diagramm auf der Seite „Performance/Volume Details“ positionieren, werden die Reaktionszeiten und die Werte der Vorgänge zwischen 3:50 Uhr angezeigt Und 3:55 Uhr Am 20. Oktober.

Anzeigen von Performance-Ereignisinformationen

Um Event-Informationen auf einem Diagramm anzuzeigen, können Sie den Mauszeiger über ein Event-Symbol positionieren, um zusammenfassende Informationen in einem Popup-Feld anzuzeigen. Alternativ können Sie auf das Event-Symbol klicken, um ausführlichere Informationen zu erhalten.



In diesem Beispiel werden auf der Seite Performance/Volume-Details durch Klicken auf ein Ereignissymbol im Latenzdiagramm detaillierte Informationen zum Ereignis in einem Popup-Feld angezeigt. Das Ereignis wird auch in der Ereignisliste hervorgehoben.

Analyse von Performance-Ereignissen

Sie können Performance-Ereignisse analysieren, um zu ermitteln, wann sie erkannt wurden, ob sie aktiv (neu oder bestätigt) oder veraltet sind, die betroffenen Workloads und Cluster-Komponenten betroffen sind und die Optionen für die Behebung von Ereignissen selbst verfügbar sind.

Anzeigen von Informationen zu Performance-Ereignissen

Auf der Seite „Ereignisinventar“ können Sie eine Liste aller neuen und veralteten Performanceereignisse auf den von Unified Manager zu überwachenden Clustern anzeigen. Durch die Anzeige dieser Informationen können Sie die kritischsten Ereignisse bestimmen und anschließend detaillierte Informationen abrufen, um die Ursache des Ereignisses zu bestimmen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue oder veraltete Performanceereignisse vorliegen.

Über diese Aufgabe

Die Liste der Ereignisse wird nach festgestellter Zeit sortiert, wobei die letzten Ereignisse zuerst aufgeführt werden. Sie können auf eine Spaltenüberschrift klicken, um die Ereignisse basierend auf dieser Spalte zu sortieren. Beispielsweise können Sie nach der Spalte Status sortieren, um Ereignisse nach dem Schweregrad

anzuzeigen. Wenn Sie nach einem bestimmten Ereignis oder nach einem bestimmten Ereignis suchen, können Sie mit den Filter- und Suchmechanismen die Liste der Ereignisse, die in der Liste angezeigt werden, verfeinern.

Ereignisse aus allen Quellen werden auf dieser Seite angezeigt:

- Benutzerdefinierte Richtlinie für Leistungsschwellenwerte
- Systemdefinierte Performance-Schwellenwertrichtlinie
- Dynamischer Performance-Schwellenwert

Die Spalte Ereignistyp enthält die Quelle des Ereignisses. Sie können ein Ereignis auswählen, um Details zum Ereignis auf der Seite Ereignisdetails anzuzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Events**.
2. Suchen Sie ein Ereignis, das Sie analysieren möchten, und klicken Sie auf den Ereignisnamen.

   Die Detailseite für das Ereignis wird angezeigt.

> Sie können die Detailseite für ein Ereignis auch anzeigen, indem Sie auf der Seite des Performance Explorers auf den Link „Ereignisname“ und aus einer E-Mail-Benachrichtigung klicken.

Analyse von Ereignissen aus benutzerdefinierten Performance-Schwellenwerten

Ereignisse, die aus benutzerdefinierten Schwellenwerten generiert werden, deuten darauf hin, dass ein Performance-Zähler für ein bestimmtes Storage-Objekt, z. B. ein Aggregat oder ein Volume, den in der Richtlinie definierten Schwellenwert überschritten hat. Dies gibt an, dass beim Cluster-Objekt ein Performance-Problem auftritt.

Auf der Seite Ereignisdetails können Sie das Leistungsereignis analysieren und bei Bedarf Korrekturmaßnahmen ergreifen, um die Leistung wieder normal zu machen.

Reaktion auf benutzerdefinierte Performance-Schwellenwertereignisse

Sie können Unified Manager verwenden, um Performance-Ereignisse zu untersuchen, die durch einen Performance-Zähler durch eine benutzerdefinierte Warnung oder einen kritischen Schwellenwert verursacht werden. Sie können auch Unified Manager verwenden, um den Systemzustand der Cluster-Komponente zu überprüfen, um zu ermitteln, ob kürzlich Systemzustandsereignisse auf der Komponente, die zum Performance-Ereignis beigetragen haben, erkannt wurden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue oder veraltete Performanceereignisse vorliegen.

Schritte

1. Rufen Sie die Seite **Event** Details auf, um Informationen zum Event anzuzeigen.
2. Lesen Sie die **Beschreibung**, die die Schwellenverletzung beschreibt, die das Ereignis verursacht hat.

   Beispielsweise hat die Meldung „`Latency value of 456 ms/op hat ein WARNEREIGNIS auf der Grundlage des Schwellenwerts von 400 ms/op` ausgelöst. Dies zeigt an, dass ein Latenzwarnereignis für das Objekt aufgetreten ist.

3. Bewegen Sie den Mauszeiger über den Richtliniennamen, um Details zur Schwellenwertrichtlinie anzuzeigen, die das Ereignis ausgelöst hat.

   Dazu zählen der Richtlinienname, der zu bewertete Performance-Zähler, der Zählerwert, der nicht durchbrochen werden muss, um es als kritisches oder Warnereignis zu betrachten, und die Dauer, bis zu der der Zähler den Wert überschreiten muss.

4. Notieren Sie sich die **Event Trigger Time**, damit Sie untersuchen können, ob gleichzeitig andere Ereignisse aufgetreten sind, die zu diesem Ereignis beigetragen haben könnten.
5. Führen Sie eine der folgenden Optionen aus, um das Ereignis genauer zu untersuchen, um festzustellen, ob Sie Maßnahmen zur Behebung des Leistungsproblems durchführen müssen:

Option	Mögliche Ermittlungsmaßnahmen
Klicken Sie auf den Namen des Quellobjekts, um die Explorer-Seite für dieses Objekt anzuzeigen.	Auf dieser Seite können Sie die Objektdetails anzeigen und dieses Objekt mit anderen ähnlichen Storage-Objekten vergleichen. So wird ersichtlich, ob es bei anderen Storage-Objekten um die gleiche Zeit ein Performance-Problem gibt. Um zum Beispiel zu sehen, ob andere Volumes auf demselben Aggregat auch ein Performance-Problem haben.
Klicken Sie auf den Cluster-Namen, um die Seite „Cluster Summary“ anzuzeigen.	Auf dieser Seite können Sie die Details für den Cluster anzeigen, auf dem dieses Objekt residiert, um zu sehen, ob weitere Performance-Probleme zur gleichen Zeit aufgetreten sind.

Analyse von Ereignissen aus systemdefinierten Performance-Schwellenwerten

Ereignisse, die aus systemdefinierten Performance-Schwellenwerten generiert werden, geben an, dass ein Performance-Zähler oder eine Gruppe von Performance-Zählern für ein bestimmtes Storage-Objekt den Schwellenwert aus einer systemdefinierten Richtlinie überschritten hat. Dies bedeutet, dass es beim Storage-Objekt, z. B. in einem Aggregat oder Node, zu einem Performance-Problem kommt.

Auf der Seite Ereignisdetails können Sie das Leistungsereignis analysieren und bei Bedarf Korrekturmaßnahmen ergreifen, um die Leistung wieder normal zu machen.

Systemdefinierte Schwellenwertrichtlinien sind auf Cloud Volumes ONTAP-, ONTAP Edge- oder ONTAP Select-Systemen nicht aktiviert.

Reaktion auf systemdefinierte Performance-Schwellenwertereignisse

Sie können Unified Manager verwenden, um Performance-Ereignisse zu untersuchen, die durch einen Performance-Zähler einen vom System definierten Warnschwellenwert verursacht werden. Sie können auch den Systemzustand der Cluster-Komponente mit Unified Manager überprüfen, um zu ermitteln, ob kürzlich entdeckte Ereignisse auf der Komponente, die zum Performance-Ereignis beigetragen hat.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue oder veraltete Performanceereignisse vorliegen.

Schritte

1. Rufen Sie die Seite **Event** Details auf, um Informationen zum Event anzuzeigen.
2. Lesen Sie die **Beschreibung**, die die Schwellenverletzung beschreibt, die das Ereignis verursacht hat.

   Beispielsweise hat die Meldung „`Node Auslastungswert von 90 % ein WARNEREIGNIS ausgelöst, basierend auf dem Schwellenwert von 85 %`“ zeigt an, dass ein Warnereignis für die Node-Auslastung des Cluster-Objekts aufgetreten ist.

3. Notieren Sie sich die **Event Trigger Time**, damit Sie untersuchen können, ob gleichzeitig andere Ereignisse aufgetreten sind, die zu diesem Ereignis beigetragen haben könnten.
4. Lesen Sie unter **Systemdiagnose** die kurze Beschreibung des Analysetyps, den die systemdefinierte Richtlinie auf dem Clusterobjekt ausführt.

   Bei einigen Ereignissen wird neben der Diagnose ein grünes oder rotes Symbol angezeigt, um anzugeben, ob bei dieser Diagnose ein Problem gefunden wurde. Für andere Typen von systemdefinierten Ereignistypen wird die Zählerdiagramme für das Objekt angezeigt.

5. Klicken Sie unter **Suggested Actions** auf den Link **Help me do this**, um die vorgeschlagenen Aktionen anzuzeigen, die Sie durchführen können, um das Aufkommen selbst zu lösen.

Reaktion auf Performance-Ereignisse der QoS-Richtliniengruppe

Unified Manager generiert Warnereignisse für die QoS-Richtlinie, wenn der Workload-Durchsatz (IOPS/TB oder MB/s) die festgelegte ONTAP-QoS-Richtlinieneinstellung überschritten hat und die Workload-Latenz sich beeinträchtigt. Diese systemdefinierten Ereignisse bieten die Möglichkeit, potenzielle Performance-Probleme zu beheben, bevor viele Workloads von der Latenz beeinträchtigt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

Über diese Aufgabe

Unified Manager generiert Warnereignisse bei Verstößen gegen QoS-Richtlinien, wenn der Workload-Durchsatz die festgelegte QoS-Richtlinieneinstellung während jeder Performance-Erfassungsfrist für die

vorherige Stunde überschritten hat. Der Workload-Durchsatz kann den QoS-Schwellenwert für nur einen kurzen Zeitraum während des jeweiligen Erfassungszeitraums überschreiten. Unified Manager zeigt jedoch während des Erfassungszeitraums auf dem Diagramm nur den „durchschnittlichen“-Durchsatz an. Aus diesem Grund erhalten Sie unter Umständen QoS-Ereignisse, während der Durchsatz für einen Workload den im Diagramm angegebenen Richtlinienschwellenwert nicht überschritten hat.

Sie können System Manager oder die Befehle ONTAP zum Verwalten von Richtliniengruppen verwenden, einschließlich der folgenden Aufgaben:

- Erstellen einer neuen Richtliniengruppe für den Workload
- Hinzufügen oder Entfernen von Workloads in einer Richtliniengruppe
- Verschieben eines Workloads zwischen Richtliniengruppen
- Ändern der Durchsatzbegrenzung einer Richtliniengruppe
- Verschieben eines Workloads in ein anderes Aggregat oder Node

Schritte

1. Rufen Sie die Seite **Event** Details auf, um Informationen zum Event anzuzeigen.
2. Lesen Sie die **Beschreibung**, die die Schwellenverletzung beschreibt, die das Ereignis verursacht hat.

   Beispielsweise hat die Meldung „IOPS-Wert von 1,352 IOPS auf vol1_NFS1 ein WARNEREIGNIS ausgelöst, um potenzielle Performance-Probleme für den Workload zu identifizieren“ zeigt, dass ein QoS max IOPS-Ereignis auf Volume vol1_NFS1 aufgetreten ist.

3. Lesen Sie den Abschnitt * Ereignisinformationen*, um weitere Informationen darüber zu erhalten, wann das Ereignis eingetreten ist und wie lange das Ereignis aktiv war.

   Außerdem können bei Volumes oder LUNs, die den Durchsatz einer QoS-Richtlinie teilen, die Namen der drei wichtigsten Workloads angezeigt werden, die die meisten IOPS oder MB/s verbrauchen.

4. Überprüfen Sie im Abschnitt **Systemdiagnose** die beiden Diagramme: Eine für den gesamten durchschnittlichen IOPS oder MB/s (je nach Ereignis) und eine für Latenz. Nach Anordnung der Workloads wird ersichtlich, welche Cluster-Komponenten sich am stärksten auf die Latenz auswirken, wenn der Workload zur Markierung für die QoS-Höchstgrenze nähert.

   Bei einem Ereignis einer Shared-QoS-Richtlinie werden die drei wichtigsten Workloads im Durchsatzdiagramm dargestellt. Wenn mehr als drei Workloads die QoS-Richtlinie nutzen, werden in der Kategorie „andere Workloads“ zusätzliche Workloads hinzugefügt. Außerdem zeigt das Latenzdiagramm die durchschnittliche Latenz aller Workloads, die Teil der QoS-Richtlinie sind.

   Beachten Sie, dass bei anpassungsfähigen QoS-Richtlinienereignissen in den Diagrammen für IOPS und MB/s IOPS- oder MB/s-Werte angezeigt werden, die in ONTAP basierend auf der Größe des Volumes aus der zugewiesenen Richtlinie für IOPS/TB-Schwellenwerte konvertiert wurden.

5. Überprüfen Sie im Abschnitt * vorgeschlagene Aktionen* die Vorschläge und bestimmen Sie, welche Maßnahmen Sie durchführen sollten, um eine Erhöhung der Latenz für den Workload zu vermeiden.

   Klicken Sie bei Bedarf auf die Schaltfläche **Hilfe**, um weitere Details zu den vorgeschlagenen Aktionen anzuzeigen, die Sie durchführen können, um das Leistungsereignis zu lösen.

Allgemeines zu Ereignissen durch anpassungsfähige QoS-Richtlinien mit einer definierten Blockgröße

Adaptive QoS-Richtliniengruppen skalieren je nach Volume-Größe automatisch eine Durchsatzdecke oder -Stellfläche und erzielen so bei veränderter Volume-Größe das Verhältnis von IOPS zu TB. Ab ONTAP 9.5 können Sie in der QoS-Richtlinie die Blockgröße festlegen, um einen MB/s-Schwellenwert gleichzeitig effektiv anzuwenden.

Durch die Zuweisung eines IOPS-Schwellenwerts in einer anpassungsfähigen QoS-Richtlinie wird nur die Anzahl der Vorgänge festgelegt, die in jedem Workload ausgeführt werden. Abhängig von der Blockgröße des Clients, die auf dem Client die Workloads generiert, enthalten einige IOPS sehr viel mehr Daten. Die Nodes, die die Vorgänge verarbeiten, werden daher deutlich entlastet.

Der MB/s-Wert für einen Workload wird mithilfe der folgenden Formel generiert:

```
MBps = (IOPS * Block Size) / 1000
```

Wenn ein Workload durchschnittlich 3,000 IOPS ist und die Blockgröße auf dem Client auf 32 KB eingestellt ist, dann sind die effektiven MB/s für diesen Workload 96. Wenn bei diesem gleichen Workload ein Mittelwert von 3,000 IOPS und die Blockgröße auf dem Client auf 48 KB eingestellt ist, dann sind die effektiven MB/s für diese Workload 144. Bei einer größeren Blockgröße verarbeitet der Node 50 % mehr Daten.

Sehen wir uns nun die folgende anpassungsfähige QoS-Richtlinie an, die über eine definierte Blockgröße verfügt und die Art der Auslösung von Ereignissen basierend auf der Blockgröße des Clients.

Erstellen Sie eine Richtlinie und legen Sie den Spitzendurchsatz auf 2,500 IOPS/TB mit einer Blockgröße von 32 KB fest. Dadurch wird der MB/s-Schwellenwert für ein Volumen mit 1 TB Kapazität effektiv auf 80 MBit/s ((2500 IOPS * 32 KB) / 1000) eingestellt. Beachten Sie, dass Unified Manager ein Warnereignis generiert, wenn der Durchsatzwert 10 % unter dem definierten Schwellenwert liegt. Ereignisse werden in den folgenden Situationen erzeugt:

Genutzte Kapazität	**Das Ereignis wird erzeugt, wenn der Durchsatz diese …**
IOPS	MB/Sek.
1 TB	2,250 IOPS
72 Mbit/s	2 TB
4,500 IOPS	144 Mbit/s
5 TB	11,250 IOPS

Wenn das Volume 2 TB des verfügbaren Speicherplatzes verwendet und der IOPS 4,000 beträgt und die QoS-Blockgröße auf 32 KB auf dem Client eingestellt ist, beträgt der MB/s-Durchsatz 128 MB/s ((4,000 IOPS * 32 KB)/1000). In diesem Szenario wird kein Ereignis generiert, da sowohl 4,000 IOPS als auch 128 Mbps unter dem Schwellenwert für ein Volume mit 2 TB Speicherplatz liegen.

Wenn das Volume 2 TB des verfügbaren Speicherplatzes verwendet und der IOPS 4,000 beträgt und die QoS-Blockgröße auf dem Client auf 64 KB gesetzt ist, dann beträgt der MB/s-Durchsatz 256 MB/s ((4,000 IOPS * 64 KB)/1000). In diesem Fall generieren die 4,000 IOPS kein Ereignis, der MB/s-Wert von 256 MB/s liegt

jedoch über dem Schwellenwert von 144 MB/s und ein Ereignis wird generiert.

Wenn aus diesem Grund ein Ereignis aufgrund einer MB/s-Verletzung für eine adaptive QoS-Richtlinie, die die Blockgröße enthält, ausgelöst wird, wird im Abschnitt Systemdiagnose der Seite Ereignisdetails ein MB/s-Diagramm angezeigt. Wenn das Ereignis aufgrund einer Verletzung des IOPS für die Richtlinie zur adaptiven QoS ausgelöst wird, wird im Abschnitt Systemdiagnose ein IOPS-Diagramm angezeigt. Wenn sowohl für IOPS als auch für MB/s eine Sicherheitsverletzung auftritt, erhalten Sie zwei Ereignisse.

Weitere Informationen zum Anpassen der QoS-Einstellungen finden Sie im Power Guide *ONTAP 9 zur Leistungsüberwachung*.

"ONTAP 9 Leistungsüberwachung – Stromversorgungshandbuch"

Reaktion auf Node-Ressourcen überlastete Performance-Ereignisse

Unified Manager generiert zu stark ausgelastete Warnmeldungen bei Node-Ressourcen, wenn ein einzelner Node über die Grenzen seiner betrieblichen Effizienz arbeitet und so die Workload-Latenzen potenziell beeinträchtigen. Diese systemdefinierten Ereignisse bieten die Möglichkeit, potenzielle Performance-Probleme zu beheben, bevor viele Workloads von der Latenz beeinträchtigt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue oder veraltete Performanceereignisse vorliegen.

Über diese Aufgabe

Unified Manager generiert Warnereignisse für überlastete Node-Ressourcen bei Richtlinienverstößen, indem Nodes gesucht werden, die mehr als 30 Minuten lang mehr als 100 % der Performance-Kapazität nutzen.

Sie können diesen Typ eines Performance-Problems mit System Manager oder den Befehlen ONTAP beheben, einschließlich der folgenden Aufgaben:

- Erstellen und Anwenden einer QoS-Richtlinie auf alle Volumes oder LUNs, die die Systemressourcen überbeanspruchen
- Reduzierung des maximalen Durchsatzes bei QoS in einer Richtliniengruppe, auf die Workloads angewendet wurden
- Verschieben eines Workloads in ein anderes Aggregat oder Node
- Erhöhung der Kapazität durch Hinzufügen von Festplatten zum Node oder durch Upgrade auf einen Node mit schnellerer CPU und mehr RAM

Schritte

1. Rufen Sie die Seite **Event** Details auf, um Informationen zum Event anzuzeigen.
2. Lesen Sie die **Beschreibung**, die die Schwellenverletzung beschreibt, die das Ereignis verursacht hat.

   Zum Beispiel die Meldung „`Perf". Die genutzte Kapazität bei der Einfachheit beträgt 139 %.-02 hat ein WARNEREIGNIS ausgelöst, um potenzielle Performance-Probleme in der Datenverarbeitungseinheit zu identifizieren.`“ zeigt an, dass die Performance auf der Einfachheit eines Node 02 überlastet ist und die Node-Performance beeinträchtigt.

3. Lesen Sie im Abschnitt **Systemdiagnose** die drei Diagramme durch: Eins für die auf dem Node genutzte Performance-Kapazität, eins für die durchschnittlichen Storage-IOPS durch die wichtigsten Workloads und eins für die Latenz bei den wichtigsten Workloads. Auf diese Weise sehen Sie, welche Workloads die Ursache der Latenz auf dem Node sind.

   Sie können die QoS-Richtlinien auf welche Workloads angewendet werden und welche nicht, indem Sie den Mauszeiger über das IOPS-Diagramm bewegen.

4. Überprüfen Sie im Abschnitt * vorgeschlagene Aktionen* die Vorschläge und bestimmen Sie, welche Maßnahmen Sie durchführen sollten, um eine Erhöhung der Latenz für den Workload zu vermeiden.

   Klicken Sie bei Bedarf auf die Schaltfläche **Hilfe**, um weitere Details zu den vorgeschlagenen Aktionen anzuzeigen, die Sie durchführen können, um das Leistungsereignis zu lösen.

Analyse von Ereignissen aus dynamischen Leistungsschwellenwerten

Ereignisse, die aus dynamischen Schwellenwerten generiert werden, geben an, dass die tatsächliche Reaktionszeit (Latenz) für einen Workload zu hoch oder zu niedrig ist im Vergleich zum erwarteten Reaktionszeitbereich. Auf der Seite Ereignisdetails können Sie das Leistungsereignis analysieren und bei Bedarf Korrekturmaßnahmen ergreifen, um die Leistung wieder normal zu machen.

Dynamische Performance-Schwellenwerte sind auf Cloud Volumes ONTAP-, ONTAP Edge- oder ONTAP Select-Systemen nicht aktiviert.

Identifizierung der Opfer-Workloads, die an einem dynamischen Performance-Ereignis beteiligt sind

In Unified Manager können Sie ermitteln, welche Volume Workloads die höchste Abweichung der Reaktionszeit (Latenz) aufweisen, die durch eine Storage-Komponente verursacht wurde. Anhand der Identifizierung dieser Workloads können Sie nachvollziehen, warum die Client-Applikationen, auf die sie zugreifen, langsamer als normal ausgeführt wurden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete dynamische Leistungsereignisse vorliegen.

Über diese Aufgabe

Auf der Seite Ereignisdetails wird eine Liste der benutzerdefinierten und systemdefinierten Workloads angezeigt, die nach der höchsten Abweichung von Aktivität oder Auslastung der Komponente oder am stärksten vom Ereignis betroffen sind. Die Werte basieren auf den Peaks, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Aktivität **Opfer-Workloads** aus.
3. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten Workloads

anzuzeigen, die sich auf die Komponente auswirken, und den Namen des Workloads mit dem Opfer anzuzeigen.

Identifizierung problematischer Workloads, die an einem dynamischen Performance-Ereignis beteiligt sind

In Unified Manager können Sie ermitteln, welche Workloads die höchste Nutzungsabweichung einer Clusterkomponente aufweisen. Anhand der Ermittlung dieser Workloads können Sie nachvollziehen, warum bestimmte Volumes des Clusters über langsame Reaktionszeiten (Latenz) verfügen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete dynamische Leistungsereignisse vorliegen.

Über diese Aufgabe

Auf der Seite Ereignisdetails wird eine Liste der benutzerdefinierten und systemdefinierten Workloads angezeigt, die nach der höchsten Nutzung der Komponente oder am stärksten von dem Ereignis betroffen sind. Die Werte basieren auf den Peaks, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Aktivität **Bully Workloads** aus.
3. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten problematischer Workloads anzuzeigen, die sich auf die Komponente auswirken.

Erkennen von Haifischlasten, die an einem dynamischen Performance-Ereignis beteiligt sind

In Unified Manager können Sie ermitteln, welche Workloads die höchste Nutzungsabweichung einer Storage-Komponente aufweisen. Anhand der Identifizierung dieser Workloads können Sie ermitteln, ob diese Workloads in ein weniger ausgelasttes Cluster verschoben werden sollen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es gibt ein neues, anerkanntes oder überholes dynamisches Ereignis für die Leistung.

Über diese Aufgabe

Auf der Seite Ereignisdetails wird eine Liste der benutzerdefinierten und systemdefinierten Workloads angezeigt, die nach der höchsten Nutzung der Komponente oder am stärksten von dem Ereignis betroffen sind. Die Werte basieren auf den Peaks, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Aktivität **Shark-Workloads** aus.
3. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten Workloads anzuzeigen, die sich auf die Komponente auswirken, und den Namen des Haifischarbeitslasts.

Performance-Ereignisanalyse für eine MetroCluster-Konfiguration

Sie können mit Unified Manager ein Performance-Ereignis für eine MetroCluster-Konfiguration analysieren. Sie können die an dem Ereignis beteiligten Workloads ermitteln und die vorgeschlagenen Maßnahmen zur Lösung prüfen.

MetroCluster-Performance-Ereignisse können auf *bully* Workloads zurückzuführen sein, die die Interswitch-Links (ISLs) zwischen den Clustern überlasten oder aufgrund von Systemzustandsproblemen. Unified Manager überwacht jedes Cluster in einer MetroCluster-Konfiguration unabhängig und berücksichtigt dabei nicht die Performance-Ereignisse in einem Partner-Cluster.

Auf der Seite Unified ManagerDashboards/Überblick werden auch Performance-Ereignisse von beiden Clustern in der MetroCluster-Konfiguration angezeigt.Sie können auch die Health-Seiten von Unified Manager anzeigen, um den Zustand der einzelnen Cluster zu überprüfen und ihre Beziehung anzuzeigen.

Analyse eines dynamischen Performance-Ereignisses auf einem Cluster in einer MetroCluster Konfiguration

Sie können Unified Manager verwenden, um das Cluster in einer MetroCluster-Konfiguration zu analysieren, bei der ein Performance-Ereignis erkannt wurde. Sie können den Cluster-Namen, die Ereigniserkennungszeit und die damit verbundenen Workloads *bully* und *victim* identifizieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Für eine MetroCluster-Konfiguration müssen neue, anerkannte oder veraltete Performance-Ereignisse vorliegen.
- Beide Cluster in der MetroCluster-Konfiguration müssen von derselben Instanz von Unified Manager überwacht werden.

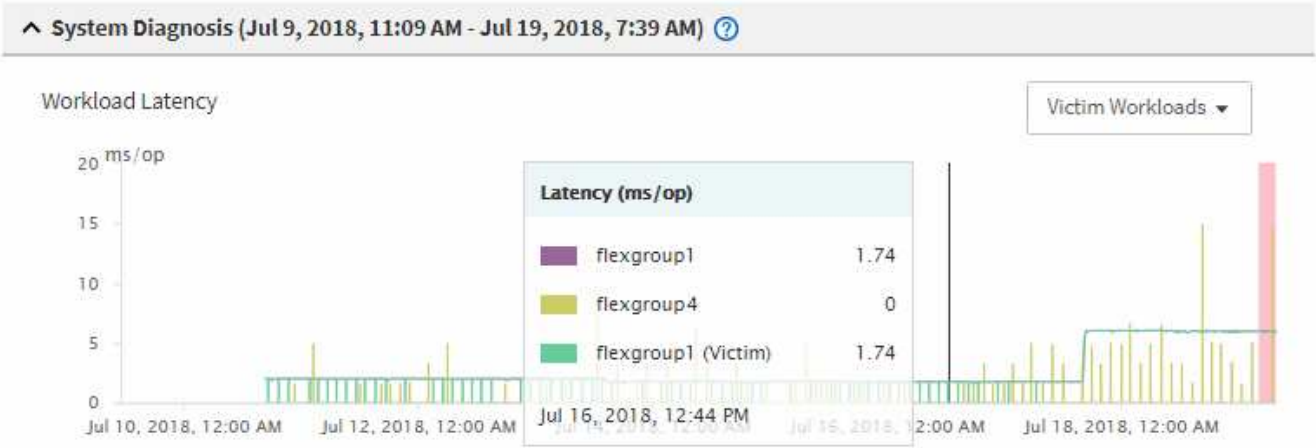
Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Die Ereignisbeschreibung enthält Namen der betroffenen Workloads sowie die Anzahl der betroffenen Workloads.

   In diesem Beispiel ist das Symbol für MetroCluster-Ressourcen rot dargestellt, was bedeutet, dass die MetroCluster-Ressourcen über Konflikte verfügen. Sie positionieren den Cursor über das Symbol, um eine Beschreibung des Symbols anzuzeigen. Oben auf der Seite in der Ereignis-ID identifiziert der Cluster-Name den Namen des Clusters, auf dem das Ereignis erkannt wurde.

3. Notieren Sie sich den Cluster-Namen und die Ereignis-Erkennungszeit, mit der Sie Performance-Ereignisse im Partner-Cluster analysieren können.
4. Überprüfen Sie in den Diagrammen die „_victim_Workloads“, um zu bestätigen, dass ihre Antwortzeiten höher sind als der Performance-Schwellenwert.

   In diesem Beispiel wird der Workload des Opfers im Hover-Text angezeigt. Die Latenzdiagramme werden auf hoher Ebene angezeigt, ein konsistentes Latenzmuster für die betroffenen Opfer-Workloads. Obwohl die anormale Latenz der betroffenen Workloads das Ereignis ausgelöst hat, kann ein konsistentes Latenzmuster darauf hindeuten, dass die Workloads innerhalb des erwarteten Bereichs liegen. Durch einen Spitzen bei den I/O wurde die Latenz erhöht und das Ereignis ausgelöst.



   Falls Sie vor Kurzem eine Applikation auf einem Client installiert haben, der auf diese Volume-Workloads zugreift und die Applikation eine hohe Anzahl an I/O-Vorgängen sendet, kann die Verzögerungen bereits vorwegnehmen. Wenn die Latenz für die Workloads innerhalb des erwarteten Bereichs zurückkehrt, ändert sich der Ereignisstatus zu veraltet und bleibt mehr als 30 Minuten in diesem Status, können Sie das Ereignis wahrscheinlich ignorieren. Wenn das Ereignis andauernde und im neuen Status verbleibt, können Sie es weiter untersuchen, um festzustellen, ob andere Probleme das Ereignis verursacht haben.

5. Wählen Sie im Workload-Durchsatzdiagramm die Option **problematische Workloads** aus, um die problematische Workloads anzuzeigen.

   Die Anwesenheit von problematischer Workloads zeigt an, dass ein Ereignis möglicherweise durch eine oder mehrere Workloads auf dem lokalen Cluster verursacht wurde, bei denen die MetroCluster-Ressourcen überlastet sind. Die anspruchsvollen Workloads weisen eine hohe Abweichung beim Schreibdurchsatz (MB/s) auf.

   Dieses Diagramm wird auf höherer Ebene das Muster des Schreibdurchsatzes (MB/s) für die Workloads angezeigt. Sie können das MB/s-Muster für Schreibvorgänge überprüfen, um einen anormalen Durchsatz zu identifizieren, der darauf hindeutet, dass ein Workload die MetroCluster-Ressourcen übernutzt.

   Wenn an diesem Ereignis keine problematische Workloads beteiligt sind, wurde dieses Ereignis möglicherweise durch ein Systemzustandsproblem mit der Verbindung zwischen den Clustern oder durch

ein Performance-Problem auf dem Partner-Cluster verursacht. Sie können Unified Manager verwenden, um den Systemzustand beider Cluster in einer MetroCluster Konfiguration zu überprüfen. Außerdem können Sie mit Unified Manager Performance-Ereignisse im Partner-Cluster überprüfen und analysieren.

Analyse eines dynamischen Performance-Ereignisses für ein Remote-Cluster auf einer MetroCluster-Konfiguration

Mit Unified Manager können Sie dynamische Performance-Ereignisse auf einem Remote-Cluster in einer MetroCluster-Konfiguration analysieren. Mit der Analyse können Sie ermitteln, ob ein Ereignis im Remote-Cluster ein Ereignis auf seinem Partner-Cluster verursacht hat.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen ein Performance-Ereignis auf einem lokalen Cluster in einer MetroCluster Konfiguration analysiert und die Ereigniserkennungszeit ermittelt haben.
- Sie müssen den Zustand des lokalen Clusters und dessen am Performance-Ereignis beteiligten Partner-Clusters überprüft und den Namen des Partner-Clusters erhalten haben.

Schritte

1. Loggen Sie sich bei der Unified Manager-Instanz ein, die das Partner-Cluster überwacht.
2. Klicken Sie im linken Navigationsbereich auf **Events**, um die Ereignisliste anzuzeigen.
3. Wählen Sie im Auswahlfeld **Zeitbereich** die Option **Letzte Stunde** aus und klicken Sie dann auf **Bereich anwenden**.
4. Wählen Sie im Auswahlfeld **Filterung** im linken Dropdown-Menü die Option **Cluster** aus, geben Sie den Namen des Partner Clusters in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.

   Wenn während der letzten Stunde keine Ereignisse für das ausgewählte Cluster vorhanden sind, zeigt dies an, dass es während des Ereignisses beim Partner keine Performance-Probleme aufgetreten sind.

5. Wenn im ausgewählten Cluster Ereignisse über die letzte Stunde erkannt wurden, vergleichen Sie die Ereignis-Erkennungszeit mit der Ereignis-Erkennungszeit für das Ereignis auf dem lokalen Cluster.

   Wenn diese Ereignisse problematische Workloads verursachen, die zu Konflikten bei der Datenverarbeitungskomponente führen, könnte ein oder mehrere dieser Punkte das Ereignis auf dem lokalen Cluster verursacht haben. Sie können auf das Ereignis klicken, um es zu analysieren und die vorgeschlagenen Aktionen für die Lösung auf der Seite Ereignisdetails zu prüfen.

   Wenn diese Ereignisse keine problematische Workloads betreffen, wurden sie nicht zum Performance-Ereignis auf dem lokalen Cluster verursacht.

Er reagiert auf ein dynamisches Performance-Ereignis, das durch die QoS-Richtliniengruppendrosselung verursacht wird

Mithilfe von Unified Manager können Sie ein Performance-Ereignis untersuchen, das durch eine Richtliniengruppe für Quality of Service (QoS) verursacht wird, die den Workload-Durchsatz (MB/s) drosselt. Die Drosselung hat die Reaktionszeiten (Latenz) von Volume-Workloads in der Richtliniengruppe erhöht. Anhand der Ereignisinformationen können Sie bestimmen, ob neue Grenzen für die

Richtliniengruppen erforderlich sind, um die Drosselung zu stoppen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Lesen Sie die **Beschreibung**, die den Namen der von der Drosselung betroffenen Workloads anzeigt.

   Die Beschreibung kann dieselbe Arbeitslast für das Opfer und den Täter anzeigen, da die Drosselung den Workload zum Opfer selbst macht.

3. Notieren Sie den Namen des Volumes mit einer Anwendung wie einem Texteditor.

   Sie können den Volume-Namen suchen, um ihn später zu finden.

4. Wählen Sie in den Diagrammen Workload-Latenz und Workload-Aktivität **Bully Workloads** aus.
5. Bewegen Sie den Mauszeiger über die Diagramme, um die obersten benutzerdefinierten Workloads anzuzeigen, die sich auf die Richtliniengruppe auswirken.

   Die Arbeitslast oben in der Liste hat die höchste Abweichung und verursacht die Drosselung. Die Aktivität entspricht dem Prozentsatz des von den einzelnen Workloads verwendeten Richtliniengruppenlimits.

6. Navigieren Sie zur Seite **Performance/Volume Details** für den Top Workload.
7. Wählen Sie **Aufbruchdaten nach** aus.
8. Aktivieren Sie das Kontrollkästchen neben **Latenz*****, um alle Latenzdiagramme auszuwählen.
9. Wählen Sie unter **IOPS** die Option **Lese-/Schreibvorgänge/Sonstiges** aus.
10. Klicken Sie Auf **Absenden**.

    Die Aufschlüsselung werden unter dem Latenzdiagramm und dem IOPS-Diagramm angezeigt.

11. Vergleichen Sie das Diagramm **Policy Group Impact** mit dem Diagramm **Latenz**, um zu sehen, welcher Prozentsatz der Drosselung sich zum Zeitpunkt des Ereignisses auf die Latenz ausgewirkt hat.

    Die Richtliniengruppe weist einen maximalen Durchsatz von 1,000 Operationen pro Sekunde (in op/s) auf, die die Workloads in ihr nicht zusammen überschreiten können. Zum Zeitpunkt des Ereignisses führten die Workloads in der Richtliniengruppe einen Gesamtdurchsatz von über 1,200 Op/s durch, sodass die Richtliniengruppe ihre Aktivität wieder auf 1,000 Op/Sek. ausbremsen konnte Das Policy Group Impact-Diagramm zeigt, dass die Drosselung 10 % der gesamten Latenz verursachte und bestätigt, dass die Drosselung das Ereignis verursacht hat.

12. Überprüfen Sie das Diagramm **Cluster Components**, das die gesamte Latenz nach Clusterkomponente anzeigt.

    Die Latenz befindet sich in der Richtliniengruppe am höchsten, was bestätigt, dass die Drosselung das Ereignis verursacht hat.

13. Vergleichen Sie das Diagramm * Lese-/Schreib-Latenz* mit dem Diagramm * Lese-/Schreibvorgänge/anderes*.

Beide Diagramme zeigen eine hohe Anzahl von Leseanforderungen mit einer hohen Latenz, jedoch ist die Anzahl der Anfragen und die Menge der Latenz für Schreibanforderungen niedrig. Anhand dieser Werte können Sie ermitteln, ob ein hoher Durchsatz oder eine höhere Anzahl an Operationen die Latenz erhöht. Sie können diese Werte verwenden, wenn Sie sich entscheiden, ein Richtliniengruppenlimit auf den Durchsatz oder die Operationen zu legen.

14. Verwenden Sie OnCommand System Manager, um die aktuelle Obergrenze für die Richtliniengruppe auf 1,300 Op/Sek. zu erhöhen
15. Kehren Sie nach einem Tag wieder zu Unified Manager zurück, und suchen Sie nach dem Namen des Workloads, den Sie in Schritt 3 aufgenommen haben.

    Die Seite Performance/Volume Details wird angezeigt.

16. Wählen Sie **Aufbrechen von Daten um** > **IOPS**.
17. Klicken Sie Auf **Absenden**.

    Das Diagramm Lese-/Schreibvorgänge/Sonstiges wird angezeigt.

18. Zeigen Sie unten auf der Seite den Cursor auf das Symbol Ereignis ändern ( ) Für die Änderung der Policy-Gruppengrenzen.
19. Vergleichen Sie das Diagramm **Lese/Schreibvorgänge/Sonstiges** mit dem Diagramm **Latenz**.

    Die Lese- und Schreibanfragen sind dieselben, aber die Drosselung hat gestoppt und die Latenz ist gesunken.

Reaktion auf ein dynamisches Performance-Ereignis aufgrund eines Festplattenausfalls

Mit Unified Manager können Sie ein Performance-Ereignis untersuchen, das durch die Überprovisionierung eines Aggregats verursacht wird. Sie können auch Unified Manager verwenden, um den Systemzustand des Aggregats zu überprüfen, um zu ermitteln, ob kürzlich auf dem Aggregat erkannte Systemzustandsereignisse zum Performance-Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Lesen Sie die **Description**, die die Workloads beschreibt, die an dem Ereignis beteiligt sind, und die Clusterkomponente, die mit einem Konflikt verbunden ist.

   Es gibt mehrere Opfer-Volumes, deren Latenz von der Cluster-Komponente mit Konflikten beeinträchtigt wurde. Das Aggregat, das sich in der Mitte eines RAID-Rekonstruktionss befindet, um die ausgefallene Festplatte durch eine Ersatzfestplatte zu ersetzen, ist die Clusterkomponente. Unter „Komponente in Konflikt“ ist das Aggregat-Symbol rot hervorgehoben und der Name des Aggregats wird in Klammern angezeigt.

3. Wählen Sie im Diagramm Workload-Auslastung die Option **Bully Workloads** aus.

4. Bewegen Sie den Mauszeiger über das Diagramm, um die obersten Workloads anzuzeigen, die sich auf die Komponente auswirken.

   Die wichtigsten Workloads mit der höchsten Spitzenauslastung seit dem Erkennen des Ereignisses werden oben in der Tabelle angezeigt. Einer der wichtigsten Workloads ist der durch das System definierte Workload Disk Health, der auf eine RAID-Rekonstruktion hinweist. Eine Rekonstruktion ist der interne Prozess zur Wiederherstellung des Aggregats mit der freien Platte. Der Disk Health Workload und die anderen Workloads im Aggregat verursachten wahrscheinlich die Konflikte im Aggregat und das zugehörige Ereignis.

5. Nachdem Sie bestätigt haben, dass die Aktivitäten des Festplatten-Status-Workloads das Ereignis verursacht haben, warten Sie ca. 30 Minuten, bis die Rekonstruktion abgeschlossen ist, und warten Sie, bis Unified Manager das Ereignis analysiert und erkennt, ob es noch im Aggregat zu Konflikten kommt.
6. Suchen Sie in Unified Manager nach der Ereignis-ID, die Sie in Schritt 2 aufgezeichnet haben.

   Das Ereignis für den Festplattenausfall wird auf der Seite „Ereignisdetails“ angezeigt. Überprüfen Sie nach Abschluss der RAID-Rekonstruktion, ob der Status veraltet ist, und geben Sie an, dass das Ereignis behoben ist.

7. Wählen Sie im Workload-Auslastungsdiagramm **Bully Workloads** aus, um die Workloads auf dem Aggregat nach Spitzenauslastung zu sehen.
8. Navigieren Sie zur Seite **Performance/Volume Details** für den Top Workload.
9. Klicken Sie auf **1d**, um die letzten 24 Stunden (1 Tag) der Daten für das ausgewählte Volumen anzuzeigen.

   Im Latenzdiagramm ist ein roter Punkt (🔴) Gibt an, wann das Ereignis des Festplattenfehlers aufgetreten ist.

10. Wählen Sie **Aufbruchdaten nach** aus.
11. Wählen Sie unter **Components** die Option **Disk Utiation**.
12. Klicken Sie Auf **Absenden**.

    Das Diagramm zur Festplattenauslastung zeigt ein Diagramm aller Lese- und Schreibanforderungen vom ausgewählten Workload bis zu den Festplatten des Zielaggregats an.

13. Vergleichen Sie die Daten im Diagramm **Disk Utiation** mit den Daten zum Zeitpunkt des Ereignisses im Diagramm **Latenz**.

    Zum Zeitpunkt des Ereignisses zeigt die Plattenauslastung einen hohen Anteil an Lese- und Schreibvorgängen durch die RAID-Rekonstruktionsprozesse an, was die Latenz des ausgewählten Volumes erhöht. Einige Stunden nach dem Ereignis waren sowohl die Lese- als auch die Schreibvorgänge sowie die Latenz gesunken, sodass die Konflikte zwischen dem Aggregat nicht mehr bestehen.

Er reagiert auf ein dynamisches Performance-Ereignis, das durch HA Takeover verursacht wird

Mit Unified Manager können Sie ein Performance-Ereignis anhand hoher Datenverarbeitung auf einem Cluster Node in einem Hochverfügbarkeitspaar (HA-Paar) untersuchen. Sie können auch Unified Manager verwenden, um den Systemzustand der Nodes zu überprüfen, ob kürzlich entdeckte Systemzustandsereignisse auf den Nodes, die zum Performance-Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis anzuzeigen.
2. Lesen Sie die **Description**, die die Workloads beschreibt, die an dem Ereignis beteiligt sind, und die Clusterkomponente, die mit einem Konflikt verbunden ist.

   Es gibt ein Opfer-Volume, dessen Latenz von der Cluster-Komponente im Konflikt beeinträchtigt wurde. Der Datenverarbeitungs-Node, der alle Workloads vom Partner-Node übernommen hat, ist die Cluster-Komponente im Konflikt. Unter Komponente in Konflikt wird das Symbol für die Datenverarbeitung rot markiert und der Name des Node, der zum Zeitpunkt des Ereignisses die Datenverarbeitung verarbeitet hat, wird in Klammern angezeigt.

3. Klicken Sie in der **Beschreibung** auf den Namen des Opfervolumens.

   Die Seite Performance/Volume Details wird angezeigt. Im unteren Bereich der Seite in der Zeile Ereignisse Zeit wird ein Symbol für das Ereignis ändern ( ) Gibt die Zeit an, zu der Unified Manager den Start der HA-Übernahme erkannt hat.

4. Zeigen Sie den Cursor auf das Änderungsereignis-Symbol für die HA-Übernahme.

   Details zum HA Takeover werden in der Tabelle „Ereignisse“ angezeigt. Im Latenzdiagramm zeigt ein Ereignis an, dass das ausgewählte Volume aufgrund einer hohen Latenz um die gleiche Zeit wie das HA-Takeover den Performance-Schwellenwert überschritten hat.

5. Wählen Sie **Aufbruchdaten nach** aus.
6. Wählen Sie unter **Latenz Cluster-Komponenten** aus.
7. Klicken Sie Auf **Absenden**.

   Das Diagramm Cluster-Komponenten wird angezeigt. Im Diagramm wird die gesamte Latenz nach Clusterkomponente unterteilt.

8. Zeigen Sie unten auf der Seite den Mauszeiger auf das Symbol für das Änderungsereignis zum Beginn der HA-Übernahme.
9. Vergleichen Sie im Diagramm **Cluster Components** die Latenz für die Datenverarbeitung mit der gesamten Latenz im Diagramm * Latenz*.

   Zum Zeitpunkt der HA-Übernahme betrug die Datenverarbeitung aufgrund der steigenden Workload-Anforderungen am Datenverarbeitungs-Node eine Spitze. Die höhere CPU-Auslastung steigerte die Latenz und löste das Ereignis aus.

10. Nach der Behebung des fehlerhaften Knotens führt OnCommand System Manager ein HA-Giveback durch, wodurch die Workloads vom Partner-Node zum festgelegten Node verschoben werden.
11. Nachdem die HA-Rückübertragung abgeschlossen ist, suchen Sie im Unified Manager nach der Ereignis-ID, die Sie in Schritt 2 aufgezeichnet haben.

    Das durch die HA-Übernahme ausgelöste Ereignis wird auf der Seite Ereignisdetails angezeigt. Das Ereignis weist nun einen Status veraltet auf, was darauf hinweist, dass das Ereignis gelöst wurde.

12. Klicken Sie in der **Beschreibung** auf den Namen des Opfervolumens.

    Die Seite Performance/Volume Details wird angezeigt. Im unteren Bereich der Seite wird in der Zeile Ereignisse die Zeit angezeigt, in der Unified Manager den Abschluss des HA-Giveback erkannt hat, ein Symbol für ein Änderungsereignis.

13. Wählen Sie **Aufbruchdaten nach** aus.
14. Wählen Sie unter **Latenz Cluster-Komponenten** aus.

    Das Diagramm Cluster-Komponenten wird angezeigt.

15. Zeigen Sie unten auf der Seite den Cursor auf das Symbol für das Änderungsereignis für das HA-Giveback.

    Das Änderungereignis wird in der Tabelle „Ereignisliste“ hervorgehoben und gibt an, dass die HA-Rückgabe erfolgreich abgeschlossen wurde.

16. Vergleichen Sie im Diagramm **Cluster Components** die Latenz für die Datenverarbeitung mit der gesamten Latenz im Diagramm * Latenz*.

    Die Latenz der Komponente für die Datenverarbeitung wurde herabgesetzt, wodurch die gesamte Latenz verringert wurde. Der Node, den das ausgewählte Volume jetzt zur Datenverarbeitung verwendet, hat das Ereignis aufgelöst.

Einrichten einer Verbindung zwischen einem Unified Manager-Server und einem externen Datenanbieter

Über die Verbindung zwischen einem Unified Manager-Server und einem externen Datenanbieter können Sie Cluster Performance-Daten an einen externen Server senden, sodass Storage Manager die Performance-Kennzahlen mithilfe von Software anderer Anbieter darstellen können.

Über die Menüoption „`Externer Datenanbieter`“ in der Wartungskonsole wird eine Verbindung zwischen einem Unified Manager-Server und einem externen Datenanbieter hergestellt.

Leistungsdaten, die an einen externen Server gesendet werden können

Unified Manager sammelt eine Vielzahl von Performance-Daten von allen überwachten Clustern. Sie können bestimmte Datengruppen an einen externen Server senden.

Abhängig von den Performance-Daten, die Sie darstellen möchten, können Sie wählen, eine der folgenden Statistikgruppen zu senden:

Statistikgruppe	Enthaltene Daten	Details
Performance Monitor	Allgemeine Performance-Statistiken für die folgenden Objekte: • LUNs • Volumes	Diese Gruppe ermöglicht IOPS oder Latenz insgesamt für alle LUNs und Volumes in allen überwachten Clustern. Diese Gruppe stellt die kleinste Anzahl von Statistiken bereit.
Ressourcenauslastung	Statistiken zur Ressourcenauslastung für die folgenden Objekte: • Knoten • Aggregate	Diese Gruppe stellt Auslastungsstatistiken für den Node bereit und aggregiert physische Ressourcen in allen überwachten Clustern. Es stellt auch die Statistiken bereit, die in der Performance Monitor-Gruppe erfasst wurden.
Drill-Down	Lese-/Schreib- und Statistiken auf niedriger Ebene für alle erfassten Objekte: • Knoten • Aggregate • LUNs • Volumes • Festplatten • LIFs • Ports/NICs	Diese Gruppe bietet Lese-/Schreib- und Protokollausfälle für alle sieben überwachten Objekttypen in allen überwachten Clustern. Er stellt außerdem die Statistiken bereit, die in der Gruppe „Performance Monitor“ und in der Gruppe „Ressourcenauslastung“ erfasst wurden. Diese Gruppe stellt die größte Anzahl von Statistiken bereit.

Wenn der Name eines Clusters oder eines Clusterobjekts auf dem Speichersystem geändert wird, enthalten sowohl die alten als auch die neuen Objekte Leistungsdaten auf dem externen Server (so genannte „`mmetric_path`“). Die beiden Objekte sind nicht mit demselben Objekt korreliert. Wenn Sie beispielsweise den Namen eines Volumes von „`volume1_acct`“ in „`acct_vol1`“ ändern, werden alte Performance-Daten für das alte Volume sowie die neuen Performance-Daten für das neue Volume angezeigt.

Im Knowledge Base-Artikel finden Sie eine Liste aller Leistungsindikatoren, die an einen externen Datenanbieter gesendet werden können.

"Unified Manager-Leistungsindikatoren, die an einen externen Datenanbieter exportiert werden können"

Einrichten von Graphite für den Empfang von Leistungsdaten von Unified Manager

Graphit ist ein offenes Software-Tool zum Erfassen und Darstellen von Performancedaten aus Computersystemen. Ihr Graphite-Server und Ihre Software müssen richtig konfiguriert sein, um statistische Daten von Unified Manager zu erhalten.

Nachdem Sie Graphite gemäß den Installationsanweisungen installiert haben, müssen Sie zur Unterstützung der statistischen Datenübertragung von Unified Manager folgende Änderungen vornehmen:

- Im `/opt/graphite/conf/carbon.conf` Datei: Die maximale Anzahl von Dateien, die auf dem Graphite-Server pro Minute erstellt werden können, muss auf *200* eingestellt sein (`MAX_CREATES_PER_MINUTE = 200`).

  Abhängig von der Anzahl der Cluster in Ihrer Konfiguration und den zu sendenden Statistikobjekten können Tausende neue Dateien erstellt werden, die zunächst erstellt werden müssen. Bei 200 Dateien pro Minute dauert es möglicherweise 15 Minuten oder länger, bevor alle metrischen Dateien ursprünglich erstellt werden. Nachdem alle eindeutigen metrischen Dateien erstellt wurden, ist dieser Parameter nicht mehr relevant.

- Wenn Sie Graphite auf einem Server ausführen, der über eine IPv6-Adresse bereitgestellt wird, wird der Wert für LINE_RECEIVER_INTERFACE im angezeigt `/opt/graphite/conf/carbon.conf` Die Datei muss von „`0.0.0.0`“ in „`::`“ geändert werden. (`LINE_RECEIVER_INTERFACE = ::`)

- Im `/opt/graphite/conf/storage-schemas.conf` Datei, der `retentions` Mit dem Parameter müssen Sie die Häufigkeit auf 5 Minuten und den Aufbewahrungszeitraum auf die Anzahl der für Ihre Umgebung relevanten Tage festlegen.

  Die Aufbewahrungsdauer kann so lange betragen, wie Ihre Umgebung es zulässt, aber der Frequenzwert muss für mindestens eine Aufbewahrungseinstellung auf 5 Minuten eingestellt sein. Im folgenden Beispiel wird ein Abschnitt für Unified Manager mithilfe des definiert `pattern` Parameter und die Werte legen die Anfangsfrequenz auf 5 Minuten und den Aufbewahrungszeitraum auf 100 Tage fest:

  Wenn die Standard-Hersteller-Tag-Nummer von „`netapp-Performance`“ in einen anderen Wert geändert wird, muss diese Änderung im widergespiegelt werden `pattern` Parameter auch.

Wenn der Graphite-Server nicht verfügbar ist, wenn der Unified Manager-Server versucht, Leistungsdaten zu senden, werden die Daten nicht gesendet und es besteht eine Lücke in den gesammelten Daten.

Konfigurieren einer Verbindung von einem Unified Manager-Server zu einem externen Datenanbieter

Unified Manager kann Cluster-Leistungsdaten an einen externen Server senden. Sie können die Art der gesendeten statistischen Daten und das Intervall angeben, in dem Daten gesendet werden.

Bevor Sie beginnen

- Sie müssen über eine Benutzer-ID verfügen, um sich bei der Wartungskonsole des Unified Manager-Servers anzumelden.
- Sie müssen über die folgenden Informationen zum externen Datenanbieter verfügen:
  - Servername oder IP-Adresse (IPv4 oder IPv6)
  - Server-Standardport (wenn kein Standardport 2003 verwendet wird)
- Sie müssen den Remote-Server und die Software von Drittanbietern so konfiguriert haben, dass er statistische Daten vom Unified Manager-Server empfangen kann.

- Sie müssen wissen, welche Statistikgruppe Sie senden möchten:
  - PERFORMANCE_INDICATOR: Statistiken zur Performance-Überwachung
  - RESOURCE_UTIAUSLASTUNG: Statistiken zur Ressourcenauslastung und Performance-Überwachung
  - DRILL_DOWN: Alle Statistiken
- Sie müssen das Zeitintervall kennen, in dem Sie Statistiken übertragen möchten: 5, 10 oder 15 Minuten

  Standardmäßig erfasst Unified Manager Statistiken in Abständen von 5 Minuten. Wenn Sie das Übertragungsintervall auf 10 (oder 15) Minuten einstellen, ist die Datenmenge, die während jeder Übertragung gesendet wird, zwei (oder drei) Mal größer als bei Verwendung des standardmäßigen 5-Minuten-Intervalls.

  Wenn Sie das Performance-Erfassungsintervall von Unified Manager auf 10 oder 15 Minuten ändern, müssen Sie das Übertragungsintervall so ändern, dass es dem Erfassungsintervall von Unified Manager entspricht oder größer ist.

Über diese Aufgabe

Sie können eine Verbindung zwischen einem Unified Manager-Server und einem externen Datenprovider-Server konfigurieren.

Schritte

1. Loggen Sie sich als Wartungsbenutzer der Wartungskonsole des Unified Manager Servers ein.

   Die Eingabeaufforderungen für die Unified ManagerMaintenance-Konsole werden angezeigt.

2. Geben Sie in der Wartungskonsole die Nummer der Menüoption **Externer Datenanbieter** ein.

   Das Menü External Server Connection wird angezeigt.

3. Geben Sie die Nummer der Menüoption **Serververbindung hinzufügen/ändern** ein.

   Die aktuellen Serververbindungsinformationen werden angezeigt.

4. Geben Sie bei der entsprechenden Aufforderung ein `y` Um fortzufahren.
5. Geben Sie bei der entsprechenden Aufforderung die IP-Adresse oder den Namen des Zielservers und die Informationen zum Serverport ein (falls sie vom Standardport 2003 abweichen).
6. Geben Sie bei der entsprechenden Aufforderung ein `y` Um zu überprüfen, ob die eingegebenen Informationen richtig sind.
7. Drücken Sie eine beliebige Taste, um zum Menü External Server Connection zurückzukehren.
8. Geben Sie die Nummer der Menüoption **Serverkonfiguration** ändern ein.

