Active IQ Unified Manager-Dokumentation

Active IQ Unified Manager 9.14

NetApp
March 13, 2025

Inhalt

Active IQ Unified Manager-Dokumentation

Versionshinweise

Bietet eine Zusammenfassung der neuen Funktionen, Einschränkungen und bekannten Probleme von Active IQ Unified Manager 9.14.

Weitere Informationen finden Sie im "Versionshinweise zu Active IQ Unified Manager".

Los geht's

Schnellstartanleitung für VMware Installationen

Sie können die Datei herunterladen `.tar`, die ein Stammzertifikat, eine Datei und eine `OVA` Datei enthält `README`, und Unified Manager als virtuelle Appliance bereitstellen.

Systemanforderungen

- Betriebssystem: VMware ESXi 7.0 und 8.0
- RAM: 12 GB
- CPU: Insgesamt 9572 MHz
- Freier Speicherplatz: 5 GB (Thin Provisioning), 152 GB (Thick Provisioning)

Detaillierte Informationen zu den Systemanforderungen finden Sie im "Anforderungen für die Installation von Unified Manager" und "Interoperabilitätsmatrix".

Active IQ Unified Manager wird installiert

Laden Sie das Installationsprogramm herunter

1. Laden Sie die Datei herunter `.tar`, die ein Stammzertifikat, eine Datei und eine `OVA` Datei enthält `README`.
2. Speichern Sie die Datei in einem lokalen Verzeichnis oder Netzwerkverzeichnis, auf das Ihr vSphere Client zugreifen kann.
3. Geben Sie im Verzeichnis, in das Sie die Datei heruntergeladen `.tar` haben, den Befehl ein `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz`. + die erforderliche `OVA` Datei, ein Stammzertifikat und eine `README` Datei werden in das Zielverzeichnis entpackt.

Überprüfen Sie die Integrität

Sie können die Integrität der Datei überprüfen `OVA`, indem Sie die in der Datei angegebenen Schritte `README` ausführen.

Installation Von Unified Manager

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. Auf der Seite „Prüfungsdetails“ im Abschnitt „Herausgeber“ bestätigt die Meldung `Entrust Code Signing - OVCS2 (Trusted certificate)`die Integrität der heruntergeladenen `OVA` Datei. Aktualisieren Sie für die Meldung `Entrust Code Signing - OVCS2 (Invalid certificate)` den VMware vCenter Server auf die Version 7.0U3E oder höher.
4. Füllen Sie auf der Seite Vorlage anpassen auf der Registerkarte Eigenschaften die Felder aus, die für den Installationstyp erforderlich sind:
    - Geben Sie für die statische Konfiguration die erforderlichen Informationen in alle Felder ein. Das Hinzufügen von Informationen für das Feld **Secondary DNS** ist nicht erforderlich.

- Wenn DHCP unter IPv4 verwendet wird, fügen Sie in keinem Feld Informationen hinzu.
- Aktivieren Sie für DHCP unter Verwendung von IPv6 das Kontrollkästchen „Automatische IPv6-Adresse aktivieren“. Fügen Sie in keinem anderen Feld Informationen hinzu.

5. Schalten Sie die VM ein.
6. Klicken Sie auf die Registerkarte Konsole, um den anfänglichen Startvorgang anzuzeigen.
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

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

Systemanforderungen

- Betriebssystem: Red hat Enterprise Linux Versionen 7.x und von 8.0 bis 8.9 oder CentOS Version 7.x basierend auf x86_64 Architektur, installiert unter Verwendung der „Server mit GUI“ Basisumgebung aus der Option **Software Selection** des OS Installers
- RAM: 12 GB, CPU: 9572 MHz insgesamt
- Freier Festplattenspeicher: 100 GB Speicherplatz im Verzeichnis, 50 GB `/opt/netapp/data` in der Root-Partition. Für separat gemountete `/opt` Verzeichnisse und `/var/log` Verzeichnisse stellen Sie sicher, dass `/opt` 15 GB, `/var/log` 16 GB und `/tmp` 10 GB freier Speicherplatz zur Verfügung stehen.

Detaillierte Systemanforderungen und Informationen zur Installation des Produkts an einem gesicherten Standort finden Sie im "Anforderungen für die Installation von Unified Manager" und im "Interoperabilitätsmatrix".

Active IQ Unified Manager wird installiert

Laden Sie das Installationsprogramm herunter

1. Laden Sie das `ActiveIQUnifiedManager-<version>.zip` Installationspaket zusammen mit Code Signing Zertifikat (`.pem`) und digitale Signatur (`.sig`) .
2. Führen Sie im Verzeichnis, in dem Sie die Installationsdatei heruntergeladen haben, folgende Schritte aus:

```
# unzip ActiveIQUnifiedManager-<version>.zip
```

Überprüfen Sie die Integrität

Führen Sie die folgenden Befehle aus, um die Integrität des Installationspakets zu überprüfen:

- Führen Sie aus `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>`, um eine Datei mit dem öffentlichen Schlüssel aus dem Code-Signaturzertifikat zu erstellen.

- Führen Sie aus `openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip`, um die Signatur auf dem Installationspaket zu überprüfen.

Überprüfung der Repository-Konfiguration

Die Vorgehensweisen für die Konfiguration von Red hat Enterprise Linux- oder CentOS-Repositorys sind standortspezifisch. Sie können das im Installationspaket enthaltene Skript verwenden `pre_install_check.sh`, um die Konfiguration Ihres Betriebssystems zu überprüfen. Wenn Ihr System mit dem Internet verbunden ist, erhalten Sie automatisch Anweisungen zum Einrichten der Red hat Enterprise Linux- oder CentOS-Repositories.

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

Installation Von Unified Manager

Unified Manager verwendet das `yum` Dienstprogramm zur Installation der Software und jeglicher abhängiger Software. Da es unterschiedliche Bilder von Red hat Enterprise Linux oder CentOS gibt, hängen die installierten Pakete von der in den Bildern vorhandenen Software ab. Das `yum` Dienstprogramm bestimmt die abhängigen Softwarepakete für die Installation. Weitere Informationen zu den abhängigen Softwarepaketen finden Sie im "Linux-Software- und Installationsanforderungen".

Um Unified Manager zu installieren, führen Sie den folgenden Befehl entweder als root-Benutzer oder mit `sudo`, aus dem Verzeichnis aus, in dem die Installationsdatei entpackt wurde:

```
# yum install netapp-um<version>.x86_64.rpm
```

Oder

```
% sudo yum install netapp-um<version>.x86_64.rpm
```

Am Ende der Installation werden die Informationen zur Verbindung mit der Unified Manager Web-Benutzeroberfläche angezeigt. Wenn Sie keine Verbindung zur Web-Benutzeroberfläche herstellen können, finden Sie weitere Informationen zu den Einschränkungen von Port 443 in der `README` mit der Software bereitgestellten Datei.

Kurzanleitung für Windows-Installationen

Sie können das Installationspaket herunterladen und Unified Manager installieren, um Probleme mit der Storage-Kapazität, Verfügbarkeit, Performance und Datensicherung zu überwachen und zu beheben.

Systemanforderungen

- Betriebssysteme
  - Microsoft Windows Server 2019 Standard und Datacenter Edition
  - Microsoft Windows Server 2022 Standard und Datacenter Edition

    Unified Manager wird auf 64-Bit-Windows-Betriebssystem für die folgenden Sprachen unterstützt:

  - Englisch

    - Japanisch
    - Vereinfachtes Chinesisch
- RAM: 12 GB
- CPU: Insgesamt 9572 MHz
- Freier Speicherplatz: 100 GB Festplattenspeicher für das Installationsverzeichnis, 50 GB Festplattenspeicher für das MySQL-Datenverzeichnis

Detaillierte Informationen zu den Systemanforderungen finden Sie im "Anforderungen für die Installation von Unified Manager" und "Interoperabilitätsmatrix".

Active IQ Unified Manager wird installiert

Laden Sie das Installationsprogramm herunter

1. Laden Sie das Installationspaket herunter `ActiveIQUnifiedManager-<version>.exe`.
2. Kopieren Sie die Installationsdatei in ein Verzeichnis auf dem Zielsystem.

Installation Von Unified Manager

Stellen Sie für die Installation von Unified Manager sicher, dass Microsoft .NET 4.5 oder eine neuere Version installiert ist. Im Rahmen des Installationsprozesses installiert Unified Manager je nach Bedarf andere Pakete von Drittanbietern. Weitere Informationen zu den abhängigen Softwarepaketen finden Sie im "Windows Software- und Installationsanforderungen".

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 auf VMware vSphere Systemen

Einführung in Active IQ Unified Manager

Mit Active IQ Unified Manager (ehemals OnCommand Unified Manager) überwachen und managen Sie den Zustand und die Performance Ihrer ONTAP Storage-Systeme über eine einzige 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

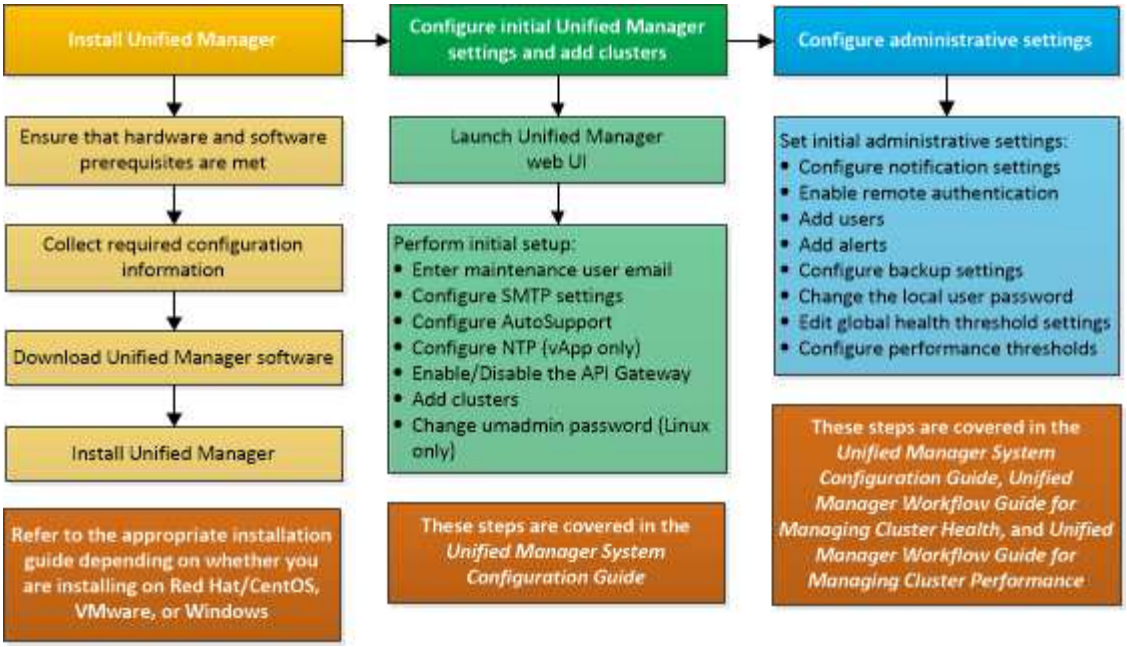
Die Unified Manager Server-Infrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Applikationsserver. Die Lösung bietet Infrastrukturservices wie beispielsweise Discovery, Monitoring, rollenbasierte Zugriffssteuerung (RBAC), Audits und Protokollierungsfunktionen.

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 diesen Abschnitten werden die im folgenden Workflow gezeigten Elemente beschrieben.



Anforderungen für die Installation von Unified Manager

Bevor Sie mit der Installation beginnen, stellen Sie sicher, dass der Server, auf dem Unified Manager installiert werden soll, die spezifischen Software-, Hardware-, CPU- und Arbeitsspeicheranforderungen erfüllt.

NetApp unterstützt keine Änderungen am Applikationscode für Unified Manager. Wenn Sie Sicherheitsmaßnahmen auf den Unified Manager-Server anwenden müssen, sollten Sie diese Änderungen am Betriebssystem vornehmen, auf dem Unified Manager installiert ist.

Weitere Informationen zum Anwenden von Sicherheitsmaßnahmen auf den Unified Manager-Server finden Sie im Knowledge Base-Artikel.

"Unterstützbarkeit von Sicherheitsmaßnahmen für Active IQ Unified Manager für Clustered Data ONTAP"

Verwandte Informationen

Weitere Informationen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool"

Systemanforderungen für virtuelle Infrastruktur und Hardware

Die Installation von Unified Manager auf einer virtuellen Infrastruktur oder auf einem physischen System sollte 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)

Hardwarekonfiguration	Empfohlene Einstellungen
Prozessoren	4 CPUs
CPU-Zykluskapazität	9572 MHz insgesamt (Mindestanforderung 9572 MHz)
Freier Speicherplatz	• 5 GB (Thin Provisioning) • 152 GB (Thick Provisioning)

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 sollten für die VM, wo Unified Manager eingesetzt wird, keine Arbeitsspeicherbeschränkungen festlegen und sollten keine Funktionen (z. B. Ballooning) aktivieren, die die Software daran hindern, den zugewiesenen Arbeitsspeicher im System 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. Weitere Informationen finden Sie unter "Unified Manager Best Practices-Leitfaden".