   Die Informationen zur aktuellen Serverkonfiguration werden angezeigt.

9. Geben Sie bei der entsprechenden Aufforderung ein `y` Um fortzufahren.
10. Geben Sie bei der entsprechenden Aufforderung die Art der zu sendenden Statistiken, das Zeitintervall, in dem die Statistiken gesendet werden, und ob Sie die Übertragung der Statistiken jetzt aktivieren möchten:

Für.	Eingeben…
Statistikgruppen-ID	`0` - LEISTUNGSANZEIGE (Standard) `1` - RESOURCE_UTIL `2` - DRILL_DOWN
Hersteller-Tag	Einen beschreibenden Namen für den Ordner, in dem die Statistiken auf dem externen Server gespeichert werden. „`netapp-Performance`“ ist der Standardname, Sie können jedoch einen anderen Wert eingeben. Durch die Verwendung von gepunkteter Notation können Sie eine hierarchische Ordnerstruktur definieren. Beispiel: Durch Eingabe `stats.performance.netapp` Die Statistiken befinden sich in **Statistik** > **Performance** > **netapp**.
Übertragungsintervall	`5` (Standard), `10`, Oder `15` Minuten
Aktivieren/deaktivieren	`0` - Deaktivieren `1` - Aktivieren (Standard)

11. Geben Sie bei der entsprechenden Aufforderung ein `y` Um zu überprüfen, ob die eingegebenen Informationen richtig sind.
12. Drücken Sie eine beliebige Taste, um zum Menü External Server Connection zurückzukehren.
13. Typ `x` Um die Wartungskonsole zu beenden.

Ergebnisse

Nachdem Sie die Verbindung konfiguriert haben, werden die ausgewählten Performancedaten zum angegebenen Zeitintervall an den Zielserver gesendet. Es dauert einige Minuten, bis die Metriken in Graphite erscheinen. Möglicherweise müssen Sie Ihren Browser aktualisieren, um die neuen Metriken in der Hierarchie der Kennzahlen anzuzeigen.

Überwachen und managen Sie den Cluster-Zustand

Einführung in das Monitoring des Systemzustands von OnCommand Unified Manager

Mit Unified Manager können Sie eine große Anzahl von Systemen mit ONTAP Software über eine zentrale Benutzeroberfläche überwachen. Die Unified Manager Serverinfrastruktur bietet Skalierbarkeit, Unterstützbarkeit sowie verbesserte Monitoring- und Benachrichtigungsfunktionen.

Zu den Schlüsselfunktionen von Unified Manager gehören Monitoring, Warnmeldungen, Management der Verfügbarkeit und Kapazität von Clustern, Management von Sicherungsfunktionen, Performance-Überwachung, Konfiguration und Management von Infinite Volumes, Annotationen von Storage-Objekten, Bündelung von Diagnosedaten und Senden an den technischen Support.

Mit Unified Manager können Sie die Cluster überwachen. Wenn im Cluster Probleme auftreten, benachrichtigt Sie Unified Manager über Ereignisse, die Einzelheiten zu solchen Problemen betreffen. Bei einigen Ereignissen erhalten Sie zudem eine Abhilfemaßung, die Sie zur Behebung der Probleme ergreifen können. Sie können Benachrichtigungen für Ereignisse so konfigurieren, dass bei Auftreten von Problemen Sie über E-Mail und SNMP-Traps benachrichtigt werden.

Mit Unified Manager können Sie Storage-Objekte in Ihrer Umgebung managen, indem Sie sie mit Annotationen verknüpfen. Sie können benutzerdefinierte Anmerkungen erstellen und Cluster, Storage Virtual Machines (SVMs) und Volumes dynamisch mit den Annotationen über Regeln verknüpfen.

Zudem können Sie die Storage-Anforderungen Ihrer Cluster-Objekte anhand der Informationen in den Kapazitäts- und Integritätsdiagrammen für das jeweilige Cluster-Objekt planen.

Unified Manager Funktionen für das Monitoring des Systemzustands

Unified Manager basiert auf einer Serverinfrastruktur, die Skalierbarkeit, Unterstützbarkeit sowie verbesserte Monitoring- und Benachrichtigungsfunktionen bietet. Unified Manager unterstützt das Monitoring von Systemen mit ONTAP Software.

Unified Manager umfasst die folgenden Funktionen:

- Bestandsaufnahme, Monitoring und Benachrichtigungen für Systeme, die mit der ONTAP Software installiert sind:
  - Physische Objekte: Nodes, Festplatten, Festplatten-Shelfs, SFO-Paare, Ports, Und Flash Cache
  - Logische Objekte: Cluster, Storage Virtual Machines (SVMs), Aggregate, Volumes, LUNs, Namespaces Qtrees, LIFs, Snapshot Kopien, Verbindungspfade, NFS-Exporte, CIFS-Freigaben, Benutzer- und Gruppenkontingente und Initiatorgruppen
  - Protokolle: CIFS, NFS, FC, iSCSI, NVMe, Und FCoE
  - Storage-Effizienz: SSD-Aggregate, Flash Pool-Aggregate, FabricPool-Aggregate, Deduplizierung und Komprimierung
  - Sicherung: SnapMirror Beziehungen (synchron und asynchron) sowie SnapVault Beziehungen

- Anzeigen des Cluster-Erkennungs- und Überwachungsstatus
- MetroCluster Konfiguration: Anzeigen und Überwachen der Konfiguration, MetroCluster Switches und Bridges, Probleme und des Konnektivitätsstatus der Cluster-Komponenten
- Erweiterte Alarmfunktionen, Ereignisse und Schwellenwertsinfrastruktur
- LDAP, LDAPS, SAML-Authentifizierung und Unterstützung lokaler Benutzer
- RBAC (für vordefinierte Rollen)
- AutoSupport und Support-Bundle
- Erweitertes Dashboard zur Anzeige des Kapazitäts-, Verfügbarkeits-, Sicherungs- und Performance-Zustands der Umgebung
- Interoperabilität bei Volume-Verschiebung, Verlauf der Volume-Verschiebung und Änderungsverlauf für Verbindungspfade
- Bereich „Auswirkungen“, in dem die Ressourcen angezeigt werden, die für Ereignisse wie fehlerhafte Festplatten, heruntergestuften MetroCluster Aggregatspiegelung und MetroCluster-Ersatzfestplatten, die bei Ereignissen noch nicht vorhanden sind, betroffen sind
- Möglicher Effektbereich, der die Wirkung der MetroCluster-Ereignisse anzeigt
- Bereich „Empfohlene Korrekturmaßnahmen“, in dem die Aktionen angezeigt werden, die zur Behebung von Ereignissen durchgeführt werden können, z. B. fehlerhafte Festplatten, eingeschränkte MetroCluster Aggregatspiegelung und nicht mehr vorhandene MetroCluster-Ersatzfestplatten
- Ressourcen, die möglicherweise betroffen sein könnten, zeigen die Ressourcen an, die für Ereignisse wie das Offline-Ereignis von Volume, das Ereignis Volume Restricted und den risikobehaftete Volume-Speicherplatz auf einem Volume mit Thin Provisioning verfügbar sein könnten
- Unterstützung für SVMs mit:
  - FlexVol Volumes
  - FlexGroup Volumes
  - Unbegrenzte Volumes
- Unterstützung für das Monitoring von Root-Volumes der Nodes
- Verbessertes Monitoring von Snapshot Kopien, einschließlich Computing von zurückforderbarem Speicherplatz und Löschen von Snapshot Kopien
- Anmerkungen für Speicherobjekte
- Berichte für die Erstellung und das Management von Storage-Objektinformationen wie physische und logische Kapazität, Auslastung, Platzeinsparungen und zugehörige Ereignisse
- Integration in OnCommand Workflow Automation zur Ausführung von Workflows

  Der Storage Automation Store enthält von NetApp zertifizierte automatisierte Workflow-Pakete für die Verwendung mit OnCommand Workflow Automation (WFA). Sie können die Pakete herunterladen und anschließend in WFA importieren, um sie auszuführen. Die automatisierten Workflows sind im folgenden verfügbar "Storage Automation Store"

Unified Manager-Schnittstellen, die zum Management des Zustands des Storage-Systems verwendet werden

Dieser Abschnitt enthält Informationen zu den beiden Benutzeroberflächen, die OnCommand Unified Manager zur Fehlerbehebung von Storage-Kapazität, -Verfügbarkeit und -Sicherung bereitstellt. Die beiden UIs sind die Unified Manager Web-

UI und die Wartungskonsole.

Um die Sicherungsfunktionen in Unified Manager nutzen zu können, müssen auch OnCommand Workflow Automation (WFA) installiert und konfiguriert werden.

Unified Manager Web-UI

Die Unified Manager Web-UI ermöglicht einem Administrator, Cluster-Probleme in Bezug auf Kapazität, Verfügbarkeit und Sicherung der Daten zu überwachen und zu beheben.

In diesem Abschnitt werden einige gängige Workflows beschrieben, die ein Administrator befolgen kann, um Fehler bei der Storage-Kapazität, Datenverfügbarkeit oder Sicherungsproblemen zu beheben, die in der Web-Benutzeroberfläche von Unified Manager angezeigt werden.

Wartungskonsole

Die Wartungskonsole ermöglicht einem Administrator, Betriebssystemprobleme, Probleme mit dem Versionsaufrüstungs-, Benutzer-Zugriffsprobleme und Netzwerkprobleme im Zusammenhang mit dem Unified Manager Server selbst zu überwachen, zu diagnostizieren und zu beheben. Wenn die Web-UI von Unified Manager nicht verfügbar ist, stellt die Wartungskonsole die einzige Zugriffsmöglichkeit auf Unified Manager dar.

Dieser Abschnitt enthält eine Anleitung zum Zugriff auf die Wartungskonsole und zur Behebung von Problemen im Zusammenhang mit der Funktionsweise des Unified Manager-Servers.

Gemeinsame Workflows und Aufgaben im Zusammenhang mit Unified Manager

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

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

Die wichtigsten Probleme in Bezug auf Cluster, Storage Virtual Machine (SVM), Volume, FlexGroup Volume oder Sicherungsbeziehung, die die Storage-Kapazität, Datenverfügbarkeit oder Zuverlässigkeit der Sicherung Ihrer gemanagten Storage-Objekte beeinträchtigen, werden in den Systemintegritätsdiagrammen und -Ereignissen auf der Seite Dashboards/Überblick angezeigt. Wenn kritische Probleme erkannt werden, enthält diese Seite Links, um entsprechende Workflows zur Fehlerbehebung zu unterstützen.

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

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

- Diagnose und Management von Verfügbarkeitsproblemen

Wenn ein Hardwarefehler oder Probleme bei der Konfiguration von Speicherressourcen dazu führen, dass die Datenverfügbarkeits-Ereignisse auf der Seite Dashboards/Überblick angezeigt werden, können Speicheradministratoren mithilfe der eingebetteten Links Verbindungsinformationen über die betroffene Speicherressource anzeigen, Tipps zur Fehlerbehebung anzeigen und anderen Administratoren eine Problembehebung zuweisen.

- Konfiguration und Monitoring von Performance-Vorfällen

  Der OnCommand Administrator kann die Performance der überwachten Storage-Systemressourcen überwachen und managen. Weitere Informationen finden Sie im *Unified Manager Workflow Guide zum Verwalten der Cluster Performance*.

- Diagnose und Management von Kapazitätsproblemen bei Volumes

  Wenn Probleme mit der Speicherkapazität von Volumes auf der Seite Dashboards/Überblick angezeigt werden, können Speicheradministratoren anhand der eingebetteten Links die aktuellen und historischen Trends in Bezug auf die Speicherkapazität des betroffenen Volumes anzeigen, Tipps zur Fehlerbehebung anzeigen und anderen Administratoren die Problembehebung zuweisen.

- Konfiguration, Monitoring und Diagnose von Problemen bei der Sicherungsbeziehung

  Nach dem Erstellen und Konfigurieren von Sicherungsbeziehungen können Storage-Administratoren auf der Seite Dashboards/Überblick die potenziellen Probleme mit Sicherungsbeziehungen anzeigen und mithilfe der eingebetteten Links den aktuellen Status der Sicherungsbeziehungen, die aktuellen und historischen Erfolgsinformationen über die betroffenen Beziehungen anzeigen. Beratung bei der Fehlerbehebung sowie Zuordnung der Problembehebung zu anderen Administratoren Storage-Administratoren können auch SnapMirror und SnapVault Beziehungen konfigurieren und managen.

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

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

- Senden eines Support Bundle an den technischen Support

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

- Neue Berichte für den Import erstellen

  Storage-Administratoren können neue erstellen `.rptdesign` Dateien mit dem Eclipse Plug-in für Business Intelligence und Reporting Tools (BIRT). Diese Berichte können in die Benutzeroberfläche von Unified Manager importiert und auf der Seite Berichte angezeigt werden.

  Die auf der Seite Berichte angezeigten Berichte geben den aktuellen Status der Speicherobjekte an. Sie können wichtige Entscheidungen treffen – beispielsweise Entscheidungen zur Storage-Beschaffung – basierend auf der aktuellen Nutzung. Diese Berichte bieten eine detaillierte Übersicht über Storage-Objekte wie Volumes, Festplatten-Shelfs und Aggregate.

  Auf der Seite Berichte in der Benutzeroberfläche von Unified Manager können Sie detaillierte Informationen zu den von Ihnen erstellten Berichten anzeigen. Sie können nach einem bestimmten Bericht

suchen, einen Bericht speichern und einen Bericht auf der Seite Berichte löschen. Sie können auch einen Bericht von dieser Seite planen, freigeben und importieren.

- Erstellung, Konfiguration, Monitoring und Sicherung von Infinite Volumes

  Nachdem Storage-Klassen für ein Infinite Volume mit dem Tool Workflow Automation erstellt, konfiguriert und definiert wurden, können Storage-Administratoren mit Unified Manager überwachen, Benachrichtigungsschwellenwerte festlegen und die Datenrichtlinie für das entsprechende Volume und seine Storage-Klassen definieren. Optional können Storage-Administratoren mit WFA und Unified Manager die Datensicherung für das Infinite Volume einrichten.

Monitoring und Fehlerbehebung der Datenverfügbarkeit

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

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

Offline-Zustand einer Flash-Karte beheben

Dieser Workflow bietet ein Beispiel dafür, wie Sie den Offline-Zustand einer Flash-Karte beheben können. In diesem Szenario sind Sie ein Administrator oder Operator, der das Dashboard überwacht, um nach Problemen mit der Verfügbarkeit zu suchen. Sie sehen eine Flash-Karte offline-Zustand und Sie möchten die mögliche Ursache und Lösung des Problems zu ermitteln.

Bevor Sie beginnen

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

Über diese Aufgabe

Die im Bereich Verfügbarkeit der Seite Unified ManagerDashboards/Übersicht angezeigten Event-Informationen und Links führen zur Überwachung der allgemeinen Verfügbarkeit von Datenspeicherressourcen auf den überwachten Clustern. Dadurch können Sie bestimmte Ereignisse diagnostizieren, die sich auf die Verfügbarkeit auswirken könnten.

In diesem Szenario zeigt die Seite Dashboards/Übersicht die Veranstaltung Flash-Karten offline im Bereich Verfügbarkeitsstörungen an. Ist eine Flash-Karte offline, wird die Verfügbarkeit gespeicherter Daten beeinträchtigt, weil die Performance des Cluster-Nodes, auf dem sie installiert ist, beeinträchtigt ist. Sie können die folgenden Schritte durchführen, um das potenzielle Problem zu lokalisieren und zu identifizieren:

Schritte

1. Klicken Sie im Bereich **Verfügbarkeit** im Bereich **ungelöste Vorfälle und Risiken** auf den Hypertext-Link, der für Flash Cards Offline angezeigt wird.

   Die Seite Ereignisdetails für den Verfügbarkeitsereignis wird angezeigt.

2. Auf der Seite **Ereignis** Details können Sie die im Feld Ursache angezeigten Informationen überprüfen und eine oder mehrere der folgenden Aufgaben ausführen:
   - Weisen Sie das Ereignis einem Administrator zu. Ereignisse werden zugewiesen
   - Klicken Sie in diesem Fall auf die Quelle des Ereignisses, in dem sich der Cluster-Node befindet, auf dem sich die Offline-Flash-Karte befindet, um weitere Informationen über den Node zu erhalten. Durchführen der Korrekturmaßnahme für eine Flash-Karte offline
   - Bestätigen Sie das Ereignis. Bestätigen und Beheben von Ereignissen

Durchführen der Korrekturmaßnahme für eine Flash-Karte offline

Nachdem Sie die Beschreibung im Feld Ursache der Seite mit den Details zu Offline-Ereignissen der Flash-Karte überprüft haben, können Sie nach zusätzlichen Informationen suchen, die bei der Behebung des Problems hilfreich sind.

Bevor Sie beginnen

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

Über diese Aufgabe

In diesem Beispielszenario enthält die Ereignisübersicht auf der Seite Ereignisdetails die folgenden Informationen über den Zustand der Offline-Flash-Karte:

```
Severity: Critical
State: New
Impact Level: Incident
Impact Area: Availability
Source: alpha-node
Source Type: Node
Acknowledged By:
Resolved By:
Assigned To:
Cause: Flash cards at slot numbers 3 are offline.
Alert Settings:
```

Die Ereignisinformationen geben an, dass die in Steckplatz 3 im Cluster-Node mit dem Namen „`alpha-Node`“ installierte Flash-Karte offline ist.

Die Informationen lokalisieren die Offline-Bedingung der Flash-Karte zu einem bestimmten Steckplatz auf einem bestimmten Cluster-Node, schlagen jedoch keinen Grund vor, dass die Flash-Karte offline ist.

Schritte

1. Um weitere Informationen zu erhalten, die Ihnen bei der Diagnose des Offline-Zustands der Flash-Karte helfen könnten, können Sie auf den Namen der Quelle des Ereignisses klicken.

   In diesem Beispiel ist die Quelle des Ereignisses der Cluster-Node „`alpha-Node`“. Wenn Sie auf den Node-Namen klicken, werden auf der Registerkarte Nodes auf der Seite Systemzustand/Cluster-Details der betroffenen Cluster die HA-Details angezeigt. In den angezeigten HA-Details werden Informationen

über das HA-Paar angezeigt, zu dem der Node gehört.

In diesem Beispiel werden die relevanten Informationen in der Zusammenfassungstabelle für Ereignisse auf den HA-Details aufgeführt. Die Tabelle gibt das Offline-Ereignis der Flash-Karte, die Uhrzeit der Generierung des Ereignisses und auch den Cluster-Node an, von dem dieses Ereignis stammt.

2. Greifen Sie über die ONTAP CLI oder den OnCommand System Manager auf die EMS-Protokolle (Event Manager System) für den betroffenen Cluster zu.

   In diesem Beispiel verwenden Sie den Ereignisnamen, die Ereigniszeit und die Ereignisquelle, um den EMS-Bericht zu diesem Ereignis zu finden. Der EMS-Bericht über das Ereignis enthält eine detaillierte Beschreibung des Ereignisses und häufig Hinweise zur Behebung des durch das Ereignis angegebenen Zustands.

Nachdem Sie fertig sind

Nach der Diagnose des Problems wenden Sie sich an den entsprechenden Administrator oder Operator, um die erforderlichen manuellen Schritte auszuführen, um die Flash-Karte wieder online zu schalten.

Scannen und Beheben von Verbindungsproblemen für Storage Failover Interconnect

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

1. Um aktuelle Verfügbarkeitsereignisse im Zusammenhang mit Problemen mit dem Storage Failover zu prüfen, lesen Sie den Abschnitt „Verfügbarkeitsstörungen“ und die Einträge „Verfügbarkeitsrisiken“ auf der Seite **Dashboards/Übersicht**.
2. So überprüfen Sie weiter, ob alle Verfügbarkeitsereignisse im Zusammenhang mit Storage Failover-Problemen auftreten können:

   a. Klicken Sie auf der Seite **Dashboards/Übersicht** auf den Link **Verfügbarkeitsvorfälle**.

      Auf der Seite Ereignisinventar werden alle Ereignisse auf den überwachten Clustern angezeigt.

   b. Wählen Sie auf der Seite **Events** Inventory in der Spalte Filter die Optionen **Vorfall** und **Risiko** aus.

   c. Klicken Sie oben in der Spalte **Events** Bestandsnamen auf Und eingeben `*failover` Im Textfeld zur Begrenzung des Ereignisses auf Ereignisse mit Speicherausfallschutz.

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

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

3. Wenn ein oder mehrere Ereignisse im Zusammenhang mit dem Speicherausfallschutz entweder auf der Seite **Dashboards/Übersicht** oder auf der Seite **Ereignisse** Bestand angezeigt werden, führen Sie die folgenden Schritte aus:

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

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

   Die Seite Ereignisdetails für dieses Ereignis wird angezeigt.

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

Durchführen von Korrekturmaßnahmen für Storage Failover Interconnect-Verbindungen als inaktiv

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

Summary

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

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

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

Schritte

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

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

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

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

Nachdem Sie fertig sind

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

Lösung von Offline-Problemen des Volumes

Dieser Workflow bietet ein Beispiel dafür, wie Sie ein Offline-Ereignis eines Volumes bewerten und beheben können, das Unified Manager im Bereich Verfügbarkeit der Seite Dashboards/Überblick anzeigen kann. In diesem Szenario sind Sie ein Administrator, der Unified Manager zur Fehlerbehebung bei einem oder mehreren Offline-Volume-Ereignissen verwendet, die auf der Seite Dashboards/Überblick angezeigt werden.

Bevor Sie beginnen

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

Über diese Aufgabe

Volumes können aus verschiedenen Gründen offline gemeldet werden:

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

Sie können die Seite Dashboards/Überblick und die Seiten „Systemzustand/Cluster, Zustand/SVM“ und „Systemzustand/Volume-Details“ verwenden, um eine oder mehrere dieser Möglichkeiten zu bestätigen oder zu eliminieren.

Schritte

1. Klicken Sie im Fenster **Verfügbarkeit** im Abschnitt **ungelöste Vorfälle und Risiken** auf den Hypertext-Link, der für das Offlinevent Volume angezeigt wird.

   Die Seite Ereignisdetails für den Verfügbarkeitsereignis wird angezeigt.

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

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

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

◦ Bestätigen Sie das Ereignis oder markieren Sie es gegebenenfalls als erledigt. Bestätigen und Beheben von Ereignissen

Durchführung von Diagnoseaktionen für Offline-Bedingungen des Volumes

Nachdem Sie zur Seite „Health/Volume Details“ eines gemeldeten Volumes aufgerufen haben, können Sie nach zusätzlichen Informationen suchen, die hilfreich sind, um die Offline-Bedingung des Volumes zu diagnostizieren.

Bevor Sie beginnen

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

Über diese Aufgabe

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

Beginnen Sie auf der Seite „Systemzustand/Volume-Details“ des Offline-Volumes. Navigieren Sie zu anderen Seiten und Fenstern, um mögliche Ursachen zu bestätigen oder zu eliminieren:

Wahlmöglichkeiten

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

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

- Klicken Sie auf die Seitenlinks **Systemzustand/Volume** Details, um festzustellen, ob das Volume offline ist und seine Host Storage Virtual Machine (SVM) angehalten wurde, da der Node, der das Root-Volume dieser SVM hostet, nicht verfügbar ist.

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

- Klicken Sie auf **Health/Volume** Details Page Links, um festzustellen, ob das Volume wegen defekter Festplatten in seinem Host-Aggregat offline ist.

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

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

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

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

   Auf der Seite Systemzustand/Volume-Inventar wird eine Tabelle mit Informationen zu allen Volumes angezeigt, die von der SVM gehostet werden.

3. Klicken Sie in der Spaltenüberschrift **Health/Volumes** Inventory page State auf das Filtersymbol , Und wählen Sie dann die Option **Offline**.

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

4. Klicken Sie auf der Seite **Health/Volumes** Inventory auf das Grid-Symbol , Und wählen Sie dann die Option **Cluster-Knoten**.

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

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

5. Suchen Sie auf der Seite **Health/Volumes** Inventory die Liste für das Offline-Volume und klicken Sie in der Spalte Cluster Node auf den Namen seines Hosting-Node.

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

Nachdem Sie fertig sind

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

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

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

3. Wenn der SVM-Status angehalten wird, klicken Sie auf **View SVMs**, um die Ursache des Anstoppens der Hosting-SVM zu ermitteln.
4. Klicken Sie in der Spaltenüberschrift **Health/Storage Virtual Machines** Inventory pageSVM auf das Filtersymbol Geben Sie dann den Namen der angehalten SVM ein.

   Die Informationen für diese SVM sind in einer Tabelle dargestellt.

5. Klicken Sie auf der Seite**Health/Storage Virtual Machines** Inventar auf Und wählen Sie dann die Option **Root Volume** aus.

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

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

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

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

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

Nachdem Sie fertig sind

Nachdem Sie bestätigt haben, dass der Offline-Zustand des Volume durch den Offline-Zustand des Host-SVM

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

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

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

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

   Die Seite „Systemzustand/Cluster-Details“ wird angezeigt.

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

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

Nachdem Sie fertig sind

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

Behebung von Kapazitätsproblemen

Dieser Workflow bietet ein Beispiel dafür, wie Sie ein Kapazitätsproblem lösen können. In diesem Szenario greifen Sie als Administrator oder Operator auf die Seite Unified

ManagerDashboards/Überblick zu, um zu sehen, ob eines der überwachten Speicherobjekte Kapazitätsprobleme haben. Sie sehen, dass ein Volume mit einem Kapazitätsrisiko besteht und möchten die mögliche Ursache und Lösung des Problems herausfinden.

Bevor Sie beginnen

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

Über diese Aufgabe

Auf der Seite Dashboards/Überblick sehen Sie sich den Bereich ungelöste Vorfälle und Risiken an und Sie sehen ein Fehlerereignis „`Volume Space Full`“ im Teilfenster „Kapazität“ unter „SVM Volume Capacity“, das gefährdet ist.

Schritte

1. Klicken Sie im Bereich **ungelöste Vorfälle und Risiken** auf der Seite **Dashboards/Übersicht** auf den Namen des Ereignisses des vollständigen Volume-Raums im Fensterbereich **Kapazität**.

   Die Seite Ereignisdetails für den Fehler wird angezeigt.

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

Durchführung von vorgeschlagenen Abhilfemaßnahmen für ein vollständiges Volumen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

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

Über diese Aufgabe

In diesem Beispiel wurde auf der Seite Unified ManagerDashboards/Übersicht ein Fehlerereignis für Volume Space Full angezeigt und auf den Namen des Ereignisses geklickt.

Mögliche Abhilfemaßnahmen für ein komplettes Volume sind:

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

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

Schritte

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

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

Erstellen, Überwachen und Beheben von Sicherungsbeziehungen

Unified Manager ermöglicht die Erstellung von Sicherungsbeziehungen, um den Spiegelschutz zu überwachen und Fehler zu beheben sowie die Sicherung von Daten, die in gemanagten Clustern gespeichert sind, zu sichern und Daten wiederherzustellen, wenn sie überschrieben oder verloren gehen.

Arten der SnapMirror Sicherung

Je nach Implementierung Ihrer Topologie des Storage können Sie mit Unified Manager mehrere Arten von SnapMirror Sicherungsbeziehungen konfigurieren. Alle Varianten des SnapMirror Schutzes bieten Failover Disaster Recovery-Schutz, bieten jedoch unterschiedliche Funktionen in Bezug auf Performance, Versionsflexibilität und Sicherung mehrerer Backup-Kopien.

Herkömmliche asynchrone Datensicherungsbeziehungen von SnapMirror

Herkömmlicher SnapMirror asynchroner Schutz bietet Sicherung der Blockreplizierung zwischen Quell- und Ziel-Volumes.

In herkömmlichen SnapMirror Beziehungen werden Spiegelvorgänge schneller ausgeführt als in alternativen

SnapMirror Beziehungen, da der Spiegelvorgang auf der Blockreplizierung basiert. Beim herkömmlichen SnapMirror Schutz muss das Ziel-Volume jedoch unter derselben oder einer höheren kleineren Version der ONTAP Software wie das Quell-Volume innerhalb derselben größeren Version (z. B. Version 8.x zu 8.x oder 9.x zu 9.x) ausgeführt werden.

SnapMirror Asynchronous Protection mit versionsflexibler Replizierung

SnapMirror asynchrone Sicherung mit versionsflexibler Replizierung bietet einen logischen Spiegelschutz der Replizierungszwischen Quell- und Ziel-Volumes, selbst wenn diese Volumes unter verschiedenen Versionen von ONTAP 8.3 oder höher ausgeführt werden (z. B. Version 8.3 zu 8.3, oder 8.3 zu 9.1 oder 9.0 zu 8.3).

In SnapMirror Beziehungen mit versionsflexibler Replizierung werden Spiegelvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror Beziehungen.

Aufgrund der langsameren Ausführung eignet sich SnapMirror mit versionsflexibler Replizierungssicherung nicht für den Einsatz unter folgenden Umständen:

- Das Quellobjekt enthält mehr als 10 Millionen Dateien, die gesichert werden müssen.
- Die Recovery-Zeitvorgabe für die geschützten Daten beträgt maximal zwei Stunden. (Das heißt, das Ziel muss immer gespiegelte, wiederherstellbare Daten enthalten, die nicht mehr als zwei Stunden älter sind als die Daten der Quelle.)

In einem der aufgeführten Situationen ist die schnellere blockbasierte Ausführung der SnapMirror Standardsicherung erforderlich.

SnapMirror Asynchronous Protection mit versionsflexibler Replizierung und Option für Backups

SnapMirror Asynchronous Protection mit der versionsflexiblen Replizierungs- und Backup-Option bietet Spiegelschutz zwischen Quell- und Ziel-Volumes und die Möglichkeit, mehrere Kopien der gespiegelten Daten am Zielspeicherort zu speichern.

Der Storage-Administrator kann festlegen, welche Snapshot Kopien vom Quell- zum Zielsystem gespiegelt werden, und er kann auch angeben, wie lange diese Kopien am Ziel aufbewahrt werden sollen, selbst wenn sie an der Quelle gelöscht werden.

In SnapMirror Beziehungen mit versionsflexibler Replizierung und Backup-Option werden Spiegelvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror Beziehungen.

SnapMirror synchroner Schutz mit strenger Synchronisierung

SnapMirror Synchronous Schutz mit „`strict`“-Synchronisierung sorgt dafür, dass das primäre und sekundäre Volume immer eine echte Kopie voneinander sind. Falls beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replizierungsfehler auftritt, wird der Client-I/O auf das primäre Volume unterbrochen.

SnapMirror synchroner Schutz mit regelmäßiger Synchronisierung

SnapMirror Synchronous Schutz mit „`regular`“-Synchronisierung erfordert nicht, dass das primäre und sekundäre Volume immer eine echte Kopie voneinander sind, wodurch die Verfügbarkeit des primären Volumes gewährleistet wird. Wenn beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replizierungsfehler auftritt, werden die primären und sekundären Volumes nicht mehr synchronisiert und die Client-I/O-Vorgänge werden weiter zum primären Volume fortgesetzt.

Die Schaltfläche „Wiederherstellen“ und die Schaltflächen zum Beziehungsvorgang sind nicht verfügbar, wenn synchrone Schutzbeziehungen auf der Seite „Gesundheits-/Volume-Bestand“ oder auf der Seite „Angaben zum Zustand/Volumen“ überwacht werden.

Einrichten von Sicherungsbeziehungen in Unified Manager

Sie müssen verschiedene Schritte durchführen, um Unified Manager und OnCommand Workflow Automation zu verwenden, um SnapMirror- und SnapVault-Beziehungen zum Schutz Ihrer Daten einzurichten.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Es müssen Peer-Beziehungen zwischen zwei Clustern oder zwei Storage Virtual Machines (SVMs) hergestellt werden.
- OnCommand Workflow Automation muss in Unified Manager integriert werden:
  - OnCommand Workflow Automation einrichten
  - Überprüfen des Quellcaches von Unified Manager in Workflow Automation

Schritte

1. Führen Sie je nach Art der Schutzbeziehung einen der folgenden Schritte aus:
   - SnapMirror Sicherungsbeziehung erstellen.
   - SnapVault Sicherungsbeziehung erstellen.
2. Wenn Sie je nach Art der Beziehung eine Richtlinie für die Beziehung erstellen möchten, führen Sie einen der folgenden Schritte aus:
   - Erstellen einer SnapVault-Richtlinie.
   - SnapMirror-Richtlinie erstellen.
3. Erstellen eines SnapMirror oder SnapVault Zeitplans.

Konfigurieren einer Verbindung zwischen Workflow Automation und Unified Manager

Es besteht die Möglichkeit, eine sichere Verbindung zwischen OnCommand Workflow Automation (WFA) und Unified Manager zu konfigurieren. Durch die Verbindung zur Workflow-Automatisierung können Unternehmen Sicherungsfunktionen wie SnapMirror und SnapVault Konfigurations-Workflows sowie Befehle zum Management von SnapMirror Beziehungen nutzen.

Bevor Sie beginnen

- Die installierte Version von Workflow Automation muss 4.2 oder höher sein.
- Sie müssen „`WFA Pack zum Management von Clustered Data ONTAP`“ Version 9.5.0 oder neuer auf dem WFA Server installiert haben. Das erforderliche Paket können Sie im NetApp Storage Automation Store herunterladen.

  "WFA Pack zum Management von ONTAP"

- Sie müssen den Namen des in Unified Manager erstellten Datenbankbenutzers haben, um WFA- und Unified Manager-Verbindungen zu unterstützen.

  Diesem Datenbankbenutzer muss die Rolle „Integration Schema“ zugewiesen worden sein.

- In Workflow Automation müssen Sie entweder die Administratorrolle oder die Rolle „Architekt“ zuweisen.
- Sie müssen über die Host-Adresse, die Portnummer 443, den Benutzernamen und das Passwort für die Workflow Automation-Einrichtung verfügen.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Setup-Menü auf **Workflow Automation**.
2. Wählen Sie im Bereich **OnCommand Unified Manager Database User** der Seite **Setup/Workflow Automation** den Namen aus und geben Sie das Kennwort für den Datenbankbenutzer ein, den Sie erstellt haben, um Unified Manager- und Workflow-Automatisierungsverbindungen zu unterstützen.
3. Geben Sie im Bereich **OnCommand Workflow Automation Credentials** der Seite **Setup/Workflow Automation** den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) sowie den Benutzernamen und das Passwort für das Setup der Workflow-Automatisierung ein.

   Sie müssen den Unified Manager Server Port (Port 443) verwenden.

4. Klicken Sie Auf **Speichern**.
5. Wenn Sie ein selbstsigniertes Zertifikat verwenden, klicken Sie auf **Ja**, um das Sicherheitszertifikat zu autorisieren.

   Die Seite Setup/Workflow-Automatisierung wird angezeigt.

6. Klicken Sie auf **Ja**, um die Web-Benutzeroberfläche neu zu laden, und fügen Sie die Workflow-Automation-Funktionen hinzu.

Überprüfen des Quellcaches von Unified Manager in Workflow Automation

Sie können feststellen, ob das Caching der Datenquelle von Unified Manager ordnungsgemäß funktioniert, indem Sie prüfen, ob die Datenerfassung in Workflow Automation erfolgreich ist. Dies kann Sie erreichen, wenn Sie Workflow Automation in Unified Manager integrieren, um sicherzustellen, dass Workflow-Automatisierung nach der Integration verfügbar ist.

Bevor Sie beginnen

Um diese Aufgabe ausführen zu können, müssen Sie in Workflow Automation entweder die Administratorrolle oder die Rolle „Architekt“ zuweisen.

Schritte

1. Wählen Sie in der Workflow Automation UI **Ausführung** > **Datenquellen** aus.
2. Klicken Sie mit der rechten Maustaste auf den Namen der Datenquelle von Unified Manager und wählen Sie dann **Jetzt erwerben** aus.

3. Vergewissern Sie sich, dass die Akquisition fehlerfrei erfolgreich ist.

   Um die Workflow-Automatisierung in Unified Manager erfolgreich zu integrieren, müssen Konfigurationsfehler behoben werden.

Erstellen einer SnapMirror Schutzbeziehung auf der Seite „Systemzustand“/„Volume-Details“

Auf der Seite „Systemzustand“/„Volume-Details“ können Sie eine SnapMirror Beziehung erstellen, sodass die Datenreplizierung zu Sicherungszwecken aktiviert ist. Die SnapMirror Replizierung ermöglicht Ihnen die Wiederherstellung von Daten vom Ziel-Volume im Falle eines Datenverlusts auf dem Quellsystem.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Über diese Aufgabe

Das Menü * Protect* wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
- Wenn es sich um ein FlexGroup Volume handelt
- Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung besteht und der Ziel-Cluster noch nicht erkannt wurde

Sie können bis zu 10 Sicherungsjobs gleichzeitig ausführen, ohne die Leistung zu beeinträchtigen. Möglicherweise haben Sie Auswirkungen auf die Leistung, wenn Sie zwischen 11 und 30 Jobs gleichzeitig ausführen. Es wird nicht empfohlen, mehr als 30 Jobs gleichzeitig auszuführen.

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Gesundheit/Volumen** mit der rechten Maustaste in die Topologieansicht auf den Namen eines Volumes, das Sie schützen möchten.
2. Wählen Sie aus dem Menü * Protect* > **SnapMirror** aus.

   Das Dialogfeld Schutz konfigurieren wird angezeigt.

3. Klicken Sie auf **SnapMirror**, um die Registerkarte **SnapMirror** anzuzeigen und die Zielinformationen zu konfigurieren.
4. Klicken Sie auf **Erweitert**, um die Platzgarantie nach Bedarf festzulegen, und klicken Sie dann auf **Anwenden**.
5. Füllen Sie im Dialogfeld **Schutz konfigurieren** den Bereich **Zielinformationen** und den Bereich **Beziehungseinstellungen** aus.
6. Klicken Sie Auf **Anwenden**.

   Sie gelangen zurück zur Seite „Health/Volume Details“.

7. Klicken Sie oben auf der Seite **Health/Volume** Details auf den Link für die Schutzkonfiguration.

Die Aufgaben und Details des Jobs werden auf der Seite „Schutz/Job-Details“ angezeigt.

8. Klicken Sie auf der Seite **Schutz/Job** Details auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist.
9. Wenn die Aufgaben abgeschlossen sind, klicken Sie auf **Zurück** in Ihrem Browser, um zur Detailseite **Gesundheit/Volumen** zurückzukehren.

   Die neue Beziehung wird auf der Topologieansicht „Systemzustand/Volume-Details“ angezeigt.

Ergebnisse

Je nachdem, welche Ziel-SVM Sie während der Konfiguration oder in den Optionen angegeben haben, die Sie in den erweiterten Einstellungen aktiviert haben, kann die SnapMirror Beziehung eine oder mehrere mögliche Varianten sein:

- Falls Sie eine Ziel-SVM angegeben haben, die unter derselben oder einer neueren Version von ONTAP im Vergleich zur des Quell-Volume ausgeführt wird, ist eine auf Replizierung basierende SnapMirror Beziehung das Standardergebnis.
- Wenn Sie eine Ziel-SVM angegeben haben, die im Vergleich zum Quell-Volume unter derselben oder einer neueren Version von ONTAP (Version 8.3 oder höher) ausgeführt wird, aber Sie in den erweiterten Einstellungen eine versionsflexible Replizierung aktiviert haben, ist das Ergebnis eine SnapMirror Beziehung mit versionsflexibler Replizierung.
- Wenn Sie eine Ziel-SVM angegeben haben, die unter einer früheren Version von ONTAP 8.3 ausgeführt wird, oder eine Version, die höher ist als die des Quell-Volume, und die frühere Version unterstützt versionsflexible Replizierung. Das automatische Ergebnis ist eine SnapMirror Beziehung mit versionsflexibler Replizierung.

Erstellen einer SnapVault-Schutzbeziehung auf der Seite „Health/Volume Details“

Sie können eine SnapVault-Beziehung auf der Seite „Systemzustand/Volume-Details“ erstellen, sodass Daten-Backups für Sicherungszwecke auf Volumes aktiviert sind.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten, um diese Aufgabe auszuführen.

Über diese Aufgabe

Das Menü * Protect* wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
- Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung vorhanden ist und der Ziel-Cluster noch nicht erkannt wurde

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Gesundheit/Volumen** mit der rechten Maustaste auf ein Volume in der Topologieansicht, die Sie schützen möchten.

2. Wählen Sie im Menü * Protect* > **SnapVault** aus.

   Das Dialogfeld Schutz konfigurieren wird gestartet.

3. Klicken Sie auf **SnapVault**, um die Registerkarte **SnapVault** anzuzeigen und die Informationen zur sekundären Ressource zu konfigurieren.
4. Klicken Sie auf **Erweitert**, um Deduplizierung, Komprimierung, Autogrow und Platzgarantie nach Bedarf festzulegen und klicken Sie dann auf **Apply**.
5. Füllen Sie im Dialogfeld **Schutz konfigurieren** den Bereich **Zielinformationen** und den Bereich **Beziehungseinstellungen** aus.
6. Klicken Sie Auf **Anwenden**.

   Sie gelangen zurück zur Seite „Health/Volume Details“.

7. Klicken Sie oben auf der Seite **Health/Volume** Details auf den Link für die Schutzkonfiguration.

   Die Seite Schutz-/Jobdetails wird angezeigt.

8. Klicken Sie auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist.

   Wenn die Aufgabenstellungen abgeschlossen sind, werden die neuen Beziehungen auf der Topologieansicht „Systemzustand/Volume-Details“ angezeigt.

Erstellen einer SnapVault-Richtlinie zur Maximierung der Übertragungseffizienz

Sie können eine neue SnapVault-Richtlinie erstellen, um die Priorität für eine SnapVault-Übertragung festzulegen. Anhand von Richtlinien wird die Effizienz der Übertragungen in einer Sicherungsbeziehung vom primären zum sekundären Volume maximiert.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.
- Sie müssen bereits den Bereich Zielinformationen im Dialogfeld Schutz konfigurieren ausgefüllt haben.

Schritte

1. Klicken Sie im Dialogfeld **Schutz konfigurieren** auf der Registerkarte **SnapVault** im Bereich **Beziehungseinstellungen** auf den Link **Richtlinien erstellen**.

   Die Registerkarte SnapVault wird angezeigt.

2. Geben Sie im Feld **Policy Name** den Namen ein, den Sie der Richtlinie geben möchten.
3. Wählen Sie im Feld **Priorität übertragen** die Übertragungspriorität aus, die Sie der Richtlinie zuweisen möchten.
4. Geben Sie im Feld **Kommentar** einen Kommentar für die Richtlinie ein.
5. Fügen Sie im Bereich **Replication Label** eine Replikationbeschriftung bei Bedarf hinzu oder bearbeiten Sie sie.

6. Klicken Sie Auf **Erstellen**.

   Die neue Richtlinie wird in der Dropdown-Liste Richtlinie erstellen angezeigt.

Erstellen einer SnapMirror-Richtlinie zur Maximierung der Übertragungseffizienz

Sie können eine SnapMirror-Richtlinie erstellen, um die SnapMirror Übertragungspriorität für Sicherungsbeziehungen festzulegen. Mithilfe der SnapMirror Richtlinien lässt sich die Übertragungseffizienz von der Quelle zum Ziel maximieren, indem Prioritäten zugewiesen werden, sodass Transfers mit niedriger Priorität nach Transfers mit normaler Priorität geplant werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.
- Bei dieser Aufgabe wird davon ausgegangen, dass Sie den Bereich Zielinformationen im Dialogfeld Schutz konfigurieren bereits abgeschlossen haben.

Schritte

1. Klicken Sie im Dialogfeld **Schutz konfigurieren** auf der Registerkarte **SnapMirror** im Bereich **Beziehungseinstellungen** auf den Link **Richtlinien erstellen**.

   Das Dialogfeld SnapMirror-Richtlinie erstellen wird angezeigt.

2. Geben Sie im Feld **Policy Name** einen Namen ein, den Sie der Richtlinie geben möchten.
3. Wählen Sie im Feld * Priorität übertragen* die Übertragungspriorität aus, die Sie der Richtlinie zuweisen möchten.
4. Geben Sie im Feld **Kommentar** einen optionalen Kommentar für die Richtlinie ein.
5. Klicken Sie Auf **Erstellen**.

   Die neue Richtlinie wird in der Dropdown-Liste SnapMirror-Richtlinie angezeigt.

Erstellen von Zeitplänen für SnapMirror und SnapVault

Sie können grundlegende oder erweiterte Zeitpläne für SnapMirror und SnapVault erstellen, um automatische Datensicherheitstransfers auf einem Quell- oder primären Volume zu ermöglichen. Dadurch werden diese je nach Häufigkeit der Datenänderungen auf Ihren Volumes häufiger oder weniger häufiger durchgeführt.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen den Bereich Zielinformationen im Dialogfeld Schutz konfigurieren bereits ausgefüllt haben.
- Sie müssen Workflow Automation einrichten, um diese Aufgabe auszuführen.

Schritte

1. Klicken Sie im Dialogfeld **Schutz konfigurieren** auf der Registerkarte **SnapMirror** oder auf der Registerkarte **SnapVault** im Bereich **Beziehungseinstellungen** auf den Link **Zeitplan erstellen**.

   Das Dialogfeld Zeitplan erstellen wird angezeigt.

2. Geben Sie im Feld **Terminplanname** den Namen ein, den Sie dem Zeitplan geben möchten.
3. Wählen Sie eine der folgenden Optionen:
   - **Einfach**

     Wählen Sie aus, wenn Sie einen grundlegenden Intervall-Stil-Zeitplan erstellen möchten.

   - **Erweitert**

     Wählen Sie aus, wenn Sie einen Zeitplan im Cron-Stil erstellen möchten.

4. Klicken Sie Auf **Erstellen**.

   Der neue Zeitplan wird in der Dropdown-Liste „SnapMirror Schedule“ oder „SnapVault Schedule“ angezeigt.

Durchführen eines Failover und Failback einer Sicherungsbeziehung

Wenn ein Quell-Volume in Ihrer Sicherungsbeziehung aufgrund eines Hardware-Ausfalls oder eines Notfalls deaktiviert wird, können Sie die Sicherungsfunktionen in Unified Manager verwenden, um den Zugriff auf Lese-/Schreibzugriff auf das Schutzziel zu ermöglichen und ein Failover auf dieses Volume durchzuführen, bis die Quelle wieder online ist; Anschließend können Sie ein Failback zur ursprünglichen Quelle erstellen, sobald Daten zur Verfügung stehen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen OnCommand Workflow Automation einrichten, um diesen Vorgang auszuführen.

Schritte

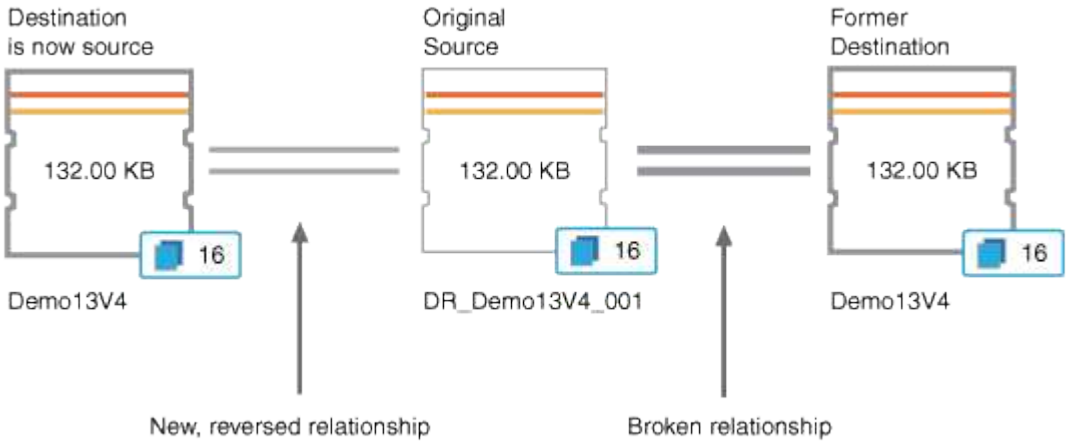
1. SnapMirror Beziehung unterbrechen.

   Sie müssen die Beziehung unterbrechen, bevor Sie das Ziel von einem Datensicherungs-Volume in ein Lese-/Schreib-Volume konvertieren können, und bevor Sie die Beziehung rückgängig machen können.

2. Die Sicherungsbeziehung wird umkehren.

   Wenn das ursprüngliche Quell-Volume wieder verfügbar ist, können Sie vielleicht entscheiden, die ursprüngliche Schutzbeziehung wiederherzustellen, indem Sie das Quell-Volume wiederherstellen. Bevor Sie die Quelle wiederherstellen können, müssen Sie sie mit den Daten synchronisieren, die auf das frühere Ziel geschrieben wurden. Sie verwenden die umgekehrte Resynchronisierung, um eine neue Schutzbeziehung zu erstellen, indem Sie die Rollen der ursprünglichen Beziehung rückgängig machen und das Quell-Volume mit dem vorherigen Ziel synchronisieren. Für die neue Beziehung wird eine neue Basis-Snapshot Kopie erstellt.

Die umgekehrte Beziehung sieht ähnlich aus wie eine kaskadierte Beziehung:



3. Die umgekehrte SnapMirror Beziehung unterbrechen.

   Wenn das ursprüngliche Quell-Volume neu synchronisiert wird und erneut Daten bereitstellen kann, unterbrechen Sie die umgekehrte Beziehung.

4. Entfernen Sie die Beziehung.

   Wenn die umgekehrte Beziehung nicht mehr erforderlich ist, sollten Sie diese Beziehung entfernen, bevor Sie die ursprüngliche Beziehung wieder herstellen.

5. Beziehung neu synchronisieren.

   Verwenden Sie den Vorgang zur erneuten Synchronisierung, um Daten von der Quelle zum Ziel zu synchronisieren und die ursprüngliche Beziehung wiederherzustellen.

Die SnapMirror-Beziehung von der Seite „Systemzustand/Volume-Details“ abbricht

Sie können eine Sicherungsbeziehung auf der Seite Systemzustand/Volume-Details unterbrechen und die Datentransfers zwischen einem Quell- und Ziel-Volume in einer SnapMirror Beziehung stoppen. Wenn Sie Daten migrieren, für Disaster Recovery-Zwecke oder zum Testen von Applikationen nutzen möchten, können Sie eine Beziehung unterbrechen. Das Zielvolume wird in ein Lese- und Schreib-Volume geändert. Man kann keine SnapVault Beziehung durchbrechen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Registerkarte **Schutz** der Seite **Gesundheit/Volume** Details aus der Topologie die SnapMirror Beziehung aus, die Sie brechen möchten.
2. Klicken Sie mit der rechten Maustaste auf das Ziel und wählen Sie im Menü die Option **Pause** aus.

Das Dialogfeld Beziehung unterbrechen wird angezeigt.

3. Klicken Sie auf **Weiter**, um die Beziehung zu brechen.
4. Stellen Sie in der Topologie sicher, dass die Beziehung unterbrochen ist.

Rückkehrung von Schutzbeziehungen auf der Seite „Gesundheits-/Volume-Details“

Wenn ein Notfall das Quellvolume in Ihrer Schutzbeziehung deaktiviert, können Sie das Zielvolume für die Bereitstellung von Daten verwenden, indem Sie es in Lese-/Schreibzugriff konvertieren, während Sie die Quelle reparieren oder ersetzen. Wenn die Quelle für den Empfang von Daten erneut verfügbar ist, können Sie mithilfe der Resynchronisierung auf umgekehrter Richtung die Beziehung herstellen und die Daten auf der Quelle mit den Daten auf dem Ziel für Lesen/Schreiben synchronisieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.
- Die Beziehung darf keine SnapVault Beziehung sein.
- Eine Schutzbeziehung muss bereits vorhanden sein.
- Die Schutzbeziehung muss gebrochen werden.
- Sowohl die Quelle als auch das Ziel müssen online sein.
- Die Quelle darf nicht Ziel eines anderen Datensicherungs-Volumes sein.

Über diese Aufgabe

- Wenn Sie diese Aufgabe ausführen, werden Daten in der Quelle, die neuer als die Daten in der gemeinsamen Snapshot Kopie ist, gelöscht.
- Die für die umgekehrte Resynchronisierung erstellten Richtlinien und Zeitpläne sind mit denen in der ursprünglichen Schutzbeziehung identisch.

  Wenn Richtlinien und Zeitpläne nicht vorhanden sind, werden sie erstellt.

Schritte

1. Suchen Sie auf der **Schutz**-Registerkarte der **Gesundheit/Volumen**-Detailseite in der Topologie die SnapMirror-Beziehung, auf der Sie Quelle und Ziel umkehren möchten, und klicken Sie mit der rechten Maustaste darauf.
2. Wählen Sie aus dem Menü die Option **Resync rückwärts**.

   Das Dialogfeld Resync umkehren wird angezeigt.

3. Stellen Sie sicher, dass die Beziehung, die im Dialogfeld **Resync** umkehren angezeigt wird, die Beziehung ist, für die Sie die Neusynchronisierung rückgängig machen möchten, und klicken Sie dann auf **Absenden**.

   Das Dialogfeld „Resync umkehren“ wird geschlossen und oben auf der Seite „Health/Volume Details“ wird ein Job-Link angezeigt.

4. Klicken Sie auf der Seite **Health/Volume** Details auf **Jobs anzeigen**, um den Status jedes umgekehrten

Neusynchronisierung zu verfolgen.

Eine gefilterte Liste von Jobs wird angezeigt.

5. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Detailseite **Gesundheit/Volumen** zurückzukehren.

   Nach erfolgreichem Abschluss aller Jobaufgaben ist die Neusynchronisierung bei umgekehrter Neusynchronisierung abgeschlossen.

Entfernen einer Schutzbeziehung von der Seite „Gesundheits-/Volume-Details“

Sie können eine Schutzbeziehung entfernen, um eine vorhandene Beziehung zwischen der ausgewählten Quelle und dem ausgewählten Ziel dauerhaft zu löschen, z. B. wenn Sie eine Beziehung unter Verwendung eines anderen Ziels erstellen möchten. Durch diesen Vorgang werden alle Metadaten entfernt und können nicht rückgängig gemacht werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Registerkarte **Protection** der Seite **Health/Volume** Details aus der Topologie die SnapMirror Beziehung aus, die Sie entfernen möchten.
2. Klicken Sie mit der rechten Maustaste auf den Namen des Ziels und wählen Sie im Menü die Option **Entfernen**.

   Das Dialogfeld Beziehung entfernen wird angezeigt.

3. Klicken Sie auf **Weiter**, um die Beziehung zu entfernen.

   Die Beziehung wird von der Seite „Health/Volume Details“ entfernt.

Erneutes Synchronisieren von Schutzbeziehungen auf der Seite „Systemzustand/Volume-Details“

Sie können Daten auf einer SnapMirror oder SnapVault-Beziehung neu synchronisieren, die unterbrochen wurde, und dann wurde das Ziel gelesen/geschrieben, sodass die Daten auf der Quelle mit den Daten auf dem Ziel übereinstimmen. Sie können auch neu synchronisieren, wenn eine erforderliche gemeinsame Snapshot Kopie auf dem Quell-Volume gelöscht wird, sodass SnapMirror oder SnapVault Updates fehlschlagen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Suchen Sie auf der Registerkarte **Schutz** der Detailseite **Gesundheit/Volumen** in der Topologie die Schutzbeziehung, die Sie neu synchronisieren möchten, und klicken Sie mit der rechten Maustaste darauf.
2. Wählen Sie im Menü * resynchronisieren* aus.

   Alternativ können Sie im Menü **Aktionen** die Option **Beziehung** > **Resynchronisieren** wählen, um die Beziehung, für die Sie die Details anzeigen, neu zu synchronisieren.

   Das Dialogfeld „Resynchronisieren“ wird angezeigt.
3. Wählen Sie auf der Registerkarte **Resynchronisierung Optionen** eine Übertragungs-Priorität und die maximale Übertragungsrate aus.
4. Klicken Sie auf **Quelle Snapshot Kopien** und dann in der Spalte **Snapshot Kopie** auf **Standard**.

   Das Dialogfeld Quell-Snapshot-Kopie auswählen wird angezeigt.
5. Wenn Sie eine vorhandene Snapshot Kopie angeben möchten, anstatt die Standard-Snapshot Kopie zu übertragen, klicken Sie auf **vorhandene Snapshot Kopie** und wählen Sie eine Snapshot Kopie aus der Liste aus.
6. Klicken Sie Auf **Absenden**.

   Sie werden wieder zum Dialogfeld „erneut synchronisieren“ angezeigt.
7. Wenn Sie mehrere Quellen zum erneuten Synchronisieren ausgewählt haben, klicken Sie für die nächste Quelle, für die Sie eine vorhandene Snapshot Kopie angeben möchten, auf **Standard**.
8. Klicken Sie auf **Senden**, um die Neusynchronisierung zu beginnen.

   Der Resynchronisierung-Job wurde gestartet, Sie werden wieder zur Seite „Details zu Funktionszustand/Volumen“ und oben auf der Seite wird ein Link zu Jobs angezeigt.
9. Klicken Sie auf der Seite **Health/Volume** Details auf **Jobs anzeigen**, um den Status der einzelnen Neusynchronisierung zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.
10. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Detailseite **Gesundheit/Volumen** zurückzukehren.

    Die Neusynchronisierung ist abgeschlossen, nachdem alle Aufgabenstellungen erfolgreich abgeschlossen wurden.

Behebung eines Schutzauftrags

Dieser Workflow bietet ein Beispiel dafür, wie Sie Fehler im Schutz über das Unified Manager-Dashboard identifizieren und beheben können.

Bevor Sie beginnen

Da für einige Aufgaben in diesem Workflow eine Anmeldung über die Rolle „OnCommand Administrator“ erforderlich ist, müssen Sie mit den Rollen vertraut sein, die für die Verwendung verschiedener Funktionen erforderlich sind, wie in beschrieben Unified Manager Benutzer-Rollen und -Funktionen.

Über diese Aufgabe

In diesem Szenario greifen Sie auf die Seite Dashboards/Übersicht zu, um zu sehen, ob es Probleme mit Ihren Schutzjobs gibt. Im Bereich Schutzvorfall stellen Sie fest, dass ein Vorfall mit dem Jobabbruch vorliegt und ein Fehler beim Schutz eines Volumes angezeigt wird. Sie untersuchen diesen Fehler, um die mögliche Ursache und mögliche Lösung zu ermitteln.

Schritte

1. Klicken Sie im Bereich **Schutz-Vorfälle** des Dashboards **ungelöste Vorfälle und Risiken** auf das Ereignis **Schutzauftrag fehlgeschlagen**.

   Der verknüpfte Text für das Ereignis wird in das Formular geschrieben `object_name:/object_name - Error Name`, Wie z. B. `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

   Die Seite Ereignisdetails für den fehlgeschlagenen Schutzauftrag wird angezeigt.

2. Prüfen Sie die Fehlermeldung im Feld Ursache im Bereich **Zusammenfassung**, um das Problem zu ermitteln und mögliche Korrekturmaßnahmen zu bewerten.

   Siehe Identifizieren des Problems und Durchführen von Korrekturmaßnahmen für einen fehlgeschlagenen Schutzauftrag.

Identifizieren des Problems und Durchführen von Korrekturmaßnahmen für einen fehlgeschlagenen Schutzauftrag

Sie überprüfen die Fehlermeldung zum Jobfehler im Feld Ursache auf der Seite Ereignisdetails und stellen fest, dass der Job aufgrund eines Fehlers bei der Snapshot-Kopie fehlgeschlagen ist. Anschließend gehen Sie zur Seite „Health/Volume Details“, um weitere Informationen zu erhalten.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Die Fehlermeldung, die im Feld Ursache auf der Seite Ereignisdetails angezeigt wird, enthält den folgenden Text über den fehlgeschlagenen Job:

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.).)
*Job Details*
```

Diese Meldung enthält folgende Informationen:

- Ein Backup- oder Spiegelungsauftrag wurde nicht erfolgreich abgeschlossen.

  Der Job umfasste eine Sicherungsbeziehung zwischen dem Quell-Volume `cluster2_src_vol2` Auf dem virtuellen Server `cluster2_src_svm` Und dem Ziel-Volume `managed_svc2_vol3` Auf dem virtuellen Server mit dem Namen `cluster3_dst_svm`.

- Fehler beim Erstellen eines Jobs für die Snapshot Kopie `0426cluster2_src_vol2snap` Auf dem Quell-Volume `cluster2_src_svm:/cluster2_src_vol2`.

In diesem Szenario können Sie die Ursache und mögliche Korrekturmaßnahmen für den Job-Fehler identifizieren. Zur Behebung des Fehlers müssen Sie jedoch entweder auf die Web-UI des System Managers oder auf die CLI-Befehle von ONTAP zugreifen.

Schritte

1. Sie überprüfen die Fehlermeldung und stellen fest, dass ein Snapshot-Kopierauftrag auf dem Quell-Volume fehlgeschlagen ist, was darauf hinweist, dass möglicherweise ein Problem mit Ihrem Quell-Volume vorliegt.

   Optional können Sie am Ende der Fehlermeldung auf den Link **Job Details** klicken, aber für die Zwecke dieses Szenarios wählen Sie nicht zu tun.

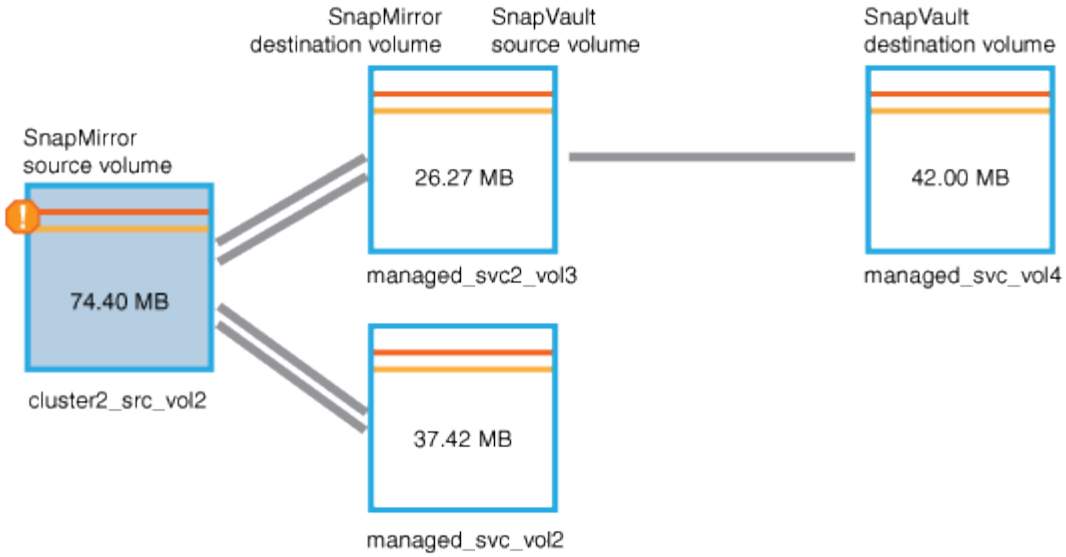
2. Sie entscheiden, dass Sie versuchen möchten, das Ereignis zu lösen, so gehen Sie wie folgt vor:
   a. Klicken Sie auf die Schaltfläche **Zuweisen zu** und wählen Sie im Menü die Option **ME** aus.
   b. Klicken Sie auf die Schaltfläche **Bestätigen**, damit Sie keine wiederholten Warnmeldungen erhalten, wenn für das Ereignis Warnmeldungen eingerichtet wurden.
   c. Optional können Sie auch Anmerkungen zum Ereignis hinzufügen.
3. Klicken Sie im Fensterbereich **Zusammenfassung** auf das Feld **Quelle**, um Details zum Quellvolumen anzuzeigen.

   Das Feld **Quelle** enthält den Namen des Quellobjekts: In diesem Fall das Volume, auf dem der Snapshot-Kopierauftrag geplant wurde.

   Die Seite Health/Volume Details wird für angezeigt `cluster2_src_vol2`, Zeigt den Inhalt der Registerkarte Schutz.

4. Wenn man sich das Topologiediagramm ansieht, wird ein Fehlersymbol angezeigt, das mit dem ersten Volume in der Topologie verknüpft ist, das das Quell-Volume für die SnapMirror Beziehung ist.

   Die horizontalen Balken im Quell-Volume-Symbol zeigen die für dieses Volume eingestellten Warn- und Fehlerschwellenwerte an.



5. Sie platzieren den Cursor über das Fehlersymbol, um das Popup-Dialogfeld anzuzeigen, in dem die Schwellenwerteinstellungen angezeigt werden. Es wird angezeigt, dass das Volume den Fehlerschwellenwert überschritten hat und ein Kapazitätsproblem angezeigt wird.
6. Klicken Sie auf die Registerkarte **Kapazität**.

   Kapazitätsinformationen zum Volume `cluster2_src_vol2` Anzeigen.

7. Im Fensterbereich **Kapazität** wird angezeigt, dass im Balkendiagramm ein Fehlersymbol angezeigt wird, das wiederum anzeigt, dass die Volumenkapazität den für das Volumen festgelegten Schwellenwert überschritten hat.
8. Unter dem Kapazitätsdiagramm sehen Sie, dass Autogrow von Volume deaktiviert wurde und eine Volume-Platzgarantie gesetzt wurde.

   Sie könnten sich für die Aktivierung von Autogrow entscheiden. In diesem Szenario entscheiden Sie sich jedoch, bis Sie eine Entscheidung treffen, wie das Kapazitätsproblem zu lösen ist, bevor Sie eine Entscheidung treffen.

9. Sie scrollen nach unten zur Liste **Ereignisse** und sehen, dass der Schutzauftrag fehlgeschlagen ist, Volume Days bis Full und Volume Space Full Events generiert wurden.
10. In der **Events**-Liste klicken Sie auf das Event **Volume Space Full**, um weitere Informationen zu erhalten, nachdem Sie entschieden haben, dass dieses Ereignis für Ihr Kapazitätsproblem am relevantesten erscheint.

    Auf der Seite Ereignisdetails wird das Ereignis Volume Space Full für das Quell-Volume angezeigt.

11. Im Bereich **Zusammenfassung** lesen Sie das Feld Ursache für das Ereignis: `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`
12. Unterhalb des Bereichs **Zusammenfassung** werden die vorgeschlagenen Korrekturmaßnahmen angezeigt.

    Die vorgeschlagenen Korrekturmaßnahmen werden nur für bestimmte Ereignisse angezeigt, sodass dieser Bereich für alle Arten von Ereignissen nicht angezeigt wird.

    Klicken Sie durch die Liste der vorgeschlagenen Aktionen, die Sie möglicherweise durchführen können, um das Ereignis Volume Space Full aufzulösen:

- Aktivieren Sie Autogrow auf diesem Volume.
- Die Volume-Größe ändern
- Aktivierung und Ausführung der Deduplizierung auf diesem Volume
- Aktivieren und führen Sie die Komprimierung auf diesem Volume durch.

13. Sie entscheiden sich für die Aktivierung von Autogrow auf dem Volume. Dazu müssen Sie jedoch den verfügbaren freien Speicherplatz im übergeordneten Aggregat und die aktuelle Wachstumsrate des Volume bestimmen:
    a. Sehen Sie sich das übergeordnete Aggregat an, `cluster2_src_aggr1`, Im Fenster **Verwandte Geräte**.

       Sie können auf den Namen des Aggregats klicken, um weitere Details zum Aggregat zu erhalten.

       Sie bestimmen, dass das Aggregat über ausreichend Platz verfügt, um die Autogrow von Volumes zu aktivieren.

    b. Sehen Sie sich oben auf der Seite das Symbol für einen kritischen Vorfall an, und überprüfen Sie den Text unter dem Symbol.

       Sie bestimmen, dass „Tage voll: Weniger als ein Tag“- Wachstumsrate: 5.4%.

14. Wechseln Sie zu System Manager oder rufen Sie die ONTAP-CLI auf, um die zu aktivieren `volume autogrow` Option.

    Notieren Sie sich die Namen des Volumes und des Aggregats, sodass Sie sie bei der Aktivierung von Autogrow zur Verfügung haben.

15. Nach der Behebung des Kapazitätsproblem kehren Sie zur Detailseite für das Unified Manager**Event** zurück und markieren das Ereignis als erledigt.

Behebung von lag-Problemen

Dieser Workflow bietet ein Beispiel dafür, wie Sie ein lag-Problem lösen können. In diesem Szenario greifen Sie als Administrator oder Operator auf die Seite Unified ManagerDashboards/Übersicht zu, um zu sehen, ob es Probleme mit Ihren Schutzbeziehungen gibt und, falls diese vorhanden sind, Lösungen zu finden.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Auf der Seite Dashboards/Übersicht sehen Sie sich den Bereich ungelöste Vorfälle und Risiken an und Sie sehen einen SnapMirror lag-Fehler im Teilfenster „Sicherung“ unter „Sicherungsrisiken“.

Schritte

1. Suchen Sie im Fensterbereich **Schutz** auf der Seite **Dashboards/Übersicht** den Fehler SnapMirror Beziehungs-lag und klicken Sie darauf.

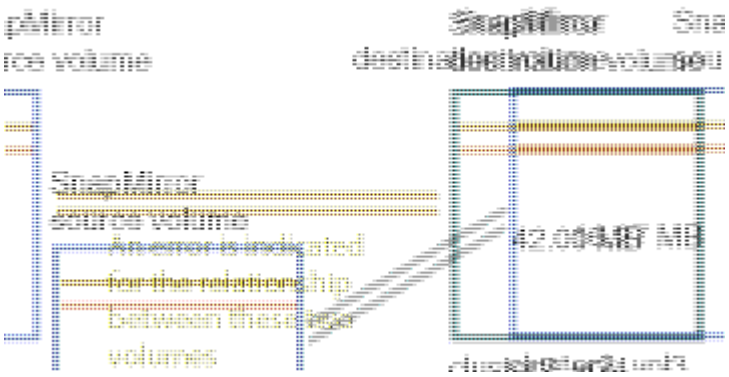
Es wird die Seite Ereignisdetails für das Ereignis lag-Fehler angezeigt.

2. Auf der Seite **Event** Details können Sie eine oder mehrere der folgenden Aufgaben ausführen:
   - Prüfen Sie die Fehlermeldung im Feld Ursache im Übersichtsbereich, um festzustellen, ob Korrekturmaßnahmen vorgeschlagen werden.
   - Klicken Sie im Feld Quelle des Übersichtsbereichs auf den Objektnamen, in diesem Fall ein Volume, um Details zum Volume anzuzeigen.
   - Suchen Sie nach Notizen, die zu diesem Event hinzugefügt wurden.
   - Fügen Sie dem Ereignis eine Notiz hinzu.
   - Weisen Sie das Ereignis einem bestimmten Benutzer zu.
   - Bestätigen oder beheben Sie das Ereignis.
3. In diesem Szenario klicken Sie im Feld Quelle des Bereichs **Zusammenfassung** auf den Objektnamen (in diesem Fall ein Volume), um Details zum Volume zu erhalten.

   Die Registerkarte Schutz der Seite Health/Volume Details wird angezeigt.

4. Auf der Registerkarte **Schutz** sehen Sie sich das Topologiediagramm an.

   Die Tatsache, dass das Volume mit dem lag-Fehler das letzte Volume einer SnapMirror Kaskadierung mit drei Volumes ist, ist zu beachten. Das ausgewählte Volume wird in Dunkelgrau dargestellt, und eine doppelte orangefarbene Linie des Quell-Volume weist auf einen SnapMirror Beziehungsfehler hin.



5. Klicken Sie auf jedes der Volumes in der SnapMirror-Kaskadierung.

   Bei der Auswahl der einzelnen Volumes sind die Schutzinformationen in der Zusammenfassung, Topologie, Verlauf, Ereignisse, Verwandte Geräte, Die Bereiche „Verwandte Warnungen“ ändern sich, um die für das ausgewählte Volume relevanten Details anzuzeigen.

6. Sie sehen den Bereich **Zusammenfassung** und positionieren den Cursor über dem Informationssymbol im Feld **Zeitplan aktualisieren** für jedes Volumen.

   In diesem Szenario beachten Sie, dass die SnapMirror-Richtlinie DPStandard ist und dass die SnapMirror-Zeitpläne stündlich innerhalb von fünf Minuten nach der Stunde aktualisiert werden. Sie wissen, dass alle Volumes in der Beziehung versuchen, einen SnapMirror Transfer gleichzeitig abzuschließen.

7. Um das lag-Problem zu beheben, ändern Sie die Zeitpläne für zwei der kaskadierten Volumes, sodass jedes Ziel nach Abschluss des Transfers einen SnapMirror Transfer beginnt.

Wiederherstellen von Daten aus Snapshot-Kopien

Wenn bei einem Ausfall Daten verloren gehen oder Verzeichnisse oder Dateien versehentlich gelöscht wurden, können Sie Unified Manager zum Auffinden und Wiederherstellen der Daten aus einer Snapshot Kopie verwenden.

Über diese Aufgabe

In der Web-UI von Unified Manager können Sie Daten von zwei Standorten wiederherstellen.

Schritte

1. Stellen Sie Daten mithilfe einer der folgenden Aufgaben wieder her:
   - Stellen Sie die Daten auf der Seite „Health/Volume Details“ wieder her.
   - Stellen Sie die Daten auf der Seite „Systemzustand/Volumes“ wieder her.

Wiederherstellen von Daten über die Seite „Health/Volume Details“

Sie können überschreibte oder gelöschte Dateien, Verzeichnisse oder ein gesamtes Volume anhand einer Snapshot Kopie wiederherstellen. Dazu verwenden Sie die Wiederherstellungsfunktion auf der Seite „Systemzustand“/„Volume-Details“.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

NTFS-Dateiströme können nicht wiederhergestellt werden.

Die Wiederherstellungsoption ist nicht verfügbar, wenn:

- Die Volume-ID ist unbekannt, z. B. wenn Sie eine Intercluster-Beziehung haben und der Ziel-Cluster noch nicht erkannt wurde.
- Das Volume ist ein FlexGroup Volume.
- Das Volume ist für die synchrone SnapMirror Replizierung konfiguriert.

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Gesundheit/Volumen** mit der rechten Maustaste in die Topologieansicht auf den Namen des Volumes, das wiederhergestellt werden soll.
2. Wählen Sie im Menü * Wiederherstellen* aus.

   Alternativ können Sie im Menü **Aktionen Restore** die aktuelle Lautstärke, für die Sie die Details anzeigen, schützen.

   Das Dialogfeld Wiederherstellen wird angezeigt.
3. Wählen Sie das Volume und die Snapshot Kopie aus, von dem Sie Daten wiederherstellen möchten, falls sie sich von dem Standard unterscheiden.
4. Wählen Sie die Elemente aus, die Sie wiederherstellen möchten.

Sie können das gesamte Volume wiederherstellen oder Ordner und Dateien angeben, die wiederhergestellt werden sollen.

5. Wählen Sie den Speicherort aus, an dem die ausgewählten Elemente wiederhergestellt werden sollen: Entweder **Originalstandort** oder **alternativer bestehender Standort**.
6. Wenn Sie einen alternativen vorhandenen Standort auswählen, führen Sie einen der folgenden Schritte aus:
   - Geben Sie im Textfeld Pfad wiederherstellen den Pfad des Speicherorts ein, zu dem die Daten wiederhergestellt werden sollen, und klicken Sie dann auf **Verzeichnis auswählen**.
   - Klicken Sie auf **Durchsuchen**, um das Dialogfeld Verzeichnisse durchsuchen zu starten und führen Sie die folgenden Schritte aus:
     i. Wählen Sie das Cluster, die SVM und das Volume aus, das Sie wiederherstellen möchten.
     ii. Wählen Sie in der Tabelle Name einen Verzeichnisnamen aus.
     iii. Klicken Sie Auf **Verzeichnis Auswählen**.
7. Klicken Sie Auf **Wiederherstellen**.

   Der Wiederherstellungsprozess beginnt.

> Wenn eine Wiederherstellung zwischen Cloud Volumes ONTAP HA Clustern mit einem NDMP-Fehler fehlschlägt, müssen Sie möglicherweise eine explizite AWS Route im Ziel-Cluster hinzufügen, damit das Ziel mit der Cluster-Management-LIF des Quellsystems kommunizieren kann. Sie führen diesen Konfigurationsschritt mithilfe von OnCommand Cloud Manager aus.

Wiederherstellen von Daten mithilfe der Seite „Health/Volumes Inventory“

Sie können überschreibende oder gelöschte Dateien, Verzeichnisse oder ein gesamtes Volume anhand einer Snapshot Kopie wiederherstellen. Dazu verwenden Sie die Wiederherstellungsfunktion auf der Seite „Systemzustand“/„Volumes-Inventar“.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

NTFS-Dateiströme können nicht wiederhergestellt werden.

Die Wiederherstellungsoption ist nicht verfügbar, wenn:

- Die Volume-ID ist unbekannt, z. B. wenn Sie eine Intercluster-Beziehung haben und der Ziel-Cluster noch nicht erkannt wurde.
- Das Volume ist ein FlexGroup Volume.
- Das Volume ist für die synchrone SnapMirror Replizierung konfiguriert.

Schritte

1. Wählen Sie auf der Seite **Health/Volumes** Inventory ein Volume aus, aus dem Sie Daten wiederherstellen möchten.

2. Klicken Sie in der Symbolleiste auf **Wiederherstellen**.

   Das Dialogfeld Wiederherstellen wird angezeigt.

3. Wählen Sie das Volume und die Snapshot Kopie aus, von dem Sie Daten wiederherstellen möchten, falls sie sich von dem Standard unterscheiden.
4. Wählen Sie die Elemente aus, die Sie wiederherstellen möchten.

   Sie können das gesamte Volume wiederherstellen oder Ordner und Dateien angeben, die wiederhergestellt werden sollen.

5. Wählen Sie den Speicherort aus, an dem die ausgewählten Elemente wiederhergestellt werden sollen; entweder **Originalstandort** oder **alternativer Standort**.
6. Klicken Sie Auf **Wiederherstellen**.

   Der Wiederherstellungsprozess beginnt.

Verwalten von Systemzustandsschwellenwerten

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

Welche Schwellenwerte für den Zustand von Storage-Kapazität sind

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

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

Konfigurieren von globalen Schwellenwerteinstellungen für den Systemzustand

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

Über diese Aufgabe

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

Auf der Seite „Schwellenwerte für Konfiguration/Zustand“ können Sie auf globale Schwellenwerteinstellungen zugreifen. Sie können Schwellwerteinstellungen für einzelne Objekte auch auf der Bestandsseite oder auf der

Detailseite für das Objekt ändern.

Wahlmöglichkeiten

- Konfigurieren von globalen Integritätsschwellenwerten für das Aggregat

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

- Konfigurieren von globalen Schwellenwerten für den Zustand des Volumes

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

- Konfigurieren von globalen qtree-Zustandsschwellenwerten

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

- Bearbeiten von Verzögerungszustands-Schwellenwerten für nicht verwaltete Schutzbeziehungen

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

Konfigurieren von globalen Integritätsschwellenwerten für das Aggregat

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

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

Systemzustandsschwellenwerte gelten nicht für das Root-Aggregat des Nodes.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Health Schwellenwerte**.
2. Klicken Sie auf der Seite **Configuration/Health Schwellenwerte** auf **Aggregate**.
3. Konfigurieren Sie die entsprechenden Schwellenwerte für Kapazität, Wachstum und Snapshot-Kopien.
4. Klicken Sie Auf **Speichern**.

Konfigurieren von globalen Schwellenwerten für den Zustand des Volumes

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Health Schwellenwerte**.
2. Klicken Sie auf der Seite **Configuration/Health Schwellenwerte** auf **Volumes**.
3. Konfigurieren Sie die entsprechenden Schwellenwerte für Kapazität, Snapshot-Kopien, qtree-Kontingente, Volume-Wachstum und Inodes.
4. Klicken Sie Auf **Speichern**.

Konfigurieren von globalen qtree-Zustandsschwellenwerten

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Health Schwellenwerte**.
2. Klicken Sie auf der Seite **Konfiguration/Gesundheit Schwellenwerte** auf **Qtrees**.
3. Konfigurieren Sie die entsprechenden Kapazitätsschwellenwerte.
4. Klicken Sie Auf **Speichern**.

Bearbeiten von Verzögerungszustands-Schwellenwerten für nicht verwaltete Schutzbeziehungen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Health Schwellenwerte**.
2. Klicken Sie auf der Seite **Konfiguration/Gesundheit Schwellenwerte** auf **Beziehungen**.
3. Erhöhen oder verringern Sie je nach Bedarf den globalen Standard-Warn- oder Fehlerverzögerungsgrad.
4. Klicken Sie Auf **Speichern**.

Bearbeiten einzelner Zustandsschwellenwerte für das Aggregat

Sie können die Statusschwellenwerte für Aggregatskapazität, Wachstum und Snapshot Kopien eines oder mehrerer Aggregate bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnungen erzeugt und Sie erhalten Benachrichtigungen.

Diese Benachrichtigungen helfen Ihnen, auf Basis des generierten Ereignisses vorbeugende Maßnahmen zu ergreifen.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

Schritte

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

Bearbeiten von Schwellenwerten für den Zustand einzelner Volumes

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **Volumes**.
2. Wählen Sie auf der Seite **Health/Volumes** Inventory ein oder mehrere Volumes aus und klicken Sie dann auf **Schwellenwerte bearbeiten**.

3. Bearbeiten Sie im Dialogfeld **Volume Schwellenwerte bearbeiten** die Schwellenwerteinstellungen eines der folgenden Werte: Kapazität, Snapshot-Kopien, qtree-Kontingent, Wachstum oder Inodes, indem Sie das entsprechende Kontrollkästchen aktivieren und dann die Einstellungen ändern.
4. Klicken Sie Auf **Speichern**.

Bearbeiten einzelner qtree-Statusschwellenwerte

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory die SVM aus, auf der sich der qtree befindet.
3. Klicken Sie auf der Seite * Health/Storage Virtual Machine* Details auf die Registerkarte qtrees.
4. Wählen Sie eine oder mehrere qtrees aus und klicken Sie dann auf **Schwellenwerte bearbeiten**.
5. Ändern Sie im Dialogfeld **Qtree Schwellenwerte bearbeiten** die Kapazitätsschwellenwerte für den ausgewählten qtree oder qtrees und klicken Sie auf **Speichern**.

Verwalten von Skripten

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

Funktionsweise von Skripten mit Warnmeldungen

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

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

Das Skript verwendet die folgenden Argumente zur Ausführung:

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

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

Beispiel zum Abrufen von Argumenten aus Skripts

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

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

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

Skripte werden hinzugefügt

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

Bevor Sie beginnen

- Sie müssen die Skripte erstellt und gespeichert haben, die Sie dem Unified Manager-Server hinzufügen möchten.
- Die unterstützten Dateiformate für Skripte sind Perl, Shell, PowerShell und `.bat` Dateien:
  - Für Perl-Skripte muss Perl auf dem Unified Manager-Server installiert sein. Wenn Perl nach Unified Manager installiert wurde, müssen Sie den Unified Manager-Server neu starten.
  - Bei PowerShell Skripten muss auf dem Server die entsprechende PowerShell Ausführungsrichtlinie festgelegt werden, damit die Skripte ausgeführt werden können.

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

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

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Scripts**.
2. Klicken Sie auf der Seite **Management/Scripts** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Skript hinzufügen** auf **Durchsuchen**, um die Skriptdatei auszuwählen.
4. Geben Sie eine Beschreibung für das ausgewählte Skript ein.
5. Klicken Sie Auf **Hinzufügen**.

Skripte werden gelöscht

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

Bevor Sie beginnen

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Scripts**.
2. Wählen Sie auf der Seite **Management/Scripts** das Skript aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang, indem Sie auf **Ja** klicken.

Skriptausführung wird getestet

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

Bevor Sie beginnen

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Scripts**.
2. Fügen Sie auf der Seite * Management/Scripts* Ihr Testskript hinzu.

3. Führen Sie auf der Seite **Konfiguration/Alarmfunktionen** eine der folgenden Aktionen aus:

An…	Tun Sie das…
Fügen Sie eine Meldung hinzu	a. Klicken Sie auf der Seite Konfiguration/Warnmeldungen auf **Hinzufügen**. b. Verknüpfen Sie im Abschnitt Aktionen den Alarm mit Ihrem Testskript.
Bearbeiten Sie eine Meldung	a. Wählen Sie auf der Seite Konfiguration/Alarmfunktionen eine Warnmeldung aus und klicken Sie dann auf **Bearbeiten**. b. Verknüpfen Sie im Abschnitt Aktionen den Alarm mit Ihrem Testskript.

4. Klicken Sie Auf **Speichern**.
5. Wählen Sie auf der Seite **Konfiguration/Alarmfunktionen** die Warnmeldung aus, die Sie hinzugefügt oder geändert haben, und klicken Sie dann auf **Test**.

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

Verwalten und Überwachen von Gruppen

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

Allgemeines zu Gruppen

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

Was eine Gruppe ist

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

- Jede Gruppe hat einen eindeutigen Namen.
- Sie müssen für jede Gruppe mindestens eine Gruppenregel konfigurieren.
- Sie können einer Gruppe mehrere Gruppenregeln zuordnen.
- Jede Gruppe kann mehrere Typen von Storage-Objekten wie Clustern, SVMs oder Volumes enthalten.
- Speicherobjekte werden einer Gruppe dynamisch hinzugefügt, basierend auf dem Zeitpunkt, an dem eine

Gruppenregel erstellt wurde oder wenn Unified Manager einen Überwachungszyklus abgeschlossen hat.

- Sie können gleichzeitig Aktionen auf alle Speicherobjekte einer Gruppe anwenden, z. B. Schwellenwerte für Volumes.

Funktionsweise von Gruppenregeln für Gruppen

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

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

Bestimmten Bedingungen

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

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

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

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

Storage-Objekttyp	Anwendbare Operanden
Cluster	• Objektname • Anmerkungen

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

- Operand

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

- Operator

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

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

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

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

  ◦ Der Operandwert enthält den für den ausgewählten Operand angegebenen Wert

- Wert

  Das Wertfeld ändert sich basierend auf dem ausgewählten Operand.

Beispiel einer Gruppenregel mit Bedingungen

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

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

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

Bedingungsgruppen

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

Beispiel einer Gruppenregel mit Bedingungsgruppen

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

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

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

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

Funktionsweise von Gruppenaktionen auf Speicherobjekten

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

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

Beispiel für Aktionen eindeutiger Gruppen

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

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

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

Hinzufügen von Gruppen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppen** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Gruppe hinzufügen** einen Namen und eine Beschreibung für die Gruppe ein.

   Der Gruppenname muss eindeutig sein.

4. Klicken Sie Auf **Hinzufügen****.

Gruppen werden bearbeitet

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppen** die Gruppe aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Gruppe bearbeiten** den Namen, die Beschreibung oder beides für die Gruppe.
4. Klicken Sie Auf **Speichern**.

Gruppen werden gelöscht

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

Bevor Sie beginnen

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

Schritte

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

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

Gruppenregeln werden hinzugefügt

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Gruppenregel hinzufügen** einen Namen für die Gruppenregel an.
4. Wählen Sie im Feld **Zielobjekttyp** den Typ des Speicherobjekts aus, das Sie gruppieren möchten.
5. Wählen Sie im Feld **Gruppe** die gewünschte Gruppe aus, für die Sie Gruppenregeln erstellen möchten.
6. Führen Sie im Abschnitt **Bedingungen** die folgenden Schritte aus, um eine Bedingung, eine Bedingungsgruppe oder beide zu erstellen:

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

7. Klicken Sie Auf **Hinzufügen**.

Beispiel für das Erstellen einer Gruppenregel

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

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

Gruppenregeln werden bearbeitet

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

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

   Sie können den Zielobjekttyp für eine Gruppenregel nicht ändern.

4. Klicken Sie Auf **Speichern**.

Gruppenregeln werden gelöscht

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

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

Gruppenaktionen werden hinzugefügt

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

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

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

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

Gruppenaktionen werden bearbeitet

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

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

Konfigurieren von Schwellenwerten für den Zustand von Volumes für Gruppen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

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

Gruppenaktionen werden gelöscht

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

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

Gruppenaktionen neu anordnen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können entweder eine einzelne Zeile oder mehrere Zeilen auswählen und dann mehrere Drag-and-Drop-

Vorgänge durchführen, um den Rang von Gruppenaktionen zu ändern. Sie müssen jedoch die Änderungen speichern, damit die Neupriorisierung im Raster Gruppenaktionen angezeigt wird.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenaktionen** auf **Neuordnung**.
3. Ziehen Sie im Dialogfeld **Gruppenaktionen neu anordnen** die Zeilen per Drag-and-Drop, um die Reihenfolge der Gruppenaktionen nach Bedarf neu anzuordnen.
4. Klicken Sie Auf **Speichern**.

Priorisieren von Storage-Objektereignissen mithilfe von Anmerkungen

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

Weitere Informationen zu Annotationen

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

Welche Anmerkungen sind

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

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

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

Funktionieren von Anmerkungsregeln in Unified Manager

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

- Sie müssen eine Anmerkungsregel einer Anmerkung zuordnen.
- Sie müssen einen Objekttyp für eine Anmerkungsregel zuordnen. Für eine Anmerkungsregel kann nur ein

Objekttyp zugeordnet werden.

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

Bestimmten Bedingungen

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

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

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

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

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

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

Beispiel einer Anmerkungsregel mit Bedingungen

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

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

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

Bedingungsgruppen

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

Beispiel einer Anmerkungsregel mit Bedingungsgruppen

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

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

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

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

Beschreibung der vordefinierten Anmerkungswerte

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

- **Datenpriorität:unternehmenskritisch**

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

- **Datenpriorität:hoch**

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

- **Datenpriorität:Niedrig**

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

Anmerkungen werden dynamisch hinzugefügt

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Klicken Sie auf der Seite **Anmerkungen** auf **Anmerkung hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkung hinzufügen** einen Namen und eine Beschreibung für die Anmerkung ein.

   Sie können beim Erstellen von Anmerkungen auch Werte zu Anmerkungen hinzufügen.

4. Optional: Klicken Sie im Abschnitt **Anmerkungswerte** auf **Hinzufügen**, um der Anmerkung Werte hinzuzufügen.
5. Klicken Sie auf **Speichern und Schließen**.

Hinzufügen von Werten zu Beschriftungen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können vordefinierten Anmerkungen keine Werte hinzufügen.

Schritte

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

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

4. Klicken Sie Auf **Hinzufügen**.

Anmerkungen werden gelöscht

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

Bevor Sie beginnen

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungen** die zu löschende Anmerkung aus.

   Die Details der ausgewählten Anmerkung werden angezeigt.

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

Ergebnisse

Die ausgewählte Beschriftung und ihr Wert werden gelöscht.

Anzeigen der Anmerkungsliste und der Details

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungen** auf den Anmerkungsnamen, um die zugehörigen Details anzuzeigen.

Löschen von Werten aus Anmerkungen

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

Bevor Sie beginnen

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

Über diese Aufgabe

Werte können nicht aus vordefinierten Anmerkungen gelöscht werden.

Schritte

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

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

Anmerkungsregeln werden erstellt

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungsregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkungsregel hinzufügen** einen Namen für die Anmerkungsregel an.
4. Wählen Sie im Feld **Zielobjekttyp** den Typ des Speicherobjekts aus, das Sie mit Anmerkungen versehen möchten.
5. Wählen Sie in den Feldern **Anmerkung anwenden** den Anmerkungs- und Anmerkungswert aus, den Sie

verwenden möchten.

6. Führen Sie im Abschnitt **Bedingungen** die entsprechende Aktion aus, um eine Bedingung, eine Bedingungsgruppe oder beide zu erstellen:

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

7. Klicken Sie Auf **Hinzufügen**.

Beispiel für das Erstellen einer Anmerkungsregel

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

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

in Schritt 9 und **unternehmenskritisch** als Wert in Schritt 10 auswählen.

13. Klicken Sie Auf **Hinzufügen**.

Anmerkungen manuell zu einzelnen Speicherobjekten hinzufügen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

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

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

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

Anmerkungsregeln werden bearbeitet

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

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

   Sie können den Zielobjekttyp für eine Anmerkungsregel nicht ändern.

4. Klicken Sie Auf **Speichern**.

Konfigurieren von Bedingungen für Anmerkungsregeln

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

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

Beispiel für die Konfiguration einer Bedingung für eine Anmerkungsregel

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

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

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

6. Geben Sie den Wert als ein `svm_data`.
7. Klicken Sie Auf **Hinzufügen**.

Anmerkungsregeln werden gelöscht

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungsregeln** die Anmerkungsregel aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie im Dialogfeld **Warnung** auf **Ja**, um den Löschvorgang zu bestätigen.

Anmerkungsregeln neu anordnen

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

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungsregeln** auf **Neuordnung**.
3. Ziehen Sie im Dialogfeld **Anmerkungsregel neu anordnen** einzelne oder mehrere Zeilen per Drag-and-Drop, um die Reihenfolge der Anmerkungsregeln neu anzuordnen.

4. Klicken Sie Auf **Speichern**.

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

Konfiguration von Backup- und Restore-Vorgängen

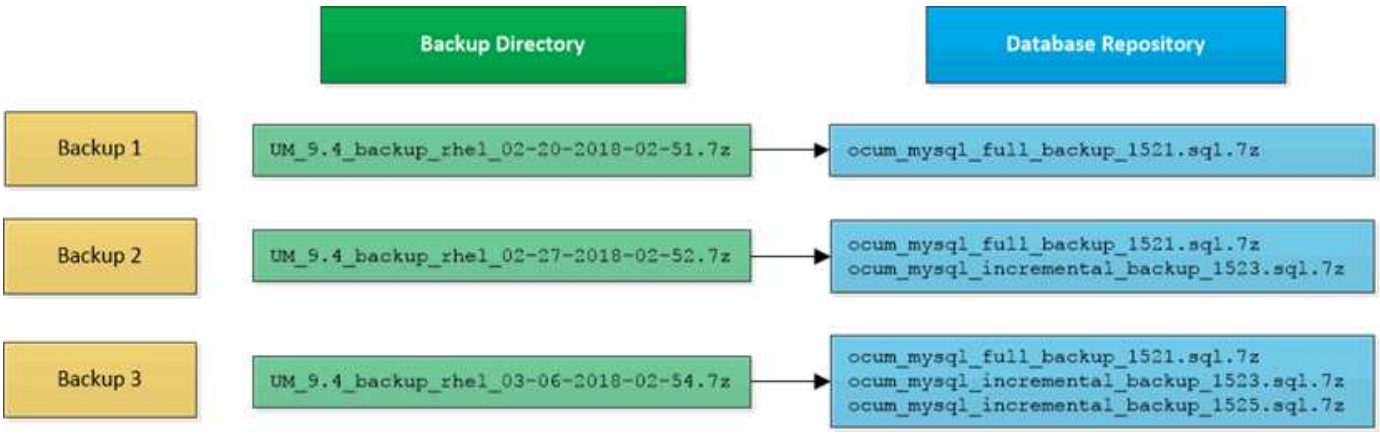
Sie können Backups von Unified Manager erstellen und die Wiederherstellungsfunktion verwenden, um das Backup im Falle eines Systemausfalls oder Datenverlust auf dasselbe (lokales) System oder ein neues (Remote-) System wiederherzustellen.

Was ist ein Datenbank-Backup

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

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

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



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

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

Vor Beginn eines Backup-Vorgangs führt Unified Manager eine Integritätsprüfung durch, um zu überprüfen, ob

alle erforderlichen Backup-Dateien und Backup-Verzeichnisse vorhanden sind und beschreibbar sind. Außerdem wird überprüft, ob genügend Speicherplatz auf dem System vorhanden ist, um die Backup-Datei zu erstellen.

Beachten Sie, dass Sie ein Backup nur auf derselben Version von Unified Manager wiederherstellen können. Wenn Sie beispielsweise ein Backup auf Unified Manager 9.4 erstellt haben, kann das Backup nur auf Unified Manager 9.4 Systemen wiederhergestellt werden.

Konfigurieren von Backup-Einstellungen für Datenbanken

Sie können die Backup-Einstellungen für die Unified Manager Datenbank so konfigurieren, dass der Datenbank-Backup-Pfad, die Aufbewahrungsanzahl und der Backup-Zeitplan festgelegt werden. Sie können tägliche oder wöchentliche geplante Backups aktivieren. Standardmäßig sind geplante Backups deaktiviert.

Bevor Sie beginnen

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

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

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

Über diese Aufgabe

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

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Datenbank-Backup**.
2. Klicken Sie auf der Seite **Management/Datenbank-Backup** auf **Aktionen** > **Einstellungen für die Datenbanksicherung**.
3. Konfigurieren Sie die entsprechenden Werte für einen Backup-Pfad und die Anzahl der Aufbewahrung.

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

4. Wählen Sie im Abschnitt **Terminhäufigkeit** das Kontrollkästchen **Aktivieren** aus, und geben Sie dann einen täglichen oder wöchentlichen Zeitplan an.
   - * Daily*

     Wenn Sie diese Option auswählen, müssen Sie eine Zeit im 24-Stunden-Format eingeben, um das Backup zu erstellen. Wenn Sie beispielsweise 18:30 angeben, wird täglich um 6:30 Uhr ein Backup

erstellt.

- **Wöchentlich**

  Wenn Sie diese Option auswählen, müssen Sie die Uhrzeit und den Tag für die Erstellung des Backups angeben. Wenn Sie beispielsweise den Tag als Montag und die Zeit als 16:30 angeben, wird jeden Montag um 4:30 Uhr ein wöchentliches Backup erstellt.

5. Klicken Sie auf **Speichern und Schließen**.

Was ist ein Datenbank-Restore

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

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

Während des Wiederherstellungsprozesses werden Sie von Unified Manager abgemeldet. Sie können sich nach Abschluss der Wiederherstellung beim System anmelden.

Die Wiederherstellungsfunktion ist versionsspezifisch und plattformspezifisch. Sie können ein Unified Manager-Backup nur auf derselben Version von Unified Manager wiederherstellen. Unified Manager unterstützt Backup und Restore in den folgenden Plattformszenarien:

- Virtuelle Appliance auf virtuelle Appliance
- Virtuelle Appliance für Red hat Enterprise Linux oder CentOS
- Red hat Enterprise Linux auf Red hat Enterprise Linux oder CentOS
- Windows zu Windows

Wenn Sie das Backup-Image auf einem neuen Server wiederherstellen, müssen Sie nach Abschluss des Wiederherstellungsvorgangs ein neues HTTPS-Sicherheitszertifikat generieren und den Unified Manager-Server neu starten. Wenn Sie das Backup-Image auf einem neuen Server wiederherstellen müssen, müssen Sie auch SAML-Authentifizierungseinstellungen neu konfigurieren.

Alte Sicherungsdateien können nicht verwendet werden, um ein Image wiederherzustellen, nachdem Unified Manager auf eine neuere Softwareversion aktualisiert wurde. Um Speicherplatz zu sparen, werden alle alten Backupdateien außer der neuesten Datei beim Upgrade von Unified Manager automatisch entfernt.

Backup- und Wiederherstellungsverfahren für virtuelle Appliances – Übersicht

Das Backup- und Restore-Modell für Unified Manager, wenn es auf einer virtuellen Appliance installiert ist, besteht darin, ein Image der gesamten virtuellen Applikation zu erfassen und wiederherzustellen.

Da der Backup-Vorgang von Unified Manager auf der virtuellen Appliance keine Möglichkeit bietet, die Backup-Datei aus der vApp zu verschieben, können Sie mit den folgenden Aufgaben ein Backup der virtuellen

Appliance durchführen:

1. Schalten Sie die VM aus und erstellen Sie einen VMware Snapshot der virtuellen Unified Manager Appliance.
2. Erstellen Sie eine NetApp Snapshot Kopie auf dem Datenspeicher, um den VMware Snapshot zu erfassen.

   Wenn der Datastore nicht auf einem System mit ONTAP-Software gehostet wird, befolgen Sie die Richtlinien des Storage-Anbieters, um ein Backup des VMware-Snapshots zu erstellen.

3. Replizierung der NetApp Snapshot Kopie (oder vergleichbarer Snapshot) in einem alternativen Storage
4. Löschen Sie den VMware Snapshot.

Sie sollten einen Backup-Zeitplan anhand dieser Aufgaben implementieren, um sicherzustellen, dass die virtuelle Unified Manager Appliance im Falle eines Problems geschützt ist.

Zum Wiederherstellen der VM können Sie den von Ihnen erstellten VMware Snapshot verwenden, um die VM auf den Point-in-Time-Zustand des Backups wiederherzustellen.

Wiederherstellen einer Datenbanksicherung auf einer virtuellen Maschine

Bei Datenverlust oder Datenbeschädigung kann Unified Manager mit der Wiederherstellungsfunktion in den vorherigen stabilen Zustand bei minimalem Verlust wiederhergestellt werden. Sie können die Unified Manager-Datenbank auf einer virtuellen Maschine über die Wartungskonsole von Unified Manager wiederherstellen.

Bevor Sie beginnen

- Sie müssen über die Anmeldeinformationen für den Wartungs-Benutzer verfügen.
- Die Backup-Dateien von Unified Manager müssen sich auf dem lokalen System befinden.
- Die Sicherungsdateien müssen aus sein `.7z` Typ.

Über diese Aufgabe

Die Backup-Kompatibilität ist Plattform- und versionsabhängig. Das Wiederherstellen eines Backups von einer virtuellen Appliance auf einer anderen virtuellen Appliance oder von einer virtuellen Appliance auf einem Red hat Enterprise Linux oder CentOS System ist möglich.

Wenn Sie einen Wiederherstellungsvorgang auf einer anderen virtuellen Appliance durchführen als auf dem System, von dem die ursprüngliche Sicherungsdatei erstellt wurde, müssen der Wartungsbenutzername und das Kennwort auf der neuen vApp identisch sein mit den Anmeldeinformationen der ursprünglichen vApp.

Schritte

1. Suchen Sie im vSphere-Client die virtuelle Unified Manager-Maschine und wählen Sie dann die Registerkarte **Konsole** aus.
2. Klicken Sie auf das Konsolenfenster, und melden Sie sich dann mit Ihrem Benutzernamen und Passwort an der Wartungskonsole an.
3. Geben Sie im **Hauptmenü** die Nummer für die Option **Systemkonfiguration** ein.
4. Geben Sie im Menü * Systemkonfiguration* die Nummer für die Option **aus einem OCUM-Backup**

wiederherstellen ein.

5. Geben Sie bei entsprechender Aufforderung den absoluten Pfad der Sicherungsdatei ein.