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.

Voraussetzung für dedizierten Einsatz

Das physische oder virtuelle System, auf dem Unified Manager installiert wird, sollte 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 planen, die Unified Manager Backup- und Restore-Funktion zu verwenden, weisen Sie zusätzliche Kapazität zu, sodass 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, sollte so konfiguriert sein, dass Sie den Host-Namen vom Host selbst erfolgreich verwenden können `ping`. Im Fall der IPv6-Konfiguration sollten Sie überprüfen, ob `ping6` der Hostname erfolgreich ist, um sicherzustellen, dass die Installation von Unified Manager 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.

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 7.0 und 8.0

> Unified Manager OVA auf VMware vSphere Systemen läuft Debian OS 11 (Bullseye) intern. Informationen zu den Versionen der Hardware virtueller Maschinen, die die unterstützten Versionen von ESXi-Servern unterstützen können, finden Sie in der VMware-Dokumentation.

Die folgenden Versionen von vSphere werden unterstützt:

- VMware vCenter Server 7.0 und 8.0

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 sollte die gleiche sein wie die NTP-Serverzeit, 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-Datenspeicher auf einem Storage-System mit ONTAP Software implementieren, nutzen Sie das NetApp NFS-Plug-in für VMware VAAI, um Thick Provisioning zu nutzen.

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.

> Bei der Installation oder beim Upgrade von Unified Manager werden die erforderlichen Software- und Sicherheits-Patches von Drittanbietern automatisch auf einem VMware vSphere System installiert oder aktualisiert. Da die Installations- und Upgrade-Prozesse von Unified Manager diese Komponenten steuern, sollten Sie keine eigenständige Installation oder Aktualisierung von Komponenten anderer Hersteller versuchen.

Unterstützte Browser

Um auf die Web-UI von Unified Manager zuzugreifen, verwenden Sie einen unterstützten Browser.

Die Interoperabilitäts-Matrix enthält eine Liste der unterstützten Browser-Versionen.

"mysupport.netapp.com/matrix"

Durch das Deaktivieren von Popup-Blockern für alle Browser wird sichergestellt, dass die Softwarefunktionen ordnungsgemäß angezeigt werden.

Wenn Sie planen, Unified Manager für SAML-Authentifizierung zu konfigurieren, damit ein Identitäts-Provider (IdP) Benutzer authentifizieren kann, sollten Sie die Liste der vom IdP unterstützten Browser überprüfen.

Protokoll- und Port-Anforderungen

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

In typischen Installationen müssen Sie bei der Verbindung zur Web-UI von Unified Manager keine Portnummern angeben, da immer Standardports verwendet werden. Da Unified Manager beispielsweise immer versucht, auf seinem Standardport ausgeführt zu werden, können Sie anstelle von `https://<host>:443` eingeben `https://<host>`.

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.
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.

Schnittstelle	Protokoll	Port	Beschreibung
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.

Der Standardport für MySQL, 3306, ist auf localhost beschränkt, während Unified Manager auf VMware vSphere-Systemen installiert wird. Dies wirkt sich nicht auf ein Upgrade-Szenario aus, in dem die vorherige Konfiguration erhalten bleibt. Diese Konfiguration kann geändert werden, und die Verbindung kann anderen Hosts über die Option auf der Wartungskonsole zur Verfügung gestellt `Control access to MySQL port 3306` werden. Weitere Informationen finden Sie unter "Zusätzliche Menüoptionen". Die für die HTTP- und HTTPS-Kommunikation verwendeten Ports (die Ports 80 und 443) können mithilfe der Unified Manager-Wartungskonsole geändert werden. Weitere Informationen finden Sie unter "Menüs für Wartungskonsolen".

Verbindungen vom Unified Manager-Server

Sie sollten Ihre Firewall so konfigurieren, dass sie Ports öffnen, die die Kommunikation zwischen dem Unified Manager-Server und verwalteten Speichersystemen, 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. Wenn Sie diesen Port oder einen anderen Port zur Verbindung mit dem VMware vCenter Server oder ESXi Server verwenden, stellen Sie sicher, dass der Port verfügbar ist und an einem sicheren Standort angeschlossen werden kann.
Storage-System	NDMP	10000/TCP	Wird für bestimmte Snapshot-Restore-Vorgänge verwendet.
AutoSupport Server	HTTPS	443	Wird zum Senden von AutoSupport-Informationen verwendet. Erfordert den Internetzugang, um diese Funktion auszuführen.
Authentifizierungsserver	LDAP	389	Wird zur Erstellung von Authentifizierungsanforderungen sowie von Benutzer- und Gruppenabfragen verwendet.

Ziel	Protokoll	Port	Beschreibung
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
IP-Adresse des ESXi-Servers	
Vollständig qualifizierter Domain-Name des Hosts	
Host-IP-Adresse	
Netzwerkmaske	
Gateway-IP-Adresse	
Primäre DNS-Adresse	
Sekundäre DNS-Adresse	
Domänen durchsuchen	

System, auf dem Software bereitgestellt wird	Ihr Wert
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	
Hostname oder IP-Adresse des SMTP-Servers	
SMTP-Benutzername	
SMTP-Passwort	
SMTP-Port	25 (Standardwert)
E-Mail, von der aus Benachrichtigungen gesendet werden	
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)	
SNMP-Trap-Ziel-Host-IP-Adressen	
SNMP-Port	

Cluster-Informationen

Angaben zu den Storage-Systemen, die Sie mit Unified Manager managen.

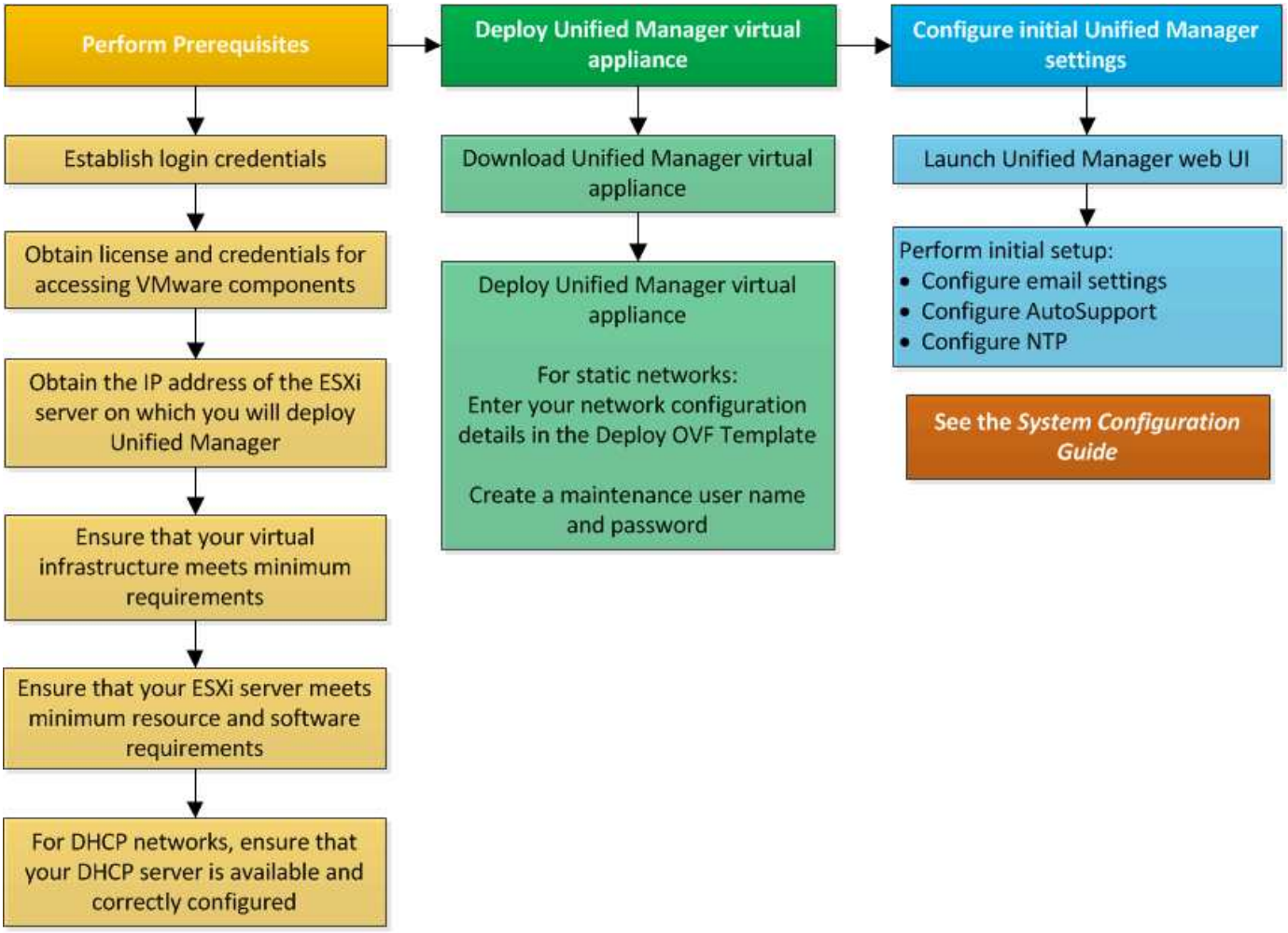
Cluster 1 von N	Ihr Wert
Host-Name oder Cluster-Management-IP-Adresse	
Benutzername des ONTAP-Administrators Dem Administrator muss die Rolle „admin“ zugewiesen worden sein.	
ONTAP-Administratorpasswort	
Protokoll	HTTPS

Installieren, Aktualisieren und Entfernen der Unified Manager Software

Auf VMware vSphere Systemen können Sie Unified Manager installieren, auf eine neuere Softwareversion aktualisieren oder die virtuelle Unified Manager Appliance (vApp) entfernen.

Überblick über den Implementierungsprozess

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.

Was Sie brauchen

- Sie sollten die Systemanforderungen für die Implementierung überprüfen und vervollständigen.

  Siehe "Systemanforderungen".

- Stellen Sie sicher, dass Sie die folgenden Informationen haben:
  - Anmeldedaten für die NetApp Support-Website
  - Anmeldeinformationen für den Zugriff auf VMware vCenter Server und vSphere Web Client
  - 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 sollte auf dem Host aktiviert sein, wenn Sie IPv6-Adressen verwenden möchten.

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

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

> Ab Unified Manager 9.8 wurden VMware Tools durch Open VM Tools ersetzt `open-vm-tools`). Sie müssen VMware Tools nicht mehr als Teil der Installation installieren, da `open-vm-tools` dies im Installationspaket von Unified Manager enthalten ist.

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.

Schritte

1. Folgen Sie den Schritten in "Laden Sie Unified Manager Herunter".
2. Befolgen Sie außerdem die Schritte in "Implementieren Sie die virtuelle Unified Manager Appliance".

Herunterladen der Installationsdatei für Unified Manager

Laden Sie die Installationsdatei für Unified Manager von der NetApp Support Site herunter, um Unified Manager als virtuelle Appliance zu implementieren.

Was Sie brauchen

Sie sollten die Anmeldedaten für die NetApp Support-Website besitzen.

Bei der Installationsdatei handelt es sich um eine `.tar` Datei, die ein Stammzertifikat, eine `README` Datei und eine `OVA` Datei mit der für eine virtuelle Appliance konfigurierten Unified Manager-Software enthält.

Schritte

1. Loggen Sie sich auf der NetApp Support Site ein und navigieren Sie zur Download-Seite für Unified Manager:

   "NetApp Support-Website"

2. Wählen Sie die erforderliche Version von Unified Manager aus, und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (Endbenutzer License Agreement, EULA).
3. Laden Sie die Datei für die VMware vSphere-Installation herunter, und speichern Sie `.tar` sie in einem lokalen Verzeichnis oder Netzwerkverzeichnis, auf das Ihr vSphere Client zugreifen kann.
4. Überprüfen Sie die Prüfsumme, um sicherzustellen, dass die Software ordnungsgemäß heruntergeladen wurde.
5. Navigieren Sie zu dem Verzeichnis, in das Sie die Datei heruntergeladen `.tar` haben, und geben Sie den folgenden Befehl in das Terminalfenster ein, um das Unified Manager-Paket zu erweitern:

   ```
   tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz
   ```

   Die erforderliche `OVA` Datei, ein Stammzertifikat und eine `README` Datei für Unified Manager werden in das Zielverzeichnis entpackt.

6. Überprüfen Sie die Integrität der `OVA` Datei, indem Sie die in der Datei angegebenen Schritte `README` ausführen.

Implementieren der virtuellen Unified Manager Appliance

Nach dem Herunterladen der Installationsdatei stellen Sie Unified Manager als virtuelle Appliance bereit. Verwenden Sie den vSphere Web Client, um die virtuelle Appliance auf einem ESXi-Server bereitzustellen. Wenn Sie die virtuelle Appliance bereitstellen, wird eine virtuelle Maschine erstellt.

Was Sie brauchen

Sie sollten die Systemanforderungen überprüfen. Nehmen Sie die erforderlichen Änderungen vor der Bereitstellung der virtuellen Unified Manager Appliance vor.

Siehe "Anforderungen an die virtuelle Infrastruktur".