```
Bundle to restore from: opt/netapp/data/ocum-
backup/UM_9.4.N151112.0947_backup_unix_02-25-2018-11-41.7z
```

   Nach Abschluss der Wiederherstellung können Sie sich bei Unified Manager einloggen.

Nachdem Sie fertig sind

Wenn der OnCommand Workflow Automation-Server nach der Wiederherstellung des Backups nicht funktioniert, führen Sie die folgenden Schritte aus:

1. Ändern Sie auf dem Workflow Automation Server die IP-Adresse des Unified Manager-Servers, um auf die neueste Maschine zu verweisen.
2. Setzen Sie auf dem Unified Manager-Server das Datenbankkennwort zurück, wenn die Erfassung in Schritt 1 fehlschlägt.

Wiederherstellen einer Datenbanksicherung auf einem Linux-System

Im Falle eines Datenverlustes oder einer Beschädigung von Daten können Sie Unified Manager in den vorherigen stabilen Zustand bei minimalem Datenverlust wiederherstellen. Die Unified Manager Datenbank kann auf einem lokalen oder Remote Red hat Enterprise Linux oder CentOS System wiederhergestellt werden.

Bevor Sie beginnen

- Unified Manager muss auf einem Server installiert sein.
- Sie müssen über die Stammbenutzeranmeldeinformationen für den Linux-Host verfügen, auf dem Unified Manager installiert ist.
- Sie müssen die Backup-Datei von Unified Manager und den Inhalt des Datenbank-Repository-Verzeichnisses auf das System kopiert haben, auf dem Sie den Wiederherstellungsvorgang ausführen möchten.

  Es wird empfohlen, die Sicherungsdatei in das Standardverzeichnis zu kopieren `/data/ocum-backup`. Die Datenbank-Repository-Dateien müssen in die kopiert werden `/database-dumps-repo` Unterverzeichnis unter dem `/ocum-backup` Verzeichnis.

- Die Sicherungsdateien müssen aus sein `.7z` Typ.

Über diese Aufgabe

Die Wiederherstellungsfunktion ist plattformspezifisch und versionsspezifisch. Sie können ein Unified Manager-Backup nur auf derselben Version von Unified Manager wiederherstellen. Sie können eine Sicherungsdatei für Linux oder eine Sicherungsdatei einer virtuellen Appliance auf einem Red hat Enterprise Linux oder CentOS System wiederherstellen.

Wenn der Name des Sicherungsordners ein Leerzeichen enthält, müssen Sie den absoluten Pfad oder den relativen Pfad in doppelte Anführungszeichen einschließen.

Schritte

1. Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager die UI nicht oder konfigurieren Sie nach Abschluss der Installation keine Cluster, Benutzer oder Authentifizierungseinstellungen. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.
2. Melden Sie sich als Root-Benutzer an dem Host an, auf dem Unified Manager installiert ist.
3. Wenn Unified Manager in VCS Setup installiert ist, stoppen Sie die Unified Manager ocie und ocieau Services mit Veritas Operations Manager.
4. Stellen Sie an der Eingabeaufforderung das Backup wieder her: `um backup restore -f <backup_file_path>/<backup_file_name>`

   ```
   um backup restore -f /data/ocum-backup/UM_9.4.N151113.1348_backup_rhel_02-20-2018-04-45.7z
   ```

Nachdem Sie fertig sind

Nach Abschluss der Wiederherstellung können Sie sich bei Unified Manager einloggen.

Wiederherstellen einer Datenbanksicherung unter Windows

Bei Datenverlust oder Datenbeschädigung kann Unified Manager mit der Wiederherstellungsfunktion in den vorherigen stabilen Zustand bei minimalem Verlust wiederhergestellt werden. Sie können die Unified Manager-Datenbank auf einem lokalen Windows-System oder einem Remote-Windows-System mithilfe des Wiederherstellungsbefehls wiederherstellen.

Bevor Sie beginnen

- Unified Manager muss auf einem Server installiert sein.
- Sie müssen über Administratorrechte für Windows verfügen.
- Sie müssen die Backup-Datei von Unified Manager und den Inhalt des Datenbank-Repository-Verzeichnisses auf das System kopiert haben, auf dem Sie den Wiederherstellungsvorgang ausführen möchten.

  Es wird empfohlen, die Sicherungsdatei in das Standardverzeichnis zu kopieren `\ProgramData\NetApp\OnCommandAppData\ocum\backup`. Die Datenbank-Repository-Dateien müssen in die kopiert werden `\database_dumps_repo` Unterverzeichnis unter dem `\backup` Verzeichnis.

- Die Sicherungsdateien müssen aus sein `.7z` Typ.

Über diese Aufgabe

Die Wiederherstellungsfunktion ist plattformspezifisch und versionsspezifisch. Sie können ein Unified Manager Backup nur auf derselben Version von Unified Manager wiederherstellen. Ein Windows Backup kann nur auf einer Windows-Plattform wiederhergestellt werden.

Wenn die Ordnernamen ein Leerzeichen enthalten, müssen Sie den absoluten Pfad oder den relativen Pfad der Sicherungsdatei in doppelten Anführungszeichen einschließen.

Schritte

1. Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager die UI nicht oder konfigurieren Sie nach Abschluss der Installation keine Cluster, Benutzer oder Authentifizierungseinstellungen. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.
2. Melden Sie sich als Administrator bei der Unified Manager-Konsole an: `um cli login -u maint_username`
3. Stellen Sie an der Eingabeaufforderung das Backup wieder her: `um backup restore -f <backup_file_path>/<backup_file_name>`

   ```
   um backup restore -f
   \ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.4.N151118.2300_backup_windows_02-20-2018-02-51.7z
   ```

Nachdem Sie fertig sind

Nach Abschluss der Wiederherstellung können Sie sich bei Unified Manager einloggen.

Migration einer virtuellen Unified Manager Appliance zu einem Linux System

Sie können eine Datensicherung einer Unified Manager Datenbank von einer virtuellen Appliance auf einem Red hat Enterprise Linux oder CentOS Linux System wiederherstellen, wenn Sie das Host-Betriebssystem ändern möchten, auf dem Unified Manager läuft.

Bevor Sie beginnen

- Auf der virtuellen Appliance:
  - Sie müssen über die Rolle Operator, OnCommand Administrator oder Storage Administrator verfügen, um das Backup zu erstellen.
  - Sie müssen den Namen des Unified Manager-Wartungsbenutzers für den Wiederherstellungsvorgang kennen.
- Auf dem Linux-System:
  - Sie müssen Unified Manager auf einem RHEL- oder CentOS-Server gemäß den Anweisungen im Installationshandbuch installiert haben.
  - Die Version von Unified Manager auf diesem Server muss mit der Version auf der virtuellen Appliance identisch sein, von der aus Sie die Sicherungsdatei verwenden.
  - Starten Sie die UI nicht oder konfigurieren Sie nach der Installation keine Cluster-, Benutzer- oder Authentifizierungseinstellungen auf dem Linux-System. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.
  - Sie müssen über die Stammbenutzeranmeldeinformationen für den Linux-Host verfügen.

Über diese Aufgabe

In diesen Schritten wird beschrieben, wie eine Sicherungsdatei auf der virtuellen Appliance erstellt, die Sicherungsdateien auf das Red hat Enterprise Linux oder CentOS System kopiert und dann die Datenbanksicherung auf das neue System wiederhergestellt wird.

Schritte

1. Klicken Sie auf der virtuellen Appliance in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Datenbank-Backup**.
2. Klicken Sie auf der Seite **Management/Datenbank-Backup** auf **Aktionen** > **Einstellungen für die Datenbanksicherung**.
3. Ändern Sie den Backuppfad in `/jail/support`.
4. Wählen Sie im Abschnitt **Terminfrequenz** das Kontrollkästchen **Aktivieren** aus, wählen Sie **Täglich** aus, und geben Sie einige Minuten nach der aktuellen Zeit ein, damit das Backup in Kürze erstellt wird.
5. Klicken Sie auf **Speichern und Schließen**.
6. Warten Sie einige Stunden, bis das Backup erstellt wird.

   Ein vollständiges Backup kann über 1 GB betragen und kann drei bis vier Stunden in Anspruch nehmen.

7. Melden Sie sich als Root-Benutzer beim Linux-Host an, auf dem Unified Manager installiert ist, und kopieren Sie die Sicherungsdateien von `/support` Auf der virtuellen Appliance mit SCP.`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .`

   `root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .`

   Stellen Sie sicher, dass Sie den kopiert haben `.7z` Backup-Datei und alle `.7z` Repository-Dateien im `/database-dumps-repo` Unterverzeichnis.

8. Stellen Sie an der Eingabeaufforderung das Backup wieder her: `um backup restore -f /<backup_file_path>/<backup_file_name>`

   `um backup restore -f /UM_9.4.N151113.1348_backup_unix_02-12-2018-04-16.7z`

9. Melden Sie sich nach Abschluss der Wiederherstellung bei der Web-UI von Unified Manager an.

Nachdem Sie fertig sind

Sie sollten die folgenden Aufgaben durchführen:

- Generieren Sie ein neues HTTPS-Sicherheitszertifikat, und starten Sie den Unified Manager-Server neu.
- Ändern Sie den Backuppfad auf die Standardeinstellung für Ihr Linux-System (`/data/ocum-backup`), oder zu einem neuen Weg Ihrer Wahl, weil es keine `/jail/support` Pfad auf dem Linux-System.
- Konfigurieren Sie beide Seiten Ihrer Workflow Automation Verbindung neu, falls WFA verwendet wird.
- Konfigurieren Sie SAML-Authentifizierungseinstellungen neu, wenn Sie SAML verwenden.

Nachdem Sie überprüft haben, dass alles auf Ihrem Linux-System wie erwartet ausgeführt wird, können Sie die virtuelle Unified Manager-Appliance herunterfahren und entfernen.

Was für ein Unified Manager-Wartungsfenster ist

Sie definieren ein Unified Manager Wartungsfenster, um Ereignisse und Warnmeldungen für einen bestimmten Zeitraum zu unterdrücken, wenn Sie für eine Cluster-Wartung geplant haben und keine unerwünschte Benachrichtigungen erhalten möchten.

Wenn das Wartungsfenster beginnt, wird ein Ereignis „`Object Maintenance Window Started`“ auf der

Seite „Events Inventory“ veröffentlicht. Dieses Ereignis wird automatisch veraltet, wenn das Wartungsfenster endet.

Während eines Wartungsfensters werden die Ereignisse, die sich auf alle Objekte im Cluster beziehen, weiterhin generiert, jedoch nicht in einer UI-Seite angezeigt und für diese Ereignisse werden keine Meldungen oder andere Arten von Benachrichtigungen gesendet. Sie können jedoch die Ereignisse anzeigen, die während eines Wartungsfensters für alle Speicherobjekte generiert wurden, indem Sie auf der Seite „Ereignisinventar“ eine der Optionen „Ansicht“ auswählen.

Sie können ein Wartungsfenster für die Zukunft planen, die Start- und Endzeit für ein geplantes Wartungsfenster ändern und ein Wartungsfenster abbrechen.

Planen eines Wartungsfensters zum Deaktivieren der Cluster-Ereignisbenachrichtigungen

Wenn Sie z. B. vor einer geplanten Ausfallzeit für ein Cluster stehen, um ein Cluster zu aktualisieren oder einen der Nodes zu verschieben, können Sie die Ereignisse und Warnungen unterdrücken, die normalerweise während dieses Zeitfensters generiert werden würden, indem Sie ein Unified Manager Wartungsfenster planen.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Während eines Wartungsfensters werden die Ereignisse, die mit allen Objekten auf dem Cluster zusammenhängen, weiterhin generiert, jedoch nicht auf der Ereignisseite angezeigt und für diese Ereignisse werden keine Meldungen oder andere Arten von Benachrichtigungen gesendet.

Die Zeit, die Sie für das Wartungsfenster eingeben, basiert auf der Zeit im Unified Manager-Server.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Cluster-Datenquellen**.
2. Wählen Sie in der Spalte **Wartungsmodus** für den Cluster die Schieberegler-Schaltfläche aus, und verschieben Sie sie nach rechts.

   Das Kalenderfenster wird angezeigt.

3. Wählen Sie das Start- und Enddatum und die Uhrzeit für das Wartungsfenster aus und klicken Sie auf **Anwenden**.

   Neben dem Schieberegler wird die Meldung „`Scheduled`“ angezeigt.

Ergebnisse

Wenn die Startzeit erreicht ist, wechselt das Cluster in den Wartungsmodus und ein Ereignis „`Object Maintenance Window gestartet`“ wird generiert.

Ändern oder Abbrechen eines geplanten Wartungsfensters

Wenn Sie ein Wartungsfenster von Unified Manager für die Zukunft konfiguriert haben, können Sie die Start- und Endzeit ändern oder das Wartungsfenster nicht mehr

ausführen.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Das Abbrechen eines derzeit ausgeführten Wartungsfensters ist hilfreich, wenn Sie die Cluster-Wartung vor dem Ende des geplanten Wartungsfensters abgeschlossen haben und Sie möchten Ereignisse und Warnmeldungen vom Cluster erneut empfangen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Cluster-Datenquellen**.
2. In der Spalte **Wartungsmodus** für den Cluster:

Ihr Ziel ist	Führen Sie diesen Schritt aus…
Ändern Sie den Zeitrahmen für ein geplantes Wartungsfenster	a. Klicken Sie neben dem Schieberegler auf den Text „`Scheduled`“. b. Ändern Sie das Start- und/oder Enddatum und die Uhrzeit, und klicken Sie auf **Anwenden**.
Verlängern Sie die Länge eines aktiven Wartungsfensters	a. Klicken Sie auf den Text „`Active`“ neben der Schieberegler-Schaltfläche. b. Ändern Sie das Enddatum und die Endzeit, und klicken Sie auf **Anwenden**.
Abbrechen eines geplanten Wartungsfensters	Wählen Sie die Schieberegler-Taste, und verschieben Sie sie nach links.
Abbrechen eines aktiven Wartungsfensters	Wählen Sie die Schieberegler-Taste, und verschieben Sie sie nach links.

Anzeigen von Ereignissen, die während eines Wartungsfensters aufgetreten sind

Bei Bedarf können Sie die Ereignisse anzeigen, die während eines Unified Manager-Wartungsfensters für alle Storage-Objekte generiert wurden. Die meisten Ereignisse werden nach Abschluss des Wartungsfensters im Status „veraltet“ angezeigt und alle Systemressourcen werden gesichert und ausgeführt.

Bevor Sie beginnen

Mindestens ein Wartungsfenster muss abgeschlossen sein, bevor Ereignisse verfügbar sind.

Über diese Aufgabe

Ereignisse, die während eines Wartungsfensters aufgetreten sind, werden standardmäßig nicht auf der Seite „Ereignisinventar“ angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Events**.

   Standardmäßig werden alle aktiven (Neu- und bestätigten) Ereignisse auf der Seite Ereignisbestand angezeigt.

2. Wählen Sie im Fensterbereich **Ansicht** die Option **Alle Ereignisse, die während der Wartung generiert wurden**.

   Die Liste der Ereignisse, die in den letzten 7 Tagen aus allen Wartungsfenster und aus allen Clustern ausgelöst wurden, wird angezeigt.

3. Wenn mehrere Wartungsfenster für einen einzelnen Cluster vorhanden waren, können Sie auf das Kalendersymbol **ausgelöste Zeit** klicken und den Zeitraum für die Wartungsfenster-Ereignisse auswählen, die Sie interessieren.

Verwalten von SAML-Authentifizierungseinstellungen

Nachdem Sie die Remote-Authentifizierungseinstellungen konfiguriert haben, können Sie die SAML-Authentifizierung (Security Assertion Markup Language) aktivieren, sodass Remote-Benutzer von einem sicheren Identitäts-Provider (IdP) authentifiziert werden, bevor sie auf die Unified Manager Web-UI zugreifen können.

Beachten Sie, dass nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager haben, nachdem die SAML-Authentifizierung aktiviert wurde. Lokale Benutzer und Wartungbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Wartungskonsole zugreifen.

Anforderungen an Identitätsanbieter

Wenn Sie Unified Manager für die Verwendung eines Identitäts-Providers (IdP) konfigurieren, um die SAML-Authentifizierung für alle Remote-Benutzer durchzuführen, müssen Sie einige erforderliche Konfigurationseinstellungen beachten, damit die Verbindung zu Unified Manager erfolgreich hergestellt wird.

Sie müssen die Unified Manager-URI und die Metadaten im IdP-Server eingeben. Sie können diese Informationen von der Seite Unified ManagerSAML Authentication kopieren. Unified Manager gilt im SAML-Standard (Security Assertion Markup Language) als Service Provider (SP).

Unterstützte Verschlüsselungsstandards

- Advanced Encryption Standard (AES): AES-128 und AES-256
- Sicherer Hash-Algorithmus (SHA): SHA-1 und SHA-256

Validierte Identitätsanbieter

- Shibboleth
- Active Directory Federation Services (ADFS)

ADFS-Konfigurationsanforderungen

- Sie müssen drei Antragsregeln in der folgenden Reihenfolge definieren, die erforderlich sind, damit Unified Manager ADFS SAML-Antworten für diesen Vertrauenseintrag der Treuhandgesellschaft analysieren kann.

Forderungsregel	Wert
SAM-Account-Name	Name-ID
SAM-Account-Name	Urne:oid:0.9.2342.19200300.100.1.1
Token-Gruppen — Unqualifizierter Name	Urne:oid:1.3.6.1.4.1.5923.1.5.1.1

- Sie müssen die Authentifizierungsmethode auf „`Forms Authentication`“ festlegen, oder Benutzer erhalten möglicherweise einen Fehler beim Abmelden von Unified Manager, wenn Sie Internet Explorer verwenden. Führen Sie hierzu folgende Schritte aus:
  a. Öffnen Sie die ADFS-Verwaltungskonsole.
  b. Klicken Sie in der linken Strukturansicht auf den Ordner Authentication Policies.
  c. Klicken Sie unter Aktionen auf der rechten Seite auf Globale primäre Authentifizierungsrichtlinie bearbeiten.
  d. Setzen Sie die Intranet-Authentifizierungsmethode auf „`Forms Authentication`“ anstatt auf die Standardauthentifizierung „`Windows Authentication`“.
- In einigen Fällen wird die Anmeldung über das IdP abgelehnt, wenn das Unified Manager-Sicherheitszertifikat CA-signiert ist. Es gibt zwei Problemumgehungen zur Lösung dieses Problems:
  - Befolgen Sie die Anweisungen im Link, um die Widerrufs-Prüfung auf dem ADFS-Server für verkettete CA-Zertifikat zugeordnete abhängige Partei zu deaktivieren:

    http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

  - Der CA-Server befindet sich im ADFS-Server, um die Zertifiktanforderung des Unified Manager-Servers zu signieren.

Sonstige Konfigurationsanforderungen

- Die Unified Manager-Taktskew ist auf 5 Minuten eingestellt, sodass der Zeitunterschied zwischen dem IdP-Server und dem Unified Manager-Server nicht mehr als 5 Minuten betragen kann oder die Authentifizierung fehlschlägt.
- Wenn Benutzer versuchen, mit Internet Explorer auf Unified Manager zuzugreifen, wird möglicherweise die Meldung angezeigt **die Webseite kann die Seite nicht anzeigen**. Stellen Sie in diesem Fall sicher, dass diese Benutzer die Option „`Sso freundliche HTTP-Fehlermeldungen`“ in **Tools** > **Internetoptionen** > **Erweitert** deaktivieren.

Aktivieren der SAML-Authentifizierung

Sie können die SAML-Authentifizierung (Security Assertion Markup Language) aktivieren, sodass Remote-Benutzer von einem Secure Identity Provider (IdP) authentifiziert werden, bevor sie auf die Web-UI von Unified Manager zugreifen können.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung konfiguriert und bestätigt haben, dass sie erfolgreich ist.
- Sie müssen mindestens einen Remote-Benutzer oder eine Remote-Gruppe mit der Rolle „OnCommand-Administrator“ erstellt haben.
- Der Identitäts-Provider (IdP) muss von Unified Manager unterstützt und konfiguriert werden.
- Sie müssen über die IdP-URL und die Metadaten verfügen.
- Sie müssen Zugriff auf den IdP-Server haben.

Über diese Aufgabe

Nachdem Sie die SAML-Authentifizierung von Unified Manager aktiviert haben, können Benutzer erst dann auf die grafische Benutzeroberfläche zugreifen, wenn das IdP mit den Hostinformationen des Unified Manager-Servers konfiguriert wurde. Daher müssen Sie darauf vorbereitet sein, beide Teile der Verbindung abzuschließen, bevor Sie mit dem Konfigurationsprozess beginnen. Das IdP kann vor oder nach der Konfiguration von Unified Manager konfiguriert werden.

Nach Aktivierung der SAML-Authentifizierung haben nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager. Lokale Benutzer und Wartungbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Wartungskonsole, die Unified Manager-Befehle oder Zapis zugreifen.

Unified Manager wird automatisch neu gestartet, nachdem Sie die SAML-Konfiguration auf dieser Seite abgeschlossen haben.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML Authentication** aus.
3. Aktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.

   Die Felder, die zum Konfigurieren der IdP-Verbindung erforderlich sind, werden angezeigt.

4. Geben Sie die IdP-URI und die IdP-Metadaten ein, die erforderlich sind, um den Unified Manager-Server mit dem IdP-Server zu verbinden.

   Wenn der IdP-Server direkt über den Unified Manager-Server erreichbar ist, können Sie nach Eingabe der IdP-URI auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um das Feld IdP-Metadaten automatisch zu füllen.

5. Kopieren Sie den Unified Manager-Host-Metadaten-URI, oder speichern Sie die Host-Metadaten in eine XML-Textdatei.

   Sie können den IdP-Server derzeit mit diesen Informationen konfigurieren.

6. Klicken Sie Auf **Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

7. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.

Ergebnisse

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldedaten auf der Anmeldeseite IdP statt auf der Anmeldeseite von Unified Manager ein.

Nachdem Sie fertig sind

Wenn noch nicht abgeschlossen ist, greifen Sie auf Ihr IdP zu, und geben Sie den URI und die Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

Wenn Sie ADFS als Identitäts-Provider verwenden, wird die Unified Manager-GUI nicht das ADFS-Timeout-Timeout erfüllt und funktioniert weiter, bis das Timeout der Unified Manager-Sitzung erreicht ist. Wenn Unified Manager auf Windows, Red hat oder CentOS bereitgestellt wird, kann das Timeout der GUI-Sitzung mit dem folgenden Unified Manager CLI-Befehl geändert werden: `um option set absolute.session.timeout=00:15:00`Mit diesem Befehl wird das Zeitlimit für die Unified Manager GUI-Sitzung auf 15 Minuten festgelegt.

Ändern des Identitäts-Providers, der für die SAML-Authentifizierung verwendet wird

Sie können den Identitäts-Provider (IdP), den Unified Manager zur Authentifizierung von Remote-Benutzern verwendet, ändern.

Bevor Sie beginnen

- Sie müssen über die IdP-URL und die Metadaten verfügen.
- Sie müssen Zugriff auf die IdP haben.

Über diese Aufgabe

Der neue IdP kann vor oder nach der Konfiguration von Unified Manager konfiguriert werden.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML Authentication** aus.
3. Geben Sie die neue IdP-URI und die IdP-Metadaten ein, die erforderlich sind, um den Unified Manager-Server mit dem IdP zu verbinden.

   Wenn der IdP direkt über den Unified Manager-Server aufgerufen werden kann, können Sie nach Eingabe der IdP-URL auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um das Feld IdP-Metadaten automatisch auszufüllen.

4. Kopieren Sie den Unified Manager-Metadaten-URI oder speichern Sie die Metadaten in eine XML-Textdatei.
5. Klicken Sie Auf **Konfiguration Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration ändern möchten.

6. Klicken Sie auf **OK**.

Nachdem Sie fertig sind

Greifen Sie auf den neuen IdP zu, und geben Sie die URI und die Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

Wenn die autorisierten Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldeinformationen auf der neuen Anmeldeseite für IdP anstelle der alten Anmeldeseite ein.

SAML-Authentifizierungseinstellungen werden nach Änderung des Unified Manager-Sicherheitszertifikats aktualisiert

Jede Änderung am HTTPS-Sicherheitszertifikat, das auf dem Unified Manager-Server installiert ist, erfordert, dass Sie die Einstellungen für die SAML-Authentifizierung aktualisieren. Das Zertifikat wird aktualisiert, wenn Sie das Hostsystem umbenennen, eine neue IP-Adresse für das Hostsystem zuweisen oder das Sicherheitszertifikat für das System manuell ändern.

Über diese Aufgabe

Nach der Änderung des Sicherheitszertifikats und dem Neustart des Unified Manager-Servers funktioniert die SAML-Authentifizierung nicht, und Benutzer können nicht auf die grafische Benutzeroberfläche von Unified Manager zugreifen. Sie müssen die SAML-Authentifizierungseinstellungen sowohl auf dem IdP-Server als auch auf dem Unified Manager-Server aktualisieren, um den Zugriff auf die Benutzeroberfläche wieder zu aktivieren.

Schritte

1. Melden Sie sich bei der Wartungskonsole an.
2. Geben Sie im **Hauptmenü** die Nummer für die Option **SAML-Authentifizierung deaktivieren** ein.

   Es wird eine Meldung angezeigt, die bestätigt, dass die SAML-Authentifizierung deaktiviert und Unified Manager neu gestartet werden soll.

3. Starten Sie die Unified Manager-Benutzeroberfläche mit der aktualisierten FQDN- oder IP-Adresse, akzeptieren Sie das aktualisierte Serverzertifikat in Ihrem Browser und melden Sie sich mit den Anmeldeinformationen für den Wartungsbenutzer an.
4. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML Authentication** aus und konfigurieren Sie die IdP-Verbindung.
5. Kopieren Sie den Unified Manager-Host-Metadaten-URI, oder speichern Sie die Host-Metadaten in eine XML-Textdatei.
6. Klicken Sie Auf **Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

7. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.
8. Greifen Sie auf Ihren IdP-Server zu, und geben Sie die URI und die Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

Identitäts-Provider	Konfigurationsschritte
ADFS	a. Löschen Sie den vorhandenen Vertrauenseintrag der Vertrauensantragenden Partei in der ADFS-Management-GUI. b. Fügen Sie mit dem einen neuen Vertrauenseintrag einer Vertrauensbasis hinzu `saml_sp_metadata.xml` Über den aktualisierten Unified Manager-Server aus. c. Definieren Sie die drei Forderungsregeln, die für Unified Manager erforderlich sind, um ADFS SAML-Antworten für diesen Vertrauenseintrag der Vertrauensbasis zu analysieren. d. Starten Sie den ADFS Windows-Dienst neu.
Shibboleth	a. Aktualisieren Sie den neuen FQDN des Unified Manager-Servers in das `attribute-filter.xml` Und `relying-party.xml` Dateien: b. Starten Sie den Apache Tomcat Webserver neu und warten Sie, bis Port 8005 online ist.

9. Melden Sie sich bei Unified Manager an und stellen Sie sicher, dass die SAML-Authentifizierung über Ihr IdP wie erwartet funktioniert.

Deaktivieren der SAML-Authentifizierung

Sie können die SAML-Authentifizierung deaktivieren, wenn Sie die Authentifizierung von Remote-Benutzern über einen sicheren Identitäts-Provider (IdP) beenden möchten, bevor sie sich in der Web-UI von Unified Manager anmelden können. Wenn die SAML-Authentifizierung deaktiviert ist, führen die konfigurierten Verzeichnisdienstanbieter wie Active Directory oder LDAP eine Anmeldeauthentifizierung durch.

Über diese Aufgabe

Nachdem Sie die SAML-Authentifizierung deaktiviert haben, können lokale Benutzer und Wartungbenutzer zusätzlich zu konfigurierten Remote-Benutzern auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML-Authentifizierung auch über die Unified Manager-Wartungskonsole deaktivieren, wenn Sie keinen Zugriff auf die grafische Benutzeroberfläche haben.

Unified Manager wird automatisch neu gestartet, nachdem die SAML-Authentifizierung deaktiviert ist.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML Authentication** aus.

3. Deaktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.
4. Klicken Sie Auf **Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

5. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.

Ergebnisse

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldedaten auf der Anmeldeseite von Unified Manager anstelle der IdP-Anmeldeseite ein.

Nachdem Sie fertig sind

Greifen Sie auf Ihren IdP zu und löschen Sie die URI und die Metadaten des Unified Manager-Servers.

Deaktivieren der SAML-Authentifizierung über die Wartungskonsole

Wenn kein Zugriff auf die Unified Manager GUI besteht, müssen Sie möglicherweise die SAML-Authentifizierung von der Wartungskonsole aus deaktivieren. Dies kann in Fällen einer Fehlkonfiguration auftreten oder wenn der IdP nicht zugänglich ist.

Bevor Sie beginnen

Sie müssen als Wartungbenutzer Zugriff auf die Wartungskonsole haben.

Über diese Aufgabe

Wenn die SAML-Authentifizierung deaktiviert ist, führen die konfigurierten Verzeichnisdienstanbieter wie Active Directory oder LDAP eine Anmeldeauthentifizierung durch. Lokale Benutzer und Wartungbenutzer können zusätzlich zu konfigurierten Remote-Benutzern auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML-Authentifizierung auch über die Seite Setup/Authentifizierung in der UI deaktivieren.

> Unified Manager wird automatisch neu gestartet, nachdem die SAML-Authentifizierung deaktiviert ist.

Schritte

1. Melden Sie sich bei der Wartungskonsole an.
2. Geben Sie im **Hauptmenü** die Nummer für die Option **SAML-Authentifizierung deaktivieren** ein.

   Es wird eine Meldung angezeigt, die bestätigt, dass die SAML-Authentifizierung deaktiviert und Unified Manager neu gestartet werden soll.

3. Geben Sie **y** ein, und drücken Sie dann die Eingabetaste, und Unified Manager wird neu gestartet.

Ergebnisse

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldedaten auf der Anmeldeseite von Unified Manager anstelle der

IdP-Anmeldeseite ein.

Nachdem Sie fertig sind

Greifen Sie bei Bedarf auf Ihr IdP zu, und löschen Sie die URL und Metadaten des Unified Manager-Servers.

Verwalten von Speicherobjekten mit der Option Favoriten

Über die Option Favoriten können Sie ausgewählte Speicherobjekte in Unified Manager anzeigen und verwalten, indem Sie sie als Favoriten markieren. So können Sie den Status Ihrer bevorzugten Storage-Objekte schnell einsehen und Probleme beheben, bevor sie kritisch werden.

Aufgaben, die Sie im Dashboard „Favoriten“ ausführen können

- Zeigen Sie die Liste der als Favorit markierten Speicherobjekte an.
- Fügen Sie der Favoritenliste Speicherobjekte hinzu.
- Entfernen Sie Speicherobjekte aus der Favoritenliste.

Anzeigen der Favoritenliste

Sie können die Kapazitäts-, Performance- und Sicherungsdetails ausgewählter Speicherobjekte in der Liste Favoriten anzeigen. Die Details von maximal 20 Speicherobjekten werden in der Favoritenliste angezeigt.

Hinzufügen von Speicherobjekten zur Favoritenliste

Sie können der Liste „Favoriten“ Storage-Objekte hinzufügen und diese Objekte dann für Zustand, Kapazität und Performance überwachen. Sie können Cluster, Volumes und Aggregate nur als Favorit markieren.

Entfernen von Speicherobjekten aus der Favoritenliste

Sie können Speicherobjekte aus der Favoritenliste entfernen, wenn sie nicht mehr als Favorit markiert werden müssen.

Hinzufügen zu und Entfernen von Speicherobjekten aus der Liste Favoriten

Sie können einer Favoritenliste Storage-Objekte hinzufügen, damit Sie diese Objekte im Hinblick auf Zustand, Kapazität und Performance überwachen können. Sie können den Objektstatus in der Favoritenliste verwenden, um Probleme zu ermitteln und zu beheben, bevor sie kritisch werden. Die Favoritenliste enthält außerdem den aktuellsten Überwachungsstatus eines Speicherobjekts. Sie können Speicherobjekte aus der Favoritenliste entfernen, wenn sie nicht mehr als Favorit markiert werden müssen.

Über diese Aufgabe

In der Favoritenliste können bis zu 20 Cluster, Nodes, Aggregate oder Volumes hinzugefügt werden. Wenn Sie der Liste „Favoriten“ einen Node hinzufügen, wird dieser als Cluster angezeigt.

Schritte

1. Rufen Sie die Seite **Details** des Speicherobjekts auf, das Sie als Favorit markieren möchten.

2. Klicken Sie auf das Sternsymbol ( ) Zum Hinzufügen des Speicherobjekts zur Favoritenliste.

Hinzufügen eines Aggregats zur Favoritenliste

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **Aggregate**.
2. Klicken Sie auf der Seite „Inventar/Aggregate“ auf das Aggregat, das Sie der Liste „Favoriten“ hinzufügen möchten.
3. Klicken Sie auf der Seite „Systemzustand/Aggregat-Details“ auf das STAR-Symbol ( ).

Nachdem Sie fertig sind

Um ein Speicherobjekt aus der Liste Favoriten zu entfernen, wechseln Sie zur Listenseite Favoriten, klicken Sie auf das Sternsymbol ( ) Auf der Objektkarte, die Sie entfernen möchten, und wählen Sie dann die Option **aus Favoriten entfernen**.

Cluster-Favorite-Karte

Mit der Cluster Favorite Card können Sie die Kapazitäts-, Konfigurations- und Performance-Details der einzelnen Cluster anzeigen, die Sie als Favoriten markiert haben.

Cluster-Attribute

Auf der Cluster Favorite Card werden die folgenden Attribute der einzelnen Cluster angezeigt:

- **Cluster-Integritätsstatus**

  Ein Symbol, das den Systemzustand des Clusters angibt. Mögliche Werte sind Normal, Warnung, Fehler und kritisch.

- **Clustername**

  Der Name des Clusters.

- * Kapazität*

  Freier Speicherplatz im Cluster.

- **Konfiguration**

  Konfigurationsdetails des Clusters.

  - **IP-Adresse**

    IP-Adresse oder Host-Name der logischen Cluster-Management-Schnittstelle (LIF), die zum Hinzufügen des Clusters verwendet wurde.

  - **Anzahl der Knoten**

    Anzahl Nodes im Cluster.

- **Leistung**

Performance-Details des Clusters.

- **IOPS**

  Durchschnittliche Anzahl von I/O-Vorgängen pro Sekunde in den letzten 72 Stunden.

- **Durchsatz**

  Durchschnittsdurchsatz der letzten 72 Stunden, in Mbps .

Aggregieren der Lieblingskarte

Die bevorzugte Karte für Aggregate ermöglicht Ihnen, die Kapazitäts- und Performance-Details der Aggregate anzuzeigen, die Sie als Favoriten markiert haben.

Aggregatattribute

Auf der Favoriten-Karte für das Aggregat werden die folgenden Aggregatattribute angezeigt:

- * Integritätsstatus aggregieren*

  Ein Symbol, das den Zustand des Aggregats angibt. Mögliche Werte sind Normal, Warnung, Fehler und kritisch.

- **Aggregatname**

  Der Name des Aggregats.

  Positionieren Sie den Cursor über den Aggregatnamen, um den Namen des Clusters anzuzeigen, zu dem das Aggregat gehört.

- * Kapazität*

  Prozentsatz des verfügbaren freien Speicherplatzes im Aggregat und die geschätzte Anzahl an Tagen, bis das Aggregat voll ist.

  Zu beachten ist, dass FabricPool diese Informationen nur die Kapazität auf der lokalen Performance-Tier widerspiegeln. Klicken Sie auf die Kachel „Kapazität“, um detaillierte Informationen auf der Detailseite „Systemzustand/Aggregat“ anzuzeigen.

- **Leistung**

  Performance-Details des Aggregats.

  - **IOPS**

    Durchschnittliche Anzahl von I/O-Vorgängen pro Sekunde in den letzten 72 Stunden.

  - **Durchsatz**

    Durchschnittsdurchsatz der letzten 72 Stunden, in Mbps .

  - **Latenz**

    Die durchschnittliche Reaktionszeit eines Vorgangs wurde in Millisekunden benötigt.

Bevorzugte Karte für Volume

Mit der Favoritkarte Volume können Sie die Kapazitäts-, Sicherungs- und Performancedetails der Volumes anzeigen, die Sie als Favoriten markiert haben.

Volume-Attribute

Die Lieblingskarte für das Volume zeigt die folgenden Volume-Attribute an:

- **Volume-Integritätsstatus**

  Ein Symbol, das den Integritätsstatus des Volumes anzeigt. Mögliche Werte sind Normal, Warnung, Fehler und kritisch.

- **Volumenname**

  Name des Volumes.

- * Kapazität*

  Prozentsatz des verfügbaren freien Speicherplatzes auf dem Volume und die geschätzte Anzahl von Tagen bis zum Abschluss des Volume.

- **Schutz**

  Schutzrolle, die für das Volume festgelegt ist. Die möglichen Werte sind ungeschützt, nicht zutreffend, geschützt und Ziel.

- **Leistung**

  Performance-Statistiken für das Volume.

  - **IOPS**

    Durchschnittliche Anzahl von I/O-Vorgängen pro Sekunde in den letzten 72 Stunden.

  - **Durchsatz**

    Durchschnittlicher Durchsatz der letzten 72 Stunden, in MB/s.

  - **Latenz**

    Die durchschnittliche Reaktionszeit eines Vorgangs wurde in Millisekunden benötigt.

Erstellen und Importieren von Berichten in Unified Manager

Während Unified Manager Berichtsfunktionen bietet, müssen Sie möglicherweise neue Berichte erstellen, die speziell auf Ihre Umgebung zugeschnitten sind. Sie können mit den Eclipse Business Intelligence and Reporting Tools (BIRT) neue Berichte erstellen und diese dann in Unified Manager importieren, um sie anzuzeigen und zu verwalten.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Sie müssen MySQL Connector/J. heruntergeladen und installiert haben Sie müssen über den Speicherort der Datei mysql-connector-java-5.1.32-bin.jar verfügen, um die JBDC-Datenquelle zu erstellen, die den Bericht mit Unified Manager verbindet.

Über diese Aufgabe

Weitere Informationen zum Erstellen von Berichten finden Sie auf der Eclipse BIRT-Website.

Herunterladen und Installieren von MySQL Connector/J

Sie müssen die MySQL Connector/J-Treiber an einem bestimmten Ort herunterladen und installieren. Sie können diese Treiber verwenden, um eine Datenquelle zu erstellen, die den Bericht mit Unified Manager verbindet.

Über diese Aufgabe

Sie müssen MySQL Connector/J Version 5.1 oder höher verwenden.

Schritte

1. Laden Sie die MySQL Connector/J Treiber unter herunter `dev.mysql.com`.
2. Installieren Sie den `.jar` Notieren Sie sich den Speicherort für eine spätere Referenz.

   Installieren Sie z. B. die `.jar` Datei unter `C:\Program Files\MySQL\MySQL Connector J\mysql-connector-java-5.1.32-bin.jar`.

Erstellen eines Datenbankbenutzers

Um eine Verbindung zwischen Workflow Automation und Unified Manager zu unterstützen oder auf Datenbankansichten zuzugreifen, müssen Sie in der Weboberfläche von Unified Manager zunächst einen Datenbankbenutzer mit dem Integrations-Schema oder dem Berichtschema erstellen.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Datenbankbenutzer ermöglichen die Integration in Workflow Automation und den Zugriff auf Berichtsspezifische Datenbankansichten. Datenbankbenutzer haben keinen Zugriff auf die Unified Manager Web-UI oder die Wartungskonsole und können keine API-Aufrufe ausführen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Benutzer**.
2. Klicken Sie auf der Seite **Verwaltung/Benutzer** auf **Hinzufügen**.

3. Wählen Sie im Dialogfeld **Benutzer hinzufügen** in der Dropdown-Liste **Typ** die Option **Datenbankbenutzer** aus.
4. Geben Sie einen Namen und ein Kennwort für den Datenbankbenutzer ein.
5. Wählen Sie in der Dropdown-Liste **Rolle** die entsprechende Rolle aus.

Ihr Unternehmen	Wählen Sie diese Rolle aus
Verbindung von Unified Manager mit Workflow Automation	Integrationsschema
Zugriff auf Berichtsdaten und andere Datenbankansichten	Berichtschema

6. Klicken Sie Auf **Hinzufügen**.

Herunterladen der Eclipse Business Intelligence and Reporting Tools (BIRT)

Zum Erstellen und Importieren von Berichten in Unified Manager müssen Sie zunächst die Eclipse Business Intelligence and Reporting Tools (BIRT) herunterladen.

Schritte

1. Laden Sie die BIRT-Software unter herunter `http://download.eclipse.org/birt/downloads/`.

Nachdem Sie fertig sind

Nach dem Herunterladen der BIRT-Software müssen Sie die resultierende .zip-Datei extrahieren.

Erstellen eines Projekts mit BIRT

Bevor Sie einen Bericht für den Import in Unified Manager erstellen, müssen Sie zunächst ein Projekt mit BIRT erstellen.

Bevor Sie beginnen

Sie müssen die BIRT .zip-Datei heruntergeladen und extrahiert haben.

Schritte

1. Wählen Sie in der Eclipse-Benutzeroberfläche **Datei** > **Neu** > **Projekt** aus.
2. Erweitern Sie den Ordner **Business Intelligence and Reporting Tools**, wählen Sie **Projekt melden** und klicken Sie auf **Weiter**.
3. Geben Sie den Projektnamen ein und klicken Sie auf **Fertig stellen**.

Erstellen eines neuen Berichts mit BIRT

Sie können mit dem Eclipse Plug-in für Business Intelligence and Reporting Tools (BIRT) einen neuen Bericht erstellen. Möglicherweise möchten Sie neue Berichte erstellen, wenn die vorhandenen Berichte in Unified Manager den Anforderungen Ihrer Umgebung nicht entsprechen.

Bevor Sie beginnen

Sie müssen BIRT heruntergeladen und extrahiert haben.

Sie müssen ein Projekt mit BIRT erstellt haben.

Schritte

1. Wählen Sie in der BIRT-Schnittstelle **Datei** > **Neu** > **Bericht** aus.
2. Wählen Sie im Dialogfeld **Neuer Bericht** den Projektordner aus, der mit dem zuvor erstellten Projektordner identisch sein sollte.

   Wenn Sie einen anderen Projektordner auswählen, können Sie die Berichtsvorgänge in Unified Manager nicht verwenden.

3. Geben Sie den Namen der Berichtsdatei ein, und klicken Sie auf **Weiter**.
4. Wählen Sie den Berichtstyp aus und klicken Sie auf **Fertig stellen**.

Erstellen einer JDBC-Datenquelle mit BIRT

Nachdem Sie den neuen Bericht mithilfe von BIRT erstellt haben, müssen Sie eine Datenquelle erstellen, um den Bericht mit Unified Manager zu verbinden.

Bevor Sie beginnen

Sie müssen einen Bericht mit BIRT erstellt haben.

Sie müssen MySQL Connector/J. heruntergeladen und installiert haben

Sie müssen einen Datenbankbenutzer mit der Rolle „Berichtschema“ erstellt haben.

Schritte

1. Wählen Sie in Eclipse **Data Explorer** > **Datenquellen** > **Neue Datenquelle** aus.
2. Wählen Sie in der folgenden Liste * aus einem Datenquellentyp erzeugen aus.
3. Wählen Sie **JDBC Datenquelle** und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Dialogfeld **New JDBC Data Source Profile** die Option **com.mysql.jdbc.Driver(v5.1)** aus.
   a. Wenn der MySQL-Treiber nicht angezeigt wird, klicken Sie auf **Treiber verwalten**.
   b. Klicken Sie im Dialogfeld * JDBC-Treiber verwalten* auf **Hinzufügen**.
   c. Navigieren Sie zu dem Speicherort, an dem sich der MySQL Connector/J befindet `.jar` Die Datei wurde installiert, und wählen Sie dann die Datei aus.
   d. Klicken Sie auf **OK**.

      Sie sollten den MySQL-Treiber anzeigen und auswählen können.

5. Geben Sie den vollständig qualifizierten Host-Namen oder die IP-Adresse der Unified Manager Instanz im entsprechenden Format ein:

Adresstyp	Formatieren
IPv4	`jdbc:mysql://xx.xx.xx.xx:3306/ocum_report`
IPv6	`jdbc:mysql://address=(protocol=tcp)(host=xx:xx:xx:xx:xx:xx:xx:xx)(port=3306)/ocum_report`

6. Geben Sie den Benutzernamen für den Datenbankbenutzer ein, geben Sie das Passwort ein und klicken Sie dann auf **Fertig stellen**.

Erstellen eines neuen MySQL-Datensatzes mit BIRT

Nach dem Erstellen der Datenquelle müssen Sie einen MySQL-Datensatz erstellen, um die Ausgabeergebnisse für Ihren Bericht zu erstellen. Sie können die Ausgabetypen auch bearbeiten, nachdem Sie den Datensatz erstellt haben.

Bevor Sie beginnen

Sie müssen eine JDBC-Datenquelle mit BIRT erstellt haben.

Sie müssen MySQL Connector/J. heruntergeladen und installiert haben

Sie müssen einen Datenbankbenutzer mit der Rolle „Berichtschema“ in Unified Manager erstellt haben.

Schritte

1. Wählen Sie in **Eclipse** einen Arbeitsbereich aus.
2. Wählen Sie **Data Explorer** > **Datensätze** > **Neuer Datensatz**.
3. Wählen Sie im Dialogfeld **Neuer Datensatz** die zuvor erstellte Datenquelle, den Datentyp und den Namen des Datensatzes aus, und klicken Sie auf **Weiter**.
4. Definieren Sie einen SQL-Abfragetext mit den verfügbaren Elementen, oder geben Sie die Abfrage manuell ein und klicken Sie auf **Fertig stellen**.
5. Klicken Sie auf **Vorschauergebnisse**, um die SQL-Abfrage zu bestätigen, und klicken Sie dann auf **OK**.
6. Definieren Sie im Dialogfeld **Datensatz bearbeiten** die Ausgabespalten nach Bedarf und klicken Sie auf **OK**.
7. Ziehen Sie Elemente in den neu erstellten Bericht.

Nachdem Sie fertig sind

Sie sollten den neu erstellten Bericht nun in Unified Manager importieren.

Berichte werden importiert

Wenn Sie einen Bericht außerhalb von Unified Manager erstellt haben, können Sie die Berichtsdatei importieren und speichern, die mit Unified Manager verwendet werden soll.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Sie müssen sicherstellen, dass der zu importierende Bericht von Unified Manager unterstützt wird.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte** und dann auf **Bericht importieren**.
2. Klicken Sie im Dialogfeld **Bericht importieren** auf **Durchsuchen** und wählen Sie die Datei aus, die Sie importieren möchten, und geben Sie dann einen Namen und eine kurze Beschreibung des Berichts ein.
3. Klicken Sie Auf **Import**.

   Wenn Sie den Bericht nicht importieren können, können Sie die Protokolldatei überprüfen, um den Fehler zu finden, der das Problem verursacht.

Verwendung von Unified Manager REST-APIs

Über REST-APIs lassen sich die von Unified Manager erfassten Daten zu Zustand, Kapazität und Performance anzeigen, um die Cluster zu managen.

Zugriff auf REST-APIs über die Swagger API-Webseite

REST-APIs sind über die Swagger Webseite zugänglich. Sie können auf die Swagger-Webseite zugreifen, um die Rest-API-Dokumentation von Unified Manager anzuzeigen und einen API-Aufruf manuell zu tätigen.

Bevor Sie beginnen

- Sie müssen über eine der folgenden Rollen verfügen: Operator, Storage Administrator oder OnCommand Administrator.
- Sie müssen die IP-Adresse oder den vollqualifizierten Domänennamen des Unified Manager Servers kennen, auf dem Sie die REST APIs ausführen möchten.

Über diese Aufgabe

Für jede REST-API auf der Swagger-Webseite wird ein Beispiel zur Erläuterung der Objekte und Attribute bereitgestellt, mit denen Sie die Informationen zurückgeben können, die Sie für die Überprüfung interessieren.

Schritte

1. Zugriff auf die Unified Manager REST-APIs

Option	Beschreibung
Über die Web-UI von Unified Manager:	Klicken Sie in der Menüleiste auf die Schaltfläche **Hilfe** und wählen Sie dann **API-Dokumentation** aus.

Option	Beschreibung
Im Browser-Fenster:	Geben Sie unter Verwendung der IP-Adresse oder des FQDN des Unified Manager-Servers die URL ein, um auf die REST-API-Seite im Format zuzugreifen `https://<Unified_Manager_IP_address_or_name>/apidocs/`. Beispiel: `https://10.10.10.10/apidocs/`

Eine Liste der API-Ressourcentypen oder -Kategorien wird angezeigt.

2. Klicken Sie auf einen API-Ressourcentyp, um die APIs in diesem Ressourcentyp anzuzeigen.

Liste der verfügbaren REST-APIs

Sie sollten über die verfügbaren REST-APIs in Unified Manager informiert sein, damit Sie planen können, wie Sie die APIs verwenden können. Die API-Aufrufe sind unter den verschiedenen Ressourcentypen oder -Kategorien organisiert.

Auf der Swagger-Webseite finden Sie eine vollständige Liste der verfügbaren API-Aufrufe sowie die Details jedes Anrufs.

Die Management-API-Aufrufe sind nach den folgenden Kategorien organisiert:

- Aggregate
- Cluster
- Veranstaltungen
- LIFs
- LUNs
- Namespaces
- Knoten
- Ports
- SVMs
- Volumes

Wenn Sie eine der Kategorien auswählen, wird eine Liste angezeigt, die die Unterkategorie API zusammen mit einer versionierten Unterkategorie anzeigt, z. B.:

- /Aggregate
- /V1/Aggregate

Die neueste Version der REST-APIs wird ohne Versionsnummer in der URL aufgeführt. Zur Integration mit Unified Manager sollten Sie immer die neueste Version der API verwenden.

Einrichtung und Monitoring einer SVM mit Infinite Volume ohne Storage-Klassen

Sie sollten OnCommand Workflow Automation (WFA) und Unified Manager verwenden,

um Storage Virtual Machines (SVMs) mit Infinite Volume einzurichten und zu überwachen. Sie sollten die SVM mit Infinite Volume mithilfe von WFA erstellen und dann mithilfe von Unified Manager das Infinite Volume überwachen. Optional können Sie die Datensicherung für das Infinite Volume konfigurieren.

Bevor Sie beginnen

Folgende Anforderungen müssen erfüllt werden:

- WFA muss installiert und die Datenquellen konfiguriert sein.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die erforderliche Anzahl an Aggregaten erstellt haben, indem Sie den entsprechenden vordefinierten Workflow in WFA anpassen.
- Sie müssen den Unified Manager-Server als Datenquelle in WFA konfiguriert haben, und Sie müssen überprüfen, ob die Daten erfolgreich im Cache gespeichert sind.

Über diese Aufgabe

- Mit Unified Manager können nur Data SVMs überwacht werden.
- Bei dieser Aufgabe müssen Sie zwischen zwei Applikationen wechseln: OnCommand Workflow Automation (WFA) und OnCommand Unified Manager.
- Die Aufgabe bietet Schritte auf hoher Ebene.

  Informationen zur Durchführung der WFA Aufgaben finden Sie in der Dokumentation „*OnCommand Workflow Automation*“.

Schritte

1. Workflow Automation Erstellen Sie eine SVM mit Infinite Volume, und erstellen Sie dann das Infinite Volume mithilfe des entsprechenden Workflows.

   Sie können Storage-Effizienztechnologien wie Deduplizierung und Komprimierung bei Erstellung des Infinite Volume aktivieren.

2. Unified Manager Fügen Sie der Unified Manager Datenbank den Cluster mit SVM und Infinite Volume hinzu.

   Sie können den Cluster hinzufügen, indem Sie die IP-Adresse oder den FQDN des Clusters angeben.

3. Unified Manager Ändern Sie die Schwellenwerte für das Infinite Volume auf der SVM entsprechend den Anforderungen Ihres Unternehmens.

   Sie sollten die standardmäßigen Schwellwerte für das Infinite Volume verwenden.

4. Unified Manager Konfigurieren von Benachrichtigungsalarme und -Traps zur Behebung aller Verfügbarkeits- und Kapazitätsprobleme im Zusammenhang mit dem Infinite Volume.

5. Workflow Automation Erstellung einer Disaster-Recovery- (DR-) SVM mit Infinite Volume, Konfiguration der Datensicherung (DP) durch folgende Schritte:
   a. Datensicherung (DP) Infinite Volume unter Verwendung des entsprechenden Workflows erstellen
   b. Richten Sie eine DP-Spiegelbeziehung zwischen Quelle und Ziel mithilfe des entsprechenden Workflows ein.

Bearbeiten der Schwellenwerteinstellungen des Infinite Volume

Wenn Sie Probleme im Storage-Bereich Ihres Infinite Volume beheben müssen, können Sie die Schwellenwerteinstellungen der Kapazität des Infinite Volume entsprechend den Anforderungen Ihres Unternehmens bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Ereignisse generiert und Sie erhalten Benachrichtigungen, wenn Sie für solche Ereignisse konfiguriert haben.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory eine SVM mit Infinite Volume aus.
3. Klicken Sie auf der Seite **Health/Storage Virtual Machine** Details auf **Actions** > **Schwellenwerte bearbeiten**.
4. Ändern Sie im Dialogfeld **SVM mit Infinite Volume Schwellenwerten** die Schwellenwerte nach Bedarf.
5. Klicken Sie auf **Speichern und Schließen**.

Management des Infinite Volume mit Storage-Klassen und Datenrichtlinien

Sie können das Infinite Volume effizient managen, indem Sie das Infinite Volume mit der erforderlichen Anzahl an Storage-Klassen erstellen, Schwellenwerte für jede Storage-Klasse konfigurieren, Regeln und eine Datenrichtlinie erstellen, um die Platzierung von auf das Infinite Volume geschriebenen Daten zu bestimmen, die Datensicherung zu konfigurieren und Benachrichtigungen optional zu konfigurieren.

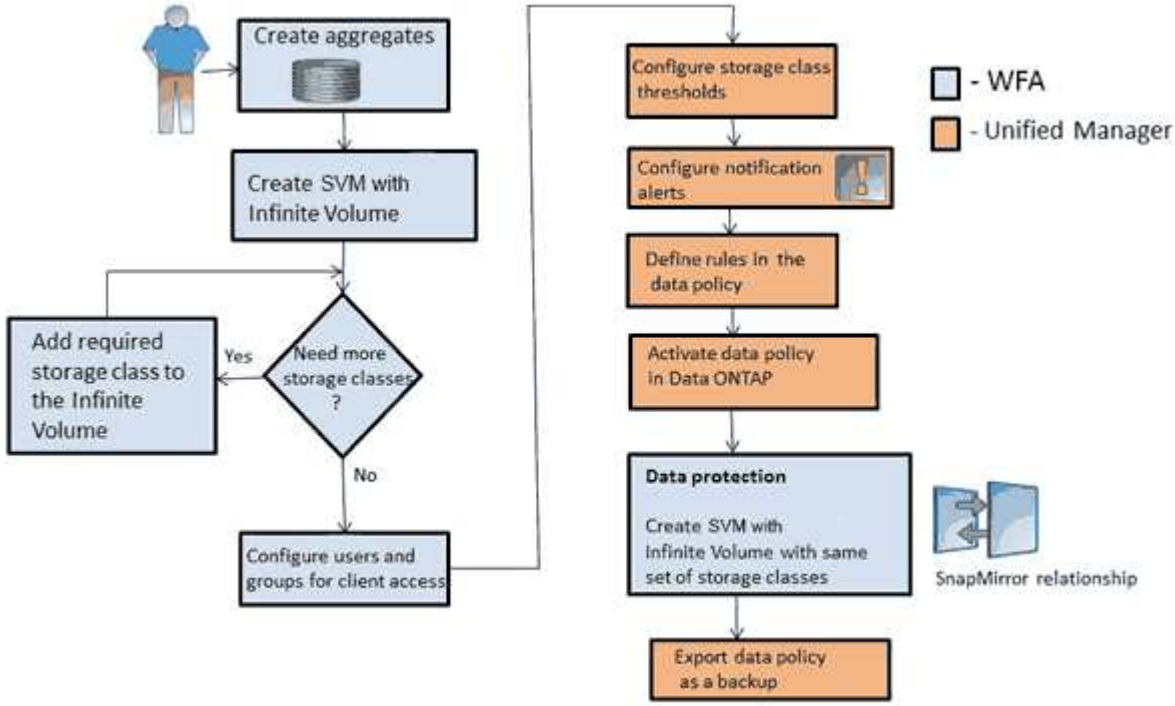
Bevor Sie beginnen

- OnCommand Workflow Automation (WFA) muss installiert sein.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die erforderliche Anzahl an Aggregaten erstellt haben, indem Sie den entsprechenden vordefinierten Workflow in WFA anpassen.
- Sie müssen die erforderliche Anzahl an Storage-Klassen erstellt haben, indem Sie den entsprechenden vordefinierten Workflow in WFA anpassen.
- Sie müssen den Unified Manager-Server als Datenquelle in WFA konfiguriert haben, und Sie müssen überprüfen, ob die Daten erfolgreich im Cache gespeichert sind.

Über diese Aufgabe

Bei dieser Aufgabe müssen Sie zwischen zwei Applikationen wechseln: OnCommand Workflow Automation (WFA) und OnCommand Unified Manager.

Die Aufgabe bietet Schritte auf hoher Ebene. Informationen zur Durchführung der WFA Aufgaben finden Sie in der Dokumentation „*OnCommand Workflow Automation*“.



Schritte

1. Workflow Automation Passen Sie den vordefinierten Workflow an, um die erforderlichen Speicherklassen zu definieren.
2. Workflow Automation Erstellen Sie mithilfe des entsprechenden Workflows eine SVM mit Infinite Volume mit der erforderlichen Anzahl an Storage-Klassen.
3. Unified Manager Fügen Sie der Unified Manager Datenbank den Cluster mit SVM und Infinite Volume hinzu.

   Sie können den Cluster hinzufügen, indem Sie die IP-Adresse oder den FQDN des Clusters angeben.

4. Unified Manager Ändern Sie die Schwellenwerte für jede Storage-Klasse basierend auf den Anforderungen Ihres Unternehmens.

   Sie sollten die Standardeinstellungen für den Schwellenwert der Storage-Klasse verwenden, um den Speicherplatz der Storage-Klasse effektiv zu überwachen.

5. Unified Manager Konfigurieren von Benachrichtigungsalarme und -Traps zur Behebung aller

Verfügbarkeits- und Kapazitätsprobleme im Zusammenhang mit dem Infinite Volume.

6. Unified Manager Legen Sie in der Datenrichtlinie Regeln fest und aktivieren Sie alle Änderungen an der Datenrichtlinie

   Die Regeln in einer Datenrichtlinie bestimmen die Platzierung der auf das Infinite Volume geschriebenen Inhalte.

   > Regeln in einer Datenrichtlinie betreffen nur neue Daten, die auf das Infinite Volume geschrieben werden. Bestehende Daten im Infinite Volume werden jedoch nicht beeinträchtigt.

7. Workflow Automation Erstellung einer Disaster-Recovery- (DR-) SVM mit Infinite Volume und Konfiguration einer Datensicherung (DP) durch folgende Schritte:
   a. Datensicherung (DP) Infinite Volume unter Verwendung des entsprechenden Workflows erstellen
   b. Richten Sie eine DP-Spiegelbeziehung zwischen Quelle und Ziel mithilfe des entsprechenden Workflows ein.

Bearbeiten der Schwellenwerteinstellungen von Speicherklassen

Wenn Sie Probleme im Zusammenhang mit dem Speicherplatz in Ihren Storage-Klassen beheben müssen, können Sie die Schwellenwerteinstellungen der Storage-Kapazität entsprechend den Anforderungen Ihres Unternehmens bearbeiten. Wenn der Schwellenwert überschritten wird, werden Ereignisse generiert und Sie erhalten Benachrichtigungen, wenn Sie für solche Ereignisse konfiguriert haben.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory eine SVM mit Infinite Volume aus.
3. Klicken Sie auf der Seite **Health/Storage Virtual Machine** Details auf **Actions** > **Schwellenwerte bearbeiten**.
4. Ändern Sie im Dialogfeld **Schwellenwerte für Speicherklassen bearbeiten** die Schwellenwerte nach Bedarf.
5. Klicken Sie auf **Speichern und Schließen**.

Hinzufügen von Meldungen

Sie können Benachrichtigungen konfigurieren, um Sie über die Erzeugung eines bestimmten Ereignisses zu benachrichtigen. Sie können Meldungen für eine einzelne Ressource, für eine Gruppe von Ressourcen oder für Ereignisse mit einem bestimmten Schweregrad konfigurieren. Sie können die Häufigkeit angeben, mit der Sie benachrichtigt werden möchten, und ein Skript der Warnmeldung zuordnen.

Bevor Sie beginnen

- Sie müssen Benachrichtigungseinstellungen wie die Benutzer-E-Mail-Adresse, SMTP-Server und SNMP-Trap-Host konfiguriert haben, damit der Unified Manager-Server diese Einstellungen verwenden kann, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Meldung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie ein Skript basierend auf dem Ereignis ausführen möchten, müssen Sie das Skript mithilfe der Seite Management/Scripts zu Unified Manager hinzugefügt haben.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Sie können eine Warnmeldung direkt auf der Seite Ereignisdetails erstellen, nachdem Sie ein Ereignis empfangen haben. Zusätzlich können Sie eine Warnung auf der Seite Konfiguration/Warnmeldungen erstellen, wie hier beschrieben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Alerting**.
2. Klicken Sie auf der Seite **Konfiguration/Alarmfunktionen** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
4. Klicken Sie auf **Ressourcen**, und wählen Sie die Ressourcen aus, die in die Warnung aufgenommen oder von ihr ausgeschlossen werden sollen.

   Sie können einen Filter festlegen, indem Sie im Feld **Name enthält** eine Textzeichenfolge angeben, um eine Gruppe von Ressourcen auszuwählen. Die Liste der verfügbaren Ressourcen zeigt auf der Grundlage der angegebenen Textzeichenfolge nur die Ressourcen an, die der Filterregel entsprechen. Die von Ihnen angegebene Textzeichenfolge ist die Groß-/Kleinschreibung.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschl- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschließregel, und die Warnung wird nicht für Ereignisse generiert, die sich auf die ausgeschlossene Ressource beziehen.

5. Klicken Sie auf **Events** und wählen Sie die Ereignisse basierend auf dem Ereignisnamen oder dem Schweregrad aus, für den Sie eine Warnung auslösen möchten.

   Um mehrere Ereignisse auszuwählen, drücken Sie die Strg-Taste, während Sie Ihre Auswahl treffen.

6. Klicken Sie auf **Actions**, und wählen Sie die Benutzer aus, die Sie benachrichtigen möchten, wählen Sie die Benachrichtigungshäufigkeit aus, wählen Sie aus, ob ein SNMP-Trap an den Trap-Empfänger gesendet wird, und weisen Sie ein Skript zu, das ausgeführt werden soll, wenn eine Warnung erzeugt wird.

   Wenn Sie die für den Benutzer angegebene E-Mail-Adresse ändern und die Warnmeldung zur Bearbeitung erneut öffnen, erscheint das Feld Name leer, da die geänderte E-Mail-Adresse dem zuvor ausgewählten Benutzer nicht mehr zugeordnet ist. Wenn Sie die E-Mail-Adresse des ausgewählten Benutzers auf der Seite Verwaltung/Benutzer geändert haben, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

Sie können auch Benutzer über SNMP-Traps benachrichtigen.

7. Klicken Sie Auf **Speichern**.

Beispiel für das Hinzufügen einer Meldung

Dieses Beispiel zeigt, wie eine Warnung erstellt wird, die die folgenden Anforderungen erfüllt:

- Alarmname: HealthTest
- Ressourcen: Enthält alle Volumes, deren Name „`abc`“ enthält und schließt alle Volumes aus, deren Name „`xyz`“ enthält
- Ereignisse: Umfasst alle kritischen Systemzustandsereignisse
- Aktionen: Enthält “sample@domain.com”, ein Skript “Test”, und der Benutzer muss alle 15 Minuten benachrichtigt werden

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

1. Klicken Sie auf **Name** und geben Sie ein `HealthTest` Im Feld **Alarmname**.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
   a. Eingabe `abc` Im Feld **Name enthält** werden die Volumes angezeigt, deren Name „`abc`“ enthält.
   b. Wählen Sie im Bereich Verfügbare Ressourcen **<<All Volumes whose name contains 'abc'>>** aus, und verschieben Sie sie in den Bereich Ausgewählte Ressourcen.
   c. Klicken Sie auf **Ausschließe**, und geben Sie ein `xyz` Klicken Sie im Feld **Name enthält** auf **Hinzufügen**.
3. Klicken Sie auf **Events** und wählen Sie im Feld Ereignis Severity * die Option **kritisch** aus.
4. Wählen Sie im Bereich passende Ereignisse die Option * Alle kritischen Ereignisse* aus, und verschieben Sie sie in den Bereich Ausgewählte Ereignisse.
5. Klicken Sie auf **Aktionen** und geben Sie ein `sample@domain.com` Im Feld „Diese Benutzer benachrichtigen“.
6. Wählen Sie **alle 15 Minuten**, um den Benutzer alle 15 Minuten zu benachrichtigen.

   Sie können eine Warnung konfigurieren, um wiederholt Benachrichtigungen an die Empfänger für eine bestimmte Zeit zu senden. Legen Sie fest, zu welchem Zeitpunkt die Ereignisbenachrichtigung für die Warnmeldung aktiv ist.

7. Wählen Sie im Menü Skript zum Ausführen auswählen die Option **Test** Skript .
8. Klicken Sie Auf **Speichern**.

Regeln werden erstellt

Sie können Ihrer Datenrichtlinie neue Regeln hinzufügen, um die Platzierung der Daten zu bestimmen, die auf das Infinite Volume geschrieben werden. Sie können Regeln entweder mithilfe von Regelvorlagen erstellen, die in Unified Manager definiert sind, oder benutzerdefinierte Regeln erstellen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Der Cluster, der die SVM mit Infinite Volume mit Storage-Klassen enthält, muss der Unified Manager Datenbank hinzugefügt werden.

Erstellen von Regeln mithilfe von Vorlagen

Neue Regeln lassen sich mithilfe von von Unified Manager definierten Regelvorlagen hinzufügen, um die Platzierung von Daten, die auf die SVM mit Infinite Volume geschrieben werden, zu bestimmen. Regeln lassen sich auf Basis von Dateitypen, Verzeichnispfaden oder Eigentümern erstellen.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Der Cluster, der die SVM mit Infinite Volume mit Storage-Klassen enthält, muss der Unified Manager Datenbank hinzugefügt werden.

Über diese Aufgabe

Die Registerkarte Datenrichtlinie ist nur für eine SVM mit Infinite Volume sichtbar.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory die entsprechende SVM aus.
3. Klicken Sie auf die Registerkarte **Datenrichtlinie**.

   Es wird eine Liste der Regeln in der Datenrichtlinie für die ausgewählte SVM mit Infinite Volume angezeigt.

4. Klicken Sie Auf **Erstellen**.
5. Wählen Sie im Dialogfeld **Regel erstellen** eine entsprechende Regelvorlage aus der Dropdown-Liste aus.

   Die Vorlage basiert auf drei Kategorien: Dateityp, Eigentümer oder Verzeichnispfad.

6. Fügen Sie auf der Grundlage der ausgewählten Vorlage die notwendigen Bedingungen im Bereich **passende Kriterien** hinzu.
7. Wählen Sie aus der Dropdown-Liste **Platzieren Sie den passenden Inhalt in der Storage Class** aus.
8. Klicken Sie Auf **Erstellen**.

   Die neue Regel, die Sie erstellt haben, wird auf der Registerkarte Datenrichtlinie angezeigt.

9. Vorschau aller anderen Änderungen an der Datenrichtlinie.
10. Klicken Sie auf **Aktivieren**, um die Änderungen in den Regeleigenschaften in der SVM zu aktivieren.

Benutzerdefinierte Regeln werden erstellt

Je nach Anforderungen im Datacenter können Sie benutzerdefinierte Regeln erstellen und einer Datenrichtlinie hinzufügen, um die Platzierung von Daten zu bestimmen, die mit

Infinite Volume auf die SVM geschrieben werden. Sie können benutzerdefinierte Regeln im Dialogfeld Regel erstellen erstellen erstellen ohne vorhandene Vorlagen zu verwenden.

Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Der Cluster, der die SVM mit Infinite Volume mit Storage-Klassen enthält, muss der Unified Manager Datenbank hinzugefügt werden.

Über diese Aufgabe

Die Registerkarte Datenrichtlinie ist nur für eine SVM mit Infinite Volume sichtbar.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory die entsprechende SVM aus.
3. Klicken Sie Auf **Datenrichtlinie**.
4. Klicken Sie Auf **Erstellen**.
5. Wählen Sie im Dialogfeld **Regel erstellen** die Option **Benutzerdefinierte Regel** aus der Liste **Vorlage** aus.
6. Fügen Sie im Bereich **passende Kriterien** die Bedingungen bei Bedarf hinzu.

   Unter Bedingungen können Sie eine Regel erstellen, die auf Dateitypen, Verzeichnispfaden oder Besitzern basiert. Eine Kombination dieser Bedingungen sind die Bedingungssätze. Zum Beispiel können Sie eine Regel haben: “Platzieren Sie alle .mp3 im Besitz von John in Bronze-Speicherklasse.”

7. Wählen Sie aus der Dropdown-Liste **Platzieren Sie den passenden Inhalt in der Storage Class** aus.
8. Klicken Sie Auf **Erstellen**.

   Die neu erstellte Regel wird auf der Registerkarte Datenrichtlinie angezeigt.

9. Vorschau aller anderen Änderungen an der Datenrichtlinie.
10. Klicken Sie auf **Aktivieren**, um die Änderungen in den Regeleigenschaften in der SVM zu aktivieren.

Konfiguration einer Datenrichtlinie exportieren

Sie können eine Konfiguration einer Datenrichtlinie aus Unified Manager in eine Datei exportieren. Nachdem Sie beispielsweise das erforderliche Backup erstellt haben und im Notfall die Konfiguration der Datenrichtlinie aus dem primären Storage exportiert haben.

Bevor Sie beginnen

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Über diese Aufgabe

Die Registerkarte Datenrichtlinie, die bei dieser Aufgabe verwendet wird, wird nur für SVMs mit Infinite Volume angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Systemzustand** > **SVMs**.
2. Wählen Sie auf der Seite **Health/Storage Virtual Machines** Inventory die entsprechende SVM aus.
3. Klicken Sie Auf **Datenrichtlinie**.

   Es wird eine Liste der Regeln in der Datenrichtlinie für die ausgewählte SVM mit Infinite Volume angezeigt.
4. Klicken Sie Auf **Exportieren**.
5. Geben Sie im browserspezifischen Dialogfeld den Speicherort an, an den die Konfiguration der Datenrichtlinie exportiert werden soll.

Ergebnisse

Die Konfiguration der Datenrichtlinien wird als JSON-Datei an den angegebenen Speicherort exportiert.

Senden eines Unified Manager Support Bundle an den technischen Support

In diesem Workflow erfahren Sie, wie Sie über die Unified Manager Wartungskonsole ein Support Bundle generieren, abrufen und an den technischen Support senden. Sie sollten ein Support-Bundle senden, wenn das Problem, das Sie haben, detailliertere Diagnose und Fehlerbehebung erfordert als eine AutoSupport-Meldung.

Über diese Aufgabe

Weitere Informationen über die Wartungskonsole und die Support-Bundles finden Sie unter Verwenden der Wartungskonsole.

Unified Manager speichert zwei generierte Support-Bundles gleichzeitig.

Zugriff auf die Wartungskonsole

Wenn die Benutzeroberfläche von Unified Manager nicht ausgeführt wird oder Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Wartungskonsole zugreifen, um Ihr Unified Manager System zu verwalten.

Bevor Sie beginnen

Sie müssen Unified Manager installiert und konfiguriert haben.

Über diese Aufgabe

Nach 15 Minuten Inaktivität meldet die Wartungskonsole sie aus.

> Wenn Sie auf VMware installiert sind und sich bereits über die VMware-Konsole als Wartungsbenutzer angemeldet haben, können Sie sich nicht gleichzeitig mit Secure Shell anmelden.

Schritte

1. Führen Sie die folgenden Schritte aus, um auf die Wartungskonsole zuzugreifen:

Auf diesem Betriebssystem…	Führen Sie die folgenden Schritte aus…
VMware	a. Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domänennamen der virtuellen Unified Manager-Appliance her. b. Melden Sie sich mit Ihrem Wartungs-Benutzernamen und -Passwort an der Wartungskonsole an.
Linux	a. Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domänennamen des Unified Manager-Systems her. b. Melden Sie sich beim System mit dem Wartungs-Benutzer (umadmin) und dem Passwort an. c. Geben Sie den Befehl ein `maintenance_console` Und drücken Sie die Eingabetaste.
Windows	a. Melden Sie sich mit den Administratoranmeldeinformationen beim Unified Manager-System an. b. Starten Sie PowerShell als Windows-Administrator. c. Geben Sie den Befehl ein `maintenance_console` Und drücken Sie die Eingabetaste. Wenn Sie unter Microsoft Windows Server 2012 einen Fehler bei der Ausführungsrichtlinie erhalten, geben Sie den folgenden Befehl ein, und versuchen Sie Schritt c erneut: `PowerShell.exe -ExecutionPolicy RemoteSigned`

Das Menü der Unified Manager-Wartungskonsole wird angezeigt.

Erstellen eines Support-Bundles

Sie können ein Support-Paket mit vollständigen Diagnoseinformationen erstellen, damit

Sie es dann abrufen und an den technischen Support zur Fehlerbehebung senden können. Da einige Datentypen große Mengen von Cluster-Ressourcen verwenden oder lange in die Fertigstellung benötigen, können Sie Datentypen angeben, die in das Support-Bundle einbezogen oder ausgeschlossen werden sollen.

Bevor Sie beginnen

Sie müssen als Wartungbenutzer Zugriff auf die Wartungskonsole haben.

Über diese Aufgabe

Unified Manager speichert nur die zwei zuletzt erstellten Support Bundles. Ältere Supportpakete werden aus dem System gelöscht.

Auf Windows-Systemen, der Befehl `supportbundle.bat` Wird zur Generierung eines Support Bundle nicht mehr unterstützt.

Schritte

1. Wählen Sie in der Wartungskonsole **Hauptmenü** die Option **Support/Diagnose**.
2. Wählen Sie **Support Bundle Generieren** Aus.
3. Wählen oder deaktivieren Sie die folgenden Datentypen aus, die im Supportpaket enthalten oder ausgeschlossen werden sollen:
   - **Datenbankauszug**

     Ein Dump der MySQL Server Datenbank.
   - **Haufendump**

     Ein Snapshot des Status der wichtigsten Unified Manager Serverprozesse. Diese Option ist standardmäßig deaktiviert und sollte nur ausgewählt werden, wenn sie vom Kundendienst angefordert wird.
   - **Aufnahmeaufzeichnungen**

     Eine Aufzeichnung der gesamten Kommunikation zwischen Unified Manager und den überwachten Clustern.

     Wenn Sie die Auswahl aller Datentypen aufheben, wird das Support-Paket immer noch mit anderen Unified Manager-Daten generiert.
4. Typ `g`, Und drücken Sie dann die Eingabetaste, um das Supportpaket zu generieren.

   Da es sich bei der Generierung eines Support-Bundles um einen speicherintensiven Vorgang handelt, werden Sie aufgefordert zu überprüfen, ob Sie das Support-Bundle derzeit sicher erstellen möchten.
5. Typ `y`, Und drücken Sie dann die Eingabetaste, um das Supportpaket zu generieren.

   Wenn Sie das Support-Bundle derzeit nicht generieren möchten, geben Sie ein `n`, Und drücken Sie dann die Eingabetaste.

6. Wenn Sie Datenbank-Dump-Dateien in das Support-Bundle aufgenommen haben, werden Sie aufgefordert, den Zeitraum anzugeben, für den Performance-Statistiken enthalten sein sollen. Das Einführen von Performance-Statistiken kann viel Zeit und Speicherplatz beanspruchen, sodass Sie auch eine Dump-Datenbank ohne inklusive der Performance-Statistiken erstellen können:

   a. Geben Sie das Startdatum im Format YYYYMMDD ein.

      Geben Sie beispielsweise ein `20170101` Für den 1. Januar 2017. Eingabe `n` Wenn Sie nicht möchten, dass Performance-Statistiken aufgenommen werden sollen.

   b. Geben Sie die Anzahl der Tage der einzuführenden Statistiken ab 12 Uhr ein Am angegebenen Startdatum.

      Sie können eine Zahl zwischen 1 und 10 eingeben.

   Wenn Sie Performance-Statistiken vorhalten, zeigt das System den Zeitraum an, für den Performance-Statistiken erfasst werden sollen.

7. Wählen Sie **Support Bundle Generieren** Aus.

   Das generierte Supportpaket befindet sich im `/support` Verzeichnis.

Nachdem Sie fertig sind

Nach dem Generieren des Support-Pakets können Sie es mithilfe eines SFTP-Clients oder unter Verwendung von UNIX- oder Linux-CLI-Befehlen abrufen. Unter Windows-Installationen können Sie Remote Desktop (RDP) verwenden, um das Supportpaket abzurufen.

Das generierte Supportpaket befindet sich im `/support` Verzeichnis auf VMware Systemen, in `/opt/netapp/data/support/` Auf Linux-Systemen und in `ProgramData\NetApp\OnCommandAppData\ocum\support` Auf Windows-Systemen.

Abrufen des Support-Pakets über einen Windows-Client

Als Windows-Benutzer können Sie ein Tool herunterladen und installieren, um das Support-Paket von Ihrem Unified Manager-Server abzurufen. Sie können das Support Bundle an den technischen Support senden, um eine detailliertere Diagnose eines Problems zu erhalten. FileZilla oder WinSCP sind Beispiele für Werkzeuge, die Sie verwenden können.

Bevor Sie beginnen

Sie müssen der Wartungbenutzer sein, um diese Aufgabe ausführen zu können.

Sie müssen ein Werkzeug verwenden, das SCP oder SFTP unterstützt.

Schritte

1. Laden Sie ein Tool herunter und installieren Sie es, um das Support Bundle abzurufen.
2. Öffnen Sie das Werkzeug.
3. Stellen Sie über SFTP eine Verbindung mit dem Unified Manager-Managementserver her.

Das Werkzeug zeigt den Inhalt des an `/support` Verzeichnis und Sie können alle bestehenden Support Bundles anzeigen.

4. Wählen Sie das Zielverzeichnis für das Supportpaket aus, das Sie kopieren möchten.
5. Wählen Sie das Supportpaket aus, das Sie kopieren möchten, und kopieren Sie die Datei vom Unified Manager-Server auf Ihr lokales System.

Verwandte Informationen

"Filezilla - https://filezilla-project.org/"

"WinSCP - http://winscp.net"

Abrufen des Support-Pakets über einen UNIX oder Linux Client

Wenn Sie UNIX- oder Linux-Benutzer sind, können Sie das Support Bundle über Ihre vApp abrufen, indem Sie die Befehlszeilenschnittstelle (CLI) auf Ihrem Linux-Client-Server verwenden. Sie können das Supportpaket entweder mit SCP oder SFTP abrufen.

Bevor Sie beginnen

Sie müssen der Wartungbenutzer sein, um diese Aufgabe ausführen zu können.

Sie müssen ein Support-Bundle mit der Wartungskonsole generiert haben und den Support-Bundle-Namen haben.

Schritte

1. Greifen Sie über Telnet oder die Konsole auf die CLI über Ihren Linux-Client-Server zu.
2. Auf das zugreifen `/support` Verzeichnis.
3. Rufen Sie das Support Bundle ab und kopieren Sie es mit dem folgenden Befehl in das lokale Verzeichnis:

Sie verwenden…	Verwenden Sie dann den folgenden Befehl…
SCP	`scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`
SFTP	`sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`

Der Name des Support-Pakets wird Ihnen bereitgestellt, wenn Sie es mit der Wartungskonsole erstellen.

4. Geben Sie das Wartungs-Benutzerpasswort ein.

Beispiele

Im folgenden Beispiel wird SCP verwendet, um das Supportpaket abzurufen:

```
        $ scp admin@10.10.12.69:/support/support_bundle_20160216_145359.7z
.
Password: <maintenance_user_password>
support_bundle_20160216_145359.7z   100%  119MB  11.9MB/s   00:10
```

Im folgenden Beispiel wird SFTP zum Abrufen des Supportpakets verwendet:

```
        $ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .
Password: <maintenance_user_password>
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

Senden eines Support Bundle an den technischen Support

Wenn ein Problem detailliertere Diagnose- und Fehlerbehebungsinformationen erfordert als eine AutoSupport Meldung, können Sie ein Support Bundle an den technischen Support senden.

Bevor Sie beginnen

Sie müssen Zugriff auf das Support-Bundle haben, um es an den technischen Support zu senden.

Sie müssen über die technische Support-Website eine Case-Nummer generiert haben.

Schritte

1. Loggen Sie sich auf der NetApp Support Site ein.
2. Laden Sie die Datei hoch.

   "Wie zum Hochladen einer Datei auf NetApp"

Aufgaben und Informationen im Zusammenhang mit mehreren Workflows

Einige Aufgaben und Referenztexte, die Ihnen helfen, einen Workflow zu verstehen und abzuschließen, sind für viele Workflows in Unified Manager üblich. Dazu gehören das Hinzufügen und Prüfen von Notizen zu einem Ereignis, das Zuweisen eines Ereignisses, das Erkennen und Beheben von Ereignissen sowie Details zu Volumes, Storage Virtual Machines (SVMs), Aggregaten, Und so weiter.

Hinzufügen und Überprüfen von Notizen zu einem Ereignis

Während Sie Ereignisse ansprechen, können Sie Informationen darüber hinzufügen, wie das Problem behoben wird, indem Sie den Bereich Hinweise und Aktualisierungen auf

der Seite Ereignisdetails verwenden. Mit diesen Informationen kann ein anderer Benutzer aktiviert werden, der dem Ereignis zugewiesen ist. Sie können auch Informationen anzeigen, die vom Benutzer hinzugefügt wurden, der ein Ereignis zuletzt adressiert hat, basierend auf dem letzten Zeitstempel.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Events**.
2. Klicken Sie auf der Seite **Events** Inventory auf das Ereignis, für das Sie die ereignisbezogenen Informationen hinzufügen möchten.
3. Fügen Sie auf der Seite **Event** Details die erforderlichen Informationen im Bereich **Hinweise und Updates** ein.
4. Klicken Sie Auf **Post**.

Zuweisen von Ereignissen zu bestimmten Benutzern

Sie können nicht zugewiesene Ereignisse selbst oder anderen Benutzern, einschließlich Remote-Benutzern, zuweisen. Sie können zugewiesene Ereignisse bei Bedarf einem anderen Benutzer zuweisen. Wenn z. B. häufig Probleme an einem Storage-Objekt auftreten, können Sie den Benutzer, der das Objekt verwaltet, die Ereignisse für diese Probleme zuweisen.

Bevor Sie beginnen

- Der Name und die E-Mail-ID des Benutzers müssen korrekt konfiguriert sein.
- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Events**.
2. Wählen Sie auf der Seite **Ereignisse** Inventar ein oder mehrere Ereignisse aus, die Sie zuweisen möchten.
3. Ordnen Sie das Ereignis zu, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie das Ereignis zuweisen möchten…	Dann tun Sie das…
Sich Selbst.	Klicken Sie Auf **Zuweisen Zu** > **Mich**.

Wenn Sie das Ereignis zuweisen möchten…	Dann tun Sie das…
Einem anderen Benutzer	a. Klicken Sie auf **Zuweisen zu** > **anderer Benutzer**. b. Geben Sie im Dialogfeld Eigentümer zuweisen den Benutzernamen ein, oder wählen Sie einen Benutzer aus der Dropdown-Liste aus. c. Klicken Sie Auf **Zuweisen**. Der Benutzer erhält eine E-Mail-Benachrichtigung. Wenn Sie keinen Benutzernamen eingeben oder einen Benutzer aus der Dropdown-Liste auswählen und auf **Zuweisen** klicken, bleibt die Zuweisung des Ereignisses aufgehoben.

Bestätigen und Beheben von Ereignissen

Sie sollten ein Ereignis bestätigen, bevor Sie mit der Bearbeitung des Problems beginnen, das das Ereignis verursacht hat, damit Sie keine wiederholten Warnmeldungen erhalten. Nachdem Sie die Korrekturmaßnahme für ein bestimmtes Ereignis durchgeführt haben, sollten Sie das Ereignis als gelöst markieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.

Über diese Aufgabe

Sie können mehrere Ereignisse gleichzeitig bestätigen und beheben.

Sie können keine Informationsereignisse bestätigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Events**.
2. Führen Sie in der Ereignisliste die folgenden Aktionen durch, um die Ereignisse zu bestätigen:

Ihr Ziel ist	Tun Sie das…
Bestätigen Sie ein einzelnes Ereignis und markieren Sie es als gelöst	a. Klicken Sie auf den Ereignisnamen. b. Bestimmen Sie auf der Seite Ereignisdetails die Ursache des Ereignisses. c. Klicken Sie Auf **Bestätigen**. d. Ergreifen Sie geeignete Korrekturmaßnahmen. e. Klicken Sie Auf **Als Gelöst Markieren**.
Bestätigen und markieren Sie mehrere Ereignisse als erledigt	a. Bestimmen Sie die Ursache der Ereignisse auf der entsprechenden Seite „Ereignisdetails“. b. Wählen Sie die Ereignisse aus. c. Klicken Sie Auf **Bestätigen**. d. Ergreifen Sie geeignete Korrekturmaßnahmen. e. Klicken Sie Auf **Als Gelöst Markieren**.

Nachdem das Ereignis als erledigt markiert wurde, wird das Ereignis in die Liste aufgelöster Ereignisse verschoben.

3. Fügen Sie im Bereich **Notizen und Updates** eine Notiz hinzu, wie Sie das Ereignis angesprochen haben, und klicken Sie dann auf **Post**.

Seite mit den Veranstaltungsdetails

Auf der Seite Ereignisdetails können Sie die Details eines ausgewählten Ereignisses anzeigen, z. B. den Schweregrad des Ereignisses, den Aufprallwert, den Aufprallbereich und die Ereignisquelle. Weitere Informationen zu möglichen Korrekturmaßnahmen können Sie zur Behebung des Problems einsehen.

- **Name Des Events**

  Der Name des Ereignisses und die Zeit, zu der das Ereignis zuletzt gesehen wurde.

  Bei Ereignissen ohne Leistungseinfall, während sich das Ereignis im Status „Neu“ oder „bestätigt“ befindet, sind die zuletzt erkannten Informationen nicht bekannt und daher verborgen.

- **Veranstaltungsbeschreibung**

  Eine kurze Beschreibung der Veranstaltung.

  In manchen Fällen wird in der Ereignisbeschreibung ein Grund für das ausgelöste Ereignis angegeben.

- **Komponente in Konflikt**

  Für dynamische Performance-Ereignisse werden in diesem Abschnitt Symbole angezeigt, die die logischen und physischen Komponenten des Clusters darstellen. Wenn eine Komponente einen Konflikt hat, ist ihr Symbol eingekreist und rot markiert.

  Die folgenden Komponenten können angezeigt werden:

- **Netzwerk**

  Zeigt die Wartezeit von I/O-Anfragen durch iSCSI-Protokolle oder Fibre Channel-Protokollen (FC) des Clusters an. Die Wartezeit liegt darin, auf die Transaktionen „iSCSI Ready to Transfer“ (R2T) oder „FCP Transfer Ready“ (XFER_RDY) zu warten, bis der Cluster auf eine I/O-Anforderung antworten kann. Wenn die Netzwerkkomponente unter einem Konflikt steht, bedeutet dies, dass hohe Wartezeiten auf der Protokollebene des Blocks die Latenz eines oder mehrerer Workloads beeinflussen.

- * Netzwerkverarbeitung*

  Repräsentiert die Softwarekomponente in dem Cluster, die mit I/O-Verarbeitung zwischen Protokollebene und Cluster beteiligt ist Der Knoten, der die Netzwerkverarbeitung verarbeitet, hat sich seit dem Erkennen des Ereignisses möglicherweise geändert. Wenn die Netzwerkverarbeitungskomponente einen Konflikt verursacht, bedeutet dies, dass eine hohe Auslastung des Node zur Netzwerkverarbeitung die Latenz eines oder mehrerer Workloads beeinträchtigt.

- **QoS-Richtlinie**

  Steht für die Storage-Richtliniengruppe für Quality of Service (QoS), der Mitglied des Workloads ist Wenn die Richtliniengruppe Konflikte hat, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch das festgelegte Durchsatzlimit gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- * Cluster Interconnect*

  Stellt die Kabel und Adapter dar, mit denen die physischen Nodes des Clustern verbunden sind. Wenn die Cluster-Interconnect-Komponente einen Konflikt verursacht, bedeutet dies hohe Wartezeiten bei I/O-Anfragen am Cluster Interconnect, die sich auf die Latenz eines oder mehrerer Workloads auswirken.

- **Datenverarbeitung**

  Zeigt die Softwarekomponente in dem Cluster an, die mit I/O-Verarbeitung zwischen dem Cluster und dem Storage-Aggregat, das den Workload enthält. Der Node, der die Datenverarbeitung verarbeitet, hat sich seit dem Erkennen des Ereignisses geändert. Wenn die Datenverarbeitungkomponente einen Konflikt verursacht, bedeutet dies, dass eine hohe Auslastung am Datenverarbeitungs-Node die Latenz eines oder mehrerer Workloads beeinträchtigt.

- **MetroCluster Ressourcen**

  Repräsentiert die MetroCluster-Ressourcen, einschließlich NVRAM und Interswitch Links (ISLs), die zur Spiegelung von Daten zwischen Clustern in einer MetroCluster Konfiguration verwendet werden. Wenn die MetroCluster Komponente Konflikte verursacht, bedeutet dies einen hohen Schreibdurchsatz von Workloads auf dem lokalen Cluster oder ein Link-Systemzustandsproblem Auswirkungen auf die Latenz einer oder mehrerer Workloads auf dem lokalen Cluster. Wenn das Cluster nicht in einer MetroCluster-Konfiguration befindet, wird dieses Symbol nicht angezeigt.

- **Aggregate oder SSD Aggregate Ops**

  Repräsentiert das Storage-Aggregat, auf dem die Workloads ausgeführt werden Wenn die Aggregat-Komponente Konflikte verursacht, bedeutet dies, dass eine hohe Auslastung des Aggregats sich auf die Latenz eines oder mehrerer Workloads auswirkt. Ein Aggregat besteht aus rein HDDs oder einer Kombination aus HDDs und SSDs (einem Flash Pool Aggregat). Ein „`SSD Aggregat`“ besteht aus

allen SSDs (ein All-Flash-Aggregat) oder einer Kombination aus SSDs und einer Cloud Tier (ein FabricPool Aggregat).

- **Cloud-Latenz**

  Stellt die Softwarekomponente in dem Cluster dar, die mit I/O-Verarbeitung zwischen dem Cluster und dem Cloud-Tier beschäftigt ist, auf dem Benutzerdaten gespeichert werden Wenn die Komponente für die Cloud-Latenz aufgrund von Konflikten vorliegen, bedeutet dies, dass sich ein großer Anteil der in der Cloud-Ebene gehosteten Lesevorgänge auf die Latenz eines oder mehrerer Workloads auswirkt.

- **Sync SnapMirror**

  Repräsentiert die Software-Komponente in dem Cluster, die mit der Replizierung von Benutzerdaten vom primären Volume auf das sekundäre Volume in einer SnapMirror Synchronous-Beziehung beteiligt ist Wenn die synchrone SnapMirror Komponente Konflikte verursacht, bedeutet dies, dass die Aktivitäten des synchronen Betriebs von SnapMirror sich auf die Latenz eines oder mehrerer Workloads auswirken.

Die Abschnitte Ereignisinformationen, Systemdiagnose und vorgeschlagene Maßnahmen werden in anderen Themen beschrieben.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Notizen-Symbol**

  Ermöglicht Ihnen das Hinzufügen oder Aktualisieren von Notizen zum Ereignis und die Überprüfung aller von anderen Benutzern verbleibenden Notizen.

Aktionen Menü

- **Mir zuweisen**

  Weist Ihnen das Ereignis zu.

- **Anderen zuweisen**

  Öffnet das Dialogfeld „Eigentümer zuweisen“, in dem Sie das Ereignis anderen Benutzern zuweisen oder neu zuweisen können.

  Wenn Sie einem Benutzer ein Ereignis zuweisen, werden der Benutzername und die Uhrzeit, zu der das Ereignis zugewiesen wurde, in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt.

  Sie können auch die Zuweisung von Ereignissen aufheben, indem Sie das Feld Eigentumsrechte leer lassen.

- * Quittieren*

  Bestätigt die ausgewählten Ereignisse, damit Sie keine Wiederholungsbenachrichtigungen erhalten.

  Wenn Sie ein Ereignis bestätigen, werden Ihr Benutzername und die Zeit, zu der Sie das Ereignis bestätigt haben, in der Ereignisliste (bestätigt von) für die ausgewählten Ereignisse hinzugefügt. Wenn Sie ein Ereignis bestätigen, übernehmen Sie die Verantwortung für die Verwaltung dieses Ereignisses.

- **Als Gelöst Markieren**

  Ermöglicht Ihnen die Änderung des Ereignisstatus in „gelöst“.

  Wenn Sie ein Ereignis auflösen, werden Ihr Benutzername und die Zeit, zu der Sie das Ereignis aufgelöst haben, in der Ereignisliste (aufgelöst von) für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie Korrekturmaßnahmen für das Ereignis ergriffen haben, müssen Sie das Ereignis als gelöst markieren.

- **Alarm Hinzufügen**

  Zeigt das Dialogfeld Alarm hinzufügen an, in dem Sie eine Warnung für das ausgewählte Ereignis hinzufügen können.

Das wird im Abschnitt „Ereignisinformationen“ angezeigt

Über den Abschnitt „Ereignisinformationen“ auf der Seite „Ereignisdetails“ können Sie Details zu einem ausgewählten Ereignis anzeigen, z. B. den Schweregrad des Ereignisses, den Aufprallgrad, den Wirkungsbereich und die Ereignisquelle.

Felder, die nicht auf den Ereignistyp anwendbar sind, werden ausgeblendet. Sie können folgende Veranstaltungsdetails anzeigen:

- **Ereignis Trigger Zeit**

  Die Zeit, zu der das Ereignis generiert wurde.

- **Bundesland**

  Der Ereignisstatus: Neu, bestätigt, aufgelöst oder veraltet.

- **Veraltete Ursache**

  Die Aktionen, durch die das Ereignis veraltet war, z. B. wurde das Problem behoben.

- **Veranstaltungsdauer**

  Bei aktiven (neuen und bestätigten) Ereignissen handelt es sich um die Zeit zwischen der Erkennung und der Zeit, zu der das Ereignis zuletzt analysiert wurde. Bei veralteten Ereignissen ist dies die Zeit zwischen der Erkennung und dem Zeitpunkt, zu dem das Ereignis gelöst wurde.

  Dieses Feld wird für alle Performanceereignisse und für andere Ereignistypen angezeigt, nachdem sie aufgelöst oder veraltet sind.

- **Zuletzt Gesehen**

  Datum und Uhrzeit, zu der das Ereignis zuletzt als aktiv angesehen wurde.

  Bei Performanceereignissen kann dieser Wert höher sein als die Ereignis-Trigger-Zeit, da dieses Feld nach jeder neuen Sammlung von Performancedaten aktualisiert wird, solange das Ereignis aktiv ist. Bei anderen Arten von Ereignissen, wenn sich der Status Neu oder bestätigt befindet, wird dieser Inhalt nicht aktualisiert und das Feld wird daher ausgeblendet.

- **Severity**

  Der Schweregrad des Ereignisses: Kritisch (), Fehler (), Warnung (), und Informationen ().

- **Impact Level**

  Die Ereigniseinwirkung: Vorfall, Risiko oder Ereignis.

- **Aufprallbereich**

  Die Auswirkung auf das Ereignis: Verfügbarkeit, Kapazität, Performance, Schutz oder Konfiguration.

- **Quelle**

  Der Name des Objekts, auf dem das Ereignis aufgetreten ist.

  Wenn sich die Details zu einem Ereignis für eine Shared QoS-Richtlinie anzeigen lassen, werden in diesem Feld bis zu drei Workload-Objekte aufgeführt, die die meisten IOPS oder MB/s verbrauchen.

  Sie können auf den Link des Quellnamens klicken, um die Seite mit den Angaben zu Systemzustand oder Performance für das Objekt anzuzeigen.

- **Quellanmerkungen**

  Zeigt den Anmerkungsnamen und -Wert für das Objekt an, dem das Ereignis zugeordnet ist.

  Dieses Feld wird nur für Systemzustandsereignisse in Clustern, SVMs und Volumes angezeigt.

- **Quellgruppen**

  Zeigt die Namen aller Gruppen an, deren Mitglied das betroffene Objekt ist.

  Dieses Feld wird nur für Systemzustandsereignisse in Clustern, SVMs und Volumes angezeigt.

- **Quelltyp**

  Den Objekttyp (z. B. SVM, Volume oder Qtree), mit dem das Ereignis verknüpft ist.

- * Auf Cluster*

  Der Name des Clusters, an dem das Ereignis aufgetreten ist.

  Sie können auf den Cluster-Link klicken, um die Seite mit den Angaben zu Systemzustand und Performance für das Cluster anzuzeigen.

- **Betroffene Objekte Zählen**

  Die Anzahl der vom Ereignis betroffenen Objekte.

  Sie können auf den Objektlink klicken, um die Bestandsseite anzuzeigen, die mit den Objekten ausgefüllt wird, die aktuell von diesem Ereignis betroffen sind.

  Dieses Feld wird nur für Performanceereignisse angezeigt.

- * Betroffene Volumen*

  Die Anzahl der Volumes, die von diesem Ereignis betroffen sind.

  Dieses Feld wird nur für Performance-Ereignisse auf Nodes oder Aggregaten angezeigt.

- * Ausgelöste Richtlinie*

  Der Name der Schwellenwertrichtlinie, die das Ereignis ausgegeben hat.

  Sie können den Mauszeiger über den Richtliniennamen bewegen, um Details zur Schwellenwertrichtlinie anzuzeigen. Für anpassungsfähige QoS-Richtlinien werden die definierte Richtlinie, die Blockgröße und der Zuweisungstyp (zugewiesener Speicherplatz oder genutzter Speicherplatz) angezeigt.

  Dieses Feld wird nur für Performanceereignisse angezeigt.

- * Bestätigt durch*

  Der Name der Person, die das Ereignis bestätigt hat und die Zeit, zu der das Ereignis bestätigt wurde.

- * Gelöst von*

  Der Name der Person, die das Ereignis gelöst hat, und die Zeit, zu der das Ereignis gelöst wurde.

- * Zugewiesen zu*

  Der Name der Person, die der Arbeit an dem Ereignis zugeordnet ist.

- **Warnmeldungseinstellungen**

  Die folgenden Informationen über Meldungen werden angezeigt:

  - Wenn dem ausgewählten Ereignis keine Warnmeldungen zugeordnet sind, wird ein Link **Alarm hinzufügen** angezeigt.

    Sie können das Dialogfeld Alarm hinzufügen öffnen, indem Sie auf den Link klicken.

  - Wenn dem ausgewählten Ereignis eine Warnung zugeordnet ist, wird der Alarmname angezeigt.

    Sie können das Dialogfeld Alarm bearbeiten öffnen, indem Sie auf den Link klicken.

  - Wenn dem ausgewählten Ereignis mehr als eine Warnung zugeordnet ist, wird die Anzahl der Warnmeldungen angezeigt.

    Sie können die Seite Konfiguration/Warnmeldungen öffnen, indem Sie auf den Link klicken, um weitere Details zu diesen Warnmeldungen anzuzeigen.

  Deaktivierte Warnmeldungen werden nicht angezeigt.

- **Letzte Benachrichtigung Gesendet**

  Das Datum und die Uhrzeit, zu der die letzte Benachrichtigung gesendet wurde.

- **Gesendet Über**

  Der Mechanismus, der zum Senden der Alarmierung verwendet wurde: E-Mail oder SNMP-Trap.

- **Vorherige Skriptausführung**

  Der Name des Skripts, das beim Generieren der Warnmeldung ausgeführt wurde.

Anzeigen des Abschnitts Systemdiagnose

Im Abschnitt Systemdiagnose der Seite Ereignisdetails finden Sie Informationen, die Ihnen bei der Diagnose von Problemen helfen können, die möglicherweise für das Ereignis verantwortlich waren.

Dieser Bereich wird nur für bestimmte Ereignisse angezeigt.

Einige Performanceereignisse bieten Diagramme, die für das Ereignis relevant sind, das ausgelöst wurde. Dies beinhaltet in der Regel ein IOPS- oder MB/s-Diagramm und ein Latenzdiagramm für die vorherigen zehn Tage. Nach Absprache sehen Sie, welche Storage-Komponenten die Latenz am meisten beeinträchtigen oder von der Latenz beeinträchtigt werden, wenn das Ereignis aktiv ist.

Für dynamische Performance-Ereignisse werden die folgenden Diagramme angezeigt:

- Workload-Latenz: Zeigt den Verlauf der Latenz für die Top-Opfer, -Bully oder -Hai-Workloads bei den zu versagenden Komponenten an.
- Workload-Aktivität: Zeigt Details zur Workload-Nutzung der Cluster-Komponente an, die durch Konflikte verursacht wird.
- Resource Activity: Zeigt historische Performance-Statistiken für eine Clusterkomponente an, die mit einem Konflikt in der Cluster-Komponente Konflikt ist.

Andere Diagramme werden angezeigt, wenn einige Clusterkomponenten mit einem Konflikt zu belegen sind.

Andere Ereignisse liefern eine kurze Beschreibung der Analysetyp, die das System auf dem Storage-Objekt durchführt. In manchen Fällen gibt es eine oder mehrere Zeilen; eine für jede analysierte Komponente, für systemdefinierte Performance-Richtlinien, die mehrere Performance-Zähler analysieren. In diesem Szenario wird neben der Diagnose ein grünes oder rotes Symbol angezeigt, um anzugeben, ob ein Problem in dieser speziellen Diagnose gefunden wurde oder nicht.

Der Abschnitt „Empfohlene Maßnahmen“ wird angezeigt

Der Abschnitt „Empfohlene Maßnahmen“ auf der Seite „Veranstaltungsdetails“ enthält mögliche Gründe für das Ereignis und schlägt einige Maßnahmen vor, damit Sie versuchen können, das Ereignis selbst zu lösen. Die vorgeschlagenen Maßnahmen werden auf Grundlage der Art des Ereignisses oder des Schwellenwerts, die nicht eingehalten wurden, angepasst.

Dieser Bereich wird nur für bestimmte Ereignistypen angezeigt.

In einigen Fällen gibt es **Hilfe** Links auf der Seite, die zusätzliche Informationen für viele empfohlene Aktionen, einschließlich Anweisungen für die Durchführung einer bestimmten Aktion. Einige der Aktionen können die Verwendung von Unified Manager, OnCommand System Manager, OnCommand Workflow Automation, ONTAP CLI-Befehlen oder einer Kombination dieser Tools umfassen.

In diesem Hilfethema werden auch einige Links angezeigt.

Die hier vorgeschlagenen Maßnahmen sollten Sie nur als Anleitung zur Lösung dieses Ereignisses betrachten. Die Maßnahmen, die Sie zur Lösung dieses Ereignisses ergreifen, sollten auf dem Kontext Ihrer Umgebung beruhen.

Beschreibung der Ereignistypen

Jedes Ereignis ist mit einem Schweregrad verknüpft, der Ihnen dabei hilft, die Ereignisse zu priorisieren, die eine unmittelbare Korrekturmaßnahme erfordern.

- * Kritisch*

  Ein Problem, das zu einer Serviceunterbrechung führen kann, wenn keine Korrekturmaßnahmen sofort ergriffen werden.

  Performance-kritische Ereignisse werden nur von benutzerdefinierten Schwellenwerten gesendet.

- **Fehler**

  Die Event-Quelle befindet sich noch in einer Performance. Zur Vermeidung von Serviceunterbrechungen sind jedoch Korrekturmaßnahmen erforderlich.

- **Warnung**

  Bei der Event-Quelle kommt es zu einem Vorfall, den Sie beachten sollten, oder ein Performance-Zähler für ein Cluster-Objekt liegt außerhalb des normalen Bereichs und sollte überwacht werden, um sicherzustellen, dass der kritische Schweregrad nicht erreicht wurde. Ereignisse dieses Schweregrades führen nicht zu einer Serviceunterbrechung und unmittelbare Korrekturmaßnahmen sind möglicherweise nicht erforderlich.

  Ereignisse mit Performance-Warnmeldungen werden von benutzerdefinierten, systemdefinierten oder dynamischen Schwellenwerten gesendet.

- **Information**

  Das Ereignis tritt auf, wenn ein neues Objekt erkannt wird oder wenn eine Benutzeraktion durchgeführt wird. Beispiel: Wenn ein Storage-Objekt gelöscht wird oder wenn Konfigurationsänderungen vorliegen, wird das Ereignis mit dem Schweregrad „Informationen“ generiert.

  Informationsereignisse werden direkt von ONTAP gesendet, wenn eine Konfigurationsänderung erkannt wird.

Beschreibung der Level der Ereignisauswirkungen

Jedes Ereignis ist mit einer Folgenabstufe (Vorfall, Risiko oder Ereignis) verbunden, um Ihnen bei der Priorisierung von Ereignissen zu helfen, für die sofortige Korrekturmaßnahmen erforderlich sind.

- **Vorfall**

  Ein Vorfall ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster keine Daten mehr für den Client bereitstellt, und nicht mehr genügend Speicherplatz zum Speichern von Daten vorhanden ist. Ereignisse mit Auswirkungen auf den Vorfall sind am schwersten. Um Serviceunterbrechungen zu vermeiden, sollten sofortige Korrekturmaßnahmen ergriffen werden.

- **Risiko**

  Ein Risiko ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster nicht mehr Daten für den Client bereitstellt, und nicht mehr genügend Speicherplatz zum Speichern von Daten vorhanden ist.

Ereignisse mit Risikoeinwirkung können zu Serviceunterbrechungen führen. Möglicherweise ist eine Korrekturmaßnahme erforderlich.

- **Veranstaltung**

  Ein Ereignis ist eine Statusänderung von Storage-Objekten und ihren Attributen. Ereignisse mit Auswirkungen auf das Ereignis dienen zur Information und erfordern keine Korrekturmaßnahmen.

Beschreibung der Bereiche für Ereignisauswirkungen

Die Ereignisse werden in fünf Bereiche mit Auswirkungen (Verfügbarkeit, Kapazität, Konfiguration, Leistung und Schutz) unterteilt, damit Sie sich auf die Arten von Ereignissen konzentrieren können, für die Sie verantwortlich sind.

- **Verfügbarkeit**

  Verfügbarkeitsereignisse melden Sie, wenn ein Storage-Objekt offline geschaltet wird, wenn ein Protokollservice ausfällt, ein Problem mit dem Storage Failover auftritt oder wenn ein Problem mit der Hardware auftritt.

- * Kapazität*

  Kapazitätsereignisse benachrichtigen Sie, wenn sich Ihre Aggregate, Volumes, LUNs oder Namespaces nähern oder einen Größenschwellenwert erreicht haben oder die Wachstumsrate für Ihre Umgebung ungewöhnlich ist.

- **Konfiguration**

  Konfigurationsereignisse informieren Sie über die Erkennung, das Löschen, das Hinzufügen, das Entfernen oder Umbenennen Ihrer Storage-Objekte. Konfigurationsereignisse haben eine Auswirkung auf das Ereignis und einen Schweregrad der Informationen.

- **Leistung**

  Bei Performance-Ereignissen werden Sie über Ressourcen, Konfigurationen oder Aktivitätsbedingungen auf dem Cluster informiert, die negative Auswirkungen auf die Geschwindigkeit der Eingabe oder den Abruf von Daten-Storage für Ihre überwachten Storage-Objekte haben können.

- **Schutz**

  Schutzereignisse benachrichtigen Sie über Vorfälle oder Risiken im Zusammenhang mit SnapMirror Beziehungen, Probleme mit Zielkapazität, Probleme mit SnapVault Beziehungen oder Probleme mit Sicherungsaufgaben. Alle ONTAP Objekte (insbesondere Aggregate, Volumes und SVMs), die sekundäre Volumes und Sicherungsbeziehungen hosten, werden im Bereich der Sicherungsauswirkungen kategorisiert.

Angaben zum Zustand/Volumen

Auf der Seite „Systemzustand/Volume-Details“ werden ausführliche Informationen zu einem ausgewählten Volume angezeigt, beispielsweise Kapazität, Storage-Effizienz, Konfiguration, Sicherung, Kommentare und erzeugte Ereignisse. Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für dieses Volume anzeigen.

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für das ausgewählte Volume ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Hier können Sie zur Seite Performance/Volume Details navigieren.

-

  Ermöglicht das Hinzufügen der ausgewählten Lautstärke zum Favoriten-Dashboard.

- **Aktionen**
  - Alarm Hinzufügen

    Ermöglicht das Hinzufügen einer Warnmeldung zum ausgewählten Volume.

  - Schwellenwerte Bearbeiten

    Ermöglicht das Ändern der Schwellenwerteinstellungen für das ausgewählte Volume.

  - Anmerkungen Hinzufügen

    Ermöglicht Ihnen, das ausgewählte Volume mit Anmerkungen zu versehen.

  - Sichern

    Ermöglicht die Erstellung von SnapMirror oder SnapVault Beziehungen für das ausgewählte Volume.

  - Beziehung

    Ermöglicht Ihnen die Ausführung folgender Sicherungsbeziehungsvorgänge:

    - Bearbeiten

      Öffnet das Dialogfeld „Beziehung bearbeiten“, in dem Sie vorhandene SnapMirror Richtlinien, Zeitpläne und maximale Übertragungsraten für eine vorhandene Sicherungsbeziehung ändern können.

    - Abbrechen

      Bricht Transfers ab, die für eine ausgewählte Beziehung in Bearbeitung sind. Optional können Sie den Checkpoint beim Neustart für andere Transfers als den Basistransfer entfernen. Sie können den Kontrollpunkt für einen Basistransfer nicht entfernen.

    - Stilllegen

      Zeitweilige Aktualisierungen für eine ausgewählte Beziehung werden vorübergehend deaktiviert. Transfers, die bereits in Bearbeitung sind, müssen vor der Stilllegung abgeschlossen werden.

    - Pause

Bricht die Beziehung zwischen Quell- und Zielvolumen ab und ändert das Ziel in ein Lese-Schreib-Volume.

- Entfernen

  Löscht dauerhaft die Beziehung zwischen der ausgewählten Quelle und dem ausgewählten Ziel. Die Volumes werden nicht zerstört und die Snapshot-Kopien auf den Volumes werden nicht entfernt. Dieser Vorgang kann nicht rückgängig gemacht werden.

- Fortsetzen

  Ermöglicht geplante Transfers für eine stillgelegte Beziehung. Beim nächsten geplanten Transferintervall wird ein Neustart-Checkpoint verwendet, falls vorhanden.

- Neu Synchronisieren

  Ermöglicht Ihnen die Neusynchronisierung einer zuvor unterbrochenen Beziehung.

- Initialisierung/Aktualisierung

  Ermöglicht Ihnen, eine erste Basistransfer für eine neue Schutzbeziehung durchzuführen oder eine manuelle Aktualisierung durchzuführen, wenn die Beziehung bereits initialisiert ist.

- Reverse Resync

  Ermöglicht Ihnen die Wiederherstellung einer zuvor unterbrochenen Schutzbeziehung, indem Sie die Funktion von Quelle und Ziel umkehren, indem Sie der Quelle eine Kopie des ursprünglichen Ziels machen. Der Inhalt der Quelle wird durch den Inhalt des Ziels überschrieben, und alle Daten, die neuer als die Daten der gemeinsamen Snapshot Kopie sind, werden gelöscht.

◦ Wiederherstellen

Ermöglicht Ihnen die Wiederherstellung von Daten von einem Volume auf einem anderen Volume.

> Die Schaltfläche „Wiederherstellen“ und die Schaltflächen für den Beziehungsvorgang stehen nicht für FlexGroup-Volumes oder für Volumes mit synchronem Schutz zur Verfügung.

- **View Volumes**

  Hier können Sie zur Seite „Health/Volumes Inventory“ navigieren.

Registerkarte „Kapazität“

Auf der Registerkarte Kapazität werden Details zum ausgewählten Volume angezeigt, z. B. seine physische Kapazität, logische Kapazität, Schwellwerte, Kontingentkapazität und Informationen über jede beliebige Volume-Verschiebung:

- **Kapazität Physisch**

  Detaillierte Informationen zur physischen Kapazität des Volumes:

  ◦ Snapshot-Überlauf

  Zeigt den Speicherplatz an, der von den Snapshot Kopien verbraucht wird.

- Verwendet

  Zeigt den Speicherplatz an, der von Daten im Volume verwendet wird.

- Warnung

  Zeigt an, dass der Speicherplatz im Volume fast voll ist. Wird diese Schwelle nicht erreicht, wird das Ereignis „Space Fast Full“ generiert.

- Fehler

  Zeigt an, dass der Speicherplatz im Volume voll ist. Wird dieser Schwellenwert nicht erreicht, wird das Ereignis „Space Full“ generiert.

- Nicht Nutzbar

  Zeigt an, dass der risikobehaftete Speicherplatz des Thin Provisioning Volume generiert wird und dass der Speicherplatz im Thin Provisioning Volume aufgrund von Kapazitätsproblemen im Aggregat gefährdet ist. Die nicht nutzbare Kapazität wird nur für Volumes angezeigt, die über Thin Provisioning bereitgestellt wurden.

- Datendiagramm

  Zeigt die Gesamtkapazität und die genutzte Datenkapazität des Volume an.

  Wenn Autogrow aktiviert ist, wird im Datendiagramm der verfügbare Speicherplatz im Aggregat angezeigt. Das Datendiagramm zeigt den effektiven Speicherplatz, der von Daten auf dem Volume genutzt werden kann. Dies kann einer der folgenden Werte sein:

  - Tatsächliche Datenkapazität des Volumes für die folgenden Bedingungen:
    - Autogrow ist deaktiviert.
    - Das autogrow-fähige Volume hat die maximale Größe erreicht.
    - Autogrow-aktivierte Volumes mit Thick Provisioning können nicht weiter wachsen.
  - Datenkapazität des Volumes unter Berücksichtigung der maximalen Volume-Größe (für Volumes mit Thin Provisioning und für Thick Provisioning Volumes, wenn das Aggregat über genügend Platz für das Volume verfügt, um die maximale Größe zu erreichen)
  - Datenkapazität des Volumes nach Berücksichtigung der nächsten möglichen Autogrow Größe (für Thick Provisioning Volumes, die einen Autogrow-Prozentwert haben)

- Diagramm Snapshot Kopien

  Dieses Diagramm wird nur angezeigt, wenn die verwendete Snapshot-Kapazität oder die Snapshot-Reserve nicht null ist.

Beide Diagramme zeigen die Kapazität an, um die die Snapshot-Kapazität die Snapshot-Reserve überschreitet, wenn die verwendete Snapshot-Kapazität die Snapshot-Reserve überschreitet.

- **Kapazität Logisch**

  Zeigt die logischen Platzeigenschaften des Volumes an. Der logische Speicherplatz gibt die tatsächliche Größe der auf Festplatte gespeicherten Daten an, ohne dabei die Einsparungen durch die ONTAP Storage-Effizienztechnologien zu verwenden.

- Bericht Zu Logischem Speicherplatz

  Zeigt an, ob für das Volume ein Bericht über den logischen Speicherplatz konfiguriert ist. Der Wert kann aktiviert, deaktiviert oder nicht zutreffend sein. „`not anwendbare`“ wird für Volumes auf älteren ONTAP-Versionen oder auf Volumes angezeigt, die kein logisches Speicherplatz-Reporting unterstützen.

- Verwendet

  Zeigt die Menge des logischen Speicherplatzes an, der von Daten im Volume verwendet wird, und den Prozentsatz des logischen Speicherplatzes, der basierend auf der Gesamtkapazität genutzt wird.

- Verfügbar

  Zeigt die Menge des logischen Speicherplatzes an, der noch für Daten im Volume verfügbar ist, und den Prozentsatz des verfügbaren logischen Speicherplatzes basierend auf der Gesamtkapazität.

- Durchsetzung Des Logischen Speicherplatzes

  Zeigt an, ob die Durchsetzung des logischen Speicherplatzes für über Thin Provisioning bereitgestellte Volumes konfiguriert ist. Bei Einstellung auf aktiviert kann die verwendete logische Größe des Volumes nicht größer sein als die aktuell eingestellte physische Volume-Größe.

- **Autogrow**

  Zeigt an, ob das Volumen automatisch wächst, wenn es nicht mehr genügend Speicherplatz hat.

- * Raumgarantie*

  Zeigt die FlexVol-Lautstärkeregelung an, wenn ein Volume freie Blöcke aus einem Aggregat entfernt. Diese Blöcke sind dann garantiert für Schreibvorgänge auf Dateien im Volume verfügbar. Die Speicherplatzgarantie kann auf eine der folgenden gesetzt werden:

  - Keine

    Es wurde keine Speicherplatzzusage für das Volume konfiguriert.

  - Datei

    Die vollständige Größe von dünn geschriebenen Dateien (zum Beispiel LUNs) ist garantiert.

  - Datenmenge

    Die volle Größe des Volumens wird garantiert.

  - Teilweise

    Das FlexCache-Volume reserviert basierend auf seiner Größe Speicherplatz. Wenn die Größe des FlexCache-Volumes 100 MB oder mehr ist, ist die Mindestplatzgarantie standardmäßig auf 100 MB gesetzt. Wenn die Größe des FlexCache-Volumes weniger als 100 MB ist, wird die Mindestplatzgarantie auf die Größe des FlexCache-Volumes gesetzt. Wenn die Größe des FlexCache-Volumes später erhöht wird, wird die Mindestplatzgarantie nicht erhöht.

    Die Speicherplatzzusage ist ein Teil, wenn es sich um ein Volume vom Typ Data-Cache handelt.

- **Details (Physisch)**

  Zeigt die physischen Merkmale des Volumes an.

- **Gesamtkapazität**

  Zeigt die gesamte physische Kapazität im Volume an.

- **Datenkapazität**

  Zeigt den vom Volume genutzten physischen Speicherplatz (genutzte Kapazität) und die Menge an verfügbarem (freier Kapazität) physischen Speicherplatz im Volume an. Diese Werte werden auch als Prozentsatz der gesamten physischen Kapazität angezeigt.

  Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, wird die vom Volume verwendete Menge an Speicherplatz (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht verwendet werden kann (nicht nutzbare Kapazität), da die Kapazität des Aggregats angezeigt wird.

- **Snapshot Reserve**

  Zeigt die Menge an Speicherplatz an, der von den Snapshot Kopien verwendet (genutzte Kapazität) und die Menge an Speicherplatz, die für Snapshot Kopien verfügbar ist (freie Kapazität) im Volume an. Diese Werte werden auch als Prozentsatz der gesamten Snapshot-Reserve angezeigt.

  Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, dann wird die Menge an Speicherplatz, der von den Snapshot Kopien verwendet wird (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht für die Erstellung von Snapshot Kopien verwendet werden kann (nicht nutzbare Kapazität). Aufgrund von Aggregat-Kapazitätsproblemen wird angezeigt.

- **Volumenschwellwerte**

  Zeigt die folgenden Schwellenwerte für die Volume-Kapazität an:

  - Nahezu Vollständig. Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Volumen fast voll ist.

  - Vollständiger Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Volume voll ist.

- **Weitere Details**

  - Autogrow Maximalgröße

    Zeigt die maximale Größe an, bis die Lautstärke automatisch erweitert werden kann. Der Standardwert ist 120 % der Volume-Größe bei der Erstellung. Dieses Feld wird nur angezeigt, wenn Autogrow für das Volume aktiviert ist.

  - Der Qtree Kontingent Verplante Kapazität

    Zeigt den Speicherplatz an, der in den Quoten reserviert wurde.

  - Qtree-Kontingent Überbeansprucht Kapazität

Zeigt die Menge an Speicherplatz an, die verwendet werden kann, bevor das System das überverplante Ereignis des Volume Qtree-Kontingents generiert.

- Fraktionale Reserve

  Steuert die Größe der Überschreibungsreserve. Standardmäßig ist die fraktionale Reserve auf 100 festgelegt und gibt an, dass 100 Prozent des erforderlichen reservierten Speicherplatzes reserviert werden, damit die Objekte für Überschreibungen vollständig gesichert sind. Wenn die fraktionale Reserve weniger als 100 Prozent beträgt, wird der reservierte Speicherplatz für alle platzreservierten Dateien in diesem Volume auf den Prozentsatz der fraktionalen Reserve reduziert.

- Tägliche Snapshot Wachstumsrate

  Zeigt die Änderung an (in Prozent oder in KB, MB, GB usw.), die alle 24 Stunden in den Snapshot Kopien des ausgewählten Volumes stattfindet.

- Snapshot Tage voll belegt

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor der für die Snapshot Kopien im Volume reservierte Speicherplatz den angegebenen Schwellenwert erreicht.

  Das Feld „Snapshot Days to Full“ zeigt einen nicht anwendbaren Wert an, wenn das Wachstum der Snapshot-Kopien im Volume null oder negativ ist oder wenn es keine Daten zur Berechnung der Wachstumsrate gibt.

- Snapshot Automatisch Löschen

  Gibt an, ob Snapshot Kopien automatisch in freien Speicherplatz gelöscht werden, wenn ein Schreibvorgang auf ein Volume aufgrund von fehlendem Speicherplatz im Aggregat ausfällt.

- Snapshots

  Zeigt Informationen über die Snapshot-Kopien im Volume an.

  Die Anzahl der Snapshot Kopien auf dem Volume wird als Link angezeigt. Wenn Sie auf den Link klicken, werden die Snapshot Kopien in dem Dialogfeld Volume geöffnet, in dem Details zu den Snapshot Kopien angezeigt werden.