Siehe "VMware Software- und Installationsanforderungen".

Wenn Sie DHCP (Dynamic Host Configuration Protocol) verwenden, stellen Sie sicher, dass der DHCP-Server verfügbar ist und dass die DHCP- und VM-Netzwerkadapter-Konfigurationen korrekt sind. Standardmäßig ist DHCP konfiguriert.

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

Informieren Sie sich vor der Bereitstellung der virtuellen Appliance über die folgenden Informationen:

- Anmeldeinformationen für den Zugriff auf VMware vCenter Server und vSphere Web Client
- 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, erhalten Sie die IPv4- oder IPv6-Adressen für die Netzwerkgeräte, 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

Ab Unified Manager 9.8 wurden VMware Tools durch Open VM Tools ersetzt (`open-vm-tools`). Sie müssen VMware Tools nicht im Rahmen des Installationsprozesses installieren, da `open-vm-tools` dies im Installationspaket von Unified Manager enthalten ist.

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 zur Bereitstellung der virtuellen Unified Manager-Appliance für die OVF-Vorlage ab.

   Auf der Seite „Prüfungsdetails“:

   - Überprüfen Sie die Details des Abschnitts Publisher. Die Meldung **Entrust Code Signing - OVCS2 (Trusted Certificate)** bestätigt die Integrität der heruntergeladenen `OVA` Datei. + Wenn die Meldung **Code-Signatur anvertrauen - OVCS2 (ungültiges Zertifikat)** angezeigt wird, dann aktualisieren Sie den VMware vCenter Server auf 7.0U3E oder eine höhere Version.

     Auf der Seite Vorlage anpassen:

   - 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. Stellen Sie sicher, 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, fügen Sie Ressourcen hinzu und wiederholen Sie die Installation.

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

   Der erste Bootvorgang dauert einige Minuten.

5. Um Ihre Zeitzone zu konfigurieren, geben Sie Ihren geografischen Bereich und Ihre Stadt oder Region wie im VM-Konsolenfenster aufgefordert ein.

   Alle angezeigten Datumsangaben verwenden die für Unified Manager konfigurierte Zeitzone, unabhängig von der Zeitzone auf Ihren verwalteten Geräten. 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, ist der Zeitstempel die Zeit des Management-Servers.

6. 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 richtig mit DNS konfiguriert ist, wird der Hostname „`UnifiedManager`“ 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.

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

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

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

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

Sie können auf die Web-Benutzeroberfläche zugreifen, um die Ersteinrichtung von Unified Manager durchzuführen, wie in beschrieben"Active IQ Unified Manager wird konfiguriert".

Upgrade Von Unified Manager

Sie können nur ein Upgrade von Active IQ Unified Manager auf Version 9.14 von Version 9.12 oder 9.13 durchführen.

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. Folgen Sie den Schritten in "Laden Sie das ISO-Image von Unified Manager herunter".
2. Befolgen Sie außerdem die unter beschriebenen Schritte"Upgrade Von Unified Manager".

Unterstützter Upgrade-Pfad für Unified Manager-Versionen

Active IQ Unified Manager unterstützt für jede Version einen bestimmten Upgrade-Pfad.

Nicht alle Versionen von Unified Manager können ein Upgrade ohne Upgrade auf neuere Versionen durchführen. Die Unified Manager Upgrades sind auf ein N-2-Modell beschränkt, d. h. ein Upgrade kann nur innerhalb der nächsten zwei Versionen auf allen Plattformen durchgeführt werden. Beispielsweise können Sie nur ein Upgrade von Unified Manager 9.12 und 9.13 auf Unified Manager 9.14 durchführen.

Wenn Sie eine Version verwenden, die vor den unterstützten Versionen liegt, muss Ihre Unified Manager Instanz zuerst auf eine der unterstützten Versionen aktualisiert und dann auf die aktuelle Version aktualisiert werden.

Wenn die installierte Version beispielsweise Unified Manager 9.9 ist und Sie auf Unified Manager 9.14 aktualisieren möchten, führen Sie eine Reihe von Upgrades aus.

Beispiel für ein Upgrade-Pfad:

1. Upgrade 9.9 → 9.11
2. Upgrade 9.11 → 9.13
3. Upgrade 9.13 → 9.14

Weitere Informationen zur Upgrade-Pfadmatrix finden Sie in diesem "Knowledge Base-Artikel (KB".

Upgrade-Datei für Unified Manager wird heruntergeladen

Laden Sie vor dem Upgrade von Unified Manager die Upgrade-Datei von der NetApp Support Site herunter.

Was Sie brauchen

Sie sollten die Anmeldedaten für die NetApp Support-Website besitzen.

Schritte

1. Loggen Sie sich auf der NetApp Support Site ein:

   "NetApp Support-Website"

2. Öffnen Sie die Download-Seite, um ein Upgrade von Unified Manager auf VMware vSphere durchzuführen.
3. Laden Sie das Image für die Aktualisierung herunter `.iso`, und speichern Sie es in einem lokalen Verzeichnis oder Netzwerkverzeichnis, auf das Ihr vSphere Client zugreifen kann.
4. Überprüfen Sie die Prüfsumme, um sicherzustellen, dass die Software ordnungsgemäß heruntergeladen wurde.

Aktualisieren der virtuellen Unified Manager Appliance

Sie können die virtuelle Active IQ Unified Manager Appliance von Version 9.12 oder 9.13 auf Version 9.14 aktualisieren.

Was Sie brauchen

Stellen Sie Folgendes sicher:

- Sie haben die Upgrade-Datei, das ISO-Image von der NetApp Support Site heruntergeladen.
- Das System, auf dem Unified Manager aktualisiert wird, erfüllt die System- und Software-Anforderungen.

  Siehe "Anforderungen an die virtuelle Infrastruktur".

  Siehe "VMware Software- und Installationsanforderungen".

- Für vSphere 6.5 und höher haben Sie die VMware Remote Console (VMRC) installiert.
- Während des Upgrades werden Sie möglicherweise aufgefordert, zu bestätigen, ob Sie die vorherigen Standardeinstellungen für die Aufbewahrung von Performancedaten für 13 Monate beibehalten oder in 6 Monate ändern möchten. Nach der Bestätigung werden die historischen Leistungsdaten nach 6 Monaten gelöscht.
- Sie haben folgende Informationen:
  - Anmeldedaten für die NetApp Support-Website
  - Anmeldeinformationen für den Zugriff auf VMware vCenter Server und vSphere Web Client
  - Anmeldedaten für den Unified Manager-Wartungsbenutzer

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, sollten 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, z. B. einen Snapshot oder einen Klon, der Unified Manager VM, um ein applikationskonsistentes Backup zu erstellen.
5. Schalten Sie über vSphere Client die Unified Manager VM ein.
6. Starten Sie die VMware Remote Console.
7. Klicken Sie auf das Symbol **CD-ROM** und wählen Sie **mit der Datenträgerbilddatei verbinden (.iso)** aus.
8. Wählen Sie die Datei aus `ActiveIQUnifiedManager-<version>-virtual-update.iso`, und klicken Sie auf **Open**.
9. Klicken Sie auf die Registerkarte **Konsole**.
10. Melden Sie sich bei der Wartungskonsole von Unified Manager an.
11. 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 werden soll.

12. Geben Sie ein, `y` um fortzufahren.

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

13. Geben Sie ein, `y` um fortzufahren.

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

14. Drücken Sie eine beliebige Taste, um fortzufahren.

    Sie werden automatisch von der Wartungskonsole abgemeldet.

15. **Optional:** Melden Sie sich an der Wartungskonsole an, und überprüfen Sie die Version von Unified Manager.

Sie können die Web-Benutzeroberfläche in einem neuen Fenster in einem unterstützten Webbrowser starten und sich 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 sollten die VM nach dem Generieren eines neuen Sicherheitszertifikats neu starten oder wenn ein Problem mit der VM auftritt.

Was Sie brauchen

- Das virtuelle Gerät sollte eingeschaltet sein.
- Sie sollten als Wartungsbenutzer bei der Unified Manager Wartungskonsole angemeldet sein.

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 die Web-UI von Unified Manager über Ihren Browser, und melden Sie sich an.

Verwandte Informationen

"VMware vSphere PowerCLI cmdlets Referenz: Neustart-VMGuest"

Unified Manager Wird Entfernt

Sie können Unified Manager deinstallieren, indem Sie die virtuelle Maschine (VM) entfernen, auf der die Unified Manager-Software installiert ist.

Was Sie brauchen

- Sie sollten Zugangsdaten für den Zugriff auf VMware vCenter Server und vSphere Web Client besitzen.
- Jede aktive Verbindung des Unified Manager-Servers zu einem Workflow Automation-Server sollte geschlossen werden.
- Alle Cluster (Datenquellen) sollten vom Unified Manager-Server entfernt werden, bevor Sie die virtuelle Maschine (VM) entfernen.

Schritte

1. Überprüfen Sie mithilfe der Unified Manager-Wartungskonsole, 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 entfernen 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 entfernen möchten, und klicken Sie auf **von Festplatte löschen**.

Installation von Unified Manager auf Linux Systemen

Einführung in Active IQ Unified Manager

Mit Active IQ Unified Manager (ehemals OnCommand Unified Manager) überwachen und managen Sie den Zustand und die Performance Ihrer ONTAP Storage-Systeme über eine einzige Benutzeroberfläche. Sie können Unified Manager auf einem Linux-Server, auf einem Windows-Server oder als virtuelle Appliance (vApp) 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

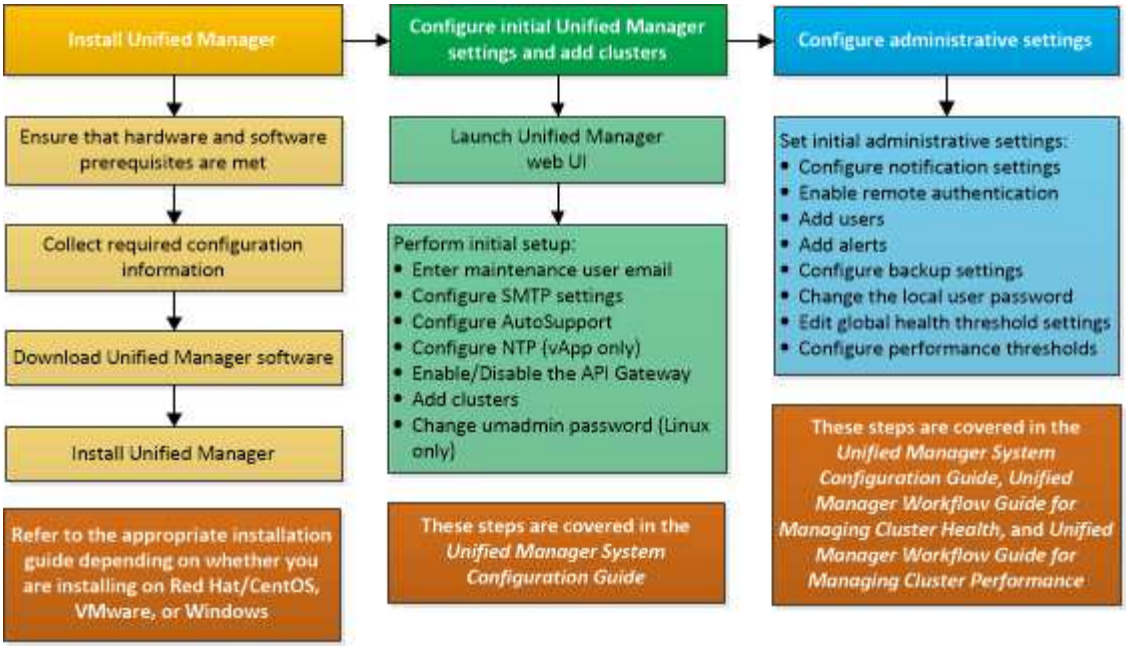
Die Unified Manager Server-Infrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Applikationsserver. Die Lösung bietet Infrastrukturservices wie beispielsweise Discovery, Monitoring, rollenbasierte Zugriffssteuerung (RBAC), Audits und Protokollierungsfunktionen.

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 diesen Abschnitten werden die im folgenden Workflow gezeigten Elemente beschrieben.



Anforderungen für die Installation von Unified Manager

Bevor Sie mit der Installation beginnen, stellen Sie sicher, dass der Server, auf dem Unified Manager installiert werden soll, die spezifischen Software-, Hardware-, CPU- und Arbeitsspeicheranforderungen erfüllt.

NetApp unterstützt keine Änderungen am Applikationscode für Unified Manager. Wenn Sie Sicherheitsmaßnahmen auf den Unified Manager-Server anwenden müssen, sollten Sie diese Änderungen am Betriebssystem vornehmen, auf dem Unified Manager installiert ist.

Weitere Informationen zum Anwenden von Sicherheitsmaßnahmen auf den Unified Manager-Server finden Sie im Knowledge Base-Artikel.