Die Anzahl der Snapshot Kopien wird etwa jede Stunde aktualisiert. Die Liste der Snapshot-Kopien wird jedoch zu dem Zeitpunkt aktualisiert, zu dem Sie auf das Symbol klicken. Dies kann zu einem Unterschied zwischen der in der Topologie angezeigten Anzahl der Snapshot Kopien und der Anzahl der aufgelisteten Snapshot Kopien führen, wenn Sie auf das Symbol klicken.

- **Volume Move**

  Zeigt den Status der aktuellen oder der letzten Volume-Verschiebung an, die am Volume durchgeführt wurde, und weitere Details an, z. B. die aktuelle Phase der Verschiebung eines Volumes – im Gange ist, das Quellaggregat, das Zielaggregat, die Startzeit, die Endzeit, Und die geschätzte Endzeit.

  Zeigt außerdem die Anzahl der Vorgänge zum Verschieben von Volumes an, die auf dem ausgewählten Volume ausgeführt werden. Weitere Informationen über die Vorgänge zum Verschieben von Volumes erhalten Sie, indem Sie auf den Link **Protokoll zum Verschieben von Volumes** klicken.

„Effizienz“

Die Registerkarte „Effizienz“ zeigt Informationen über den in den Volumes gespeicherten Speicherplatz mithilfe von Storage-Effizienzfunktionen wie Deduplizierung, Komprimierung und FlexClone Volumes an.

- **Deduplizierung**
  - Aktiviert

    Gibt an, ob die Deduplizierung auf einem Volume aktiviert oder deaktiviert ist.

  - Speicherersparnis

    Zeigt die Menge an gespeichertem Speicherplatz (in Prozent oder in KB, MB, GB usw.) in einem Volume mithilfe der Deduplizierung an.

  - Letzter Lauf

    Zeigt die Zeit an, die seit dem letzten Deduplizierungsvorgang verstrichen ist. Außerdem gibt an, ob der Deduplizierungsvorgang erfolgreich war.

  Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, der den Zeitpunkt der Durchführung des Vorgangs darstellt.

  - Modus

    Gibt an, ob der auf einem Volume aktivierte Deduplizierungsvorgang ein manueller, geplanter oder richtlinienbasierter Vorgang ist. Wenn der Modus auf „geplant“ eingestellt ist, wird der Betriebsplan angezeigt, und wenn der Modus auf eine Richtlinie festgelegt ist, wird der Richtlinienname angezeigt.

  - Status

    Zeigt den aktuellen Status des Deduplizierungsvorgangs an. Der Status kann „Idle“, „Initialisieren“, „aktiv“, „Rückgängig“, „Ausstehend“, „Ausstehend“ sein. Downgrade oder deaktiviert.

  - Typ

    Gibt den Typ des Deduplizierungsvorgangs an, der auf dem Volume ausgeführt wird. Wenn das Volume eine SnapVault-Beziehung hat, wird als SnapVault angezeigt. Für jedes andere Volumen wird der Typ als normal angezeigt.

- **Komprimierung**
  - Aktiviert

    Gibt an, ob die Komprimierung auf einem Volume aktiviert oder deaktiviert ist.

  - Speicherersparnis

    Zeigt den eingesparten Speicherplatz (in Prozent oder in KB, MB, GB usw.) in einem Volume mithilfe der Komprimierung an.

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration werden Details zum ausgewählten Volume angezeigt, z. B. Richtlinie für den Export, RAID-Typ, Kapazität und Storage-Effizienz-Funktionen des Volumes:

- **Übersicht**
  - Vollständiger Name

    Zeigt den vollständigen Namen des Volumes an.

  - Aggregate

    Zeigt den Namen des Aggregats, auf dem sich das Volume befindet, oder die Anzahl der Aggregate an, auf denen sich das FlexGroup Volume befindet.

  - Tiering-Richtlinie

    Zeigt die Tiering-Richtlinie für das Volume an; wenn das Volume auf einem FabricPool-fähigen Aggregat implementiert wird. Die Richtlinie kann „Keine“, „nur Snapshot“, „Backup“ oder „automatisch“ lauten.

  - Storage Virtual Machine

    Zeigt den Namen der Storage Virtual Machine (SVM) an, die das Volume enthält.

  - Verbindungspfad

    Zeigt den Status des Pfads an, der aktiv oder inaktiv sein kann. Der Pfad in der SVM, auf den das Volume angehängt ist, wird ebenfalls angezeigt. Sie können auf den Link **Verlauf** klicken, um die letzten fünf Änderungen am Verbindungspfad anzuzeigen.

  - Exportrichtlinie

    Zeigt den Namen der Exportrichtlinie an, die für das Volume erstellt wurde. Über den Link können Sie Details zu den Exportrichtlinien, den Authentifizierungsprotokollen und den aktivierten Zugriff auf die Volumes anzeigen, die zu der SVM gehören.

  - Stil

    Zeigt den Volumenstil an. Der Volume-Stil kann FlexVol oder FlexGroup sein.

  - Typ

    Zeigt den Typ des ausgewählten Volumens an. Der Volume-Typ kann Lese-/Schreibvorgänge, Lastverteilung, Datensicherung, Daten-Cache oder temporär sein.

  - RAID-Typ

    Zeigt den RAID-Typ des ausgewählten Volumes an. Der RAID-Typ kann RAID0, RAID4, RAID-DP oder RAID-TEC sein.

    > Es können mehrere RAID-Typen für FlexGroup Volumes angezeigt werden, da sich die zusammengehörigen Volumes für FlexGroups auf Aggregaten unterschiedlicher Typen sein können.

  - SnapLock-Typ

    Zeigt den SnapLock-Typ des Aggregats an, der das Volume enthält.

- SnapLock Expiry

  Zeigt das Ablaufdatum des SnapLock-Volume an.

- * Kapazität*
  - Thin Provisioning

    Zeigt an, ob Thin Provisioning für das Volume konfiguriert ist.

  - Autogrow

    Zeigt an, ob das flexible Volume automatisch innerhalb eines Aggregats wächst.

  - Snapshot Automatisch Löschen

    Gibt an, ob Snapshot Kopien automatisch in freien Speicherplatz gelöscht werden, wenn ein Schreibvorgang auf ein Volume aufgrund von fehlendem Speicherplatz im Aggregat ausfällt.

  - Kontingente

    Gibt an, ob die Quoten für das Volume aktiviert sind.

- * Effizienz*
  - Deduplizierung

    Gibt an, ob die Deduplizierung für das ausgewählte Volume aktiviert oder deaktiviert ist.

  - Komprimierung

    Gibt an, ob die Komprimierung für das ausgewählte Volume aktiviert oder deaktiviert ist.

- **Schutz**
  - Snapshots

    Gibt an, ob die automatischen Snapshot Kopien aktiviert oder deaktiviert sind.

Registerkarte „Schutz“

Auf der Registerkarte Schutz werden Sicherungsdetails zum ausgewählten Volume angezeigt, z. B. Verzögerungsinformationen, Beziehungstyp und Topologie der Beziehung.

- **Zusammenfassung**

  Zeigt die Eigenschaften von SnapMirror- und SnapVault-Beziehungen für ein ausgewähltes Volume an. Für einen anderen Beziehungstyp wird nur die Eigenschaft Beziehungstyp angezeigt. Wenn ein primäres Volume ausgewählt wird, werden nur die Richtlinie für verwaltete und lokale Snapshot-Kopien angezeigt. Für SnapMirror und SnapVault Beziehungen werden folgende Eigenschaften angezeigt:

  - Quell-Volume

    Zeigt den Namen der Quelle des ausgewählten Volumes an, wenn das ausgewählte Volume ein Ziel ist.

  - Verzögerungsstatus

Zeigt den Status der Update- oder Transferverzögerungen für eine Schutzbeziehung an. Der Status kann „Fehler“, „Warnung“ oder „kritisch“ sein.

Der lag-Status gilt nicht für synchrone Beziehungen.

◦ Verzögerungsdauer

Zeigt die Zeit an, mit der die Daten auf dem Spiegel hinter der Quelle liegen.

◦ Letzte Erfolgreiche Aktualisierung

Zeigt Datum und Uhrzeit der letzten erfolgreichen Schutzaktualisierung an.

Die letzte erfolgreiche Aktualisierung gilt nicht für synchrone Beziehungen.

◦ Storage Service-Mitglied

Zeigt entweder Ja oder Nein an, um anzugeben, ob das Volume zu einem Storage-Service gehört und von diesem gemanagt wird.

◦ Versionsflexible Replizierung

Zeigt entweder Ja, Ja mit Sicherungsoption oder Keine an. Ja zeigt an, dass die SnapMirror Replizierung möglich ist, auch wenn auf Quell- und Ziel-Volumes unterschiedliche Versionen der ONTAP Software ausgeführt werden. Ja, mit der Backup-Option bezeichnet die Implementierung von SnapMirror Sicherung mit der Möglichkeit, mehrere Versionen von Backup-Kopien auf dem Zielsystem aufzubewahren. Keine gibt an, dass die Version Flexible Replikation nicht aktiviert ist.

◦ Beziehungsfähigkeit

Zeigt die ONTAP-Funktionen an, die für die Sicherungsbeziehung verfügbar sind.

◦ Protection Service

Zeigt den Namen des Schutzdienstes an, wenn die Beziehung von einer Schutzpartneranwendung verwaltet wird.

◦ Beziehungstyp

Zeigt alle Beziehungstypen an, einschließlich Asynchronous Mirror, Asynchronous Vault, StrictSync und Sync.

◦ Beziehungsstatus

Zeigt den Status der SnapMirror oder SnapVault Beziehung an. Der Staat kann ohne Initialisierung, SnapMirrored oder Abbruch erfolgen. Wenn ein Quell-Volume ausgewählt ist, ist der Beziehungsstatus nicht zutreffend und wird nicht angezeigt.

◦ Übertragungsstatus

Zeigt den Übertragungsstatus der Schutzbeziehung an. Der Übertragungsstatus kann einer der folgenden Werte sein:

▪ Wird Abgebrochen

SnapMirror-Transfers sind aktiviert; ein Vorgang, bei dem der Transfer abgebrochen wird, während

das Checkpoint entfernt wird.

- Prüfen

  Das Zielvolumen wird einer Diagnose-Prüfung unterzogen und es wird keine Übertragung durchgeführt.

- Abschließen

  SnapMirror Transfers sind aktiviert. Das Volume befindet sich derzeit in der Phase nach dem Transfer für inkrementelle SnapVault Transfers.

- Leerlauf

  Transfers sind aktiviert, und es wird keine Übertragung durchgeführt.

- Synchronisiert

  Die Daten in den beiden Volumes in der synchronen Beziehung werden synchronisiert.

- Out-of-Sync

  Die Daten im Ziel-Volume werden nicht mit dem Quell-Volume synchronisiert.

- Vorbereitung

  SnapMirror Transfers sind aktiviert. Das Volume befindet sich derzeit in der Phase vor der Übertragung für inkrementelle SnapVault Transfers.

- Warteschlange

  SnapMirror Transfers sind aktiviert. Es werden keine Transfers durchgeführt.

- Stillgelegt

  SnapMirror Transfers sind deaktiviert. Es wird keine Übertragung durchgeführt.

- Wird Stillgelegt

  Ein SnapMirror Transfer läuft. Zusätzliche Transfers sind deaktiviert.

- Übertragung

  SnapMirror Transfers sind aktiviert, und ein Transfer läuft.

- Übergang

  Der asynchrone Datentransfer aus dem Quell- zum Ziel-Volume ist abgeschlossen, und der Übergang zum synchronen Betrieb wurde gestartet.

- Warten

  Ein SnapMirror Transfer wurde initiiert, aber einige zugehörige Aufgaben warten darauf, in die Warteschlange verschoben zu werden.

◦ Max. Übertragungsrate

Zeigt die maximale Übertragungsrate für die Beziehung an. Die maximale Übertragungsrate kann ein numerischer Wert in Kilobyte pro Sekunde (Kbit/s), Megabyte pro Sekunde (Mbit/s), Gigabyte pro Sekunde (Gbit/s) oder Terabyte pro Sekunde (Tbit/s) sein. Wenn kein Limit angezeigt wird, ist die Basistransfer zwischen Beziehungen unbegrenzt.

- SnapMirror Richtlinie

  Zeigt die Schutzrichtlinie für das Volume an. DPStandard gibt die standardmäßige Richtlinie für den Schutz der asynchronen Spiegelung an, und XDPStandard gibt die standardmäßige asynchrone Vault-Richtlinie an. StrictSync gibt die standardmäßige Richtlinie für den synchronen strengen Schutz an, und Sync gibt die standardmäßige synchrone Richtlinie an. Sie können auf den Richtliniennamen klicken, um die mit dieser Richtlinie verknüpften Details anzuzeigen, einschließlich der folgenden Informationen:

  - Übertragungspriorität
  - Einstellung der Zugriffszeit ignorieren
  - Limit für Versuche
  - Kommentare
  - SnapMirror-Labels
  - Aufbewahrungseinstellungen
  - Tatsächliche Snapshot Kopien
  - Bewahren Sie Snapshot Kopien auf
  - Schwellenwert für Warnung bei Aufbewahrung
  - Snapshot-Kopien ohne Aufbewahrungseinstellungen in einer kaskadierenden SnapVault-Beziehung, wobei die Quelle ein Datensicherungs-Volume (DP) ist, gilt nur die Regel „`sm_created`“.

- Zeitplan Aktualisieren

  Zeigt den SnapMirror Zeitplan an, der der Beziehung zugewiesen ist. Wenn Sie den Cursor über das Informationssymbol positionieren, werden die Terminplandetails angezeigt.

- Lokale Snapshot-Richtlinie

  Zeigt die Snapshot Kopie-Richtlinie für das Volume an. Die Richtlinie ist Standard, Keine oder ein beliebiger Name, der einer benutzerdefinierten Richtlinie zugewiesen wurde.

- **Ausblick**

  Zeigt die Schutztopologie des ausgewählten Volumes an. Die Topologie enthält grafische Darstellungen aller Volumes, die sich auf das ausgewählte Volume beziehen. Das ausgewählte Volumen wird durch einen dunkelgrauen Rahmen angezeigt, und Linien zwischen Volumes in der Topologie geben den Schutzbeziehungstyp an. Die Richtung der Beziehungen in der Topologie wird von links nach rechts angezeigt, wobei die Quelle jeder Beziehung auf der linken Seite und das Ziel auf der rechten Seite.

  Doppelte Fett gedruckte Zeilen geben eine asynchrone Spiegelbeziehung an, eine einzelne, fettgedruckte Zeile gibt eine asynchrone Vault-Beziehung an, und eine fettgedruckte Zeile und eine nicht-bold-Zeile gibt eine synchrone Beziehung an. Die folgende Tabelle gibt an, ob die Beziehung StrictSync oder Sync ist.

  Durch Klicken mit der rechten Maustaste auf ein Volume wird ein Menü angezeigt, aus dem Sie entweder das Volume schützen oder Daten darauf wiederherstellen können. Mit der rechten Maustaste auf eine

Beziehung klicken wird ein Menü angezeigt, aus dem Sie entweder bearbeiten, abbrechen, stilllegen, brechen, entfernen, Oder nehmen Sie eine Beziehung wieder auf.

Die Menüs werden in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
- Wenn es sich um ein FlexGroup Volume handelt
- Wenn sich das Volume in einer synchronen Schutzbeziehung befindet
- Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung vorliegt und das Ziel-Cluster noch nicht erkannt wurde, wird durch Klicken auf ein anderes Volume in der Topologie Informationen für das entsprechende Volume ausgewählt und angezeigt. Ein Fragezeichen ( ) In der linken oberen Ecke eines Volumens gibt an, dass entweder das Volumen fehlt oder es noch nicht entdeckt wurde. Sie können außerdem angeben, dass Kapazitätsinformationen nicht vorhanden sind. Wenn Sie den Mauszeiger über das Fragezeichen positionieren, werden weitere Informationen angezeigt, einschließlich Vorschläge für Korrekturmaßnahmen.

  In der Topologie werden Informationen zur Volume-Kapazität, Verzögerung, Snapshot-Kopien und zum letzten erfolgreichen Datentransfer angezeigt, wenn sie einer von mehreren gängigen Topologievorlagen entspricht. Wenn eine Topologie keiner dieser Vorlagen entspricht, werden Informationen zur Volume-Verzögerung und zum letzten erfolgreichen Datentransfer in einer Beziehungstabelle unter der Topologie angezeigt. In diesem Fall gibt die markierte Zeile in der Tabelle das ausgewählte Volume an, und in der Topologieansicht zeigen fettgedruckte Linien mit einem blauen Punkt die Beziehung zwischen dem ausgewählten Volume und seinem Quellvolumen an.

Topologieansichten umfassen folgende Informationen:

- Kapazität

  Zeigt die Gesamtkapazität des Volumes an. Wenn Sie den Cursor auf ein Volumen in der Topologie positionieren, werden im Dialogfeld Aktuelle Schwellenwerteinstellungen die aktuellen Warn- und kritischen Schwellwerte für dieses Volume angezeigt. Sie können die Schwellenwerteinstellungen auch bearbeiten, indem Sie im Dialogfeld Aktuelle Schwellenwerteinstellungen auf den Link **Schwellenwerte bearbeiten** klicken. Wenn Sie das Kontrollkästchen **Kapazität** deaktivieren, werden alle Kapazitätsinformationen für alle Volumes in der Topologie ausgeblendet.

- Verzögerung

  Zeigt die Verzögerungsdauer und den Verzögerungsstatus der eingehenden Schutzbeziehungen an. Wenn Sie das Kontrollkästchen **lag** deaktivieren, werden alle lag-Informationen für alle Volumes in der Topologie ausgeblendet. Wenn das Kontrollkästchen **lag** gedimmt ist, werden die Verzögerungsinformationen für das ausgewählte Volume in der Beziehungstabelle unter der Topologie sowie die lag-Informationen für alle zugehörigen Volumes angezeigt.

- Snapshot

  Zeigt die Anzahl der für ein Volume verfügbaren Snapshot Kopien an. Wenn Sie das Kontrollkästchen **Snapshot** deaktivieren, werden alle Snapshot Kopie-Informationen für alle Volumes in der Topologie ausgeblendet. Klicken auf das Symbol für die Snapshot Kopie ( ) Zeigt die Liste der Snapshot Kopien für ein Volume an. Die Anzahl der Snapshot Kopien neben dem Symbol wird ungefähr jede Stunde aktualisiert. Die Liste der Snapshot-Kopien wird jedoch beim Klicken auf das Symbol aktualisiert. Dies kann zu einem Unterschied zwischen der in der Topologie angezeigten Anzahl der Snapshot Kopien und der Anzahl der aufgelisteten Snapshot Kopien führen, wenn Sie auf

das Symbol klicken.

- Letzte Erfolgreiche Übertragung

  Zeigt den Betrag, die Dauer, die Zeit und das Datum der letzten erfolgreichen Datenübertragung an. Wenn das Kontrollkästchen **Letzter erfolgreicher Transfer** abgeblendet ist, werden die letzten erfolgreichen Übertragungsinformationen für das ausgewählte Volume in der Beziehungstabelle unter der Topologie sowie die letzten erfolgreichen Übertragungsinformationen für alle zugehörigen Volumes angezeigt.

- **Geschichte**

  Zeigt die Historie der eingehenden SnapMirror- und SnapVault-Sicherungsbeziehungen für das ausgewählte Volume in einem Diagramm an. Es sind drei Verlaufsdiagramme verfügbar: Die Dauer des eingehenden Beziehungsverzögerungsablaufs, die Dauer der eingehenden Beziehungstransfers und die Größe der eingehenden Beziehung, die übertragen wurde. Die Verlaufsdaten werden nur angezeigt, wenn Sie ein Zielvolume auswählen. Wenn Sie ein primäres Volume auswählen, sind die Diagramme leer und die Meldung `No data found` Wird angezeigt.

  Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Historische Grafiken können Ihnen bei der Identifizierung von Trends helfen: Wenn zum Beispiel große Datenmengen zur gleichen Zeit des Tages oder der Woche übertragen werden oder wenn der lag-Warn- oder lag-Fehlerschwellenwert konsistent verletzt wird, können Sie geeignete Maßnahmen ergreifen. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

  Sicherungsverlauf-Diagramme zeigen die folgenden Informationen an:

  - **Beziehungsdauer**

    Anzeige von Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Anzeige von Tagen, Monaten oder Jahren auf der horizontalen Achse (x), abhängig vom ausgewählten Zeitraum. Der obere Wert auf der Y-Achse gibt die maximale Verzögerungsdauer an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. In der orangefarbenen Linie im Diagramm wird der lag-Fehlerschwellenwert angezeigt, während die horizontale gelbe Linie den lag-Warnungsschwellenwert darstellt. Wenn Sie den Mauszeiger über diese Zeilen positionieren, wird die Schwellenwerteinstellung angezeigt. Die waagerechte blaue Linie zeigt die Verzögerungsdauer an. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen interessanten Bereich positionieren.

  - **Dauer Der Beziehungsübertragung**

    Anzeige von Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Anzeige von Tagen, Monaten oder Jahren auf der horizontalen Achse (x), abhängig vom ausgewählten Zeitraum. Der obere Wert auf der Y-Achse gibt die maximale Übertragungsdauer an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den Bereich von Interesse positionieren.

    > Dieses Diagramm ist nicht für Volumes verfügbar, die sich in synchronen Sicherungsbeziehungen befinden.

  - **Beziehung Übertragen Größe**

    Zeigt Bytes, Kilobyte, Megabyte usw. auf der vertikalen Achse (y) je nach Übertragungsgröße an und

zeigt Tage, Monate oder Jahre auf der horizontalen Achse (x) je nach ausgewähltem Zeitraum an. Der obere Wert auf der Y-Achse gibt die maximale Übertragungsgröße an, die im auf der x-Achse angezeigten Zeitraum erreicht wurde. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen interessanten Bereich positionieren.

Dieses Diagramm ist nicht für Volumes verfügbar, die sich in synchronen Sicherungsbeziehungen befinden.

Historienbereich

Im Bereich Verlauf werden Diagramme angezeigt, die Informationen über die Kapazität und die Platzreservierungen des ausgewählten Volumes enthalten. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

Diagramme sind möglicherweise leer und die Meldung `No data found` Wird angezeigt, wenn die Daten oder der Status des Volumes über einen Zeitraum hinweg unverändert bleiben.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Verlaufsdiagramme können Ihnen dabei helfen, Trends zu erkennen - wenn beispielsweise die Volumennutzung den Schwellenwert „nahezu voll“ konsistent überschreitet, können Sie entsprechende Maßnahmen ergreifen.

Verlaufsdiagramme zeigen folgende Informationen an:

- **Verwendete Volume-Kapazität**

  Zeigt die verwendete Kapazität im Volume und den Trend in der Art und Weise an, wie die Volume-Kapazität basierend auf dem Nutzungsverlauf verwendet wird, als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende zu „Volume Used Capacity“ klicken, wird die Zeile des Diagramms „Volume Used Capacity“ ausgeblendet.

- **Verwendete Volume-Kapazität vs Gesamt**

  Zeigt den Trend der Volume-Kapazität basierend auf dem Nutzungsverlauf sowie der verwendeten Kapazität, der Gesamtkapazität und den Details der Speicherersparnis durch Deduplizierung und Komprimierung an. Dies sind Liniendiagramme in Byte, Kilobyte, Megabyte, Und so weiter, auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „verwendete Trend-Kapazität“ klicken, wird das Diagramm „verwendete Trendkapazität“ ausgeblendet.

- **Verwendete Volume-Kapazität (%)**

  Zeigt die verwendete Kapazität im Volumen und den Trend in der Art und Weise an, wie die Volume-Kapazität basierend auf dem Nutzungsverlauf, als Liniendiagramme, in Prozent, auf der vertikalen (y) Achse verwendet wird. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu

bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende zu „Volume Used Capacity“ klicken, wird die Zeile des Diagramms „Volume Used Capacity“ ausgeblendet.

- **Verwendete Snapshot-Kapazität (%)**

  Zeigt den Schwellenwert für die Snapshot-Reserve und die Snapshot-Warnung als Liniendiagramme und die von den Snapshot Kopien verwendete Kapazität als Diagramm in Prozent auf der vertikalen Achse (y) an. Der Snapshot-Überlauf ist mit verschiedenen Farben dargestellt. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende der Snapshot Reserve klicken, wird die Grafik der Snapshot Reserve ausgeblendet.

Ereignisliste

In der Ereignisliste werden Details zu neuen und bestätigten Ereignissen angezeigt:

- **Severity**

  Zeigt den Schweregrad des Ereignisses an.

- **Veranstaltung**

  Zeigt den Ereignisnamen an.

- **Auslösezeit**

  Zeigt die Zeit an, die seit der Erzeugung des Ereignisses verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, zu dem das Ereignis generiert wurde.

Bereich „Verwandte Anmerkungen“

Im Bereich Verwandte Anmerkungen können Sie Anmerkungsdetails anzeigen, die mit dem ausgewählten Volume verknüpft sind. Die Details umfassen den Anmerkungsnamen und die Anmerkungswerte, die auf das Volumen angewendet werden. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie SVMs, Aggregate, qtrees, LUNs und Snapshot Kopien anzeigen und navigieren, die mit dem Volume zusammenhängen:

- **Storage Virtual Machine**

  Zeigt die Kapazität und den Integritätsstatus der SVM an, die das ausgewählte Volume enthält.

- * Aggregat*

  Zeigt die Kapazität und den Integritätsstatus des Aggregats an, das das ausgewählte Volume enthält. Für FlexGroup Volumes wird die Anzahl der Aggregate aufgelistet, die die FlexGroup umfassen.

- **Volumen im Aggregat**

Zeigt die Anzahl und Kapazität aller Volumes an, die zum übergeordneten Aggregat des ausgewählten Volumes gehören. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt. Wenn beispielsweise ein Aggregat zehn Volumes enthält, von denen fünf den Warnstatus und die übrigen fünf den kritischen Status anzeigen, ist der angezeigte Status kritisch. Diese Komponente wird für FlexGroup-Volumes nicht angezeigt.

- **Qtrees**

  Zeigt die Anzahl der vom ausgewählten Volume enthaltenen qtrees sowie die Kapazität von qtrees mit Kontingent an, die das ausgewählte Volume enthält. Die Kapazität der qtrees mit Kontingent wird in Bezug auf die Volume-Datenkapazität angezeigt. Auf der Grundlage des höchsten Schweregrades wird auch der Integritätsstatus der qtrees angezeigt. Wenn ein Volume beispielsweise zehn qtrees, fünf mit Warnstatus und die verbleibenden fünf mit kritischem Status aufweist, ist der angezeigte Status kritisch.

- **NFS Exporte**

  Zeigt die Anzahl und den Status der NFS-Exporte an, die dem Volume zugeordnet sind.

- **CIFS-Freigaben**

  Zeigt die Anzahl und den Status der CIFS-Freigaben an.

- **LUNs**

  Zeigt die Anzahl und Gesamtgröße aller LUNs im ausgewählten Volume an. Auf der Grundlage des höchsten Schweregrades wird außerdem der Systemzustand der LUNs angezeigt.

- **Benutzer- und Gruppenquoten**

  Zeigt die Anzahl und den Status der Quoten für Benutzer und Benutzergruppen im Zusammenhang mit dem Volume und seinen qtrees an.

- **FlexClone Volumes**

  Zeigt die Anzahl und Kapazität aller geklonten Volumes des ausgewählten Volumes an. Anzahl und Kapazität werden nur angezeigt, wenn das ausgewählte Volume geklonte Volumes enthält.

- **Parent Volume**

  Zeigt den Namen und die Kapazität des übergeordneten Volume eines ausgewählten FlexClone Volume an. Das übergeordnete Volume wird nur angezeigt, wenn das ausgewählte Volume ein FlexClone Volume ist.

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ können Sie die Liste der Gruppen anzeigen, die dem ausgewählten Volume zugeordnet sind.

Bereich „Verwandte Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnmeldungen anzeigen, die für das ausgewählte Volume erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Detailseite „Systemzustand/Speicher-Virtual Machine“

Auf der Seite Systemzustand/Storage Virtual Machine-Details können Sie detaillierte Informationen zur ausgewählten SVM anzeigen, z. B. Systemzustand, Kapazität, Konfiguration, Datenrichtlinien, logische Schnittstellen (LIFs), LUNs, qtrees sowie Benutzer- und Gruppenkontingente. Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für die SVM anzeigen.

Es können nur Data SVMs überwacht werden.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für die ausgewählte SVM ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Hiermit können Sie zur Detailseite zu Performance/SVM navigieren.

- **Aktionen**

  - Alarm Hinzufügen

    Hiermit können Sie eine Warnung zur ausgewählten SVM hinzufügen.

  - Schwellenwerte Bearbeiten

    Ermöglicht Ihnen das Bearbeiten der SVM-Schwellenwerte.

    Diese Schaltfläche ist nur aktiviert, wenn sie auf der Registerkarte qtrees oder für eine SVM mit Infinite Volume angezeigt wird.

  - Anmerkungen Hinzufügen

    Ermöglicht Ihnen, die ausgewählte SVM zu kommentieren.

- **Storage Virtual Machines Anzeigen**

  Hier können Sie zur Seite „Health/Storage Virtual Machines Inventory“ navigieren.

Registerkarte Systemzustand

Auf der Registerkarte Systemzustand werden detaillierte Informationen zur Datenverfügbarkeit, Datenkapazität und Sicherung verschiedener Objekte wie Volumes, Aggregate, NAS LIFs, SAN LIFs, LUNs, angezeigt. Protokolle, Services, NFS-Exporte und CIFS-Freigaben.

Sie können auf das Diagramm eines Objekts klicken, um die gefilterte Liste der Objekte anzuzeigen. Beispielsweise können Sie auf das Diagramm für die Volume-Kapazität klicken, das Warnungen anzeigt, um die Liste der Volumes mit Kapazitätsproblemen mit dem Schweregrad „Warnung“ anzuzeigen.

- **Verfügbarkeitsprobleme**

  Zeigt als Diagramm die Gesamtzahl der Objekte an, einschließlich Objekten mit Verfügbarkeitsproblemen und Objekten, die keine Probleme mit der Verfügbarkeit haben. Die Farben im Diagramm stellen die

verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Verfügbarkeitsproblemen, die sich auf die Verfügbarkeit von Daten in der SVM auswirken oder bereits davon betroffen sein können. Beispielsweise werden Informationen zu den NAS-LIFs und den SAN-LIFs angezeigt, die ausgefallen sind und die Volumes offline sind.

Sie können auch Informationen zu aktuell ausgeführten Protokollen und Services sowie zur Anzahl und dem Status von NFS-Exporten und CIFS-Freigaben anzeigen.

Wenn es sich bei der ausgewählten SVM um eine SVM mit Infinite Volume handelt, können Sie Verfügbarkeitsinformationen über das Infinite Volume anzeigen.

- **Kapazitätsprobleme**

  Zeigt als Diagramm die Gesamtzahl der Objekte an, einschließlich Objekten mit Kapazitätsproblemen und Objekten, die keine Kapazitätsprobleme haben. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die nachfolgende Grafik liefert Details zu Kapazitätsproblemen, die sich auf die Kapazität der Daten der SVM auswirken oder bereits beeinträchtigen können. Beispielsweise werden Informationen zu Aggregaten angezeigt, die mit hoher Wahrscheinlichkeit die festgelegten Schwellenwerte überschreiten.

  Wenn es sich bei der ausgewählten SVM um eine SVM mit Infinite Volume handelt, können Sie die Kapazitätsdetails über das Infinite Volume anzeigen.

- **Schutzprobleme**

  Er bietet eine schnelle Übersicht über den Schutz der SVM, indem die Gesamtzahl der Beziehungen, einschließlich Beziehungen mit Schutzproblemen und Beziehungen, bei denen keine Sicherungsprobleme auftreten, als Diagramm angezeigt werden. Wenn nicht geschützte Volumes vorhanden sind, führt ein Klick auf den Link zur Seite Systemzustand/Volumes-Inventar, auf der eine gefilterte Liste der nicht geschützten Volumes in der SVM angezeigt werden kann. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Durch Klicken auf ein Diagramm gelangen Sie zur Seite „Schutz/Volume-Beziehungen“, auf der eine gefilterte Liste mit Details zu den Schutzbeziehungen angezeigt werden kann. Die nachfolgenden Informationen enthalten Details zu Sicherungsproblemen, die sich auf den Schutz der Daten in der SVM auswirken oder bereits beeinträchtigen können. Beispielsweise werden Informationen über Volumes angezeigt, die eine Snapshot Kopie-Reserve haben, die fast voll ist, oder über Probleme mit der SnapMirror Beziehungs-Verzögerung.

  Wenn die ausgewählte SVM eine Repository-SVM ist, wird der Schutzbereich nicht angezeigt.

Registerkarte „Kapazität“

Auf der Registerkarte Kapazität werden ausführliche Informationen zur Datenkapazität der ausgewählten SVM angezeigt.

Folgende Informationen werden für eine SVM mit FlexVol-Volume oder FlexGroup-Volume angezeigt:

- * Kapazität*

  Im Kapazitätsbereich werden Details zur verwendeten und verfügbaren Kapazität angezeigt, die aus allen Volumes zugewiesen sind:

  - Gesamtkapazität

    Zeigt die Gesamtkapazität (in MB, GB usw.) der SVM an.

- Verwendet

  Zeigt den Speicherplatz an, der von Daten in den Volumes verwendet wird, die zur SVM gehören.

- Garantiert Verfügbar

  Zeigt den garantierten verfügbaren Speicherplatz für Daten an, die für Volumes in der SVM verfügbar sind.

- Nicht Garantiert

  Zeigt den verfügbaren Speicherplatz für Daten an, die in der SVM für Thin Provisioning Volumes zugewiesen sind.

- **Volumen mit Kapazitätsproblemen**

  Die Liste der Volumes mit Kapazitätsproblemen zeigt in tabellarischer Form Details zu den Volumes mit Kapazitätsproblemen an:

  - Status

    Zeigt an, dass das Volumen ein kapazitätsbezogenes Problem mit einem angezeigten Schweregrad hat.

    Sie können den Mauszeiger über den Status bewegen, um weitere Informationen zu dem kapazitätsbezogenen Ereignis oder den für das Volume generierten Ereignissen anzuzeigen.

    Wenn der Status des Volumes durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen wurde, und die Ursache des Ereignisses anzeigen. Sie können die Schaltfläche **Details anzeigen** verwenden, um weitere Informationen über die Veranstaltung anzuzeigen.

    Wenn der Status des Volumes durch mehrere Ereignisse desselben Schweregrades bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

    > Ein Volume kann mehrere Ereignisse desselben Schweregrades oder unterschiedlicher Schweregrade aufweisen. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Volume zwei Ereignisse mit Schweregraden für Fehler und Warnung enthält, wird nur der Schweregrad Fehler angezeigt.

  - Datenmenge

    Zeigt den Namen des Volumes an.

  - Genutzte Datenkapazität

    Zeigt als Diagramm Informationen zur Auslastung der Volume-Kapazität (in Prozent) an.

  - Tage voll

Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor das Volume die volle Kapazität erreicht.

- Thin Provisioning

  Zeigt an, ob die Platzgarantie für das ausgewählte Volume festgelegt ist. Gültige Werte sind Ja und Nein

- Aggregate

  Zeigt für FlexVol Volumes den Namen des Aggregats an, das das Volume enthält. Für FlexGroup-Volumes zeigt die Anzahl der Aggregate an, die in der FlexGroup verwendet werden.

Für eine SVM mit Infinite Volume werden folgende Informationen angezeigt:

- * Kapazität*

  Zeigt die folgenden kapazitätsbezogenen Details an:

  - Prozentsatz der genutzten und freien Datenkapazität
  - Prozentsatz der genutzten und freien Snapshot-Kapazität
  - Snapshot-Überlauf

    Zeigt den Speicherplatz an, der von den Snapshot Kopien verbraucht wird.

  - Verwendet

    Zeigt den Speicherplatz an, der von Daten in der SVM mit Infinite Volume genutzt wird.

  - Warnung

    Zeigt an, dass der Speicherplatz in der SVM mit Infinite Volume fast voll ist. Wird diese Schwelle nicht erreicht, wird das Ereignis „Space Fast Full“ generiert.

  - Fehler

    Zeigt an, dass der Speicherplatz in der SVM mit Infinite Volume, falls voll, verfügbar ist. Wird dieser Schwellenwert nicht erreicht, wird das Ereignis „Space Full“ generiert.

- **Weitere Details**
  - Gesamtkapazität

    Zeigt die Gesamtkapazität in der SVM mit Infinite Volume an.

  - Datenkapazität

    Zeigt die genutzte Datenkapazität, verfügbare Datenkapazität und Details zur Snapshot Überlaufkapazität der SVM mit Infinite Volume an.

  - Snapshot-Reserve

    Zeigt die verwendeten und freien Details der Snapshot-Reserve an.

  - Systemkapazität

Zeigt die genutzte Systemkapazität und die verfügbare Systemkapazität der SVM mit Infinite Volume an.

- Schwellenwerte

  Zeigt die nahezu vollständigen und vollständigen Schwellenwerte der SVM mit Infinite Volume an.

- **Storage Class Capacity Details**

  Zeigt Informationen zur Kapazitätsauslastung in Ihren Speicherklassen an. Diese Informationen werden nur angezeigt, wenn Sie Storage-Klassen für Ihre SVM mit Infinite Volume konfiguriert haben.

- **Storage Virtual Machine Storage Class Schwellenwerte**

  Zeigt die folgenden Schwellenwerte (in Prozent) Ihrer Speicherklassen an:

  - Nahezu Vollständig. Schwellenwert

    Gibt den Prozentsatz an, bei dem eine Storage-Klasse in einer SVM mit Infinite Volume als nahezu voll erachtet wird.

  - Vollständiger Schwellenwert

    Gibt den Prozentsatz an, bei dem die Storage-Klasse in einer SVM mit Infinite Volume als voll erachtet wird.

  - Limit Der Snapshot-Nutzung

    Gibt das Limit in Prozent im Speicherplatz an, der für Snapshot Kopien in der Storage-Klasse reserviert ist.

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration werden Konfigurationsdetails zu der ausgewählten SVM, z. B. Cluster, Root-Volume, die enthaltenen Volumes (Infinite Volume oder FlexVol Volumes) und die auf der SVM erstellten Richtlinien angezeigt:

- **Übersicht**
  - Cluster

    Zeigt den Namen des Clusters an, zu dem die SVM gehört.

  - Zulässiger Volume-Typ

    Zeigt den Typ der Volumes an, die in der SVM erstellt werden können. Der Typ kann InfiniteVol, FlexVol oder FlexVol/FlexGroup sein.

  - Root-Volume

    Zeigt den Namen des Root-Volumes der SVM an.

  - Zulässige Protokolle

    Zeigt den Typ der Protokolle an, die für die SVM konfiguriert werden können. Außerdem gibt an, ob ein Protokoll aktiv ist ( ), unten ( ), oder ist nicht konfiguriert ( ).

- **Daten-LIFs**
  - NAS

    Zeigt die Anzahl der NAS-LIFs an, die der SVM zugeordnet sind. Außerdem gibt an, ob die LIFs aktiv sind (Oder runter ().

  - San

    Zeigt die Anzahl der SAN-LIFs an, die der SVM zugeordnet sind. Außerdem gibt an, ob die LIFs aktiv sind (Oder runter ().

  - FC-NVMe

    Zeigt die Anzahl der FC-NVMe LIFs an, die der SVM zugeordnet sind. Außerdem gibt an, ob die LIFs aktiv sind (Oder runter ().

  - Verbindungspfad

    Zeigt den Pfad an, auf dem das Infinite Volume gemountet ist. Für eine SVM wird nur ein Verbindungspfad mit Infinite Volume angezeigt.

  - Speicherklassen

    Zeigt die Storage-Klassen an, die der ausgewählten SVM mit Infinite Volume zugeordnet sind. Es werden nur Storage-Klassen für eine SVM mit Infinite Volume angezeigt.

- **Management-LIFs**
  - Gesteigerte

    Zeigt die Anzahl der Management-LIFs an, die der SVM zugeordnet sind. Außerdem gibt an, ob die Management-LIFs aktiv sind (Oder runter ().

- **Richtlinien**
  - Snapshots

    Zeigt den Namen der Snapshot-Richtlinie an, die auf der SVM erstellt wurde.

  - Exportrichtlinien

    Zeigt entweder den Namen der Exportrichtlinie an, wenn eine einzelne Richtlinie erstellt wird, oder zeigt die Anzahl der Exportrichtlinien an, wenn mehrere Richtlinien erstellt werden.

  - Datenrichtlinie

    Zeigt an, ob eine Datenrichtlinie für die ausgewählte SVM mit Infinite Volume konfiguriert ist.

- **Services**
  - Typ

    Zeigt den Service-Typ an, der für die SVM konfiguriert ist. Der Typ kann Domain Name System (DNS) oder Network Information Service (NIS) sein.

  - Bundesland

Zeigt den Status des Dienstes an, der aktiv sein kann ( ), Down ( ), oder nicht konfiguriert ( ).

- Domain-Name

  Zeigt die vollständig qualifizierten Domänennamen (FQDNs) des DNS-Servers für die DNS-Dienste oder NIS-Server für die NIS-Dienste an. Wenn der NIS-Server aktiviert ist, wird der aktive FQDN des NIS-Servers angezeigt. Wenn der NIS-Server deaktiviert ist, wird die Liste aller FQDNs angezeigt.

- IP-Adresse

  Zeigt die IP-Adressen des DNS- oder NIS-Servers an. Wenn der NIS-Server aktiviert ist, wird die aktive IP-Adresse des NIS-Servers angezeigt. Wenn der NIS-Server deaktiviert ist, wird die Liste aller IP-Adressen angezeigt.

Registerkarte LIFs

Die Registerkarte LIFs zeigt Details zu den Daten-LIFs an, die auf der ausgewählten SVM erstellt wurden:

- **LIF**

  Zeigt den Namen der logischen Schnittstelle an, die auf der ausgewählten SVM erstellt wird.

- **Betriebsstatus**

  Zeigt den Betriebsstatus der logischen Schnittstelle an. Diese kann im aktiv sein ( ), Down (Oder Unbekannt ( ). Der Betriebsstatus einer logischen Schnittstelle wird vom Status ihrer physischen Ports bestimmt.

- **Verwaltungsstatus**

  Zeigt den Administrationsstatus der logischen Schnittstelle an. Dieser kann im aktiv sein ( ), Down (Oder Unbekannt ( ). Der Administrationsstatus einer LIF wird vom Storage-Administrator gesteuert, um Änderungen an der Konfiguration oder zu Wartungszwecken vorzunehmen. Der Administrationsstatus kann sich vom Betriebsstatus unterscheiden. Wenn jedoch der Administrationsstatus eines LIF „Inaktiv“ lautet, ist der Betriebsstatus standardmäßig „Inaktiv“.

- **IP-Adresse / WWPN**

  Zeigt die IP-Adresse für Ethernet LIFs und den World Wide Port Name (WWPN) für FC LIFs an.

- **Protokolle**

  Zeigt die Liste der für das LIF angegebenen Datenprotokolle an, z. B. CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe und FlexCache. Bei Infinite Volume sind die SAN-Protokolle nicht anwendbar.

- * Rolle*

  Zeigt die LIF-Rolle an. Die Rollen können Daten oder Management sein.

- * Home Port*

  Zeigt den physischen Port an, dem die LIF ursprünglich zugeordnet war.

- **Aktueller Port**

  Zeigt den physischen Port an, dem das LIF derzeit zugeordnet ist. Wenn das LIF migriert wird,

unterscheidet sich der aktuelle Port möglicherweise vom Home Port.

- **Portsatz**

  Zeigt den Port-Satz an, dem das LIF zugeordnet ist.

- **Failover-Richtlinie**

  Zeigt die für das LIF konfigurierte Failover-Richtlinie an. Für LIFs für NFS, CIFS und FlexCache ist die standardmäßige Failover-Richtlinie Next verfügbar. Failover-Richtlinie gilt nicht für FC- und iSCSI-LIFs.

- **Routing-Gruppen**

  Zeigt den Namen der Routinggruppe an. Sie können weitere Informationen zu den Routen und dem Ziel-Gateway anzeigen, indem Sie auf den Namen der Routinggruppe klicken.

  Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt. Daher wird für diese Cluster eine leere Spalte angezeigt.

- **Failover-Gruppe**

  Zeigt den Namen der Failover-Gruppe an.

Registerkarte „qtrees“

Auf der Registerkarte qtrees werden Details zu qtrees und ihren Kontingenten angezeigt. Sie können auf die Schaltfläche **Schwellenwerte bearbeiten** klicken, wenn Sie die gesundheitlichen Schwellenwerte für qtree-Kapazität für eine oder mehrere qtrees bearbeiten möchten.

Verwenden Sie die Schaltfläche **Exportieren**, um einen kommagetrennten Wert zu erstellen (`.csv`) Datei mit den Details aller überwachten qtrees. Beim Export in eine CSV-Datei können Sie wahlweise einen qtrees-Bericht für die aktuelle SVM, für alle SVMs im aktuellen Cluster oder alle SVMs für alle Cluster in Ihrem Datacenter erstellen. In der exportierten CSV-Datei werden einige zusätzliche Felder „qtrees“ angezeigt.

Die Registerkarte „qtrees“ wird für eine SVM mit Infinite Volume nicht angezeigt.

- **Status**

  Zeigt den aktuellen Status des qtree an. Der Status kann kritisch sein (), Fehler (), Warnung (Oder normal ().

  Sie können den Mauszeiger über das Statussymbol bewegen, um weitere Informationen zu dem für den qtree generierten Ereignis oder Ereignissen anzuzeigen.

  Wenn der Status des qtree durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Sie können **Details anzeigen** verwenden, um weitere Informationen über die Veranstaltung anzuzeigen.

  Wenn der Status des qtree durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch **Alle Ereignisse anzeigen** verwenden, um die Liste der generierten Ereignisse anzuzeigen.

Ein qtree kann mehrere Ereignisse des gleichen Schweregrads oder unterschiedlicher Schweregrade aufweisen. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn ein qtree z. B. zwei Ereignisse mit Schweregraden für Fehler und Warnung hat, wird nur der Schweregrad „Fehler“ angezeigt.

- **Qtree**

  Zeigt den Namen des qtree an.

- * Cluster*

  Zeigt den Namen des Clusters an, der den qtree enthält. Wird nur in der exportierten CSV-Datei angezeigt.

- **Storage Virtual Machine**

  Zeigt den Namen der Storage Virtual Machine (SVM) an, die den qtree enthält. Wird nur in der exportierten CSV-Datei angezeigt.

- **Lautstärke**

  Zeigt den Namen des Volume an, das den qtree enthält.

  Sie können den Zeiger über den Volume-Namen verschieben, um weitere Informationen zum Volume anzuzeigen.

- **Quota Set**

  Gibt an, ob ein Kontingent aktiviert oder auf dem qtree deaktiviert ist.

- **Quotentyp**

  Gibt an, ob das Kontingent für einen Benutzer, eine Benutzergruppe oder einen qtree ist. Wird nur in der exportierten CSV-Datei angezeigt.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Für jeden Benutzer und jede Benutzergruppe werden mehrere Zeilen angezeigt. Wenn der Kontingenttyp qtree ist oder nicht festgelegt ist, ist die Spalte leer. Wird nur in der exportierten CSV-Datei angezeigt.

- **Verwendete Festplatte %**

  Zeigt den Prozentsatz des verwendeten Festplattenspeichers an. Wenn ein Festplattenlimit festgelegt ist, basiert dieser Wert auf dem Festplattenlimit. Wenn das Kontingent ohne Festplattenlimit festgelegt wird, basiert der Wert auf dem Volume-Datenraum. Wenn das Kontingent nicht festgelegt ist oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört, wird „`not anwendbare`“ auf der Grid-Seite angezeigt und das Feld in den CSV-Exportredaten leer ist.

- **Festplatten-Hard-Limit**

  Zeigt die maximale Menge an Festplattenspeicher an, die für den qtree zugewiesen ist. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht wird und keine weiteren Festplattenschreibvorgänge mehr zulässig sind. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein Festplattenlimit gesetzt wird, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört.

- **Soft Limit Für Festplatten**

  Zeigt die Menge an Festplattenspeicher an, die dem qtree zugewiesen ist, bevor ein Warnereignis generiert wird. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein Disk-Softlimit gesetzt wird, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört. Standardmäßig ist diese Spalte ausgeblendet.

- **Datenträgerschwellenwert**

  Zeigt den Schwellenwert an, der für den Festplattenspeicher festgelegt wurde. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein Festplattenschwellenwert eingestellt ist, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im qtree verwendeten Dateien an. Wenn das harte Limit für die Datei festgelegt ist, basiert dieser Wert auf dem harten Limit der Datei. Es wird kein Wert angezeigt, wenn das Kontingent ohne harte Dateibegrenzung festgelegt ist. Wenn das Kontingent nicht festgelegt ist oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört, wird „`not anwendbare`“ auf der Grid-Seite angezeigt und das Feld in den CSV-Exportredaten leer ist.

- **Harte Dateibegrenzung**

  Zeigt das endgültige Limit für die Anzahl der Dateien an, die auf den qtrees zulässig sind. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne eine feste Dateibegrenzung festgelegt wird, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört.

- **Soft Limit Für Dateien**

  Zeigt den Softlimit für die Anzahl der Dateien an, die auf qtrees zulässig sind. Der Wert wird für die folgenden Bedingungen als „`Unlimited`“ angezeigt: Wenn das Kontingent ohne ein Datei-Softlimit gesetzt wird, wenn das Kontingent nicht festgelegt ist, oder wenn Quoten auf dem Volumen deaktiviert sind, zu dem der qtree gehört. Standardmäßig ist diese Spalte ausgeblendet.

Registerkarte „Benutzer- und Gruppenkontingente“

Zeigt Details zu den Quoten für Benutzer und Benutzergruppen für die ausgewählte SVM an. Sie können Informationen wie den Status des Kontingents, den Namen des Benutzers oder der Benutzergruppe, die auf den Festplatten und Dateien festgelegten Soft- und Hard-Limits, den Speicherplatz und die Anzahl der verwendeten Dateien sowie den Schwellenwert für die Festplatte anzeigen. Sie können auch die E-Mail-Adresse ändern, die einem Benutzer oder einer Benutzergruppe zugeordnet ist.

- **Schaltfläche 'Email-Adresse bearbeiten'**

  Öffnet das Dialogfeld E-Mail-Adresse bearbeiten, in dem die aktuelle E-Mail-Adresse des ausgewählten Benutzers oder der ausgewählten Benutzergruppe angezeigt wird. Sie können die E-Mail-Adresse ändern. Wenn das Feld**E-Mail-Adresse bearbeiten** leer ist, wird die Standardregel verwendet, um eine E-Mail-Adresse für den ausgewählten Benutzer oder die ausgewählte Benutzergruppe zu generieren.

  Wenn mehrere Benutzer das gleiche Kontingent haben, werden die Namen der Benutzer als kommagetrennte Werte angezeigt. Außerdem wird die Standardregel nicht verwendet, um die E-Mail-Adresse zu generieren; Sie müssen daher die erforderliche E-Mail-Adresse angeben, damit

Benachrichtigungen gesendet werden können.

- **Schaltfläche E-Mail-Regeln konfigurieren**

  Mit dieser Option können Sie Regeln erstellen oder ändern, um eine E-Mail-Adresse für die auf der SVM konfigurierten Benutzer- oder Benutzergruppen-Quoten zu generieren. Bei einer Quota-Verletzung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

- **Status**

  Zeigt den aktuellen Status des Kontingents an. Der Status kann kritisch sein ( ), Warnung (Oder normal ( ).

  Sie können den Zeiger über das Statussymbol verschieben, um weitere Informationen über das Ereignis oder die Ereignisse anzuzeigen, die für das Kontingent generiert wurden.

  Wenn der Status des Kontingents durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugeordnet ist, und die Ursache des Ereignisses anzeigen. Sie können **Details anzeigen** verwenden, um weitere Informationen über die Veranstaltung anzuzeigen.

  Wenn der Status des Kontingents durch mehrere Ereignisse desselben Schweregrades bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum angezeigt, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch **Alle Ereignisse anzeigen** verwenden, um die Liste der generierten Ereignisse anzuzeigen.

  > Eine Quote kann mehrere Ereignisse desselben Schweregrades oder unterschiedlicher Schweregrade haben. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Kontingent zwei Ereignisse mit Schweregraden für Fehler und Warnung enthält, wird nur der Schweregrad „Fehler“ angezeigt.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Wenn mehrere Benutzer das gleiche Kontingent haben, werden die Namen der Benutzer als kommagetrennte Werte angezeigt.

  Der Wert wird als „`Unbekannt`“ angezeigt, wenn ONTAP aufgrund von SECD-Fehlern keinen gültigen Benutzernamen liefert.

- **Typ**

  Gibt an, ob das Kontingent für einen Benutzer oder eine Benutzergruppe gilt.

- **Volumen oder Qtree**

  Zeigt den Namen des Volume oder qtree an, auf dem das Benutzer- oder Benutzergruppenkontingent angegeben ist.

  Sie können den Mauszeiger über den Namen des Volume oder qtree bewegen, um weitere Informationen zum Volume oder qtree anzuzeigen.

- **Verwendete Festplatte %**

Zeigt den Prozentsatz des verwendeten Festplattenspeichers an. Der Wert wird als „not anwendbares“ angezeigt, wenn das Kontingent ohne Festplattenlimit festgelegt wird.

- **Festplatten-Hard-Limit**

  Zeigt den maximalen Speicherplatz an, der dem Kontingent zugewiesen ist. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht wird und keine weiteren Festplattenschreibvorgänge mehr zulässig sind. Der Wert wird als „Unlimited“ angezeigt, wenn das Kontingent ohne Festplattenlimit festgelegt wird.

- **Soft Limit Für Festplatten**

  Zeigt die Menge an Festplattenspeicher an, die für das Kontingent zugewiesen ist, bevor ein Warnereignis generiert wird. Der Wert wird als „Unlimited“ angezeigt, wenn das Kontingent ohne Laufwerk-Softlimit festgelegt wird. Standardmäßig ist diese Spalte ausgeblendet.

- **Datenträgerschwellenwert**

  Zeigt den Schwellenwert an, der für den Festplattenspeicher festgelegt wurde. Der Wert wird als „Unlimited“ angezeigt, wenn das Kontingent ohne Datenträgerschwellenwert eingestellt ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im qtree verwendeten Dateien an. Der Wert wird als „not anwendbares“ angezeigt, wenn das Kontingent ohne harte Dateibegrenzung festgelegt ist.

- **Harte Dateibegrenzung**

  Zeigt das harte Limit für die Anzahl der Dateien an, die auf dem Kontingent zulässig sind. Der Wert wird als „Unlimited“ angezeigt, wenn das Kontingent ohne hartes Dateilimit festgelegt wird.

- **Soft Limit Für Dateien**

  Zeigt das Softlimit für die Anzahl der Dateien an, die auf dem Kontingent zulässig sind. Der Wert wird als „Unlimited“ angezeigt, wenn das Kontingent ohne DateiSoftlimit festgelegt wird. Standardmäßig ist diese Spalte ausgeblendet.

- **E-Mail-Adresse**

  Zeigt die E-Mail-Adresse des Benutzers oder der Benutzergruppe an, an die Benachrichtigungen gesendet werden, wenn eine Verletzung der Quoten vorhanden ist.

Registerkarte NFS Exporte

Auf der Registerkarte NFS-Exporte werden Informationen zu NFS-Exporten angezeigt, z. B. sein Status, der dem Volume zugeordnete Pfad (Infinite Volumes, FlexGroup Volumes oder FlexVol-Volumes), die Zugriffsebenen von Clients auf die NFS-Exporte und die für die exportierten Volumes definierte Exportrichtlinie. NFS-Exporte werden unter den folgenden Bedingungen nicht angezeigt: Wenn das Volume nicht angehängt ist oder wenn die mit der Exportrichtlinie für das Volume verknüpften Protokolle keine NFS-Exporte enthalten.

Verwenden Sie die Schaltfläche **Exportieren**, um einen kommagetrennten Wert zu erstellen (`.csv`) Datei mit den Details aller überwachten NFS-Exporte. Beim Export in eine CSV-Datei können Sie wählen, einen NFS Exports-Bericht für die aktuelle SVM, für alle SVMs im aktuellen Cluster oder für alle SVMs für alle Cluster in Ihrem Datacenter zu erstellen. In der exportierten CSV-Datei werden einige zusätzliche Felder für die

Exportrichtlinie angezeigt.

- **Status**

  Zeigt den aktuellen Status des NFS-Exports an. Der Status kann „Fehler“ sein ( ) Oder normal ( ).

- **Verbindungspfad**

  Zeigt den Pfad an, auf den das Volume angehängt ist. Wird auf einen qtree eine explizite NFS Exportrichtlinie angewendet, zeigt die Spalte den Pfad des Volume an, über das auf den qtree zugegriffen werden kann.

- **Verbindungspfad Aktiv**

  Zeigt an, ob der Pfad für den Zugriff auf das bereitgestellte Volume aktiv oder inaktiv ist.

- **Volumen oder Qtree**

  Zeigt den Namen des Volumes oder qtree an, auf das die NFS-Exportrichtlinie angewendet wird. Bei Infinite Volumes wird der Name der SVM mit dem Infinite Volume angezeigt. Wenn eine NFS-Exportrichtlinie auf einen qtree im Volume angewendet wird, werden in der Spalte sowohl die Namen des Volume als auch der qtree angezeigt.

  Sie können auf den Link klicken, um Details zum Objekt auf der entsprechenden Detailseite anzuzeigen. Wenn es sich bei dem Objekt um einen qtree handelt, werden sowohl für den qtree als auch für das Volume Links angezeigt.

- * Cluster*

  Zeigt den Namen des Clusters an. Wird nur in der exportierten CSV-Datei angezeigt.

- **Storage Virtual Machine**

  Zeigt den Namen der SVM mit NFS-Exportrichtlinien an. Wird nur in der exportierten CSV-Datei angezeigt.

- **Volume-Status**

  Zeigt den Status des Volumes an, das exportiert wird. Der Status kann Offline, Online, eingeschränkt oder gemischt sein.

  - Offline

    Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

  - Online

    Lese- und Schreibzugriff auf das Volume ist zulässig.

  - Eingeschränkt

    Begrenzte Vorgänge, wie etwa die Paritätsrekonstruktion, sind zulässig, der Datenzugriff jedoch nicht.

  - Gemischt

    Die Komponenten eines FlexGroup-Volumes sind nicht alle im selben Zustand.

- **Sicherheitsstil**

  Zeigt die Zugriffsberechtigung für die exportierten Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder gemischt sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume haben UNIX Berechtigungen.

  - Virtualisierung

    Dateien und Verzeichnisse im Volume weisen einen einheitlichen Sicherheitsstil auf.

  - NTFS (CIFS-Clients)

    Dateien und Verzeichnisse im Volume haben Windows NTFS-Berechtigungen.

  - Gemischt

    Dateien und Verzeichnisse auf dem Volume können entweder UNIX Berechtigungen oder Windows NTFS Berechtigungen haben.

- **UNIX-Erlaubnis**

  Zeigt die UNIX-Berechtigungsbits in einem Oktal-String-Format an, das für die exportierten Volumes festgelegt ist. Es ähnelt den Berechtigungsbits im UNIX-Stil.

- **Exportrichtlinie**

  Zeigt die Regeln an, die die Zugriffsberechtigung für exportierte Volumes definieren. Sie können auf den Link klicken, um Details zu den Regeln anzuzeigen, die mit der Exportrichtlinie verknüpft sind, z. B. die Authentifizierungsprotokolle und die Zugriffsberechtigung.

  Wenn Sie einen Bericht für die Seite NFS-Exporte erstellen, werden alle Regeln, die zur Exportrichtlinie gehören, in die CSV-Datei exportiert. Wenn z. B. zwei Regeln in der Exportrichtlinie enthalten sind, sehen Sie nur eine Zeile in der NFS-Export-Grid-Seite, die exportierten Daten haben jedoch zwei Zeilen, die den beiden Regeln entsprechen.

- **Regelindex**

  Zeigt die Regeln an, die der Exportrichtlinie zugeordnet sind, z. B. die Authentifizierungsprotokolle und die Zugriffsberechtigung. Wird nur in der exportierten CSV-Datei angezeigt.

- **Zugriffsprotokolle**

  Zeigt die Protokolle an, die für die Regeln für die Exportrichtlinie aktiviert sind. Wird nur in der exportierten CSV-Datei angezeigt.

- * Client Match*

  Zeigt die Clients an, die über die Berechtigung zum Zugriff auf Daten auf den Volumes verfügen. Wird nur in der exportierten CSV-Datei angezeigt.

- **Nur-Lese-Zugriff**

  Zeigt das Authentifizierungsprotokoll an, das zum Lesen von Daten auf den Volumes verwendet wird. Wird

nur in der exportierten CSV-Datei angezeigt.

- **Schreibzugriff Lesen**

  Zeigt das Authentifizierungsprotokoll an, das zum Lesen oder Schreiben von Daten auf den Volumes verwendet wird. Wird nur in der exportierten CSV-Datei angezeigt.

Registerkarte CIFS Shares

Zeigt Informationen zu den CIFS-Freigaben auf der ausgewählten SVM an. Sie können Informationen anzeigen, wie z. B. den Status der CIFS-Freigabe, den Freigabennamen, den mit der SVM verknüpften Pfad, den Status des Verbindungspfads der Freigabe, das Objekt enthält, den Status des enthaltenden Volumes, die Sicherheitsdaten der Freigabe und die für die Freigabe definierten Exportrichtlinien. Sie können auch feststellen, ob ein äquivalenter NFS-Pfad für die CIFS-Freigabe vorhanden ist.

Freigaben in Ordnern werden auf der Registerkarte CIFS-Freigaben nicht angezeigt.

- **Befehlsschaltfläche Benutzerzuordnung anzeigen**

  Öffnet das Dialogfeld Benutzerzuordnung.

  Sie können sich die Details der Benutzerzuordnung für die SVM anzeigen lassen.

- **ACL-Befehlstaste anzeigen**

  Öffnet das Dialogfeld „Zugriffskontrolle“ für die Freigabe.

  Sie können Benutzer- und Berechtigungsdetails für die ausgewählte Freigabe anzeigen.

- **Status**

  Zeigt den aktuellen Status der Freigabe an. Der Status kann Normal ( ) Oder Fehler ( ).

- **Name Der Weitergabe**

  Zeigt den Namen der CIFS-Freigabe an.

- **Pfad**

  Zeigt den Verbindungspfad an, auf dem die Freigabe erstellt wird.

- **Verbindungspfad Aktiv**

  Zeigt an, ob der Pfad für den Zugriff auf die Freigabe aktiv oder inaktiv ist.

- **Objekt**

  Zeigt den Namen des enthaltenden Objekts an, zu dem die Freigabe gehört. Das zugehörige Objekt kann ein Volume oder ein qtree sein.

  Durch Klicken auf den Link können Sie auf der entsprechenden Detailseite Details über das zugehörige Objekt anzeigen. Wenn es sich bei dem enthaltenen Objekt um einen qtree handelt, werden sowohl für qtree als auch für das Volume Links angezeigt.

- **Volume-Status**

Zeigt den Status des Volumes an, das exportiert wird. Der Status kann Offline, Online, eingeschränkt oder gemischt sein.

- Offline

  Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

- Online

  Lese- und Schreibzugriff auf das Volume ist zulässig.

- Eingeschränkt

  Begrenzte Vorgänge, wie etwa die Paritätsrekonstruktion, sind zulässig, der Datenzugriff jedoch nicht.

- Gemischt

  Die Komponenten eines FlexGroup-Volumes sind nicht alle im selben Zustand.

- **Sicherheit**

  Zeigt die Zugriffsberechtigung für die exportierten Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder gemischt sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume haben UNIX Berechtigungen.

  - Virtualisierung

    Dateien und Verzeichnisse im Volume weisen einen einheitlichen Sicherheitsstil auf.

  - NTFS (CIFS-Clients)

    Dateien und Verzeichnisse im Volume haben Windows NTFS-Berechtigungen.

  - Gemischt

    Dateien und Verzeichnisse auf dem Volume können entweder UNIX Berechtigungen oder Windows NTFS Berechtigungen haben.

- **Exportrichtlinie**

  Zeigt den Namen der Exportrichtlinie an, die für die Freigabe gilt. Wenn keine Exportrichtlinie für die SVM angegeben ist, wird der Wert als nicht aktiviert angezeigt.

  Sie können auf den Link klicken, um Details zu den Regeln anzuzeigen, die der Exportrichtlinie zugeordnet sind, z. B. Zugriffsprotokolle und Berechtigungen. Die Verknüpfung ist deaktiviert, wenn die Exportrichtlinie für die ausgewählte SVM deaktiviert ist.

- **NFS-Äquivalent**

  Gibt an, ob ein Äquivalent zu NFS für die Freigabe vorhanden ist.

REGISTERKARTE „SAN“

Zeigt Details zu LUNs, Initiatorgruppen und Initiatoren für die ausgewählte SVM an. Standardmäßig wird die Ansicht LUNs angezeigt. Sie können Details zu den Initiatorgruppen auf der Registerkarte Initiatorgruppen und Details zu Initiatoren auf der Registerkarte Initiatoren anzeigen.

- **LUNs-Registerkarte**

  Zeigt Details zu den LUNs an, die zur ausgewählten SVM gehören. Sie können Informationen anzeigen, wie z. B. den LUN-Namen, den LUN-Zustand (online oder offline), den Namen des Filesystems (Volume oder qtree), das die LUN enthält, den Typ des Host-Betriebssystems, die Gesamtkapazität und die Seriennummer der LUN. Sie können auch anzeigen, ob Thin Provisioning auf der LUN aktiviert ist und ob die LUN einer Initiatorgruppe zugeordnet ist.

  Sie können auch die Initiatorgruppen und Initiatoren anzeigen, die der ausgewählten LUN zugeordnet sind.

- **Registerkarte Initiatorgruppen**

  Zeigt Details zu Initiatorgruppen an. Sie können Details anzeigen, z. B. den Namen der Initiatorgruppe, den Zugriffsstatus, den Typ des Host-Betriebssystems, das von allen Initiatoren in der Gruppe verwendet wird, und das unterstützte Protokoll. Wenn Sie in der Spalte Zugriffsstatus auf den Link klicken, können Sie den aktuellen Zugriffsstatus der Initiatorgruppe anzeigen.

  - **Normal**

    Die Initiatorgruppe ist mit mehreren Zugriffspfaden verbunden.

  - * Einzelner Pfad*

    Die Initiatorgruppe ist mit einem einzelnen Zugriffspfad verbunden.

  - **Keine Pfade**

    Es ist kein Zugriffspfad mit der Initiatorgruppe verbunden.

    Sie können anzeigen, ob Initiatorgruppen über einen Port-Satz allen LIFs oder spezifischen LIFs zugeordnet werden. Wenn Sie in der Spalte zugewiesene LIFs auf den Link zum Zählen klicken, werden entweder alle LIFs angezeigt oder bestimmte LIFs für einen Port-Satz angezeigt. LIFs, die über das Zielportal zugeordnet sind, werden nicht angezeigt. Es wird die Gesamtzahl der Initiatoren und LUNs angezeigt, die einer Initiatorgruppe zugeordnet sind.

  Sie können auch die LUNs und Initiatoren anzeigen, die der ausgewählten Initiatorgruppe zugeordnet sind.

- **Registerkarte Initiatoren**

  Zeigt den Namen und Typ des Initiators und die Gesamtzahl der Initiatorgruppen an, die diesem Initiator für die ausgewählte SVM zugeordnet sind.

  Sie können auch die LUNs und Initiatorgruppen anzeigen, die der ausgewählten Initiatorgruppe zugeordnet sind.

Datenrichtlinie

Auf der Registerkarte Datenrichtlinie können Sie eine oder mehrere Regeln in einer Datenrichtlinie erstellen, ändern, aktivieren oder löschen. Sie können die Datenrichtlinie auch in die Unified Manager-Datenbank importieren und die Datenrichtlinie auf Ihren Computer exportieren:

Die Registerkarte Datenrichtlinie wird nur für SVMs mit Infinite Volume angezeigt.

- **Regelliste**

  Zeigt die Liste der Regeln an. Wenn Sie die Regel erweitern, können Sie die entsprechenden übereinstimmenden Kriterien der Regel und der Speicherklasse anzeigen, in der der Inhalt auf der Grundlage der Regel platziert wird.

  Die Standardregel ist die letzte Regel in der Liste. Sie können die Reihenfolge der Standardregel nicht ändern.

  - Übereinstimmende Kriterien

    Zeigt die Bedingungen für die Regel an. Eine Regel kann z. B. „`Dateipfad beginnt mit `/eng/Nightly`` “ lauten.

    Der Dateipfad muss immer mit einem Verbindungspfad beginnen.

  - Platzierung Von Inhalten

    Zeigt die entsprechende Speicherklasse für die Regel an.

- **Regelfilter**

  Mit dieser Funktion können Sie Regeln filtern, die einer bestimmten Speicherklasse zugeordnet sind, die in der Liste aufgeführt ist.

- **Aktionsschaltflächen**
  - Erstellen

    Öffnet das Dialogfeld Regel erstellen, in dem Sie eine neue Regel für Ihre Datenrichtlinie erstellen können.

  - Bearbeiten

    Öffnet das Dialogfeld Regel bearbeiten, in dem Sie Regeleigenschaften wie Verzeichnispfade, Dateitypen und Eigentümer ändern können.

  - Löschen

    Löscht die ausgewählte Regel.

  - Nach Oben

    Verschiebt die ausgewählte Regel in der Liste nach oben. Sie können die Standardregel jedoch nicht in der Liste nach oben verschieben.

  - Nach Unten Verschieben

    Verschiebt die ausgewählte Regel nach unten in der Liste. Sie können die Standardregel jedoch nicht nach unten in der Liste verschieben.

  - Aktivieren

Aktiviert die Regeln und Änderungen an der Datenrichtlinie in der SVM mit Infinite Volume.

- Zurücksetzen

  Setzt alle Änderungen zurück, die an der Konfiguration der Datenrichtlinien vorgenommen wurden.

- Importieren

  Importiert eine Konfiguration der Datenrichtlinien aus einer Datei.

- Exportieren

  Exportiert eine Konfiguration von Datenrichtlinien in eine Datei.

Bereich für zugehörige Geräte

Im Bereich „Verwandte Geräte“ können Sie LUNs, CIFS Shares und die Quoten für Benutzer und Benutzergruppen anzeigen und navigieren, die mit dem qtree in Verbindung stehen:

- **LUNs**

  Zeigt die Gesamtzahl der LUNs an, die dem ausgewählten qtree zugeordnet sind.

- **NFS-Exporte**

  Zeigt die Gesamtzahl der NFS-Exportrichtlinien an, die mit dem ausgewählten qtree verknüpft sind.

- **CIFS-Freigaben**

  Zeigt die Gesamtzahl der CIFS-Shares an, die mit dem ausgewählten qtree verbunden sind.

- **Benutzer- und Gruppenquoten**

  Zeigt die Gesamtzahl der Benutzer- und Benutzergruppenkontingente an, die mit dem ausgewählten qtree verknüpft sind. Auf der Grundlage des höchsten Schweregrads wird auch der Integritätsstatus der Kontingente von Benutzern und Benutzergruppen angezeigt.

Bereich „Verwandte Anmerkungen“

Im Fensterbereich Verwandte Anmerkungen können Sie die mit der ausgewählten SVM verknüpften Anmerkungsdetails anzeigen. Details umfassen den Anmerkungsnamen und die auf die SVM angewandten Anmerkungswerte. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie Cluster, Aggregate und Volumes anzeigen, die mit der SVM in Verbindung stehen:

- * Cluster*

  Zeigt den Integritätsstatus des Clusters an, zu dem die SVM gehört.

- **Aggregate**

Zeigt die Anzahl der Aggregate an, die zur ausgewählten SVM gehören. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt. Wenn eine SVM z. B. zehn Aggregate enthält, von denen fünf den Warnstatus und die verbleibenden fünf den kritischen Status anzeigen, ist der angezeigte Status „kritisch“.

- * Zugewiesene Aggregate*

  Zeigt die Anzahl der Aggregate an, die einer SVM zugewiesen sind. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt.

- **Bände**

  Zeigt die Anzahl und Kapazität der Volumes an, die zur ausgewählten SVM gehören. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt. In der SVM sind FlexGroup Volumes vorhanden, auch die Zählung FlexGroups. FlexGroup-Komponenten sind darin nicht enthalten.

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ können Sie eine Liste der Gruppen anzeigen, die der ausgewählten SVM zugeordnet sind.

Bereich „Verwandte Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnmeldungen anzeigen, die für die ausgewählte SVM erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link **Alarm hinzufügen** klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Namen der Warnmeldung klicken.

„Systemzustand/Cluster-Details“-Seite

Auf der Seite Systemzustand/Cluster-Details finden Sie ausführliche Informationen über ein ausgewähltes Cluster, z. B. Angaben zu Systemzustand, Kapazität und Konfiguration. Sie können außerdem Informationen zu den logischen Schnittstellen (LIFs), Nodes, Festplatten, zugehörigen Geräten und zugehörigen Warnmeldungen für das Cluster anzeigen.

Der Status neben dem Cluster-Namen, z. B. (gut), stellt den Kommunikationsstatus dar, ob Unified Manager mit dem Cluster kommunizieren kann. Er stellt nicht den Failover-Status oder den Gesamtstatus des Clusters dar.

Befehlsschaltflächen

Mit den Schaltflächen des Befehls können Sie die folgenden Aufgaben für das ausgewählte Cluster ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Hier können Sie zur Seite Performance/Cluster-Details navigieren.

-

  Hiermit können Sie den ausgewählten Cluster zum Dashboard „Favoriten“ hinzufügen.

- **Aktionen**
  - Alarm hinzufügen: Öffnet das Dialogfeld Alarm hinzufügen, in dem Sie dem ausgewählten Cluster eine Warnung hinzufügen können.
  - Erneut entdecken: Initiiert eine manuelle Aktualisierung des Clusters, sodass Unified Manager die neuesten Änderungen am Cluster erkennen kann.

    Bei Kombination von Unified Manager mit OnCommand Workflow Automation erfasst der Wiederauffindungvorgang ggf. auch zwischengespeicherte Daten von WFA.

  Nachdem der Vorgang zur erneuten Erkennung initiiert wurde, wird ein Link zu den zugehörigen Jobdetails angezeigt, um die Nachverfolgung des Jobstatus zu ermöglichen.

  - Anmerkungen: Ermöglicht es Ihnen, das ausgewählte Cluster zu kommentieren.
- **Cluster Anzeigen**

  Hier können Sie zur Seite „Health/Clusters Inventory“ navigieren.

Registerkarte Systemzustand

Zeigt detaillierte Informationen zur Datenverfügbarkeit und zu Kapazitätsproblemen der verschiedenen Cluster-Objekte wie Nodes, SVMs und Aggregate an. Verfügbarkeitsprobleme hängen von der Datenserverfunktion der Cluster-Objekte ab. Kapazitätsprobleme stehen im Zusammenhang mit der Datenspeicherfunktion der Cluster-Objekte.

Sie können auf das Diagramm eines Objekts klicken, um eine gefilterte Liste der Objekte anzuzeigen. Beispielsweise können Sie auf das SVM-Kapazitätsdiagramm klicken, in dem Warnungen angezeigt werden, um eine gefilterte Liste der SVMs anzuzeigen. Diese Liste enthält SVMs mit Volumes oder qtrees, deren Kapazitätsprobleme mit einem Schweregrad von Warnung auftreten. Sie können auch auf das Diagramm „SVMs Verfügbarkeit“ klicken, in dem Warnungen angezeigt werden, um die Liste der SVMs mit Verfügbarkeitsproblemen und einem Schweregrad „Warnung“ anzuzeigen.

- **Verfügbarkeitsprobleme**

  Grafische Darstellung der Gesamtzahl an Objekten, einschließlich Objekten mit Verfügbarkeitsproblemen und Objekten, bei denen keine Probleme mit der Verfügbarkeit auftreten Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Verfügbarkeitsproblemen, die sich auf die Verfügbarkeit von Daten im Cluster auswirken oder bereits davon betroffen sein können. Beispielsweise werden Informationen über Festplatten-Shelfs angezeigt, die ausgefallen sind und Aggregate, die offline sind.

  Die für das SFO-Balkendiagramm angezeigten Daten basieren auf dem HA-Status der Nodes. Die für alle anderen Balkendiagramme angezeigten Daten werden auf Grundlage der generierten Ereignisse berechnet.

- **Kapazitätsprobleme**

  Grafische Darstellung der Gesamtzahl an Objekten, einschließlich Objekten mit Kapazitätsproblemen und Objekten, die keine Kapazitätsprobleme haben. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Kapazitätsproblemen, die sich auf die Kapazität von Daten im Cluster auswirken oder bereits sie beeinträchtigen können. Beispielsweise werden Informationen zu Aggregaten angezeigt, die mit hoher Wahrscheinlichkeit die festgelegten Schwellenwerte überschreiten.

Registerkarte „Kapazität“

Zeigt detaillierte Informationen zur Kapazität des ausgewählten Clusters an.

- * Kapazität*

  Zeigt das Datenkapazitätsdiagramm zu der genutzten Kapazität und der verfügbaren Kapazität aus allen zugewiesenen Aggregaten an:

  - Gesamtkapazität

    Zeigt die Gesamtkapazität des Clusters an. Dies schließt nicht die Kapazität ein, die Parität zugewiesen ist.

  - Verwendet

    Zeigt die Kapazität an, die von Daten verwendet wird. Dies schließt nicht die Kapazität ein, die für Parität, richtige Dimensionierung und Reservierung verwendet wird.

  - Verfügbar

    Zeigt die für Daten verfügbare Kapazität an.

  - Ersatzteile

    Zeigt die verfügbare Speicherkapazität für die Speicherung aller freien Festplatten an.

  - Provisioniert

    Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

- * Cloud Tier*

  Zeigt Kapazitätsdetails über das Cloud-Tier für FabricPool-fähige Aggregate auf dem Cluster an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

  - Verwendet

    Zeigt den Speicherplatz an, der von Daten in konfigurierten Cloud-Tiers verwendet wird.

  - Datendiagramm

    Bei Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage oder Alibaba Cloud Object Storage werden die Gesamtkapazität, die von diesem Cluster lizenziert wurde, und die von Aggregaten verwendete Menge angezeigt.

  Bei einer StorageGRID wird im Diagramm nur die Gesamtkapazität angezeigt, die von Aggregaten verwendet wird.

- **Details**

  Zeigt detaillierte Informationen zur verwendeten und verfügbaren Kapazität an.

  - Gesamtkapazität

    Zeigt die Gesamtkapazität des Clusters an. Dies schließt nicht die Kapazität ein, die Parität

zugewiesen ist.

- Verwendet

  Zeigt die Kapazität an, die von Daten verwendet wird. Dies schließt nicht die Kapazität ein, die für Parität, richtige Dimensionierung und Reservierung verwendet wird.

- Verfügbar

  Zeigt die für Daten verfügbare Kapazität an.

- Provisioniert

  Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

- Ersatzteile

  Zeigt die verfügbare Speicherkapazität für die Speicherung aller freien Festplatten an.

- Cloud-Tier

  Zeigt den Speicherplatz an, der von Daten in konfigurierten Cloud-Tiers verwendet wird. Bei Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage oder Alibaba Cloud Object Storage wird auch die Gesamtkapazität, die von diesem Cluster lizenziert wurde, angezeigt.

- **Kapazität Breakout nach Datenträgertyp**

  Im Bereich Capacity Breakout nach Disk Type werden ausführliche Informationen zur Festplattenkapazität der verschiedenen Festplattentypen im Cluster angezeigt. Durch Klicken auf den Festplattentyp werden weitere Informationen zum Festplattentyp auf der Registerkarte Laufwerke angezeigt.

  - Nutzbare Gesamtkapazität –

    Zeigt die verfügbare Kapazität und freie Kapazität der Datenfestplatten an.

  - HDD

    Grafische Darstellung der verwendeten Kapazität und der verfügbaren Kapazität aller Festplatten im Cluster. Die gestrichelte Linie stellt die freie Kapazität der Datenfestplatten dar.

  - Flash
    - SSD-Daten

      Grafische Darstellung der verwendeten Kapazität und der verfügbaren Kapazität der SSD-Datenfestplatten im Cluster

    - SSD Cache

      Zeigt grafisch die speicherbare Kapazität der SSD-Cache-Laufwerke im Cluster an.

    - SSD Spare

      Grafische Darstellung der freien Kapazität der SSD-, Daten- und Cache-Festplatten im Cluster

  - Nicht Zugewiesene Festplatten

Zeigt die Anzahl der nicht zugewiesenen Festplatten im Cluster an.

- **Aggregate mit Kapazitätsprobleme Liste**

  Zeigt Details zur verwendeten Kapazität und zur verfügbaren Kapazität der Aggregate mit Kapazitätsproblemen in Tabellenform an.

  - Status

    Zeigt an, dass das Aggregat ein kapazitätsbezogenes Problem mit einem bestimmten Schweregrad hat.

    Sie können den Zeiger auf den Status verschieben, um weitere Informationen zu dem für das Aggregat generierten Ereignis oder Ereignissen anzuzeigen.

    Wenn der Status des Aggregats durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen wurde, und die Ursache des Ereignisses anzeigen. Sie können auf die Schaltfläche **Details anzeigen** klicken, um weitere Informationen über die Veranstaltung anzuzeigen.

    Wenn der Status des Aggregats durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen angezeigt, z. B. Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst werden, und der Name des Administrators, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

    > Ein Aggregat kann mehrere kapazitätsbezogene Ereignisse vom gleichen Schweregrad oder verschiedene Schweregrade aufweisen. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Aggregat zwei Ereignisse mit dem Schweregrad „Fehler“ und „kritisch“ hat, wird nur der Schweregrad „kritisch“ angezeigt.

  - Aggregat

    Zeigt den Namen des Aggregats an.

  - Genutzte Datenkapazität

    Grafische Anzeige von Informationen zur Kapazitätsauslastung des Aggregats (in Prozent)

  - Tage voll

    Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor die volle Kapazität des Aggregats erreicht ist.

Registerkarte Konfiguration

Zeigt Details zum ausgewählten Cluster an, z. B. IP-Adresse, Seriennummer, Kontakt und Standort:

- **Cluster Übersicht**
  - Management-LIF

    Zeigt die Cluster-Management-LIF an, die Unified Manager zum Herstellen einer Verbindung mit dem

Cluster verwendet. Der Betriebsstatus der LIF wird ebenfalls angezeigt.

- Host-Name oder IP-Adresse

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse der Clusterverwaltungs-LIF an, die Unified Manager zur Verbindung mit dem Cluster verwendet.

- FQDN

  Zeigt den vollständig qualifizierten Domänennamen (FQDN) des Clusters an.

- Betriebssystemversion

  Zeigt die ONTAP-Version an, die das Cluster ausführt. Wenn im Cluster die Nodes unterschiedliche Versionen von ONTAP ausführen, wird die früheste ONTAP-Version angezeigt.

- Seriennummer

  Zeigt die Seriennummer des Clusters an.

- Kontakt

  Zeigt Details zum Administrator an, an den Sie bei Cluster-Problemen wenden sollten.

- Standort

  Zeigt den Speicherort des Clusters an.

- **Remote Cluster Übersicht**

  Enthält Details zum Remote-Cluster in einer MetroCluster-Konfiguration. Diese Informationen werden nur für MetroCluster-Konfigurationen angezeigt.

  - Cluster

    Zeigt den Namen des Remote-Clusters an. Sie können auf den Cluster-Namen klicken, um zur Detailseite des Clusters zu navigieren.

  - Hostname oder IP-Adresse

    Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Remote-Clusters an.

  - Seriennummer

    Zeigt die Seriennummer des Remote-Clusters an.

  - Standort

    Zeigt den Speicherort des Remote-Clusters an.

- **MetroCluster Übersicht**

  Bietet Details zum lokalen Cluster in einer MetroCluster Konfiguration. Diese Informationen werden nur für MetroCluster-Konfigurationen angezeigt.

  - Typ

Zeigt an, ob es sich bei dem MetroCluster-Typ um zwei oder vier Nodes handelt.

◦ Konfiguration

Zeigt die MetroCluster-Konfiguration an, die die folgenden Werte aufweisen kann:

- Stretch-Konfiguration mit SAS-Kabeln
- Stretch-Konfiguration mit FC-SAS Bridge
- Fabric-Konfiguration mit FC Switches

Bei einem MetroCluster mit vier Nodes wird nur eine Fabric-Konfiguration mit FC-Switches unterstützt.

+

◦ Automatisiertes ungeplantes Switchover (AUSO)

Zeigt an, ob das automatisierte ungeplante Switchover für das lokale Cluster aktiviert ist. Standardmäßig ist AUSO für alle Cluster in einer MetroCluster-Konfiguration mit zwei Knoten in Unified Manager aktiviert. Sie können die AUSO-Einstellung über die Befehlszeilenschnittstelle ändern.

- **Knoten**
  - ◦ Gesteigerte

    Zeigt die Anzahl der Knoten an, die aktiv sind (Oder runter ( ) Im Cluster.

  - ◦ Betriebssystemversionen

    Zeigt die ONTAP-Versionen, die die Nodes ausführen, sowie die Anzahl der Nodes, auf denen eine bestimmte Version von ONTAP ausgeführt wird. Beispielsweise gibt 9.0 (2), 8.3 (1) an, dass zwei Nodes ONTAP 9.0 ausführen und auf einem Node ONTAP 8.3 ausgeführt wird.
- **Storage Virtual Machines**
  - ◦ Gesteigerte

    Zeigt die Anzahl der SVMs an, die aktiv sind (Oder runter ( ) Im Cluster.
- **LIFs**
  - ◦ Gesteigerte

    Zeigt die Anzahl der nicht-Daten-LIFs an, die in der aktiv sind (Oder runter ( ) Im Cluster.

  - ◦ Cluster-Management-LIFs

    Zeigt die Anzahl der Cluster-Management-LIFs an.

  - ◦ Node-Management-LIFs

    Zeigt die Anzahl der LIFs für das Node-Management an.

  - ◦ Cluster-LIFs

    Zeigt die Anzahl der Cluster-LIFs an.

- Intercluster LIFs

  Zeigt die Anzahl der Intercluster-LIFs an.

- **Protokolle**
  - Datenprotokolle

    Zeigt die Liste der lizenzierten Datenprotokolle an, die für den Cluster aktiviert sind. Datenprotokolle sind iSCSI, CIFS, NFS, NVMe und FC/FCoE.

- **Cloud-Tiers**

  In sind die Namen der Cloud-Tiers aufgeführt, mit denen dieses Cluster verbunden ist. Außerdem werden die Typen (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Alibaba Cloud Object Storage oder StorageGRID) und die Status der Cloud-Tiers (verfügbar oder nicht verfügbar) aufgelistet.

Registerkarte MetroCluster-Konnektivität

Zeigt die Probleme und den Konnektivitätsstatus der Clusterkomponenten der MetroCluster Konfiguration an. Ein Cluster wird in einem roten Feld angezeigt, wenn der Disaster-Recovery-Partner des Clusters Probleme hat.

Die Registerkarte MetroCluster-Konnektivität wird nur für Cluster angezeigt, die sich in einer MetroCluster-Konfiguration befinden.

Sie können zur Detailseite eines Remote-Clusters navigieren, indem Sie auf den Namen des Remote-Clusters klicken. Sie können die Details der Komponenten auch anzeigen, indem Sie auf den Zähllink einer Komponente klicken. Wenn Sie beispielsweise auf den Zähllink des Node im Cluster klicken, wird auf der Detailseite des Clusters die Registerkarte Node angezeigt. Wenn Sie auf den Link Zählen der Festplatten im Remote-Cluster klicken, wird die Registerkarte Festplatte auf der Detailseite des Remote-Clusters angezeigt.

Beim Verwalten einer MetroCluster Konfiguration mit acht Nodes wird durch Klicken auf den Zähllink der Komponente Platten-Shelfs nur die lokalen Shelfs des Standard-HA-Paars angezeigt. Es gibt auch keine Möglichkeit, die lokalen Shelfs auf dem anderen HA-Paar anzuzeigen.

Sie können den Mauszeiger über die Komponenten bewegen, um bei jedem Problem die Details und den Konnektivitätsstatus der Cluster anzuzeigen. Außerdem werden weitere Informationen zu dem für das Problem erzeugten Ereignis oder Ereignissen angezeigt.

Wenn der Status des Verbindungsproblem zwischen den Komponenten durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugeordnet ist, und die Ursache des Ereignisses anzeigen. Die Schaltfläche Details anzeigen enthält weitere Informationen zum Ereignis.

Wenn der Status des Verbindungsproblem zwischen den Komponenten durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum bei Auslösung der Ereignisse und dem Namen des Administrators angezeigt, dem das Ereignis zugeordnet ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

Registerkarte „MetroCluster-Replikation“

Zeigt den Status der Daten an, die repliziert werden. Sie können die Registerkarte MetroCluster-Replikation verwenden, um die Datensicherung durch synchrones Spiegeln der Daten mit den bereits Peering-Clustern zu gewährleisten. Ein Cluster wird in einem roten Feld angezeigt, wenn der Disaster-Recovery-Partner des Clusters Probleme hat.

Die Registerkarte MetroCluster-Replikation wird nur für Cluster angezeigt, die sich in einer MetroCluster-Konfiguration befinden.

In einer MetroCluster-Umgebung können Sie diese Registerkarte verwenden, um die logischen Verbindungen und Peering des lokalen Clusters mit dem Remote-Cluster zu überprüfen. Sie können die objektive Darstellung der Cluster-Komponenten mit ihren logischen Verbindungen anzeigen. Dadurch werden Probleme identifiziert, die bei der Spiegelung von Metadaten und Daten auftreten können.

Auf der Registerkarte MetroCluster-Replikation bietet das lokale Cluster eine detaillierte grafische Darstellung des ausgewählten Clusters. MetroCluster-Partner bezieht sich auf das Remote-Cluster.

Registerkarte LIFs

Zeigt Details zu allen nicht-Daten-LIFs an, die auf dem ausgewählten Cluster erstellt wurden.

- **LIF**

  Zeigt den Namen der logischen Schnittstelle an, die im ausgewählten Cluster erstellt wird.

- **Betriebsstatus**

  Zeigt den Betriebsstatus der logischen Schnittstelle an. Diese kann im aktiv sein ( ), Down (Oder Unbekannt ( ). Der Betriebsstatus einer logischen Schnittstelle wird vom Status ihrer physischen Ports bestimmt.

- **Verwaltungsstatus**

  Zeigt den Administrationsstatus der logischen Schnittstelle an. Dieser kann im aktiv sein ( ), Down (Oder Unbekannt ( ). Sie können den Administrationsstatus einer logischen Schnittstelle steuern, wenn Sie Änderungen an der Konfiguration oder während der Wartung vornehmen. Der Administrationsstatus kann sich vom Betriebsstatus unterscheiden. Wenn jedoch der Administrationsstatus eines LIF „Inaktiv“ lautet, ist der Betriebsstatus standardmäßig „Inaktiv“.

- **IP-Adresse**

  Zeigt die IP-Adresse des LIF an.

- * Rolle*

  Zeigt die Rolle des LIF an. Mögliche Rollen sind Cluster-Management-LIFs, Node-Management-LIFs, Cluster-LIFs und Intercluster-LIFs.

- * Home Port*

  Zeigt den physischen Port an, dem die LIF ursprünglich zugeordnet war.

- **Aktueller Port**

Zeigt den physischen Port an, dem das LIF derzeit zugeordnet ist. Nach der LIF-Migration kann sich der aktuelle Port vom Home Port unterscheiden.

- **Failover-Richtlinie**

  Zeigt die für das LIF konfigurierte Failover-Richtlinie an.

- **Routing-Gruppen**

  Zeigt den Namen der Routinggruppe an. Sie können weitere Informationen zu den Routen und dem Ziel-Gateway anzeigen, indem Sie auf den Namen der Routinggruppe klicken.

  Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt. Daher wird für diese Cluster eine leere Spalte angezeigt.

- **Failover-Gruppe**

  Zeigt den Namen der Failover-Gruppe an.

Registerkarte Knoten

Zeigt Informationen zu Nodes im ausgewählten Cluster an. Sie können ausführliche Informationen zu HA-Paaren, Festplatten-Shelfs und Ports anzeigen:

- **HA Details**

  Stellt eine bildliche Darstellung des HA-Status und des Integritätsstatus der Nodes im HA-Paar bereit. Der Integritätsstatus des Node wird durch die folgenden Farben angezeigt:

  - **Grün**

    Der Node befindet sich in einem Betriebszustand.

  - **Gelb**

    Der Node hat den Partner-Node übernommen oder der Node weist einige Umgebungsprobleme auf.

  - * Rot*

    Der Node ist ausgefallen.

    Sie können Informationen zur Verfügbarkeit des HA-Paars anzeigen und erforderliche Maßnahmen ergreifen, um Risiken zu vermeiden. Im Fall eines möglichen Übernahmevorgangs wird beispielsweise die folgende Meldung angezeigt: `Storage failover possible`.

    Sie können eine Liste der Ereignisse anzeigen, die zum HA-Paar und seiner Umgebung betreffen, z. B. Lüfter, Netzteile, NVRAM-Batterie, Flash-Karten, Serviceprozessor und Verbindung von Festplatten-Shelfs: Sie können auch die Uhrzeit anzeigen, zu der die Ereignisse ausgelöst wurden.

    Sie können weitere Informationen zu Nodes anzeigen, z. B. die Modellnummer und die Seriennummer.

  Bei Single-Node-Clustern können Sie auch Details zu den Nodes anzeigen.

- **Platten-Shelves**

  Zeigt Informationen über die Festplatten-Shelfs im HA-Paar an.

Sie können auch Ereignisse anzeigen, die für die Festplatten-Shelfs und die Umgebungskomponenten generiert wurden, sowie die Zeit, zu der die Ereignisse ausgelöst wurden.

- **Regal-ID**

  Zeigt die ID des Shelf an, in dem sich die Festplatte befindet.

- **Komponentenstatus**

  Zeigt Umgebungsdetails der Festplatten-Shelfs an, z. B. Netzteile, Lüfter, Temperatursensor, aktuelle Sensoren, Festplattenkonnektivität. Und Spannungssensoren. Die Umgebungsdetails werden als Symbole in den folgenden Farben angezeigt:

  - **Grün**

    Die Umgebungskomponenten funktionieren ordnungsgemäß.

  - **Grau**

    Für die Umgebungskomponenten sind keine Daten verfügbar.

  - * Rot*

    Einige Umgebungskomponenten sind nicht verfügbar.

- **Bundesland**

  Zeigt den Status des Festplatten-Shelf an. Mögliche Status sind Offline, Online, kein Status, Initialisierung erforderlich, fehlt, Und Unbekannt.

- **Modell**

  Zeigt die Modellnummer des Festplatten-Shelf an.

- **Lokales Festplatten-Shelf**

  Gibt an, ob sich das Festplatten-Shelf auf dem lokalen Cluster oder dem Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

- * Unique ID*

  Zeigt die eindeutige ID des Festplatten-Shelf an.

- **Firmware-Version**

  Zeigt die Firmware-Version des Festplatten-Shelf an.

- **Ports**

Zeigt Informationen zu den zugehörigen FC-, FCoE- und Ethernet-Ports an. Sie können Details zu den Ports und den zugehörigen LIFs anzeigen, indem Sie auf die Port-Symbole klicken.

Sie können auch die für die Ports generierten Ereignisse anzeigen.

Sie können folgende Portdetails anzeigen:

- Port-ID

  Zeigt den Namen des Ports an. Die Port-Namen können beispielsweise E0M, e0a und e0b sein.

- Rolle

  Zeigt die Rolle des Ports an. Mögliche Rollen sind Cluster, Data, Intercluster, Node-Management und Undefined.

- Typ

  Zeigt das Protokoll der physischen Schicht an, das für den Port verwendet wird. Mögliche Typen sind Ethernet, Fibre Channel und FCoE.

- WWPN

  Zeigt den WWPN (World Wide Port Name) des Ports an.

- Firmware-Version

  Zeigt die Firmware-Version des FC/FCoE-Ports an.

- Status

  Zeigt den aktuellen Status des Ports an. Mögliche Zustände sind up, Down, Link not connected. Oder Unbekannt ( ).

Sie können die portbezogenen Ereignisse in der Ereignisliste anzeigen. Sie können auch die zugehörigen LIF-Details anzeigen, z. B. LIF-Name, Betriebsstatus, IP-Adresse oder WWPN, Protokolle, den Namen der zu dieser LIF gehörenden SVM, den aktuellen Port, die Failover-Richtlinie und die Failover-Gruppe.

Registerkarte „Festplatten“

Zeigt Details zu den Festplatten im ausgewählten Cluster an. Sie können Festplatten-bezogene Informationen wie die Anzahl der verwendeten Festplatten, Ersatzfestplatten, fehlerhafte Festplatten und nicht zugewiesene Laufwerke anzeigen. Sie können auch weitere Details anzeigen, z. B. den Festplattennamen, den Festplattentyp und den Besitzer-Node der Festplatte.

- **Disk Pool Zusammenfassung**

  Zeigt die Anzahl der Laufwerke an, die nach effektiven Typen (FCAL, SAS, SATA, MSATA, SSD, Array-LUN und VMDISK) und der Zustand der Festplatten. Sie können auch andere Details anzeigen, wie z. B. die Anzahl der Aggregate, freigegebenen Festplatten, Ersatzfestplatten, defekte Festplatten, nicht zugewiesene Laufwerke, Und nicht unterstützten Festplatten. Wenn Sie auf den Link zur Anzahl der effektiven Festplattentypen klicken, werden Festplatten mit dem ausgewählten Status und dem effektiven Typ angezeigt. Wenn Sie beispielsweise auf den Zähllink für den Festplattenstatus „beschädigt“ und „effektiver Typ SAS“ klicken, werden alle Festplatten mit dem Festplattenstatus „beschädigt“ und „effektiver Typ „SAS“ angezeigt.

- **Datenträger**

  Zeigt den Namen der Festplatte an.

- **RAID-Gruppen**

Zeigt den Namen der RAID-Gruppe an.

- **Owner Node**

  Zeigt den Namen des Node an, zu dem die Festplatte gehört. Wenn die Festplatte nicht zugewiesen ist, wird in dieser Spalte kein Wert angezeigt.

- **Bundesland**

  Zeigt den Status der Festplatte an: Aggregate, Shared, Spare, broken, Unassigned, Nicht unterstützt oder Unbekannt. Standardmäßig wird diese Spalte sortiert, um die Status in der folgenden Reihenfolge anzuzeigen: Gebrochen, nicht zugewiesen, nicht unterstützt, Spare, Aggregat, Und Shared IT.

- **Lokaler Datenträger**

  Zeigt entweder Ja oder Nein an, um anzugeben, ob sich das Laufwerk im lokalen Cluster oder im Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

- **Position**

  Zeigt die Position des Laufwerks basierend auf seinem Container-Typ an, z. B. Kopieren, Daten oder Parität. Standardmäßig ist diese Spalte ausgeblendet.

- **Betroffene Aggregate**

  Zeigt die Anzahl der Aggregate an, die aufgrund der ausgefallenen Festplatte betroffen sind. Sie können den Mauszeiger über den Zähllink verschieben, um die betroffenen Aggregate anzuzeigen. Klicken Sie dann auf den Aggregatnamen, um Details zum Aggregat anzuzeigen. Sie können auch auf die Aggregatanzahl klicken, um die Liste der betroffenen Aggregate auf der Seite „Systemzustand/Aggregate Inventory“ anzuzeigen.

  In dieser Spalte wird für die folgenden Fälle kein Wert angezeigt:

  - Für fehlerhafte Festplatten, wenn ein Cluster mit solchen Festplatten zu Unified Manager hinzugefügt wird
  - Wenn keine ausgefallenen Festplatten vorhanden sind

- **Speicherpool**

  Zeigt den Namen des Speicherpools an, zu dem die SSD gehört. Sie können den Zeiger über den Speicherpool verschieben, um Details des Speicherpools anzuzeigen.

- **Speicherbare Kapazität**

  Zeigt die verfügbare Festplattenkapazität an.

- **Rohkapazität**

  Zeigt die Kapazität der unformatierten RAW-Festplatte vor der richtigen Dimensionierung und RAID-Konfiguration an. Standardmäßig ist diese Spalte ausgeblendet.

- **Typ**

  Zeigt die Festplattentypen an, z. B. ATA, SATA, FCAL oder VMDISK.

- * Effektiver Typ*

Zeigt den von ONTAP zugewiesenen Festplattentyp an.

Bestimmte ONTAP-Festplattentypen werden als gleichbedeutend mit dem Erstellen und Hinzufügen zu Aggregaten und mit Ersatzmanagement angesehen. ONTAP weist jedem Festplattentyp einen effektiven Festplattentyp zu.

- **Spare Blocks Verbraucht %**

  Zeigt in Prozent die Spare-Blöcke an, die in der SSD-Festplatte verbraucht werden. Diese Spalte ist bei anderen Festplatten als SSD-Festplatten leer.

- **Bewertete Lebensdauer %**

  Zeigt prozentual eine Schätzung der verwendeten SSD-Lebensdauer an, basierend auf der tatsächlichen SSD-Nutzung und der Vorhersage der SSD-Lebensdauer des Herstellers. Ein Wert größer als 99 zeigt an, dass die geschätzte Haltbarkeit verbraucht wurde, weist aber möglicherweise nicht auf einen SSD-Ausfall hin. Wenn der Wert unbekannt ist, wird die Platte weggelassen.

- **Firmware**

  Zeigt die Firmware-Version der Festplatte an.

- **U/MIN**

  Zeigt die Umdrehungen pro Minute (U/min) der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

- **Modell**

  Zeigt die Modellnummer der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

- * Anbieter*

  Zeigt den Namen des Festplattenanbieters an. Standardmäßig ist diese Spalte ausgeblendet.

- **Regal-ID**

  Zeigt die ID des Shelf an, in dem sich die Festplatte befindet.

- **Bucht**

  Zeigt die ID des Einschubschachts an, in dem sich die Festplatte befindet.

Bereich „Verwandte Anmerkungen“

Hiermit können Sie die mit dem ausgewählten Cluster verknüpften Anmerkungsdetails anzeigen. Die Details umfassen den Anmerkungsnamen und die auf das Cluster angewandten Anmerkungswerte. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Mit dieser Option können Sie Gerätedetails anzeigen, die mit dem ausgewählten Cluster verknüpft sind.

Zu den Details gehören Eigenschaften des mit dem Cluster verbundenen Geräts, wie z. B. Gerätetyp, Größe, Anzahl und Integritätsstatus. Sie können auf den Zähllink klicken, um weitere Analysen zu diesem Gerät

durchzuführen.

Mithilfe des Teilfensters MetroCluster können Sie Anzahl und auch Details zum Remote MetroCluster Partner sowie zu den zugehörigen Cluster-Komponenten wie Nodes, Aggregaten und SVMs abrufen. Das Teilfenster „MetroCluster Partner“ wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

Im Bereich „Verwandte Geräte“ können Sie die Nodes, SVMs und Aggregate anzeigen und navigieren, die mit dem Cluster in Verbindung stehen:

- **MetroCluster Partner**

  Zeigt den Integritätsstatus des MetroCluster Partners an. Über den Link „count“ können Sie weitere Informationen über Zustand und Kapazität der Cluster-Komponenten abrufen.

- **Knoten**

  Zeigt die Anzahl, die Kapazität und den Systemzustand der Nodes an, die zum ausgewählten Cluster gehören. Kapazität gibt die nutzbare Gesamtkapazität über die verfügbare Kapazität an.

- **Storage Virtual Machines**

  Zeigt die Anzahl der SVMs an, die zum ausgewählten Cluster gehören.

- **Aggregate**

  Zeigt die Anzahl, Kapazität und den Systemzustand der Aggregate an, die zum ausgewählten Cluster gehören.

Bereich „Verwandte Gruppen“

Mit können Sie die Liste der Gruppen anzeigen, die den ausgewählten Cluster enthalten.

Bereich „Verwandte Warnungen“

Im Teilfenster „Related Alerts“ können Sie die Liste der Meldungen für das ausgewählte Cluster anzeigen. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Angaben zum Systemzustand/Aggregat

Sie können auf der Seite „Systemzustand/Aggregat-Details“ detaillierte Informationen über das ausgewählte Aggregat anzeigen, z. B. Kapazität, Festplatteninformationen, Konfigurationsdetails und erzeugte Ereignisse. Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für das Aggregat anzeigen.

Befehlsschaltflächen

Bei der Überwachung eines FabricPool-fähigen Aggregats gelten die überzugesund auf dieser Seite überzuschichtenden Werte nur für die lokale Kapazität oder das Performance-Tier. Der auf dem Cloud-Tier verfügbare Speicherplatz wird nicht in den überengagierten Werten dargestellt. Ebenso gelten die Werte für die Aggregatschwellenwerte nur für die lokale Performance-Tier.

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für das ausgewählte Aggregat ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Ermöglicht Ihnen die Navigation zur Seite mit den Details zu Performance/Aggregat.

-

  Ermöglicht Ihnen das Hinzufügen des ausgewählten Aggregats zum Favoriten-Dashboard.

- **Aktionen**
  - Alarm Hinzufügen

    Ermöglicht Ihnen das Hinzufügen einer Warnung zum ausgewählten Aggregat.

  - Schwellenwerte Bearbeiten

    Ermöglicht Ihnen das Ändern der Schwellenwerteinstellungen für das ausgewählte Aggregat.

- **Aggregate Anzeigen**

  Ermöglicht Ihnen die Navigation zur Seite „Bestandsaufnahme“/„Systemzustand“/„Aggregate“.

Registerkarte „Kapazität“

Auf der Registerkarte Kapazität werden ausführliche Informationen zum ausgewählten Aggregat, z. B. Kapazität, Schwellenwerte und tägliche Wachstumsrate, angezeigt.

Standardmäßig werden Kapazitätsereignisse nicht für die Root-Aggregate generiert. Darüber hinaus gelten die von Unified Manager verwendeten Schwellenwertwerte nicht für die Root-Aggregate der Nodes. Nur ein Mitarbeiter des technischen Supports kann die Einstellungen für diese zu erstellenden Ereignisse ändern. Wenn die Einstellungen von einem Mitarbeiter des technischen Supports geändert werden, werden die Schwellenwerte auf das Root-Aggregat des Nodes angewendet.

- * Kapazität*

  Zeigt das Datenkapazitätsdiagramm und das Diagramm Snapshot Kopien an, in dem Kapazitätsdetails zum Aggregat angezeigt werden:

  - Verwendet

    Zeigt den Speicherplatz an, der von Daten im Aggregat verwendet wird.

  - Überengagiert

    Gibt an, dass der Speicherplatz im Aggregat zu hoch belegt ist.

  - Warnung

    Zeigt an, dass der Speicherplatz im Aggregat fast voll ist. Wird diese Schwelle nicht erreicht, wird das Ereignis „Space Fast Full“ generiert.

  - Fehler

    Gibt an, dass der Speicherplatz im Aggregat voll ist. Wird dieser Schwellenwert nicht erreicht, wird das Ereignis „Space Full“ generiert.

◦ Datendiagramm

Zeigt die Gesamtkapazität und die genutzte Datenkapazität des Aggregats an. Wenn das Aggregat zu hoch eingestellt ist, wird ein Flag mit der überzuviel Kapazität angezeigt.

◦ Diagramm Snapshot Kopien

Dieses Diagramm wird nur angezeigt, wenn die verwendete Snapshot-Kapazität oder die Snapshot-Reserve nicht null ist.

Beide Diagramme zeigen die Kapazität an, in der die Snapshot-Kapazität die Snapshot-Reserve überschreitet, wenn die genutzte Snapshot-Kapazität die Snapshot-Reserve überschreitet.

- * Cloud Tier*

Zeigt Kapazitätsdetails über das Cloud-Tier für FabricPool-fähige Aggregate an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

◦ Verwendet

Zeigt den Speicherplatz an, der von Daten im Cloud-Tier verwendet wird.

◦ Nicht Verfügbar

Zeigt den Speicherplatz in der Cloud-Tier für ein Objekt aus Amazon S3, Microsoft Azure Cloud FabricPool oder IBM Cloud Object Storage an, das nicht verwendet werden kann. Dieser Speicherplatz kann mit einem anderen FabricPool-fähigen Aggregat gemeinsam genutzt werden.

◦ Datendiagramm

Bei Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage oder Alibaba Cloud Object Storage werden die Gesamtkapazität, die von diesem Cluster lizenziert wurde, die von diesem Aggregat verwendete Menge und die nicht nutzbare Menge von anderen Aggregaten, die die Cloud-Tier verwenden, in der Übersicht angezeigt.

Bei einer StorageGRID wird nur die von diesem Aggregat genutzte Gesamtkapazität angezeigt.

- **Details**

Zeigt detaillierte Informationen zur Kapazität an.

◦ Gesamtkapazität

Zeigt die Gesamtkapazität im Aggregat an.

◦ Datenkapazität

Zeigt den vom Aggregat (genutzte Kapazität) verwendeten Speicherplatz und die Menge des verfügbaren Speicherplatzes im Aggregat an (freie Kapazität).

◦ Snapshot-Reserve

Zeigt die verwendete und freie Snapshot Kapazität des Aggregats an.

◦ Überzuviel Kapazität

Zeigt die Überbelegung des Aggregats an. Aufgrund einer Überbelegung von Aggregaten bieten Sie mehr Storage, als tatsächlich in einem bestimmten Aggregat verfügbar ist, sofern nicht alle Storage-Ressourcen derzeit verwendet werden. Bei Nutzung von Thin Provisioning kann die Gesamtgröße der Volumes im Aggregat die Gesamtkapazität des Aggregats überschreiten.

Wenn Sie Ihr Aggregat zu hoch ansetzen, müssen Sie den verfügbaren Speicherplatz sorgfältig überwachen und Storage nach Bedarf hinzufügen, um Schreibfehler aufgrund von unzureichendem Speicherplatz zu vermeiden.

- Cloud-Tier

  Bei Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage oder Alibaba Cloud Object Storage werden die gesamte lizenzierte Kapazität, die durch dieses Aggregat benötigte Menge, die in anderen Aggregaten benötigte Menge und die freie Kapazität für das Cloud-Tier angezeigt. Bei einer StorageGRID wird nur die von diesem Aggregat genutzte Gesamtkapazität angezeigt.

- Cache-Speicherplatz Insgesamt

  Zeigt den gesamten Speicherplatz der Solid State-Laufwerke (SSDs) bzw. Zuweisungseinheiten an, die einem Flash Pool Aggregat hinzugefügt werden. Wenn Sie Flash Pool für ein Aggregat aktiviert, aber keine SSDs hinzugefügt haben, wird der Cache-Speicherplatz als 0 KB angezeigt.

  Dieses Feld ist ausgeblendet, wenn Flash Pool für ein Aggregat deaktiviert ist.

- Schwellenwerte Für Aggregate

  Zeigt die folgenden Kapazitätsschwellenwerte für das Aggregat an:

  - Nahezu Vollständig. Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Aggregat fast voll ist.

  - Vollständiger Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Aggregat voll ist.

  - Nahezu Überbeanspruchung Des Schwellenwerts

    Gibt den Prozentsatz an, mit dem ein Aggregat fast überbelegt ist.

  - Überbeanspruchung Des Schwellenwerts

    Gibt den Prozentsatz an, zu dem ein Aggregat überengagiert ist.

- Weitere Details: Tägliche Wachstumsrate

  Zeigt den im Aggregat verwendeten Festplattenspeicher an, wenn die Änderungsrate zwischen den letzten beiden Proben 24 Stunden andauert.

  Wenn ein Aggregat beispielsweise 10 GB Festplattenspeicher bei 2:00 Uhr und 12 GB bei 6:00 Uhr nutzt, beträgt die tägliche Wachstumsrate (GB) für dieses Aggregat 2 GB.

- Volume-Verschiebung

  Zeigt die Anzahl der aktuell laufenden Volume-Move-Vorgänge an:

- Volumes Aus

  Zeigt die Anzahl und Kapazität der Volumes an, die aus dem Aggregat verschoben werden.

Über den Link können Sie weitere Details anzeigen, beispielsweise den Volume-Namen, die Aggregate, zu denen das Volume verschoben wird, den Status der Verschiebung eines Volumes und die geschätzte Endzeit.

- Volumes In

  Zeigt die Anzahl und die verbleibende Kapazität der Volumes an, die in das Aggregat verschoben werden.