"Unterstützbarkeit von Sicherheitsmaßnahmen für Active IQ Unified Manager für Clustered Data ONTAP"

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Systemanforderungen für virtuelle Infrastruktur und Hardware

Die Installation von Unified Manager auf einer virtuellen Infrastruktur oder auf einem physischen System sollte 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)

Hardwarekonfiguration	Empfohlene Einstellungen
Prozessoren	4 CPUs
CPU-Zykluskapazität	9572 MHz insgesamt (Mindestanforderung 9572 MHz)
Freier Speicherplatz	150 GB, wobei die Kapazität wie folgt zugewiesen wird: • 50 GB der Root-Partition zugewiesen • 100 GB freier Festplattenspeicher, der dem Verzeichnis zugewiesen `/opt/netapp/data` ist, das auf einem LVM-Laufwerk oder auf einem separaten lokalen Laufwerk, das an das Zielsystem angeschlossen ist, gemountet ist Für separat gemountete `/opt` Verzeichnisse und `/var/log` Verzeichnisse, stellen Sie sicher, dass `/opt` 15 GB und 16 GB freien Speicherplatz hat `/var/log`. Das `/tmp` Verzeichnis sollte mindestens 10 GB freien Speicherplatz haben.

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 sollten für die VM, wo Unified Manager eingesetzt wird, keine Arbeitsspeicherbeschränkungen festlegen und sollten keine Funktionen (z. B. Ballooning) aktivieren, die die Software daran hindern, den zugewiesenen Arbeitsspeicher im System 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. 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.

Voraussetzung für dedizierten Einsatz

Das physische oder virtuelle System, auf dem Unified Manager installiert wird, sollte 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 planen, die Unified Manager Backup- und Restore-Funktion zu verwenden, weisen Sie zusätzliche Kapazität zu, sodass 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, sollte so konfiguriert sein, dass Sie den Host-Namen vom Host selbst erfolgreich verwenden können `ping`. Im Fall der IPv6-Konfiguration sollten Sie überprüfen, ob `ping6` der Hostname erfolgreich ist, um sicherzustellen, dass die Installation von Unified Manager 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.

Linux-Software- und Installationsanforderungen

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 Version 7.x und von 8.0 bis 8.9, basierend auf x86_64-Architektur.
- CentOS Version 7.x basiert auf x86_64 Architektur. CentOS Stream wird 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"

Der Server sollte dediziert sein für die Ausführung von Unified Manager. Auf dem Server sollten keine anderen Anwendungen installiert sein. Es ist möglich, dass Vulnerability Scanner wie Qualys auf Ihrem Linux-System aufgrund von Unternehmensvorschriften installiert ist. Sie sollten den Schwachstellenscanner vor der Installation von Unified Manager deaktivieren, um einen Fehler bei der Installation zu verhindern.

Schwachstellenscanner (wie Qualys) können zu einer hohen CPU-Auslastung führen, wenn die virtuelle Maschine (VM) intern (wo Unified Manager und der Schwachstellenscanner auf derselben VM installiert sind) oder extern gescannt wird (wobei Unified Manager und der Schwachstellenscanner auf zwei verschiedenen Servern installiert sind und der Schwachstellenscanner die VM scannt, auf der Unified Manager installiert ist). Dieses Problem führt häufig dazu, dass die VM nicht reagiert und die Unified Manager-Services beeinträchtigt werden. Daher empfiehlt NetApp, die Schwachstellenprüfung in der VM zu deaktivieren, auf der Unified Manager installiert ist. Wenn keine Option zum Deaktivieren des Scanners besteht, scannen Sie die VM außerhalb der Geschäftszeiten und starten Sie die Services nach Abschluss des Scanvorgangs neu.

Software von anderen Anbietern

Unified Manager wird auf einem WildFly Web-Server bereitgestellt. WildFly 26.1.3 ist gebündelt und mit Unified Manager konfiguriert.

Die folgenden Drittanbieterpakete sind erforderlich, jedoch nicht in Unified Manager enthalten. Diese Pakete werden während der Installation automatisch vom Installationsprogramm installiert `yum`, vorausgesetzt, Sie haben die Repositorys wie in den folgenden Abschnitten beschrieben konfiguriert.

- MySQL Community Edition Version 8.0.34 (aus dem MySQL-Repository).
- OpenJDK Version 11.0.21 (aus dem Red hat Extra Enterprise Linux Server-Repository)
- Python 3.6.x
- P7zip Version 16.02 oder höher (aus dem Red hat Extra Packages for Enterprise Linux Repository)

Vor dem Upgrade von Software anderer Anbieter müssen Sie eine laufende Instanz von Unified Manager herunterfahren. Nach Abschluss der Softwareinstallation von Drittanbietern können Sie Unified Manager neu starten.

Anforderungen an die Benutzerautorisierung

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

Installationsvoraussetzungen

Die Best Practices für die Installation von Red hat Enterprise Linux oder CentOS und den zugehörigen Repositorys auf Ihrem System sind unten aufgeführt. Systeme, die unterschiedlich installiert oder konfiguriert sind oder extern bereitgestellt werden (in der Cloud), erfordern möglicherweise weitere Schritte und Unified Manager kann in solchen Implementierungen nicht ordnungsgemäß ausgeführt werden.

- Sie müssen Red hat Enterprise Linux oder CentOS nach Red hat Best Practices installieren, und Sie sollten die folgenden Standardoptionen wählen, die die Auswahl der Basisumgebung „`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.
- Damit der `yum` Installer abhängige Software in den Red hat Enterprise Linux-Repositorys finden kann, müssen Sie das System während der Installation von Red hat Enterprise Linux oder danach mit einer gültigen Red hat Subskription 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.

  Siehe "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.

  Siehe "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 mit dem Internet verbundene System herunterladen und die Dateien auf das System kopieren `.rpm`, auf dem Sie Unified Manager installieren möchten. Um die Artefakte und Pakete herunterzuladen, müssen Sie den Befehl verwenden `yum install`. 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 Enterprise Linux und CentOS blockieren möglicherweise externen Zugriff auf Port 443. Aufgrund dieser Einschränkung können Sie nach der Installation von Unified Manager möglicherweise keine Verbindung zur Administrator-Web-UI herstellen. Der folgende Befehl ermöglicht den Zugriff auf Port 443 für alle externen Benutzer und Anwendungen auf einem generischen Red hat Enterprise Linux oder CentOS System.

```
# firewall-cmd --zone=public --add-port=443/tcp --permanent; firewall-cmd
--reload
```

Sie müssen Red hat Enterprise Linux und CentOS in der Basisumgebung „`SServer mit GUI`“ installieren. Er stellt die Befehle bereit, die von der Installationsanleitung für Unified Manager verwendet werden. Bei anderen Basisumgebungen müssen Sie möglicherweise zusätzliche Befehle installieren, um die Installation zu validieren oder abzuschließen. Wenn das `firewall-cmd` auf Ihrem System nicht verfügbar ist, müssen Sie es mit dem folgenden Befehl installieren:

```
# sudo yum install firewalld
```

Wenden Sie sich an Ihre IT-Abteilung, bevor Sie die Befehle ausführen, um zu prüfen, ob Ihre

Sicherheitsrichtlinien ein anderes Verfahren erfordern.

> THP (Transparent Riesen Pages) sollte auf CentOS- und Red hat-Systemen deaktiviert werden. Wenn diese Option aktiviert ist, kann dies dazu führen, dass Unified Manager heruntergefahren wird, wenn bestimmte Prozesse zu viel Arbeitsspeicher in Anspruch nehmen und beendet werden.

Unterstützte Browser

Um auf die Web-UI von Unified Manager zuzugreifen, verwenden Sie einen unterstützten Browser.

Die Interoperabilitäts-Matrix enthält eine Liste der unterstützten Browser-Versionen.

"mysupport.netapp.com/matrix"

Durch das Deaktivieren von Popup-Blockern für alle Browser wird sichergestellt, dass die Softwarefunktionen ordnungsgemäß angezeigt werden.

Wenn Sie planen, Unified Manager für SAML-Authentifizierung zu konfigurieren, damit ein Identitäts-Provider (IdP) Benutzer authentifizieren kann, sollten Sie die Liste der vom IdP unterstützten Browser überprüfen.

Protokoll- und Port-Anforderungen

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

In typischen Installationen müssen Sie bei der Verbindung zur Web-UI von Unified Manager keine Portnummern angeben, da immer Standardports verwendet werden. Da Unified Manager beispielsweise immer versucht, auf seinem Standardport ausgeführt zu werden, können Sie anstelle von `https://<host>:443` eingeben `https://<host>`.

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.

Schnittstelle	Protokoll	Port	Beschreibung
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.
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.

Der Standardport für MySQL, 3306, ist nur auf localhost beschränkt, während Unified Manager auf Linux-Systemen installiert wird. Dies wirkt sich nicht auf ein Upgrade-Szenario aus, in dem die vorherige Konfiguration erhalten bleibt. Diese Konfiguration kann geändert werden, und die Verbindung kann anderen Hosts über die Option auf der Wartungskonsole zur Verfügung gestellt `Control access to MySQL port 3306` werden. Weitere Informationen finden Sie unter "Zusätzliche Menüoptionen". Die für die HTTP- und HTTPS-Kommunikation verwendeten Ports (die Ports 80 und 443) können mithilfe der Unified Manager-Wartungskonsole geändert werden. Weitere Informationen finden Sie unter "Menüs für Wartungskonsolen".

Verbindungen vom Unified Manager-Server

Sie sollten Ihre Firewall so konfigurieren, dass sie Ports öffnen, die die Kommunikation zwischen dem Unified Manager-Server und verwalteten Speichersystemen, 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. Erfordert den Internetzugang, um diese Funktion auszuführen.
Authentifizierungsserver	LDAP	389	Wird zur Erstellung von Authentifizierungsanforderungen sowie von Benutzer- und Gruppenabfragen verwendet.
LDAPS	636	Wird für sichere LDAP-Kommunikation verwendet.	Mailserver

Ziel	Protokoll	Port	Beschreibung
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
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	
Hostname oder IP-Adresse des SMTP-Servers	
SMTP-Benutzername	
SMTP-Passwort	
SMTP-Port	25 (Standardwert)
E-Mail, von der aus Benachrichtigungen gesendet werden	
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)	
SNMP-Trap-Ziel-Host-IP-Adressen	
SNMP-Port	

Cluster-Informationen

Angaben zu den Storage-Systemen, die Sie mit Unified Manager managen.

Cluster 1 von N	Ihr Wert
Host-Name oder Cluster-Management-IP-Adresse	

Cluster 1 von N	Ihr Wert
Benutzername des ONTAP-Administrators Dem Administrator muss die Rolle „admin“ zugewiesen worden sein.	
ONTAP-Administratorpasswort	
Protokoll	HTTPS

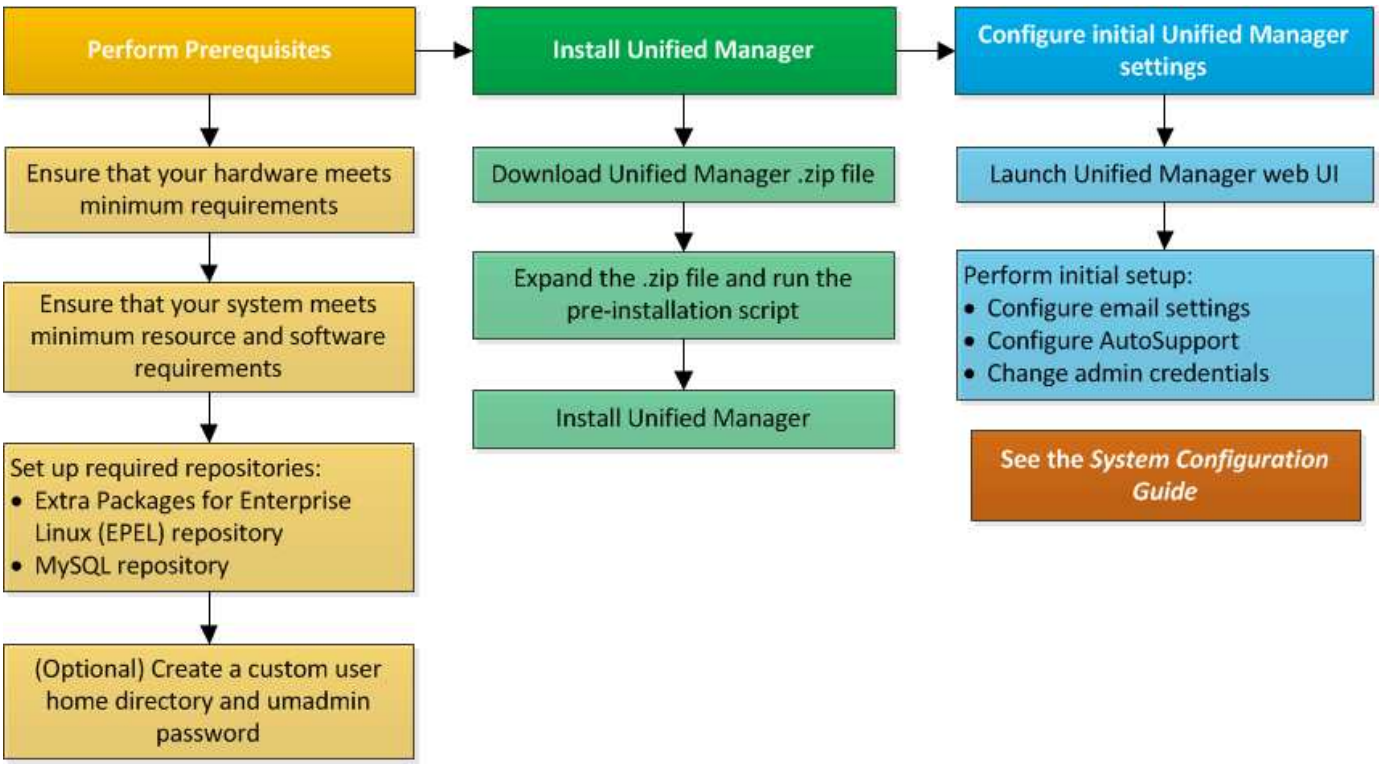
Installieren, Aktualisieren und Entfernen der Unified Manager Software

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

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.