Über den Link können Sie weitere Details anzeigen, beispielsweise den Volume-Namen, das Aggregat, aus dem das Volume verschoben wird, den Status der Verschiebung des Volumes und die geschätzte Endzeit.

- Geschätzte genutzte Kapazität nach der Verschiebung eines Volumes

  Zeigt den geschätzten belegten Speicherplatz (in Prozent und in KB, MB, GB usw.) im Aggregat an, nachdem die Verschiebevorgänge des Volumes abgeschlossen sind.

- **Kapazitätsüberblick - Volumen**

  Zeigt Diagramme an, die Informationen zur Kapazität der Volumes im Aggregat enthalten sind. Es wird die Menge an Speicherplatz angezeigt, die vom Volume (genutzte Kapazität) und die Menge des verfügbaren Speicherplatzes (freie Kapazität) im Volume verwendet wird. Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, wird die vom Volume verwendete Menge an Speicherplatz (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht verwendet werden kann (nicht nutzbare Kapazität), da die Kapazität des Aggregats angezeigt wird.

  Sie können das anzuangezeigte Diagramm in den Dropdown-Listen auswählen. Sie können die im Diagramm angezeigten Daten sortieren, um Details wie die genutzte Größe, die bereitgestellte Größe, die verfügbare Kapazität, die schnellste tägliche Wachstumsrate und die langsamste Wachstumsrate anzuzeigen. Sie können die Daten auf Grundlage der Storage Virtual Machines (SVMs) filtern, die die Volumes im Aggregat enthalten. Sie können auch Details zu Volumes anzeigen, die über Thin Provisioning bereitgestellt wurden. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den Bereich von Interesse positionieren. Standardmäßig werden im Diagramm die Top 30 der gefilterten Volumes im Aggregat angezeigt.

Registerkarte „Festplatteninformationen“

Zeigt detaillierte Informationen zu den Festplatten im ausgewählten Aggregat an, einschließlich RAID-Typ und -Größe sowie Typ der im Aggregat verwendeten Festplatten. Auf der Registerkarte werden auch die RAID-Gruppen und die verwendeten Festplatten (z. B. SAS, ATA, FCAL, SSD oder VMDISK) grafisch dargestellt. Weitere Informationen, wie z. B. der Schacht, das Shelf und die Drehgeschwindigkeit der Festplatte, können Sie mit dem Cursor über die Parity-Festplatten und die Daten-Festplatten anzeigen.

- * Daten*

  Grafische Anzeige von Details zu dedizierten Datenträgern, freigegebenen Datenträgern oder beidem. Wenn die Datenfestplatten freigegebene Laufwerke enthalten, werden grafische Details der freigegebenen Laufwerke angezeigt. Wenn die Datenfestplatten dedizierte Laufwerke und freigegebene Festplatten enthalten, werden grafische Details sowohl der dedizierten Datenlaufwerke als auch der freigegebenen Datenträger angezeigt.

- **RAID-Details**

  RAID-Details werden nur für dedizierte Festplatten angezeigt.

  - Typ

    Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

  - Gruppengröße

    Zeigt die maximale Anzahl an Laufwerken an, die in der RAID-Gruppe zulässig sind.

  - Gruppen

    Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

- **Verwendete Festplatten**
  - Effektiver Typ

    Zeigt die Typen der Datenfestplatten an (z. B. ATA, SATA, FCAL, SSD, Oder VMDISK) im Aggregat.

  - Datenfestplatten

    Zeigt die Anzahl und Kapazität der Datenfestplatten an, die einem Aggregat zugewiesen sind. Details zur Datenfestplatte werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Festplatten enthält.

  - Parity-Festplatten

    Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat zugewiesen werden. Details zur Parity-Festplatte werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Festplatten enthält.

  - Gemeinsame Festplatten

    Zeigt die Anzahl und Kapazität der freigegebenen Datenfestplatten an, die einem Aggregat zugewiesen sind. Details zu gemeinsam genutzten Festplatten werden nur angezeigt, wenn das Aggregat freigegebene Festplatten enthält.

- **Ersatzfestplatten**

  Zeigt den effektiven Typ, die Nummer und die Kapazität der Ersatzfestplatten an, die für den Knoten im ausgewählten Aggregat verfügbar sind.

  Bei einem Failover eines Aggregats an den Partner-Node zeigt Unified Manager nicht alle freien Festplatten an, die mit dem Aggregat kompatibel sind.

- **SSD Cache**

  Enthält Details zu dedizierten Cache-SSD-Festplatten und Shared Cache SSD-Festplatten.

  Für die dedizierten Cache-SSD-Festplatten werden folgende Details angezeigt:

  - **RAID-Details**

- Typ

  Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

- Gruppengröße

  Zeigt die maximale Anzahl an Laufwerken an, die in der RAID-Gruppe zulässig sind.

- Gruppen

  Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

◦ **Verwendete Festplatten**

- Effektiver Typ

  Gibt an, dass die Festplatten, die für den Cache im Aggregat verwendet werden, vom Typ SSD sind.

- Datenfestplatten

  Zeigt die Anzahl und Kapazität der Datenfestplatten an, die einem Aggregat für den Cache zugewiesen werden.

- Parity-Festplatten

  Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat für den Cache zugewiesen werden.

◦ **Ersatzfestplatten**

Zeigt den effektiven Typ, die Nummer und die Kapazität der Ersatzfestplatten an, die für den Knoten im ausgewählten Aggregat für den Cache verfügbar sind.

Bei einem Failover eines Aggregats an den Partner-Node zeigt Unified Manager nicht alle freien Festplatten an, die mit dem Aggregat kompatibel sind.

Enthält die folgenden Details für den gemeinsamen Cache:

◦ **Speicherpool**

Zeigt den Namen des Speicherpools an. Sie können den Zeiger über den Speicherpool-Namen verschieben, um folgende Details anzuzeigen:

- Status

  Zeigt den Status des Speicherpools an, der gesund oder ungesund sein kann.

- Gesamtzuweisungen

  Zeigt die Gesamtzuordnungseinheiten und die Größe im Speicherpool an.

- Größe Der Zuordnungseinheit

  Zeigt den minimalen Speicherplatz im Speicherpool an, der einem Aggregat zugewiesen werden kann.

        - Festplatten

          Zeigt die Anzahl der Laufwerke an, die zum Erstellen des Speicherpools verwendet werden. Wenn die Anzahl der Laufwerke in der Spalte „Speicherpool“ und die Anzahl der Festplatten, die auf der Registerkarte „Laufwerksinformationen“ für diesen Speicherpool angezeigt werden, nicht übereinstimmen, zeigt dies an, dass eine oder mehrere Festplatten beschädigt sind und der Speicherpool ungesund ist.

        - Zuweisung Verwendet

          Zeigt Anzahl und Größe der von den Aggregaten verwendeten Zuordnungseinheiten an. Sie können auf den Aggregatnamen klicken, um Details zum Aggregat anzuzeigen.

        - Verfügbare Zuweisung

          Zeigt die Anzahl und Größe der für die Nodes verfügbaren Zuweisungseinheiten an. Sie können auf den Node-Namen klicken, um weitere Details zum Aggregat anzuzeigen.

    - **Zugewiesener Cache**

      Zeigt die Größe der vom Aggregat verwendeten Zuordnungseinheiten an.

    - **Zuordnungseinheiten**

      Zeigt die Anzahl der vom Aggregat verwendeten Zuordnungseinheiten an.

    - **Festplatten**

      Zeigt die Anzahl der Festplatten im Speicherpool an.

    - **Details**
        - Storage-Pool

          Zeigt die Anzahl der Speicherpools an.

        - Gesamtgröße

          Zeigt die Gesamtgröße der Speicherpools an.

- * Cloud Tier*

  Zeigt den Namen des Cloud-Tiers an, sofern Sie ein FabricPool-fähiges Aggregat konfiguriert haben und die gesamte lizenzierte Kapazität für Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage oder Alibaba Cloud Object Storage Objekte anzeigt.

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration werden Details zum ausgewählten Aggregat angezeigt, z. B. hinsichtlich seines Cluster-Nodes, des Blocktyps, des RAID-Typs, der RAID-Größe und der Anzahl der RAID-Gruppen:

- **Übersicht**
    - Knoten

      Zeigt den Namen des Node an, der das ausgewählte Aggregat enthält.

- Blocktyp

  Zeigt das Blockformat des Aggregats an: Entweder 32-Bit oder 64-Bit.

- RAID-Typ

  Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP, RAID-TEC oder gemischtes RAID).

- RAID-Größe

  Zeigt die Größe der RAID-Gruppe an.

- RAID-Gruppen

  Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

- SnapLock-Typ

  Zeigt den SnapLock-Typ des Aggregats an.

- * Cloud Tier*

  Wenn es sich um ein FabricPool-fähiges Aggregat handelt, werden die Details für den Objektspeicher angezeigt. Je nach Speicheranbieter sind einige Felder unterschiedlich:

  - Name

    Zeigt den Namen des Objektspeichers an, als er von ONTAP erstellt wurde.

  - Objekt-Storage-Provider

    Zeigt den Namen des Storage-Providers an, z. B. StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud oder Alibaba Cloud Object Storage.

  - Objektspeichername (FQDN) oder Servername

    Zeigt den FQDN des Objektspeichers an.

  - Auf Schlüssel oder Konto zugreifen

    Zeigt den Zugriffsschlüssel oder das Konto für den Objektspeicher an.

  - Bucket-Name oder Container-Name

    Zeigt den Bucket- oder Container-Namen des Objektspeichers an.

  - SSL

    Zeigt an, ob die SSL-Verschlüsselung für den Objektspeicher aktiviert ist.

Historienbereich

Im Bereich Verlauf werden Diagramme angezeigt, die Informationen über die Kapazität des ausgewählten Aggregats enthalten. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Verlaufsdiagramme können Ihnen bei der Identifizierung von Trends helfen: Wenn beispielsweise die Aggregatnutzung konsistent den Schwellenwert „nahezu voll“ überschreitet, können Sie die entsprechenden Maßnahmen ergreifen.

Verlaufsdiagramme zeigen folgende Informationen an:

- **Verwendete Aggregatskapazität (%)**

  Zeigt die verwendete Kapazität im Aggregat und den Trend in der Art und Weise an, wie die aggregierte Kapazität basierend auf dem Nutzungsverlauf als Liniendiagramme in Prozentsätzen auf der vertikalen (y) Achse verwendet wird. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Kapazität verwendet“ klicken, wird die Diagramm-Zeile mit der verwendeten Kapazität ausgeblendet.

- **Verwendete Aggregatskapazität vs Gesamtkapazität**

  Zeigt den Trend in der Verwendung der Aggregatskapazität basierend auf dem Nutzungsverlauf sowie der verwendeten Kapazität und der Gesamtkapazität als Liniendiagramme in Byte, Kilobyte, Megabyte, Und so weiter, auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „verwendete Trend-Kapazität“ klicken, wird das Diagramm „verwendete Trendkapazität“ ausgeblendet.

- **Verwendete Aggregatskapazität (%) gegenüber dem Einsatz (%)**

  Zeigt den Trend an, wie die aggregierte Kapazität basierend auf dem Nutzungsverlauf verwendet wird, sowie den belegten Speicherplatz als Liniendiagramme in Prozent auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Space engagierte“ klicken, wird die Zeile „Space engagierte“ ausgeblendet.

Ereignisliste

In der Ereignisliste werden Details zu neuen und bestätigten Ereignissen angezeigt:

- **Severity**

  Zeigt den Schweregrad des Ereignisses an.

- **Veranstaltung**

  Zeigt den Ereignisnamen an.

- **Auslösezeit**

Zeigt die Zeit an, die seit der Erzeugung des Ereignisses verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel für den Zeitpunkt angezeigt, zu dem das Ereignis generiert wurde.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie den Clusterknoten, Volumes und Festplatten anzeigen, die mit dem Aggregat in Verbindung stehen:

- **Knoten**

  Zeigt die Kapazität und den Integritätsstatus des Node an, der das Aggregat enthält. Kapazität gibt die nutzbare Gesamtkapazität über die verfügbare Kapazität an.

- **Aggregate im Knoten**

  Zeigt die Anzahl und Kapazität aller Aggregate im Cluster-Node an, der das ausgewählte Aggregat enthält. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt. Wenn z. B. ein Cluster-Node zehn Aggregate enthält, von denen fünf den Warnstatus und die verbleibenden fünf den kritischen Status anzeigen, ist der angezeigte Status „kritisch“.

- **Bände**

  Zeigt die Anzahl und Kapazität der FlexVol Volumes und FlexGroup Volumes im Aggregat an. Die Anzahl umfasst keine FlexGroup-Komponenten. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt.

- **Ressourcen-Pool**

  Zeigt die mit dem Aggregat verbundenen Ressourcen-Pools an.

- **Festplatten**

  Zeigt die Anzahl der Festplatten im ausgewählten Aggregat an.

Bereich „Verwandte Warnungen“

Im Bereich „Related Alerts“ können Sie die Liste der Warnmeldungen anzeigen, die für das ausgewählte Aggregat erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Einzelheiten zu Sicherung/Auftrag

Auf der Seite „Schutz-/Jobdetails“ können Sie den Status und weitere Informationen zu laufenden, in der Warteschlange befindlichen oder abgeschlossenen Sicherungsaufgaben anzeigen. Diese Informationen können Sie zur Überwachung des Arbeitsfortschritts des Schutzjobs und zur Behebung von Fehlern bei Jobs verwenden.

Jobzusammenfassung

In der Jobübersicht werden die folgenden Informationen angezeigt:

- Job-ID

- Typ
- Bundesland
- Einreichungszeit
- „Ende“
- Dauer

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Aktualisieren**

  Aktualisiert die Aufgabenliste und die Eigenschaften, die jeder Aufgabe zugeordnet sind.

- **Jobs Anzeigen**

  Kehrt zur Seite „Schutz/Jobs“ zurück.

Aufgabenliste

Die Aufgabenliste zeigt in einer Tabelle alle Aufgaben an, die mit einem bestimmten Job verknüpft sind, und die Eigenschaften, die mit jeder Aufgabe verknüpft sind.

- **Startzeit**

  Zeigt den Tag und die Uhrzeit an, zu der die Aufgabe gestartet wurde. Standardmäßig werden die letzten Aufgaben oben in der Spalte angezeigt, und ältere Aufgaben werden unten angezeigt.

- **Typ**

  Zeigt den Aufgabentyp an.

- **Bundesland**

  Der Status einer bestimmten Aufgabe:

  - **Abgeschlossen**

    Die Aufgabe ist abgeschlossen.

  - **Queued**

    Die Aufgabe wird ausgeführt.

  - **Laufen**

    Die Aufgabe wird ausgeführt.

  - **Warten**

    Ein Job wurde gesendet, und einige zugeordnete Aufgaben warten darauf, in die Warteschlange gestellt und ausgeführt zu werden.

- **Status**

  Zeigt den Aufgabenstatus an:

  - **Fehler (❗)**

    Die Aufgabe ist fehlgeschlagen.

  - **Normal (✅)**

    Die Aufgabe war erfolgreich.

  - **Übersprungen (↷)**

    Eine Aufgabe ist fehlgeschlagen, sodass nachfolgende Aufgaben übersprungen werden.

- **Dauer**

  Zeigt die verstrichene Zeit seit Beginn der Aufgabe an.

- **Abgeschlossene Zeit**

  Zeigt die Zeit an, zu der die Aufgabe abgeschlossen ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Task-ID**

  Zeigt die GUID an, die eine einzelne Aufgabe für einen Job identifiziert. Die Spalte kann sortiert und gefiltert werden. Standardmäßig ist diese Spalte ausgeblendet.

- **Abhängigkeitsreihenfolge**

  Zeigt eine Ganzzahl an, die die Tasksequenz in einem Diagramm darstellt, wobei der ersten Aufgabe Null zugewiesen wird. Standardmäßig ist diese Spalte ausgeblendet.

- **Fenster mit den Aufgabendetails**

  Zeigt zusätzliche Informationen zu jeder Aufgabe an, einschließlich des Aufgabennamens, der Aufgabenbeschreibung und, falls die Aufgabe fehlgeschlagen ist, einen Grund für den Fehler.

- **Aufgabenbereich Messages**

  Zeigt Meldungen an, die für die ausgewählte Aufgabe spezifisch sind. Meldungen können einen Grund für den Fehler und Vorschläge zur Behebung enthalten. Nicht alle Aufgaben zeigen Aufgabenmeldungen an.

Benutzer hinzufügen

Sie können lokale Benutzer oder Datenbankbenutzer über die Seite Verwaltung/Benutzer hinzufügen. Sie können auch Remote-Benutzer oder -Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Sie können diesen Benutzern Rollen zuweisen. Anhand der Berechtigungen der Rollen können Benutzer Storage-Objekte und -Daten mit Unified Manager managen oder die Daten in einer Datenbank anzeigen.

Bevor Sie beginnen

- Sie müssen die OnCommand-Administratorrolle besitzen.
- Um einen Remote-Benutzer oder eine Remotegruppe hinzuzufügen, müssen Sie die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsserver konfiguriert haben.
- Wenn Sie die SAML-Authentifizierung so konfigurieren möchten, dass ein Identitäts-Provider (IdP) Benutzer authentifiziert, die auf die grafische Schnittstelle zugreifen, stellen Sie sicher, dass diese Benutzer als „`remote`“-Benutzer definiert sind.

  Der Zugriff auf die Benutzeroberfläche ist Benutzern vom Typ „`local`“ oder „`maintBuße`“ nicht erlaubt, wenn die SAML-Authentifizierung aktiviert ist.

Über diese Aufgabe

Wenn Sie eine Gruppe aus Windows Active Directory hinzufügen, können sich alle direkten Mitglieder und geschachtelten Untergruppen bei Unified Manager authentifizieren, es sei denn, geschachtelte Untergruppen sind deaktiviert. Wenn Sie eine Gruppe von OpenLDAP oder anderen Authentifizierungsdiensten hinzufügen, können sich nur die direkten Mitglieder dieser Gruppe bei Unified Manager authentifizieren.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.
2. Klicken Sie auf der Seite **Verwaltung/Benutzer** auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld **Benutzer hinzufügen** den Benutzertyp aus, den Sie hinzufügen möchten, und geben Sie die erforderlichen Informationen ein.

   Wenn Sie die erforderlichen Benutzerinformationen eingeben, müssen Sie eine E-Mail-Adresse angeben, die für diesen Benutzer eindeutig ist. Sie müssen vermeiden, E-Mail-Adressen anzugeben, die von mehreren Benutzern gemeinsam verwendet werden.

4. Klicken Sie Auf **Hinzufügen**.

Definitionen von Benutzerrollen

Der Wartungs-Benutzer oder der OnCommand-Administrator weist jedem Benutzer eine Rolle zu. Jede Rolle enthält bestimmte Berechtigungen. Der Umfang der Aktivitäten, die Sie in Unified Manager ausführen können, hängt von der Ihnen zugewiesenen Rolle ab und welchen Berechtigungen die Rolle enthält.

Unified Manager enthält die folgenden vordefinierten Benutzerrollen:

- **Betreiber**

  Anzeige von Storage-Systeminformationen und anderen von Unified Manager erfassten Daten, einschließlich Verläufe und Kapazitätstrends Mit dieser Rolle kann der Speicherbetreiber Notizen zu den Ereignissen anzeigen, zuweisen, bestätigen, auflösen und hinzufügen.

- * Storage Administrator*

  Konfiguration von Storage-Managementvorgängen in Unified Manager Diese Rolle ermöglicht es dem Storage-Administrator, Schwellenwerte zu konfigurieren und Alarme sowie andere für das Storage-Management spezifische Optionen und Richtlinien zu erstellen.

- **OnCommand-Administrator**

  Konfiguriert Einstellungen, die in keinem Zusammenhang mit dem Storage-Management stehen. Diese Rolle ermöglicht das Management von Benutzern, Sicherheitszertifikaten, Datenbankzugriff und Verwaltungsoptionen, einschließlich Authentifizierung, SMTP, Networking und AutoSupport.

  > Wenn Unified Manager auf Linux-Systemen installiert wird, heißt der ursprüngliche Benutzer mit der OnCommand-Administratorrolle automatisch „`umadmin`“.

- **Integrationsschema**

  Diese Rolle bietet schreibgeschützten Zugriff auf Unified Manager Datenbankansichten für die Integration von Unified Manager mit OnCommand Workflow Automation (WFA).

- **Schema Melden**

  Diese Rolle ermöglicht einen schreibgeschützten Zugriff auf Reporting und andere Datenbankansichten direkt aus der Unified Manager Datenbank. Folgende Datenbanken stehen zur Verfügung:

  - netapp_Modell_Ansicht
  - netapp_Performance
  - Okum
  - Ocum_Report
  - Ocum_Report_birt
  - opm
  - Skalemonitor

Definitionen der Benutzertypen

Ein Benutzertyp gibt die Art des Kontos an, das der Benutzer besitzt und umfasst Remote-Benutzer, Remote-Gruppen, lokale Benutzer, Datenbankbenutzer und Wartungbenutzer. Jeder dieser Typen hat seine eigene Rolle, die von einem Benutzer mit der Rolle „OnCommand Administrator“ zugewiesen wird.

Unified Manager-Benutzertypen sind wie folgt:

- **Benutzer der Wartung**

  Erstellt während der Erstkonfiguration von Unified Manager. Der Wartungsbenutzer erstellt dann weitere Benutzer und weist Rollen zu. Der Benutzer der Wartung ist außerdem der einzige Benutzer, der Zugriff auf die Wartungskonsole hat. Wenn Unified Manager auf einem Red hat Enterprise Linux- oder CentOS-System installiert ist, erhält der Wartungbenutzer den Benutzernamen „`umadmin.`“.

- **Lokaler Benutzer**

  Greift auf die Unified Manager-Benutzeroberfläche zu und führt Funktionen basierend auf der Rolle durch, die der Wartungsbenutzer oder Benutzer mit der OnCommand-Administratorrolle angegeben hat.

- **Remote-Gruppe**

  Eine Gruppe von Benutzern, die mit den auf dem Authentifizierungsserver gespeicherten

Anmeldeinformationen auf die Benutzeroberfläche von Unified Manager zugreifen. Der Name dieses Kontos muss mit dem Namen einer auf dem Authentifizierungsserver gespeicherten Gruppe übereinstimmen. Allen Benutzern innerhalb der Remote-Gruppe wird über ihre individuellen Benutzeranmeldeinformationen der Zugriff auf die Unified Manager-Benutzeroberfläche gewährt. Remote-Gruppen können Funktionen entsprechend ihren zugewiesenen Rollen ausführen.

- **Remote-Benutzer**

  Greift über die auf den Authentifizierungsserver gespeicherten Anmeldeinformationen auf die Unified Manager-UI zu. Ein Remote-Benutzer führt Funktionen basierend auf der Rolle aus, die der Wartungsbenutzer oder ein Benutzer mit der OnCommand-Administratorrolle zugewiesen hat.

- **Datenbankbenutzer**

  Hat schreibgeschützten Zugriff auf Daten in der Unified Manager-Datenbank, hat keinen Zugriff auf die Unified Manager-Webschnittstelle oder die Wartungskonsole und kann keine API-Aufrufe ausführen.

Unified Manager Benutzer-Rollen und -Funktionen

Anhand der Ihnen zugewiesenen Benutzerrolle können Sie festlegen, welche Vorgänge Sie in Unified Manager ausführen können.

In der folgenden Tabelle sind die Funktionen aufgeführt, die die einzelnen Benutzerrollen ausführen können:

Funktion	Operator	Storage-Administrator	OnCommand Administrator	Integrationsschema	Berichtschema
Anzeigen von Speichersysteminformationen	•	•	•	•	•
Andere Daten wie Verläufe und Kapazitätstrends anzeigen	•	•	•	•	•
Ereignisse anzeigen, zuweisen und lösen	•	•	•		
Anzeigen von Storage-Serviceobjekten, z. B. SVM-Zuordnungen und Ressourcenpools	•	•	•		

Funktion	Operator	Storage-Administrator	OnCommand Administrator	Integrationsschema	Berichtschema
Anzeigen von Schwellenwertrichtlinien	•	•	•		
Management von Storage-Serviceobjekten wie SVM-Zuordnungen und Ressourcenpools		•	•		
Definieren von Warnmeldungen		•	•		
Optionen für das Storage Management managen		•	•		
Storage Management-Richtlinien managen		•	•		
Benutzer managen			•		
Management von Verwaltungsoptionen			•		
Definieren Sie Schwellenwertrichtlinien			•		
Datenbankzugriff managen			•		

Funktion	Operator	Storage-Administrator	OnCommand Administrator	Integrationsschema	Berichtschema
Managen Sie die Integration in WFA und erhalten Sie Zugriff auf die Datenbankansichten				•	
Schreibgeschützter Zugriff auf Berichte und andere Datenbankansichten					•
Planen und Speichern von Berichten	•	•	•		
Importierte Berichte importieren und löschen			•		

Unterstützte CLI-Befehle von Unified Manager

Als Storage-Administrator führen Sie mit den CLI-Befehlen Abfragen für die Storage-Objekte durch, z. B. für Cluster, Aggregate, Volumes, Qtrees und LUNs. Sie können die CLI-Befehle verwenden, um die interne Datenbank von Unified Manager und die ONTAP-Datenbank abzufragen. Sie können auch CLI-Befehle in Skripten verwenden, die zu Beginn oder am Ende eines Vorgangs ausgeführt oder ausgeführt werden, wenn eine Meldung ausgelöst wird.

Allen Befehlen muss der Befehl vorangestellt sein `um cli login` Und einen gültigen Benutzernamen und ein gültiges Passwort für die Authentifizierung.

CLI-Befehl	Beschreibung	Ausgabe
`um run cmd [ -t <timeout> ] <cluster> <command>`	Die einfachste Methode, einen Befehl auf einem oder mehreren Hosts auszuführen. Hauptsächlich wird verwendet für Alert Scripting um ONTAP zu erhalten oder eine Operation durchzuführen. Das optionale Argument für die Zeitüberschreitung setzt eine maximale Zeitgrenze (in Sekunden), damit der Befehl auf dem Client ausgeführt werden kann. Der Standardwert ist 0 (ewig warten).	Nach Erhalt bei ONTAP.
`um run query <sql command>`	Führt eine SQL-Abfrage aus. Es sind nur Abfragen erlaubt, die aus der Datenbank gelesen werden. Aktualisierungsvorgänge, Einfügevorgänge oder Löschvorgänge werden nicht unterstützt.	Die Ergebnisse werden in tabellarischer Form angezeigt. Wenn ein leerer Satz zurückgegeben wird, oder wenn ein Syntaxfehler oder eine fehlerhafte Anforderung vorliegt, wird die entsprechende Fehlermeldung angezeigt.
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Fügt der Liste der gemanagten Speichersysteme eine Datenquelle hinzu. Eine Datenquelle beschreibt, wie Verbindungen zu Speichersystemen hergestellt werden. Beim Hinzufügen einer Datenquelle müssen die Optionen -U (Benutzername) und -P (Passwort) angegeben werden. Die Option -t (Protocol) gibt das Protokoll an, das zur Kommunikation mit dem Cluster verwendet wird (http oder https). Wenn das Protokoll nicht angegeben wird, werden beide Protokolle versucht, die Option -p (Port) gibt den Port an, der zur Kommunikation mit dem Cluster verwendet wird. Wenn der Port nicht angegeben wird, wird versucht, den Standardwert des entsprechenden Protokolls zu verwenden. Dieser Befehl kann nur vom Storage-Admin ausgeführt werden.	Fordert den Benutzer auf, das Zertifikat anzunehmen, und druckt die entsprechende Meldung.

CLI-Befehl	Beschreibung	Ausgabe
`um datasource list [ <datasource-id>]`	Zeigt die Datenquellen für verwaltete Speichersysteme an.	Zeigt die folgenden Werte im Tabellenformat an: `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message.`
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	Ändert eine oder mehrere Datenquellenoptionen. Kann nur vom Storage-Administrator ausgeführt werden.	Zeigt die entsprechende Meldung an.
`um datasource remove <datasource-id>`	Entfernt die Datenquelle aus Unified Manager.	Zeigt die entsprechende Meldung an.
`um option list [ <option> .. ]`	Listenoptionen.	Zeigt die folgenden Werte im Tabellenformat an: `Name, Value, Default Value, and Requires Restart.`
`um option set <option-name>=<option-value> [ <option-name>=<option-value> ... ]`	Legt eine oder mehrere Optionen fest. Der Befehl kann nur vom Storage-Admin ausgeführt werden.	Zeigt die entsprechende Meldung an.
`um version`	Zeigt die Softwareversion von Unified Manager an.	`Version ("7.0")`
`um lun list [-q] [ -ObjectType <object-id>]`	Führt die LUNs nach dem Filtern auf das angegebene Objekt auf. -q ist für alle Befehle geeignet, keine Kopfzeile anzuzeigen. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, svm: Beispiel: `um lun list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Mit dem Befehl werden alle LUNs im Cluster mit der ID 1 aufgeführt.	Zeigt die folgenden Werte im Tabellenformat an: `ID and LUN path.`

CLI-Befehl	Beschreibung	Ausgabe
`um svm list [-q] [ -ObjectType <object-id>]`	Listet die SVMs nach dem Filtern auf dem angegebenen Objekt auf. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, svm: Beispiel: `um svm list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle SVMs innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an: `Name and Cluster ID`.
`um qtree list [-q] [ -ObjectType <object-id>]`	Führt die qtrees nach dem Filtern auf dem angegebenen Objekt auf. -q ist für alle Befehle geeignet, keine Kopfzeile anzuzeigen. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, svm: Beispiel: `um qtree list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Mit dem Befehl werden alle qtrees im Cluster mit der ID 1 aufgelistet.	Zeigt die folgenden Werte im Tabellenformat an: `Qtree ID and Qtree Name`.
`um disk list [-q] [- ObjectType <object-id>]`	Listet die Festplatten nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster sein. Beispiel: `um disk list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Festplatten im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `ObjectType and object-id`.
`um cluster list [-q] [- ObjectType <object-id>]`	Listet die Cluster nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster, lun, sein Qtree, Volume, Kontingent, svm. Beispiel:`um cluster list -aggr 1` In diesem Beispiel ist "-aggr" der objectType und "1" die objectId. Der Befehl listet das Cluster auf, zu dem das Aggregat mit der ID 1 gehört.	Zeigt die folgenden Werte im Tabellenformat an: `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key`.

CLI-Befehl	Beschreibung	Ausgabe
`um cluster node list [-q] [-ObjectType <object-id>]`	Führt die Cluster-Nodes nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster sein. Beispiel: `um cluster node list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Nodes im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Name and Cluster ID.`
`um volume list [-q] [-ObjectType <object-id>]`	Listet die Volumes nach dem Filtern auf dem angegebenen Objekt auf. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, svm, Aggregat: Beispiel: `um volume list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Volumes im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Volume ID and Volume Name.`
`um quota user list [-q] [-ObjectType <object-id>]`	Listet die Quota-Benutzer nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann qtree, Cluster, Volume, Kontingent und svm sein. Beispiel: `um quota user list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Kontingentbenutzer innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `ID, Name, SID and Email.`
`um aggr list [-q] [-ObjectType <object-id>]`	Führt die Aggregate nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster, Volume sein. Beispiel: `um aggr list -cluster 1` In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Aggregate innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Aggr ID, and Aggr Name.`

CLI-Befehl	Beschreibung	Ausgabe
`um event ack <event-ids>`	Bestätigt ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event resolve <event-ids>`	Löst ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event assign -u <username> <event-id>`	Weist einem Benutzer ein Ereignis zu.	Zeigt die entsprechende Meldung an.
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Listet die vom System oder Benutzer generierten Ereignisse auf. Filtern von Ereignissen nach Quelle, Status und IDs	Zeigt die folgenden Werte im Tabellenformat an `Source, Source type, Name, Severity, State, User and Timestamp.`
`um cli login -u <username> [-p <password>`	Melden Sie sich bei der CLI an. Die Sitzung läuft nach drei Stunden ab dem Zeitpunkt der Anmeldung ab. Danach muss sich der Benutzer erneut anmelden.	Zeigt die entsprechende Meldung an.
`um cli logout`	Melden Sie sich über die CLI ab.	Zeigt die entsprechende Meldung an.
`um backup restore -f <backup_file_path_and_name>`	Stellt eine Datenbanksicherung mithilfe von .7z-Dateien wieder her.	Zeigt die entsprechende Meldung an.
`um help`	Zeigt alle Unterbefehle der ersten Ebene an.	Zeigt alle Unterbefehle der ersten Ebene an.

Verwenden der Wartungskonsole

Sie können mit der Wartungskonsole Netzwerkeinstellungen konfigurieren, das System, auf dem Unified Manager installiert ist, konfigurieren und verwalten sowie andere Wartungsaufgaben ausführen, mit denen Sie mögliche Probleme vermeiden und beheben können.

Welche Funktionen bietet die Wartungskonsole

Über die Unified Manager-Wartungskonsole können Sie die Einstellungen Ihres Unified Manager-Systems beibehalten und die erforderlichen Änderungen vornehmen, um mögliche Probleme zu vermeiden.

Je nach Betriebssystem, auf dem Unified Manager installiert ist, bietet die Wartungskonsole folgende

Funktionen:

- Beheben Sie alle Probleme mit Ihrer virtuellen Appliance, insbesondere wenn die Unified Manager Webschnittstelle nicht verfügbar ist
- Upgrade auf neuere Versionen von Unified Manager
- Generieren Sie Support Bundles, um den technischen Support zu erhalten
- Netzwerkeinstellungen konfigurieren
- Ändern Sie das Wartungs-Benutzerpasswort
- Stellen Sie eine Verbindung zu einem externen Datenanbieter her, um Leistungsstatistiken zu senden
- Ändern Sie die interne Erfassung von Performance-Daten
- Stellen Sie die Unified Manager-Datenbank- und Konfigurationseinstellungen aus einer zuvor gesicherten Version wieder her.

Was der Wartungsbenutzer tut

Der Wartungbenutzer wird während der Installation von Unified Manager auf einem Red hat Enterprise Linux oder CentOS System erstellt. Der Wartungs-Benutzername ist der Benutzer „`umadmin`“. Der Wartungsbenutzer hat die OnCommand-Administratorrolle in der Web-UI, und dieser Benutzer kann nachfolgende Benutzer erstellen und ihnen Rollen zuweisen.

Der Wartungsbenutzer oder umadmin-Benutzer kann auch auf die Unified Manager Wartungskonsole zugreifen.

Funktionen von Benutzern zur Diagnose

Der Diagnosezugriff dient dazu, Ihnen den technischen Support bei der Fehlerbehebung zu ermöglichen, und Sie sollten ihn nur verwenden, wenn Sie sich an den technischen Support wenden.

Der Diagnose-Benutzer kann Befehle auf Betriebssystemebene ausführen, wenn sie von dem technischen Support gesteuert werden, um die Fehlerbehebung zu ermöglichen.

Menüs für Wartungskonsolen

Die Wartungskonsole besteht aus verschiedenen Menüs, mit denen Sie spezielle Funktionen und Konfigurationseinstellungen des Unified Manager Servers pflegen und managen können.

Je nach Betriebssystem, auf dem Sie Unified Manager installiert haben, besteht die Wartungskonsole aus den folgenden Menüs:

- Upgrade von Unified Manager (nur VMware)
- Netzwerkkonfiguration (nur VMware)
- Systemkonfiguration (nur VMware)
- Support/Diagnose

- Serverzertifikat Zurücksetzen
- Externer Daten-Provider
- Konfiguration Des Leistungsintervalls

Menü Netzwerkkonfiguration

Über das Menü Netzwerkkonfiguration können Sie die Netzwerkeinstellungen verwalten. Sie sollten dieses Menü verwenden, wenn die Benutzeroberfläche von Unified Manager nicht verfügbar ist.

Dieses Menü ist nicht verfügbar, wenn Unified Manager auf Red hat Enterprise Linux, CentOS oder unter Microsoft Windows installiert ist.

Folgende Menüoptionen stehen zur Verfügung:

- **IP-Adresseinstellungen anzeigen**

  Zeigt die aktuellen Netzwerkeinstellungen für die virtuelle Appliance an, einschließlich IP-Adresse, Netzwerk, Broadcast-Adresse, Netmask, Gateway Und DNS-Server.

- **IP-Adresseinstellungen ändern**

  Ermöglicht Ihnen das Ändern der Netzwerkeinstellungen für die virtuelle Appliance, einschließlich IP-Adresse, Netzmaske, Gateway oder DNS-Server. Wenn Sie die Netzwerkeinstellungen über die Wartungskonsole von DHCP in statisches Netzwerk wechseln, können Sie den Host-Namen nicht bearbeiten. Sie müssen **Änderungen übergeben** wählen, damit die Änderungen durchgeführt werden.

- **Domain Name-Sucheinstellungen Anzeigen**

  Zeigt die Liste der Domänennamen an, die für die Auflösung von Hostnamen verwendet wird.

- **Ändern Sie Die Einstellungen Für Die Domänennamensuche**

  Ermöglicht Ihnen das Ändern der Domänennamen, nach denen Sie suchen möchten, wenn Sie Hostnamen auflösen. Sie müssen **Änderungen übergeben** wählen, damit die Änderungen durchgeführt werden.

- **Statische Routen Anzeigen**

  Zeigt die aktuellen statischen Netzwerkrouten an.

- **Statische Routen Ändern**

  Ermöglicht das Hinzufügen oder Löschen statischer Netzwerkrouten. Sie müssen **Änderungen übergeben** wählen, damit die Änderungen durchgeführt werden.

  - **Route Hinzufügen**

    Ermöglicht das Hinzufügen einer statischen Route.

  - **Route Löschen**

    Ermöglicht das Löschen einer statischen Route.

- **Zurück**

  Bringt Sie zurück zum **Hauptmenü**.

- **Ausgang**

  Beendet die Wartungskonsole.

- **Netzwerkschnittstelle Deaktivieren**

  Deaktiviert alle verfügbaren Netzwerkschnittstellen. Wenn nur eine Netzwerkschnittstelle verfügbar ist, können Sie sie nicht deaktivieren. Sie müssen **Änderungen übergeben** wählen, damit die Änderungen durchgeführt werden.

- **Netzwerkschnittstelle Aktivieren**

  Aktiviert verfügbare Netzwerkschnittstellen. Sie müssen **Änderungen übergeben** wählen, damit die Änderungen durchgeführt werden.

- **Änderungen Begehen**

  Wendet alle Änderungen an den Netzwerkeinstellungen für die virtuelle Appliance an. Sie müssen diese Option auswählen, um alle vorgenommenen Änderungen zu übernehmen, oder die Änderungen werden nicht durchgeführt.

- **Ping a Host**

  Sendet einen Zielhost, um IP-Adressänderungen oder DNS-Konfigurationen zu bestätigen.

- **Wiederherstellen der Standardeinstellungen**

  Setzt alle Einstellungen auf die Werkseinstellungen zurück. Sie müssen **Änderungen übergeben** wählen, damit die Änderungen durchgeführt werden.

- **Zurück**

  Bringt Sie zurück zum **Hauptmenü**.

- **Ausgang**

  Beendet die Wartungskonsole.

Menü Systemkonfiguration

Über das Menü Systemkonfiguration können Sie Ihre virtuelle Appliance verwalten, indem Sie verschiedene Optionen angeben, z. B. den Serverstatus anzeigen und die virtuelle Maschine neu starten und herunterfahren.

Das Menü Systemkonfiguration ist nicht verfügbar, wenn Unified Manager auf Red hat Enterprise Linux, CentOS oder Microsoft Windows installiert ist.

Folgende Menüoptionen stehen zur Verfügung:

- **Serverstatus Anzeigen**

Zeigt den aktuellen Serverstatus an. Die Statusoptionen umfassen „Ausführen“ und „nicht ausgeführt“.

Wenn der Server nicht ausgeführt wird, müssen Sie sich möglicherweise an den technischen Support wenden.

- **Virtuelle Maschine Neu Starten**

  Startet die virtuelle Maschine neu und stoppt alle Dienste. Nach dem Neustart werden die virtuelle Maschine und die Dienste neu gestartet.

- **Virtuelle Maschine Herunterfahren**

  Fährt die virtuelle Maschine herunter und stoppt alle Dienste.

  Sie können diese Option nur über die Virtual Machine-Konsole auswählen.

- **Ändern <angemeldeter Benutzer> Benutzerkennwort**

  Ändert das Kennwort des aktuell angemeldeten Benutzers, der nur der Wartungbenutzer sein kann.

- **Größe Der Datenfestplatte Erhöhen**

  Vergrößert die Größe der Datenfestplatte (Festplatte 3) in der virtuellen Maschine.

- **Größe Des Swap-Datenträgers Erhöhen**

  Vergrößert die Größe der Swap-Festplatte (Festplatte 2) in der virtuellen Maschine.

- **Zeitzone Ändern**

  Ändert die Zeitzone an Ihren Standort.

- **NTP Server ändern**

  Ändert die NTP-Server-Einstellungen, z. B. IP-Adresse oder vollqualifizierter Domain-Name (FQDN).

- **Wiederherstellen aus einem OCUM-Backup**

  Stellt die Unified Manager Datenbank- und Konfigurationseinstellungen aus einer zuvor gesicherten Version wieder her.

- **Serverzertifikat Zurücksetzen**

  Setzt das Sicherheitszertifikat des Servers zurück.

- **Hostname ändern**

  Ändert den Namen des Hosts, auf dem die virtuelle Appliance installiert ist.

- **Zurück**

  Beendet das Menü Systemkonfiguration und kehrt zum Hauptmenü zurück.

- **Ausgang**

  Beendet das Menü der Wartungskonsole.

Menü „Support und Diagnose“

Über das Menü Support and Diagnostics können Sie ein Support Bundle erstellen.

Die folgende Menüoption ist verfügbar:

- * Unterstützungspaket Generieren*

  Mit dieser Funktion können Sie eine 7-Zip-Datei mit vollständigen Diagnoseinformationen im Home-Verzeichnis des Diagnosebenutzers erstellen. Die Datei umfasst Informationen, die durch eine AutoSupport Meldung, den Inhalt der Unified Manager Datenbank, detaillierte Daten zu den internen Unified Manager Servern und ausführliche Protokolle, die normalerweise nicht in AutoSupport Meldungen enthalten sind.

Zusätzliche Menüoptionen

Mit den folgenden Menüoptionen können Sie verschiedene administrative Aufgaben auf dem Unified Manager-Server ausführen.

Folgende Menüoptionen stehen zur Verfügung:

- **Serverzertifikat Zurücksetzen**

  Generiert das HTTPS-Serverzertifikat erneut.

  Sie können das Serverzertifikat in der Benutzeroberfläche von Unified Manager neu generieren, indem Sie auf * klicken * > **HTTPS-Zertifikat** > **HTTPS-Zertifikat neu erstellen**.

- **SAML-Authentifizierung deaktivieren**

  Deaktiviert die SAML-Authentifizierung, sodass der Identitäts-Provider (IdP) keine Anmeldeauthentifizierung für Benutzer bereitstellt, die auf die Unified Manager-GUI zugreifen. Diese Konsolenoption wird in der Regel verwendet, wenn ein Problem mit der IdP-Server- oder SAML-Konfiguration Benutzer vom Zugriff auf die Unified Manager-GUI blockiert.

- * Externer Datenanbieter*

  Bietet Optionen zum Verbinden von Unified Manager mit einem externen Datenanbieter. Nachdem Sie die Verbindung hergestellt haben, werden Performance-Daten an einen externen Server gesendet, sodass Storage Performance-Experten mithilfe von Software von Drittanbietern die Performance-Kennzahlen abstellen können. Folgende Optionen werden angezeigt:

  - **Server-Konfiguration anzeigen**--zeigt die aktuellen Verbindungs- und Konfigurationseinstellungen für einen externen Datenanbieter an.
  - **Serververbindung hinzufügen/ändern**--ermöglicht Ihnen die Eingabe neuer Verbindungseinstellungen für einen externen Datenanbieter oder die Änderung vorhandener Einstellungen.
  - **Serverkonfiguration ändern**--ermöglicht die Eingabe neuer Konfigurationseinstellungen für einen externen Datenanbieter oder das Ändern vorhandener Einstellungen.
  - **Serververbindung löschen**--Löscht die Verbindung zu einem externen Datenanbieter.

    Nach dem Löschen der Verbindung verliert Unified Manager die Verbindung zum externen Server.

- **Konfiguration Des Leistungsintervalls**

  Bietet eine Option für die Konfiguration, wie häufig Unified Manager Performance-statistische Daten aus Clustern erfasst. Das Standard-Erfassungsintervall beträgt fünf Minuten.

  Sie können dieses Intervall auf zehn oder fünfzehn Minuten ändern, wenn Sie feststellen, dass Sammlungen von großen Clustern nicht rechtzeitig abgeschlossen werden.

- **Ausgang**

  Beendet das Menü der Wartungskonsole.

Ändern des Wartungsbenutzerkennworts unter Windows

Sie können bei Bedarf das Passwort des Unified Manager-Wartungsbenutzers ändern.

Schritte

1. Klicken Sie auf der Anmeldeseite der Web-Benutzeroberfläche von Unified Manager auf **Passwort vergessen**.

   Es wird eine Seite angezeigt, die den Namen des Benutzers auffordert, dessen Kennwort Sie zurücksetzen möchten.

2. Geben Sie den Benutzernamen ein und klicken Sie auf **Absenden**.

   Eine E-Mail mit einem Link zum Zurücksetzen des Passworts wird an die für diesen Benutzernamen definierte E-Mail-Adresse gesendet.

3. Klicken Sie in der E-Mail auf den Link **Passwort zurücksetzen** und definieren Sie das neue Passwort.
4. Kehren Sie zur Web-Benutzeroberfläche zurück und melden Sie sich mit dem neuen Passwort bei Unified Manager an.

Nachdem Sie fertig sind

Wenn Unified Manager in einer Microsoft Cluster Server (MSCS) Umgebung installiert ist, müssen Sie das Wartungsbenutzerkennwort auf dem zweiten Node des MSCS-Setups ändern. Das Wartungs-Benutzer-Passwort für beide Nodes muss das gleiche sein.

Ändern des umadmin-Passworts auf Linux-Systemen

Aus Sicherheitsgründen müssen Sie das Standardpasswort für den Unified Manager umadmin-Benutzer sofort nach Abschluss des Installationsprozesses ändern. Sie können das Passwort bei Bedarf jederzeit später wieder ändern.

Bevor Sie beginnen

- Unified Manager muss auf einem Red hat Enterprise Linux oder CentOS Linux System installiert sein.
- Sie müssen über die Stammbenutzer-Anmeldeinformationen für das Linux-System verfügen, auf dem Unified Manager installiert ist.

Schritte

1. Melden Sie sich als Root-Benutzer an dem Linux-System an, auf dem Unified Manager ausgeführt wird.
2. Ändern Sie das umadmin-Passwort: `passwd umadmin`

   Das System fordert Sie zur Eingabe eines neuen Passworts für den umadmin-Benutzer auf.

Nachdem Sie fertig sind

Wenn Unified Manager in einer Veritas Cluster Server (VCS) Umgebung installiert ist, müssen Sie das umadmin Passwort auf dem zweiten Knoten des VCS Setup ändern. Das umadmin-Passwort für beide Nodes muss das gleiche sein.

Hinzufügen von Netzwerkschnittstellen

Sie können neue Netzwerkschnittstellen hinzufügen, wenn Sie den Netzwerkverkehr trennen müssen.

Bevor Sie beginnen

Sie müssen die Netzwerkschnittstelle der virtuellen Appliance mit vSphere hinzugefügt haben.

Die virtuelle Appliance muss eingeschaltet sein.

Über diese Aufgabe

Dieser Vorgang kann nicht ausgeführt werden, wenn Unified Manager auf Red hat Enterprise Linux oder unter Microsoft Windows installiert ist.

Schritte

1. Wählen Sie in der vSphere-Konsole **Hauptmenü** die Option **Systemkonfiguration** > **Betriebssystem neu starten**.

   Nach dem Neubooten kann die Wartungskonsole die neu hinzugefügte Netzwerkschnittstelle erkennen.

2. Öffnen Sie die Wartungskonsole.
3. Wählen Sie **Netzwerkkonfiguration** > **Netzwerkschnittstelle Aktivieren**.
4. Wählen Sie die neue Netzwerkschnittstelle aus, und drücken Sie **Enter**.

   Wählen Sie **eth1** und drücken Sie **Enter**.

5. Geben Sie **y** ein, um die Netzwerkschnittstelle zu aktivieren.
6. Netzwerkeinstellungen eingeben.

   Sie werden aufgefordert, die Netzwerkeinstellungen einzugeben, wenn Sie eine statische Schnittstelle verwenden oder wenn DHCP nicht erkannt wird.

   Nach Eingabe der Netzwerkeinstellungen kehren Sie automatisch zum Menü **Netzwerkkonfiguration** zurück.

7. Wählen Sie **Änderungen Übergeben**.

   Sie müssen die Änderungen festlegen, um die Netzwerkschnittstelle hinzuzufügen.

Hinzufügen von Festplattenspeicher zum Datenbankverzeichnis von Unified Manager

Das Datenbankverzeichnis von Unified Manager enthält sämtliche Gesundheits- und Performance-Daten, die von ONTAP Systemen erfasst wurden. Unter bestimmten Umständen kann es erforderlich sein, dass Sie die Größe des Datenbankverzeichnisses erhöhen.

Das Datenbankverzeichnis kann beispielsweise voll erhalten, wenn Unified Manager Daten von einer großen Anzahl von Clustern erfasst, in denen jedes Cluster über viele Nodes verfügt. Sie erhalten ein Warnereignis, wenn das Datenbankverzeichnis zu 90 % voll ist, und ein kritisches Ereignis, wenn das Verzeichnis zu 95 % voll ist.

Nach 95 % Auslastung des Verzeichnisses werden keine zusätzlichen Daten aus Clustern erfasst.

Je nachdem, ob Unified Manager auf einem VMware ESXi Server, auf einem Red hat oder CentOS Linux Server oder auf einem Microsoft Windows Server ausgeführt wird, welche Schritte zum Hinzufügen von Kapazität zum Datenverzeichnis erforderlich sind, unterscheiden sie sich.

Hinzufügen von Speicherplatz zum Datenverzeichnis des Linux-Hosts

Wenn Sie dem nicht genügend Speicherplatz zugewiesen haben `/opt/netapp/data` Verzeichnis zur Unterstützung von Unified Manager Wenn Sie ursprünglich den Linux-Host eingerichtet und dann Unified Manager installiert haben, können Sie nach der Installation Speicherplatz hinzufügen, indem Sie den Speicherplatz auf dem erhöhen `/opt/netapp/data` Verzeichnis.

Bevor Sie beginnen

Sie müssen Root-Benutzerzugriff auf die Red hat Enterprise Linux oder CentOS Linux Maschine haben, auf der Unified Manager installiert ist.

Über diese Aufgabe

Wir empfehlen, dass Sie ein Backup der Unified Manager-Datenbank erstellen, bevor Sie die Größe des Datenverzeichnisses vergrößern.

Schritte

1. Melden Sie sich als Root-Benutzer an dem Linux-Rechner an, auf dem Sie Speicherplatz hinzufügen möchten.
2. Beenden Sie den Unified Manager-Service und die zugehörige MySQL-Software in der folgenden Reihenfolge:
3. Erstellen eines temporären Sicherungsordners (z. B. `/backup-data`) Mit genügend Speicherplatz, um die Daten im aktuellen zu enthalten `/opt/netapp/data` Verzeichnis.

4. Kopieren Sie den Inhalt und die Berechtigungskonfiguration des vorhandenen `/opt/netapp/data` Verzeichnis zum Verzeichnis der Sicherungsdaten: `cp -rp /opt/netapp/data/* /backup-data`
5. Wenn SE Linux aktiviert ist:

   a. Holen Sie sich den SE Linux-Typ für Ordner auf bestehenden `/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 wie die folgende aus:

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Führen Sie die aus `chcon` Befehl zum Festlegen des SE Linux-Typs für das Backup-Verzeichnis: `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 750 GB über LVM-Befehle oder durch Hinzufügen zusätzlicher Festplatten.

   Montieren des `/opt/netapp/data` Das Verzeichnis in einem NFS-Export oder einer CIFS-Freigabe wird nicht unterstützt.
8. Bestätigen Sie das `/opt/netapp/data` Verzeichnis-Inhaber (mysql) und Gruppe (root) bleiben unverändert: `ls -ltr / | grep opt/netapp/data`

   Das System gibt eine Bestätigung wie die folgende aus:

   ```
   drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
   ```
9. Wenn SE Linux aktiviert ist, bestätigen Sie den Kontext für das `/opt/netapp/data` Verzeichnis ist noch auf mysqld_db_t eingestellt: `touch /opt/netapp/data/abc``ls -Z /opt/netapp/data/abc`

   Das System gibt eine Bestätigung wie die folgende aus:

   ```
   -rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
   /opt/netapp/data/abc
   ```
10. Kopieren Sie den Inhalt von `backup-data`, Zurück zu den erweiterten `/opt/netapp/data` Verzeichnis: `cp -rp /backup-data/* /opt/netapp/data/`
11. Starten Sie den MySQL-Dienst: `service mysqld start`

12. Nachdem der MySQL-Dienst gestartet wurde, starten sie die ocie- und ocieau-Dienste in der folgenden Reihenfolge: `service ocie start``service ocieau start`
13. Löschen Sie nach dem Start aller Dienste den Sicherungsordner `/backup-data`: `rm -rf /backup-data`

Hinzufügen von Speicherplatz zur Datenfestplatte der virtuellen VMware-Maschine

Wenn Sie die Menge an Speicherplatz auf der Datenfestplatte für die Unified Manager-Datenbank erhöhen müssen, können Sie nach der Installation Kapazität hinzufügen, indem Sie den Festplattenspeicher erhöhen `disk 3`.

Bevor Sie beginnen

- Sie müssen Zugriff auf den vSphere Client haben.
- Auf der virtuellen Maschine dürfen keine Snapshots lokal gespeichert werden.
- Sie müssen über die Anmeldeinformationen für den Wartungs-Benutzer verfügen.

Über diese Aufgabe

Wir empfehlen, dass Sie Ihre virtuelle Maschine sichern, bevor Sie die Größe der virtuellen Laufwerke erhöhen.

Schritte

1. Wählen Sie im vSphere-Client die Virtual Machine Unified Manager aus und fügen Sie den Daten dann weitere Festplattenkapazität hinzu `disk 3`. Details finden Sie in der VMware Dokumentation.
2. Wählen Sie im vSphere-Client die virtuelle Unified Manager-Maschine aus und wählen Sie dann die Registerkarte **Konsole** aus.
3. Klicken Sie auf das Konsolenfenster, und melden Sie sich dann mit Ihrem Benutzernamen und Passwort an der Wartungskonsole an.
4. Geben Sie im **Hauptmenü** die Nummer für die Option **Systemkonfiguration** ein.
5. Geben Sie im Menü * Systemkonfiguration* die Nummer für die Option **Datenfestplattengröße erhöhen** ein.

Hinzufügen von Speicherplatz zum logischen Laufwerk des Microsoft Windows-Servers

Wenn Sie mehr Festplattenspeicher für die Unified Manager-Datenbank benötigen, können Sie das logische Laufwerk, auf dem Unified Manager installiert ist, um Kapazität erweitern.

Bevor Sie beginnen

Sie müssen über Administratorrechte für Windows verfügen.

Über diese Aufgabe

Wir empfehlen, dass Sie die Unified Manager-Datenbank sichern, bevor Sie Speicherplatz hinzufügen.

Schritte

1. Melden Sie sich als Administrator beim Windows-Server an, auf dem Sie Speicherplatz hinzufügen möchten.
2. Befolgen Sie den Schritt, der der Methode entspricht, die Sie verwenden möchten, um mehr Speicherplatz hinzuzufügen:

Option	Beschreibung
Fügen Sie auf einem physischen Server die Kapazität des logischen Laufwerks hinzu, auf dem der Unified Manager-Server installiert ist.	Folgen Sie den Schritten im Microsoft Thema: "Erweitern Sie ein Basisvolume"
Fügen Sie auf einem physischen Server ein Festplattenlaufwerk hinzu.	Folgen Sie den Schritten im Microsoft Thema: "Hinzufügen Von Festplattenlaufwerken"
Erhöhen Sie auf einer virtuellen Maschine die Größe einer Laufwerkspartition.	Folgen Sie den Schritten im VMware Thema: "Vergrößern einer Laufwerkspartition"

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

"Hinweis zu OnCommand Unified Manager 9.5"

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.