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 Enterprise Linux- oder CentOS-System installieren.

Schritte

1. Laden Sie das EPEL-Repository für Ihre Installation herunter. Für Red hat Enterprise Linux 7 können Sie ihn unter folgender Adresse herunterladen:

   ```
   wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
   ```

   Laden Sie die Version 8 unter folgender Adresse herunter:

   ```
   wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

2. EPEL-Repository konfigurieren:

   ```
   yum install epel-release-latest-<version>.noarch.rpm
   ```

Wenn Sie beispielsweise interne Repositorys mit modularen RPM-Paketen für Red hat Enterprise Linux 8-Systeme haben *`javapackages-filesystem-<version>.module.rpm`*, stellen Sie sicher, dass die Metadaten für die modularen Pakete auch im gleichen Repository verfügbar sind.

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.

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

> Diese Aufgabe kann fehlschlagen, wenn das System nicht über die Internetverbindung verfügt. Lesen 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. Für Red hat Enterprise Linux 7 können Sie ihn unter folgender Adresse herunterladen:

```
wget http://repo.mysql.com/yum/mysql-8.0-community/el/7/x86_64/mysql80-
community-release-el7-3.noarch.rpm
```

Laden Sie die Version 8 unter folgender Adresse herunter:

```
wget http://repo.mysql.com/yum/mysql-8.0-community/el/8/x86_64/mysql80-
community-release-el8-1.noarch.rpm
```

2. Konfigurieren Sie das MySQL-Repository:

```
yum install mysql80-community-release-<version>.noarch.rpm
```

Wenn Sie für Red hat Enterprise Linux 8 interne Repositorys mit java-11-openjdk, p7zip und anderen vom AppStream-Repository bereitgestellten Softwarepaketen haben, müssen Sie Ihr AppStream-Repository deaktivieren und MySQL Community Server installieren. Führen Sie den folgenden Befehl aus:

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install  mysql-
community-server
```

Wenn Sie einen Fehler bei fehlender Schlüssel- oder Schlüsselübereinstimmung erhalten und Ihre Installation fehlschlägt, führen Sie die folgenden Schritte aus:

- Importieren Sie auf einem angeschlossenen System den aktualisierten MySQL-Schlüssel, indem Sie den folgenden Befehl ausführen:

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-<xxxx>

for example:

rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022
```

- Aktualisieren Sie auf einem System, das keine Internetverbindung hat, Ihre MySQL-Repo-Datei und deaktivieren Sie `gpgcheck` sie, indem Sie markieren `gpgcheck=0`.

SELinux-Anforderungen für NFS- und CIFS-Freigaben

Wenn Sie planen, `/opt/netapp/data` auf einem NAS- oder SAN-Gerät zu mounten `/opt/netapp` und SELinux aktiviert ist, müssen Sie einige Überlegungen beachten.

Wenn Sie planen, `/opt/netapp/data` von einem anderen Ort als dem Root-Dateisystem zu mounten `/opt/netapp` und SELinux in Ihrer Umgebung aktiviert ist, sollten Sie den richtigen Kontext für die gemounteten Verzeichnisse festlegen. Befolgen Sie für das anwendbare Szenario in Ihrer Umgebung die folgenden Schritte zum Festlegen und Bestätigen des korrekten SELinux-Kontexts.

Konfigurieren des SELinux-Kontexts, wenn `/opt/netapp/data` gemountet ist

Wenn Sie in Ihrem System gemountet haben `/opt/netapp/data` und SELinux auf eingestellt `Enforcing` ist, stellen Sie sicher, dass der SELinux-Kontexttyp für `/opt/netapp/data` auf, gesetzt ist `mysqld_db_t`,

was das Standard-Kontextelement für den Speicherort der Datenbankdateien ist.

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` . Sie sollten diesen Kontext in ändern `mysqld_db_t`.

2. Führen Sie diese Schritte aus, um den Kontext basierend auf der Art und Weise einzustellen, wie Sie gemountet haben `/opt/netapp/data`.

   a. Führen Sie die folgenden Befehle aus, um den Kontext auf zu setzen `mysqld_db_t`:
   `semanage fcontext -a -t mysqld_db_t "/opt/netapp/data"`
   `` `restorecon -R -v /opt/netapp/data ``

   b. Wenn Sie in `/etc/fstab` konfiguriert haben `/opt/netapp/data`, sollten Sie die Datei bearbeiten `/etc/fstab`. Fügen Sie für die `/opt/netapp/data/` Mount-Option die MySQL-Beschriftung hinzu als:

   `context=system_u:object_r:mysqld_db_t:s0`

   c. Heben Sie die Bereitstellung auf, und installieren Sie sie erneut `/opt/netapp/data/`, um den Kontext zu aktivieren.

   d. Wenn Sie einen direkten NFS-Mount haben, führen Sie den folgenden Befehl aus, um den Kontext auf `mysqld_db_t`:

   `mount <nfsshare>:/<mountpoint> /opt/netapp/data -o context=system_u:object_r:mysqld_db_t:s0`

3. Überprüfen Sie, ob der Kontext richtig eingestellt ist:

`ls -dZ /opt/netapp/data/`

Beispielausgabe:

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

Konfigurieren des SELinux-Kontexts, wenn `/opt/netapp` gemountet ist, und `/opt/netapp/data/` wird auch separat gemountet

In diesem Szenario sollten Sie zunächst den Kontext für festlegen `/opt/netapp/data/`, wie im vorherigen Abschnitt beschrieben. Stellen Sie nach dem Setzen des richtigen Kontexts für `/opt/netapp/data/` sicher, dass das übergeordnete Verzeichnis `/opt/netapp` den SELinux-Kontext nicht auf gesetzt `file_t` hat.

Schritte

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 sollte der Kontext `file_t` geändert werden. Die folgenden Befehle setzen den Kontext auf `usr_t`. Sie können den Kontext auf einen anderen Wert als basierend auf Ihren Sicherheitsanforderungen festlegen `file_t`.

2. Führen Sie diese Schritte aus, um den Kontext festzulegen, je nachdem, wie Sie gemountet 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
```

1. Wenn Sie in `/etc/fstab` konfiguriert haben `/opt/netapp`, sollten Sie die Datei bearbeiten `/etc/fstab`. Fügen Sie für die `/opt/netapp` Mount-Option die MySQL-Beschriftung hinzu als:

   `context=system_u:object_r:usr_t:s0`

2. Unmounten und dann erneut mounten, `/opt/netapp` um den Kontext zu aktivieren.
3. 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
   ```

   a. Überprüfen Sie, ob der Kontext richtig eingestellt ist:

      `ls -dZ /opt/netapp`

   Beispielausgabe

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

Konfigurieren des SELinux-Kontexts, wenn `/opt/netapp` gemountet ist und `/opt/netapp/data/` nicht separat gemountet wird

Wenn Sie in Ihrem System gemountet haben `/opt/netapp`und SELinux auf eingestellt `Enforcing` ist, stellen Sie sicher, dass der SELinux-Kontexttyp für `/opt/netapp` auf, gesetzt ist `mysqld_db_t`, was das Standard-Kontextelement für den Speicherort der Datenbankdateien ist.

Schritte

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:default_t:s0 /opt/netapp
   ```

   In dieser Ausgabe ist der Kontext `default_t` . Sie sollten diesen Kontext in ändern `mysqld_db_t`.

2. Führen Sie die folgenden Schritte aus, um den Kontext basierend auf der Art und Weise festzulegen, wie Sie gemountet haben `/opt/netapp`.

   a. Führen Sie die folgenden Befehle aus, um den Kontext auf zu setzen `mysqld_db_t`:
   `semanage fcontext -a -t mysqld_db_t "/opt/netapp"`
   `` `restorecon -R -v /opt/netapp ``

   b. Wenn Sie in `/etc/fstab` konfiguriert haben `/opt/netapp`, bearbeiten Sie die `/etc/fstab` Datei. Fügen Sie für die `/opt/netapp/` Mount-Option die MySQL-Beschriftung hinzu als:
   `context=system_u:object_r:mysqld_db_t:s0`

   c. Unmounten und dann erneut mounten, `/opt/netapp/` um den Kontext zu aktivieren.

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

3. Überprüfen Sie, ob der Kontext richtig eingestellt ist:

```
ls -dZ /opt/netapp/
```

Beispielausgabe:

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

Installation von Unified Manager auf Linux Systemen

Sie müssen wissen, dass die Schritte zum Herunterladen und Installieren von Unified Manager je nach Installationsszenario unterschiedlich sind.

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.

Was Sie brauchen

- 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.

Die Standardinstallation von Unified Manager führt die folgenden Aufgaben aus:

- Erstellt den umadmin-Benutzer mit `/home/umadmin` als Home-Verzeichnis.
- Weist dem umadmin-Benutzer das Standardpasswort „`admin`“ zu.

Da einige Installationsumgebungen den Zugriff auf einschränken `/home`, schlägt die Installation 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.

Außerdem enthält die Standard-Installation von Unified Manager 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.

Die Sicherheitsrichtlinien in Ihrer Umgebung dürfen die Sudo-Berechtigungen für den Unified Manager-Wartungsbenutzer nicht einschränken. Einige Vorgänge von Unified Manager können fehlschlagen, wenn die Berechtigungen eingeschränkt sind. Überprüfen Sie, ob Sie den folgenden sudo-Befehl ausführen können, wenn Sie sich nach der erfolgreichen Installation als umadmin-Benutzer angemeldet haben.

```
sudo systemctl status ocie
```

Dieser Befehl sollte den entsprechenden Status des ocie-Dienstes fehlerfrei zurückgeben.

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

Download Von Unified Manager

Sie müssen die Unified Manager-Datei von der NetApp Support-Website herunterladen `.zip`, um Unified Manager zu installieren.

Was Sie brauchen

Sie müssen Anmeldedaten für die NetApp Support-Website besitzen.

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

Schritte

1. Loggen Sie sich auf der NetApp Support Site ein und navigieren Sie zur Download-Seite für Unified Manager:

   "NetApp Support-Website"

2. Wählen Sie die erforderliche Version von Unified Manager aus, und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (Endbenutzer License Agreement, EULA).
3. Laden Sie die Unified Manager-Installationsdatei für Linux herunter, und speichern Sie die `.zip` Datei in einem Verzeichnis auf dem Zielsystem.

   - Stellen Sie sicher, dass Sie die korrekte Version der Installationsdatei für Ihr Red hat Enterprise Linux-System herunterladen. Je nachdem, ob Sie Red hat Enterprise Linux 7 oder 8 installiert haben, stellen Sie sicher, dass Sie die entsprechende Version der Unified Manager-Datei herunterladen `.zip`.
   - NetApp empfiehlt, dass Sie das Code Signing Zertifikat herunterladen (`.pem`) und digitale Signatur (`.sig`) zusammen mit der `.zip` Datei.

4. Überprüfen Sie die Prüfsumme für die Integrität der heruntergeladenen Software.
5. Wenn Sie das Code-Signaturzertifikat und die digitale Signatur heruntergeladen haben, können Sie die Integrität der Installationsdatei überprüfen. Sie können die Integrität der Installationsdatei mit den folgenden Befehlen überprüfen:
   - Mit diesem Befehl wird eine Datei mit dem öffentlichen Schlüssel aus dem Code-Signing-Zertifikat erstellt:

     ```
     openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem >
     <public_key_file_name>
     ```

    - Wobei **AIQUM-RHEL-CLIENT-INTER-ROOT.pem** die Datei ist, die das Code-Signierungszertifikat enthält.
  - Mit diesem Befehl wird die Signatur der Installationsdatei überprüft:

```
openssl dgst -sha256 -verify <public_key_file_name> -signature
<signature_file_name> ActiveIQUnifiedManager-<version>.zip
```

    Die Meldung ähnlich wie `Verified Ok` bestätigt, dass die Installationsdatei sicher verwendet werden kann.

Installation Von Unified Manager

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

Was Sie brauchen

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

  Siehe "Hardwaresystemanforderungen".

  Siehe "Linux-Software- und Installationsanforderungen".

- Sie müssen die Datei des Unified Managers von der NetApp Support-Website auf das Zielsystem heruntergeladen haben `.zip`.
- Sie sollten die Integrität der heruntergeladenen Datei überprüft haben `.zip`.
- Sie benötigen einen unterstützten Webbrowser.
- Die Terminalemulationssoftware muss ScRollback aktiviert haben.

Auf dem Red hat Enterprise Linux oder CentOS System sind möglicherweise alle erforderlichen Versionen der erforderlichen Hilfssoftware (Java, MySQL, zusätzliche Dienstprogramme) installiert, nur einige der erforderlichen Software installiert oder es kann sich um ein neu installiertes System mit keiner der erforderlichen Software handelt.

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 11.0.21	`java -version`
MySQL 8.0.34 Community Edition	`rpm -qa

Erforderliche Software und Mindestversion	Befehl zum Überprüfen der Software und der Version
grep -i mysql`	P7zip 16.02
`rpm -qa	grep p7zip`

3. Wenn die installierte Version von MySQL älter als die MySQL 8.0.34 Community Edition ist, geben Sie den folgenden Befehl ein, um sie zu deinstallieren:

   ```
   rpm -e <mysql_package_name>
   ```

   Wenn Sie Abhängigkeitsfehler erhalten, müssen Sie die Option hinzufügen `--nodeps`, um die Komponente zu deinstallieren.

4. Navigieren Sie zu dem Verzeichnis, in dem Sie die Installationsdatei heruntergeladen `.zip` haben, und erweitern Sie das Unified Manager-Paket:

   ```
   unzip ActiveIQUnifiedManager-<version>.zip
   ```

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

5. Stellen Sie sicher, dass das folgende Modul im Verzeichnis verfügbar ist:

   ```
   ls *.rpm
   ```

   ```
   netapp-um<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 könnten:

   ```
   sudo ./pre_install_check.sh
   ```

   Das Skript vor der Installation überprüft, ob das System über ein gültiges Red hat Enterprise Linux-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.

   Wenn Sie für Red hat Enterprise Linux 8 interne Repositorys mit JDK 11 - OpenJDK, p7zip und anderen Softwarepaketen des AppStream-Repositorys haben, müssen Sie das AppStream-Repository deaktivieren und MySQL Community Server installieren. Führen Sie den folgenden Befehl aus:

   ```
   # sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install
   mysql-community-server
   ```

7. **Optional:** Sie müssen Schritt 7 nur ausführen, wenn Ihr System nicht mit dem Internet verbunden ist und Sie die für Ihre Installation erforderlichen Pakete manuell herunterladen müssen. Wenn Ihr System über den Internetzugang verfügt und alle benötigten Pakete verfügbar sind, fahren Sie mit Schritt 8 fort. 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 netapp-um<version>.x86_64.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`“ auf Red hat Enterprise Linux-Systemen nicht immer aktiviert ist, müssen Sie möglicherweise die Funktionalität aktivieren, um ein Paket herunterzuladen, ohne es zu installieren:
> `yum install yum-plugin-downloadonly`

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

8. Führen Sie als root-Benutzer oder mit den `sudo` folgenden Befehl aus, um die Software zu installieren:

`yum install netapp-um<version>.x86_64.rpm`

Mit diesem Befehl werden die .rpm-Pakete, alle anderen erforderlichen Hilfssoftware und die Unified Manager-Software installiert.

Wenn die Installation mit dem GPG NOKEY-Fehler fehlschlägt, verwenden Sie `rpm --import`, um die Schlüssel aus einer URL zu importieren:

`rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022`

> Versuchen Sie nicht, die Installation mithilfe alternativer Befehle (wie `rpm -ivh`) durchzuführen. Für eine 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 einer bestimmten Verzeichnisstruktur installiert werden, die automatisch durch den Befehl erzwungen wird `yum install netapp-um<version>.x86_64.rpm`.

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:

```
Active IQ 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
    ```

Greifen Sie auf die Web-Benutzeroberfläche zu, um das Standardpasswort des umadmin-Benutzers zu ändern, und führen Sie die Ersteinrichtung von Unified Manager durch"Active IQ Unified Manager wird konfiguriert", wie unter beschrieben. Das Standardpasswort des umadmin-Benutzers muss geändert werden.

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 „`Anwendungsadministrator`“ 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 das Instanzspezifische JBoss-Passwort zurücksetzen, das während der Installation festgelegt wurde. Sie können das Passwort optional zurücksetzen, falls Ihr Standort diese Sicherheitsfunktion erfordert, um die Installationseinstellung für Unified Manager zu überschreiben. Dieser Vorgang ändert auch das Passwort, das JBoss zum Zugriff auf MySQL verwendet.

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

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:

   ```
   systemctl stop ocieau

   systemctl stop ocie
   ```

   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 entsprechender Aufforderung das neue JBoss-Passwort ein und bestätigen Sie es anschließend erneut.

   Beachten Sie, dass das Passwort zwischen 8 und 16 Zeichen lang sein muss und mindestens eine Ziffer, ein Großbuchstaben und ein Kleinbuchstaben sowie mindestens eines der folgenden Sonderzeichen enthalten muss:

   ```
   !@%^*-_=[]:<>.?/~+
   ```

5. Starten Sie nach Abschluss des Skripts die Unified Manager Services, indem Sie in der angezeigten Reihenfolge die folgenden Befehle eingeben:

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

6. Nachdem alle Services gestartet wurden, können Sie sich in der UI von Unified Manager einloggen.

Upgrade von Unified Manager auf Red hat Enterprise Linux oder CentOS

Sie können ein Upgrade von Unified Manager durchführen, wenn eine neue Version 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.

Unterstützter Upgrade-Pfad für Unified Manager-Versionen

Active IQ Unified Manager unterstützt für jede Version einen bestimmten Upgrade-Pfad.

Nicht alle Versionen von Unified Manager können ein Upgrade ohne Upgrade auf neuere Versionen durchführen. Die Unified Manager Upgrades sind auf ein N-2-Modell beschränkt, d. h. ein Upgrade kann nur innerhalb der nächsten zwei Versionen auf allen Plattformen durchgeführt werden. Beispielsweise können Sie nur ein Upgrade von Unified Manager 9.12 und 9.13 auf Unified Manager 9.14 durchführen.

Wenn Sie eine Version verwenden, die vor den unterstützten Versionen liegt, muss Ihre Unified Manager Instanz zuerst auf eine der unterstützten Versionen aktualisiert und dann auf die aktuelle Version aktualisiert werden.

Wenn die installierte Version beispielsweise Unified Manager 9.9 ist und Sie auf Unified Manager 9.14 aktualisieren möchten, führen Sie eine Reihe von Upgrades aus.

Beispiel für ein Upgrade-Pfad:

1. Upgrade 9.9 → 9.11
2. Upgrade 9.11 → 9.13
3. Upgrade 9.13 → 9.14

Weitere Informationen zur Upgrade-Pfadmatrix finden Sie in diesem "Knowledge Base-Artikel (KB".

Upgrade Von Unified Manager

Sie können ein Upgrade von Unified Manager 9.12 oder 9.13 auf 9.14 durchführen, indem Sie die Installationsdatei auf die Linux-Plattform herunterladen und ausführen.

Was Sie brauchen

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

  Siehe "Hardwaresystemanforderungen".

  Siehe "Linux-Software- und Installationsanforderungen".

- Sie müssen über ein Abonnement für den Red hat Enterprise Linux Subscription Manager verfügen.

- Sie müssen die korrekte Version von OpenJDK installieren oder aktualisieren, bevor Sie Unified Manager aktualisieren.

  Siehe "Aktualisieren von JRE auf Linux".

- Um Datenverlust zu vermeiden, müssen Sie ein Backup der Unified Manager-Datenbank erstellt haben, falls während des Upgrades ein Problem auftritt. NetApp empfiehlt, die Sicherungsdatei aus dem Verzeichnis an einen externen Speicherort zu verschieben `/opt/netapp/data`.
- Während des Upgrades werden Sie möglicherweise aufgefordert zu bestätigen, ob Sie die vorherigen Standardeinstellungen für die Aufbewahrung von Performancedaten für 13 Monate beibehalten oder in 6 Monate ändern möchten. Nach der Bestätigung werden die historischen Leistungsdaten nach 6 Monaten gelöscht.
- Sie sollten alle laufenden Vorgänge abgeschlossen haben, da Unified Manager während des Upgrades nicht verfügbar ist.
- MySQL Community Edition wird beim Unified Manager Upgrade automatisch aktualisiert. Wenn die auf Ihrem System installierte Version von MySQL älter als 8.0.34 ist, führt das Upgrade von MySQL durch Unified Manager automatisch ein Upgrade auf 8.0.34 durch.

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.

   Siehe "Herunterladen von Unified Manager für Linux".

3. Navigieren Sie zum Zielverzeichnis und erweitern Sie das Unified Manager Bundle:

   ```
   unzip ActiveIQUnifiedManager-<version>.zip
   ```

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

4. Stellen Sie sicher, dass das folgende Modul im Verzeichnis verfügbar ist:

   ```
   ls *.rpm
   ```

   ```
   netapp-um<version>.x86_64.rpm
   ```

5. Führen Sie das Skript vor der Installation aus, um sicherzustellen, dass es keine Systemkonfigurationseinstellungen oder keine installierte Software gibt, die mit dem Upgrade in Konflikt geraten könnte:

   ```
   sudo ./pre_install_check.sh
   ```

   Das Skript vor der Installation überprüft, ob das System über ein gültiges Red hat Enterprise Linux-Abonnement verfügt und dass es Zugriff auf die erforderlichen Software-Repositorys hat. Wenn das Skript Probleme erkennt, müssen Sie die Probleme beheben und mit dem Upgrade fortfahren.

   Wenn fehlende Pakete erkannt werden, führen Sie die unter genannten Schritte "Weitere Schritte, die bei fehlenden Paketen ausgeführt werden müssen"aus. Wenn keine Pakete vorhanden sind, fahren Sie mit den nächsten Schritten fort.

6. 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 in Konflikt stehen könnten. Wenn das Skript Probleme erkennt, müssen Sie die Probleme beheben, bevor Sie Unified Manager aktualisieren. Wenn Sie zuvor Pakete wie *net-snmp* vor dem Upgrade von Unified Manager installiert haben, kann die MySQL-Abhängigkeit das Paket während des Upgrades deinstallieren. Sie müssen das Paket erneut manuell installieren, um es weiterhin verwenden zu können.

7. 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:

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

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

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

Weitere Schritte, die bei fehlenden Paketen ausgeführt werden müssen

Wenn während des Upgrades an Ihrer Site fehlende Pakete erkannt wurden, oder wenn Ihr System nicht mit dem Internet verbunden ist oder Sie die Red hat Enterprise Linux-Repositories nicht verwenden, führen Sie die folgenden Schritte aus, um festzustellen, ob erforderliche Pakete fehlen und diese Pakete heruntergeladen werden.

> Diese Schritte müssen nach Schritt *5* des Hauptverfahrens ausgeführt werden. Dieses Verfahren aktualisiert Unified Manager und Sie müssen keine weiteren Schritte für ein Upgrade ausführen.

1. Die Liste der verfügbaren und nicht verfügbaren Pakete anzeigen:

   ```
   yum install netapp-um<version>.x86_64.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.

2. Führen Sie auf einem anderen System, das über den Internetzugang verfügt, den folgenden Befehl aus, um die fehlenden Pakete herunterzuladen.

   ```
   yum install package_name --downloadonly --downloaddir=.
   ```

Die Pakete werden in dem als angegebenen Verzeichnis heruntergeladen `--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
```

3. Kopieren Sie die heruntergeladenen Pakete in das Verzeichnis, in dem Sie das Unified Manager-Paket auf dem Installationssystem entpackt haben.
4. Ändern Sie Verzeichnisse in dieses Verzeichnis, und führen Sie den folgenden Befehl aus, um die fehlenden Pakete zusammen mit ihren Abhängigkeiten zu installieren.

   ```
   yum install *.rpm
   ```

5. Starten Sie den Unified Manager Server. Führen Sie folgende Befehle aus:

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

Hiermit ist das Upgrade-Verfahren für Unified Manager abgeschlossen. Geben Sie die angegebene IP-Adresse oder URL in ein neues Fenster eines unterstützten Webbrowsers ein, um die Unified Manager Web-UI zu starten, und melden Sie sich dann mit demselben Wartungs-Benutzernamen (umadmin) und Kennwort an, das Sie zuvor festgelegt haben.

Aktualisieren des Host-Betriebssystems von Red hat Enterprise Linux 7.x auf 8.x

Wenn Sie bereits Unified Manager auf einem Red hat Enterprise Linux 7.x-System installiert haben und ein Upgrade auf Red hat Enterprise Linux 8.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 7.x-System erstellen und anschließend die Sicherung auf einem Red hat Enterprise Linux 8.x-System wiederherstellen. Beachten Sie, dass die unterstützten Versionen von Red hat Enterprise Linux zwischen 8.0 und 8.9 liegen.

Der Unterschied zwischen den beiden unten aufgeführten Optionen besteht darin, dass Sie in einem Fall die Wiederherstellung von Unified Manager auf einem neuen 8.x-Server durchführen und im anderen Fall den Wiederherstellungsvorgang auf demselben Server ausführen.

Da diese Aufgabe erfordert, dass Sie auf dem Red hat Enterprise Linux 7.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. Lücken in gesammelten Daten erscheinen in der Unified Manager-Benutzeroberfläche für den Zeitraum, in dem das Red hat Enterprise Linux 7.x-System heruntergefahren wird und bevor das neue Red hat Enterprise Linux 8.x gestartet wird.

"Managen von Backup- und Restore-Vorgängen"Lesen Sie, ob Sie detaillierte Anweisungen zu den Sicherungs- und Wiederherstellungsprozessen lesen müssen.

Führen Sie diese Schritte aus, wenn Sie über ein Ersatzsystem verfügen, auf dem Sie die Red hat Enterprise Linux 8.x-Software installieren können, damit Sie die Unified Manager-Wiederherstellung auf diesem System

durchführen können, während das Red hat Enterprise Linux 7.x-System weiterhin verfügbar ist.

1. Installieren und konfigurieren Sie einen neuen Server mit der Red hat Enterprise Linux 8.x-Software.

   Siehe "Linux-Software- und Installationsanforderungen".

2. Installieren Sie auf dem Red hat Enterprise Linux 8.x-System dieselbe Version der Unified Manager-Software, die Sie auf dem vorhandenen Red hat Enterprise Linux 7.x-System verwenden.

   Siehe "Installation von Unified Manager unter 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 7.x-System im Menü Administration in der Web-Benutzeroberfläche ein Unified Manager-Backup und kopieren Sie dann die Sicherungsdatei(`.7z`) und den Inhalt des Unterverzeichnisses des Datenbank-Repository(`/database-dumps-repo`) an einen externen Speicherort.
4. Fahren Sie auf dem Red hat Enterprise Linux 7.x-System Unified Manager herunter.
5. Kopieren Sie auf dem Red hat Enterprise Linux 8.x-System die Sicherungsdatei(`.7z`) vom externen Speicherort in `/opt/netapp/data/ocum-backup/` und die Datenbank-Repository-Dateien in das `/database-dumps-repo` Unterverzeichnis unter dem `/ocum-backup` Verzeichnis.
6. Geben Sie den folgenden Befehl ein, um die Unified Manager-Datenbank aus der Backup-Datei wiederherzustellen:

   ```
   um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
   ```

7. Geben Sie die IP-Adresse oder URL in Ihren Webbrowser ein, um die Web-UI von Unified Manager 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 7.x-System entfernen.

Aktualisierung des Host-Betriebssystems auf demselben Server

Führen Sie diese Schritte aus, wenn Sie kein Ersatzsystem besitzen, auf dem Sie Red hat Enterprise Linux 8.x-Software installieren können.

1. Erstellen Sie im Menü Administration in der Web-Benutzeroberfläche ein Unified Manager-Backup und kopieren Sie dann die Sicherungsdatei(`.7z`) und den Inhalt des Datenbank-Repository-Verzeichnisses(`/database-dumps-repo`) an einen externen Speicherort.
2. Entfernen Sie das Red hat Enterprise Linux 7.x-Image aus dem System, und löschen Sie das System vollständig.
3. Installation und Konfiguration der Red hat Enterprise Linux 8.x-Software auf demselben System

   Siehe "Linux-Software- und Installationsanforderungen".

4. Installieren Sie auf dem Red hat Enterprise Linux 8.x-System dieselbe Version der Unified Manager-Software, die Sie auf dem Red hat Enterprise Linux 7.x-System hatten.

   Siehe "Installation von Unified Manager unter 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(`.7z`) vom externen Speicherort in `/opt/netapp/data/ocum-backup/` und die Datenbank-Repository-Dateien in das `/database-dumps-repo` Unterverzeichnis unter dem `/ocum-backup` Verzeichnis.
6. Geben Sie den folgenden Befehl ein, um die Unified Manager-Datenbank aus der Backup-Datei wiederherzustellen:

   ```
   um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
   ```

7. Geben Sie die IP-Adresse oder URL in Ihren Webbrowser ein, um die Web-UI von Unified Manager zu starten, und melden Sie sich anschließend beim System an.

Upgrade von Drittanbieterprodukten nach der Installation von Unified Manager

Sie können Produkte von Drittanbietern wie JRE aktualisieren, wenn Unified Manager bereits auf Linux-Systemen installiert ist.

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 OpenJDK unter Linux

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

Was Sie brauchen

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

Sie können OpenJDK-Versionen innerhalb von Versionsfamilien aktualisieren. Sie können beispielsweise von OpenJDK 11.0.14 auf OpenJDK 11.0.17 aktualisieren, aber Sie können nicht direkt von OpenJDK 11 auf OpenJDK 12 aktualisieren.

Schritte

1. Melden Sie sich als Root-Benutzer auf dem Unified Manager-Hostcomputer an.
2. Laden Sie die entsprechende Version von OpenJDK (64-Bit) auf das Zielsystem herunter.
3. Beenden Sie die Unified Manager Services:

   ```
   systemctl stop ocieau

   systemctl stop ocie
   ```

4. Installieren Sie das neueste OpenJDK auf dem System.
5. Starten Sie die Unified Manager Services:

   ```
   systemctl start ocie
   ```

```
systemctl start ocieau
```

Neustart Von Unified Manager

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

Was Sie brauchen

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. Stoppen Sie den Unified Manager-Dienst und den zugehörigen MySQL-Dienst in dieser Reihenfolge:

```
systemctl stop ocieau

systemctl stop ocie

systemctl stop mysqld
```

3. Starten Sie die MySQL und Unified Manager Services in dieser Reihenfolge:

```
systemctl start mysqld

systemctl start ocie

systemctl start ocieau
```

`mysqld` Ist ein Daemon-Programm erforderlich, um den MySQL-Server zu starten und zu stoppen.

Unified Manager Wird Entfernt

Sie können Unified Manager über Red hat Enterprise Linux oder CentOS Host mit einem einzigen Befehl anhalten und deinstallieren.

Was Sie brauchen

- Sie müssen über Root-Benutzerzugriff auf den Server verfügen, von dem Sie Unified Manager entfernen möchten.
- Security-Enhanced Linux (SELinux) muss auf dem Linux-System deaktiviert sein. Ändern Sie den SELinux-Laufzeitmodus mit dem Befehl in „`permissive`“ `setenforce 0`.
- Alle Cluster (Datenquellen) müssen vor dem Entfernen der Software vom Unified Manager-Server entfernt werden.
- Sie sollten die Firewall-Regeln, die erstellt werden, manuell löschen, um MySQL-Port 3306 zu ermöglichen oder zu blockieren. Die Firewall-Regeln werden nicht automatisch gelöscht.

Schritte

1. Melden Sie sich als Root-Benutzer an dem Server an, auf dem Sie Unified Manager entfernen möchten.
2. Beenden Sie Unified Manager, und entfernen Sie ihn vom Server:

   ```
   rpm -e netapp-um
   ```

   In diesem Schritt werden alle zugehörigen NetApp RPM Pakete entfernt. Die erforderlichen Softwaremodule wie Java, MySQL und p7zip werden nicht entfernt.

3. **Optional:** Entfernen Sie gegebenenfalls die unterstützenden Softwaremodule wie Java, MySQL und p7zip:

   ```
   rpm -e p7zip mysql-community-client mysql-community-server mysql-community-common mysql-community-libs java-x.y
   ```

Nach Abschluss dieses Vorgangs wird die Software entfernt. Alle Daten aus dem `/opt/netapp/data` Verzeichnis werden nach der Deinstallation in den Ordner verschoben `/opt/netapp/data/BACKUP`. Durch die Deinstallation von Unified Manager werden auch die Java- und MySQL-Pakete entfernt, es sei denn, die Pakete werden von einer anderen Anwendung im System benötigt und verwendet. MySQL-Daten werden jedoch nicht gelöscht.

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.

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
   ```

Installation von Unified Manager auf Windows Systemen

Einführung in Active IQ Unified Manager

Mit Active IQ Unified Manager (ehemals OnCommand Unified Manager) überwachen und managen Sie den Zustand und die Performance Ihrer ONTAP Storage-Systeme über eine einzige 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

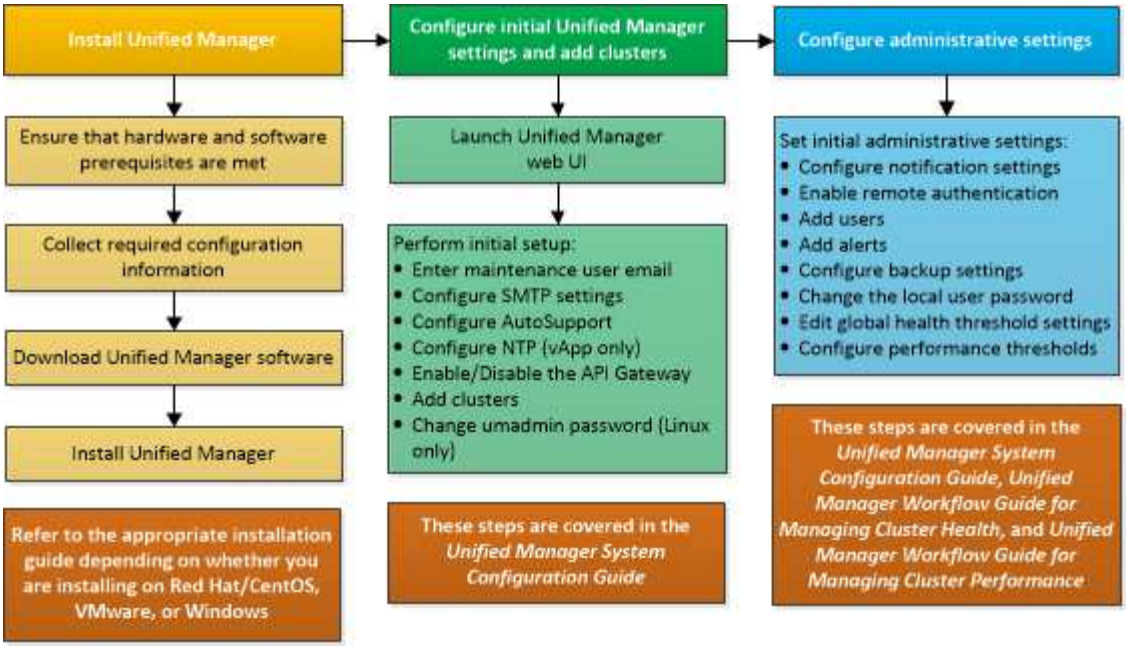
Die Unified Manager Server-Infrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Applikationsserver. Die Lösung bietet Infrastrukturservices wie beispielsweise Discovery, Monitoring, rollenbasierte Zugriffssteuerung (RBAC), Audits und Protokollierungsfunktionen.

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 diesen Abschnitten werden die im folgenden Workflow gezeigten Elemente beschrieben.



Anforderungen für die Installation von Unified Manager

Bevor Sie mit der Installation beginnen, stellen Sie sicher, dass der Server, auf dem Unified Manager installiert werden soll, die spezifischen Software-, Hardware-, CPU- und Arbeitsspeicheranforderungen erfüllt.

NetApp unterstützt keine Änderungen am Applikationscode für Unified Manager. Wenn Sie Sicherheitsmaßnahmen auf den Unified Manager-Server anwenden müssen, sollten Sie diese Änderungen am Betriebssystem vornehmen, auf dem Unified Manager installiert ist.

Weitere Informationen zum Anwenden von Sicherheitsmaßnahmen auf den Unified Manager-Server finden Sie im Knowledge Base-Artikel.

"Unterstützbarkeit von Sicherheitsmaßnahmen für Active IQ Unified Manager für Clustered Data ONTAP"

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Systemanforderungen für virtuelle Infrastruktur und Hardware

Die Installation von Unified Manager auf einer virtuellen Infrastruktur oder auf einem physischen System sollte 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)

Hardwarekonfiguration	Empfohlene Einstellungen
Prozessoren	4 CPUs
CPU-Zykluskapazität	9572 MHz insgesamt (Mindestanforderung 9572 MHz)
Freier Speicherplatz	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 sollten für die VM, wo Unified Manager eingesetzt wird, keine Arbeitsspeicherbeschränkungen festlegen und sollten keine Funktionen (z. B. Ballooning) aktivieren, die die Software daran hindern, den zugewiesenen Arbeitsspeicher im System 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. 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.

Voraussetzung für dedizierten Einsatz

Das physische oder virtuelle System, auf dem Unified Manager installiert wird, sollte 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 planen, die Unified Manager Backup- und Restore-Funktion zu verwenden, weisen Sie zusätzliche Kapazität zu, sodass 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, sollte so konfiguriert sein, dass Sie den Host-Namen vom Host selbst erfolgreich verwenden können `ping`. Im Fall der IPv6-Konfiguration sollten Sie überprüfen, ob `ping6` der Hostname erfolgreich ist, um sicherzustellen, dass die

Installation von Unified Manager 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.

Windows Software- und Installationsanforderungen

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

Betriebssystem-Software

Sie können Unified Manager unter folgenden Windows-Editionen installieren:

- Microsoft Windows Server 2019 Standard und Datacenter Edition
- Microsoft Windows Server 2022 Standard und Datacenter Edition

Unified Manager wird auf 64-Bit-Windows-Betriebssystem für die folgenden Sprachen unterstützt:

- Englisch
- Japanisch
- Vereinfachtes Chinesisch

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

"mysupport.netapp.com/matrix"

NetApp unterstützt die Installation von Unified Manager mithilfe von Tools von Drittanbietern, wie z. B. Microsoft System Center Configuration Manager (SCCM), nicht.

Der Server sollte dediziert sein für die Ausführung von Unified Manager. Auf dem Server sollten keine anderen Anwendungen installiert sein. Es ist möglich, dass eine aktive Anti-Virus-Software auf Ihrem Windows-System aufgrund von Firmenvorschriften installiert wird. Sie sollten die Virenschutzsoftware vor der Installation von Unified Manager deaktivieren, um einen Ausfall der Installation zu verhindern.

Software von anderen Anbietern

Die folgenden Drittanbieterpakete werden mit Unified Manager gebündelt. Wenn diese Pakete von Drittanbietern nicht auf Ihrem System installiert sind, installiert Unified Manager sie als Teil der Installation.

- Microsoft Visual C++ 2015 Redistributable Package Version 14.26.28720,3
- Microsoft Visual C++ weiterverteilbare Pakete für Visual Studio 2013 Version 12.0.40660.0
- MySQL Community Edition Version 8.0.34

- Python 3.11.6
- OpenJDK Version 11.0.20
- P7zip Version 23.01 oder höher

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, sollten Sie Folgendes sicherstellen:

- Er verwendet den Standardport.
- Die Beispieldatenbanken sind nicht installiert.
- Der Servicename lautet “MYSQL8”.

Unified Manager wird auf einem WildFly Web-Server bereitgestellt. WildFly 26.1.3 ist gebündelt und mit Unified Manager konfiguriert.

Vor dem Upgrade von Software anderer Anbieter sollten Sie eine laufende Instanz von Unified Manager herunterfahren. Nach Abschluss der Softwareinstallation von Drittanbietern können Sie Unified Manager neu starten.

Installationsvoraussetzungen

- Microsoft .NET 4.5 oder höher sollte installiert sein.
- Das `temp` Verzeichnis sollte mit 2 GB Festplattenspeicher zum Extrahieren der Installationsdateien konfiguriert werden. Um zu überprüfen, ob das Verzeichnis erstellt wurde, führen Sie den folgenden Befehl auf der Befehlszeilenschnittstelle aus: `echo %temp%`
- Sie sollten 2 GB Festplattenspeicher im Windows-Laufwerk für das Caching der MSI-Dateien von Unified Manager reservieren.
- Der Microsoft Windows Server, auf dem Sie Unified Manager installieren möchten, sollte mit einem vollständig qualifizierten Domänennamen (FQDN) konfiguriert werden, so dass `ping` Antworten auf den Hostnamen und den FQDN erfolgreich sind.
- Sie sollten den weltweiten Webveröffentlichungsservice von Microsoft IIS deaktivieren und sicherstellen, dass die Ports 80 und 443 frei sind.
- Sie sollten sicherstellen, dass die Einstellung des Host für Remote-Desktop-Sitzungen für „`Windows Installer RDS Compatibility`“ während der Installation deaktiviert ist.
- UDP-Port 514 sollte frei sein und nicht von anderen Diensten verwendet werden.
- Vor der Installation von Unified Manager sollten Sie alle Virenschutzsoftware auf Ihrem System deaktivieren. Stellen Sie nach Abschluss der Installation sicher, dass Sie die folgenden Pfade von Anti-Virus-Scan manuell ausschließen:
  - Beispielsweise das Unified Manager-Datenverzeichnis `C:\ProgramData\NetApp\OnCommandAppData\`
  - Installationsverzeichnis für Unified Manager, zum Beispiel `\C:\Program Files\NetApp\`
  - MySQL-Datenverzeichnis, zum Beispiel `C:\ProgramData\MySQL\MySQLServerData`

Unterstützte Browser

Um auf die Web-UI von Unified Manager zuzugreifen, verwenden Sie einen unterstützten Browser.

Die Interoperabilitäts-Matrix enthält eine Liste der unterstützten Browser-Versionen.

"mysupport.netapp.com/matrix"

Durch das Deaktivieren von Popup-Blockern für alle Browser wird sichergestellt, dass die Softwarefunktionen ordnungsgemäß angezeigt werden.

Wenn Sie planen, Unified Manager für SAML-Authentifizierung zu konfigurieren, damit ein Identitäts-Provider (IdP) Benutzer authentifizieren kann, sollten Sie die Liste der vom IdP unterstützten Browser überprüfen.

Protokoll- und Port-Anforderungen

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

In typischen Installationen müssen Sie bei der Verbindung zur Web-UI von Unified Manager keine Portnummern angeben, da immer Standardports verwendet werden. Da Unified Manager beispielsweise immer versucht, auf seinem Standardport ausgeführt zu werden, können Sie anstelle von `https://<host>:443` eingeben `https://<host>`.

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.
Wartungskonsole	SSH/SFTP	22	Wird verwendet, um auf die Wartungskonsole zuzugreifen und Supportpakete abzurufen.

Schnittstelle	Protokoll	Port	Beschreibung
Linux Befehlszeile	SSH/SFTP	22	Wird verwendet, um auf die Red hat Enterprise Linux oder CentOS Befehlszeile zuzugreifen und Supportpakete abzurufen.
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.
MySQL Datenbank	MySQL	3306	Wird verwendet, um den Zugriff von OnCommand Workflow Automation und OnCommand API Services auf Unified Manager zu aktivieren.
AMQP QPID-Broker	TCP/IP	56072	Wird für die interne Nachrichtenkommunikation verwendet.
AMQP QPID-Broker	WebSocket über TCP	56080	Wird verwendet, um an diesem Port Nachrichten abzuhören, die von ONTAP (Cloud-Agent) empfangen werden.

Schnittstelle	Protokoll	Port	Beschreibung
AMQP QPID-Broker	WebSocket über TCP	56443	Wird verwendet, um an diesem Port Nachrichten abzuhören, die von ONTAP (Cloud-Agent) empfangen werden. Die Kommunikation über diesen Port unterstützt die von TLS oder SSL bereitgestellte Verschlüsselung.
AMQP QPID-Broker	HTTP	9000	Wird zum Starten der AMQP-Verwaltungsbenutzeroberfläche auf dieser Seite verwendet.

Der Standardport für MySQL, 3306, ist nur auf localhost beschränkt, während Unified Manager auf Windows-Systemen installiert wird. Aktivieren Sie die Firewall, um den Zugriff für den Port MySQL, 3306, nach Abschluss der Installation einzuschränken. Dies wirkt sich nicht auf ein Upgrade-Szenario aus, in dem die vorherige Konfiguration erhalten bleibt. Diese Konfiguration kann geändert werden, und die Verbindung kann anderen Hosts über die Option auf der Wartungskonsole zur Verfügung gestellt `Control access to MySQL port 3306` werden. Weitere Informationen finden Sie unter "Zusätzliche Menüoptionen". Die für die HTTP- und HTTPS-Kommunikation verwendeten Ports (die Ports 80 und 443) können mithilfe der Unified Manager-Wartungskonsole geändert werden. Weitere Informationen finden Sie unter "Active IQ Unified Manager wird konfiguriert".

Verbindungen vom Unified Manager-Server

Sie sollten Ihre Firewall so konfigurieren, dass sie Ports öffnen, die die Kommunikation zwischen dem Unified Manager-Server und verwalteten Speichersystemen, 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.

Ziel	Protokoll	Port	Beschreibung
AutoSupport Server	HTTPS	443	Wird zum Senden von AutoSupport-Informationen verwendet. Erfordert den Internetzugang, um diese Funktion auszuführen.
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
NTP	123/UDP	Wird verwendet, um die Zeit auf dem Unified Manager-Server mit einem externen NTP-Zeitserver zu synchronisieren. (Nur VMware Systeme)	AMQP QPID-Broker
TCP/IP	56072	Wird für die interne Nachrichtenkommunikation verwendet.	AMQP QPID-Broker

Ziel	Protokoll	Port	Beschreibung
WebSocket über TCP	56080	Wird verwendet, um an diesem Port Nachrichten abzuhören, die von ONTAP (Cloud-Agent) empfangen werden.	AMQP QPID-Broker

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
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	

Einstellung	Ihr Wert
Hostname oder IP-Adresse des SMTP-Servers	
SMTP-Benutzername	
SMTP-Passwort	
SMTP-Port	25 (Standardwert)
E-Mail, von der aus Benachrichtigungen gesendet werden	
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)	
SNMP-Trap-Ziel-Host-IP-Adressen	
SNMP-Port	

Cluster-Informationen

Angaben zu den Storage-Systemen, die Sie mit Unified Manager managen.

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	

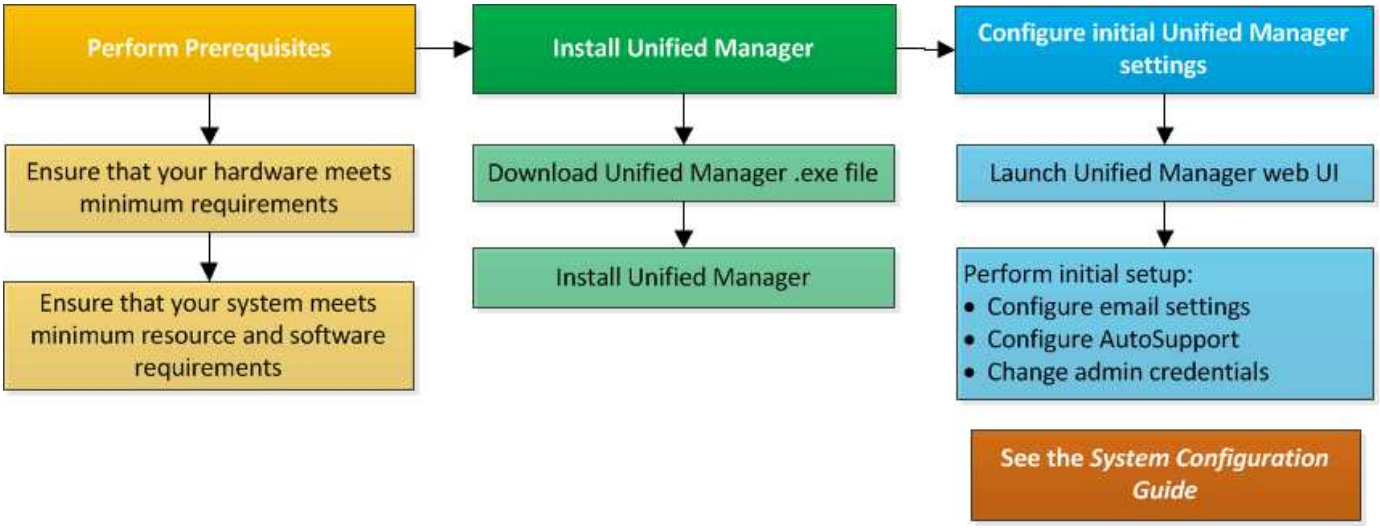
Cluster 1 von N	Ihr Wert
Protokoll	HTTPS

Installieren, Aktualisieren und Entfernen der Unified Manager Software

Sie können Unified Manager installieren, auf eine neuere Version aktualisieren oder die Unified Manager-Anwendung entfernen.

Überblick über den Installationsprozess

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.

Installation Von Unified Manager

Wird Unified Manager installiert, um Storage-Kapazität, -Verfügbarkeit, -Performance und -Sicherungsprobleme zu überwachen und Fehler zu beheben.

Was Sie brauchen

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

  Siehe "Hardwaresystemanforderungen".

  Siehe "Windows Software- und Installationsanforderungen".

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

- Sie sollten über Windows-Administratorrechte verfügen. Stellen Sie sicher, dass Ihr Benutzername nicht mit einem Ausrufezeichen "!" beginnt!". `Installation of Unified Manager might fail if the user name of user running the installation begins with "`.
- Sie sollten über einen unterstützten Webbrowser verfügen.
- Das Unified Manager-Wartungsbenutzerkennwort sollte zwischen 8 und 20 Zeichen lang sein. Es sollte Groß-/Kleinschreibung oder Buchstaben, 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 navigieren Sie zur Download-Seite für Unified Manager:

   "NetApp Support-Website"

3. Wählen Sie die erforderliche Version von Unified Manager aus, und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (Endbenutzer License Agreement, EULA).
4. Laden Sie die Installationsdatei für Unified Manager Windows in ein Zielverzeichnis auf dem Windows-System herunter.
5. Navigieren Sie zum Verzeichnis, in dem sich die Installationsdatei befindet.
6. Klicken Sie mit der rechten Maustaste, und führen Sie die ausführbare Datei des Unified Manager-Installationsprogramms (.exe) als Administrator aus.

   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.

7. Klicken Sie Auf **Weiter**.
8. Geben Sie den Benutzernamen und das Kennwort ein, um den Wartungbenutzer zu erstellen.
9. Geben Sie im Datenbankverbindungsassistenten das MySQL-Root-Passwort ein.
10. 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.

11. Klicken Sie Auf **Weiter**.
12. Klicken Sie im Assistenten Ready to Install Shield auf **Install**.
13. Klicken Sie nach Abschluss der Installation auf **Fertig stellen**.
14. Wenn auf Ihrem Windows-System eine aktive Antiviren-Software installiert ist, schließen Sie nach Abschluss der Installation die folgenden Pfade von Anti-Virus Scan manuell aus:

- Unified Manager-Datenverzeichnis
- Unified Manager Installationsverzeichnis vorhanden
- MySQL-Datenverzeichnis

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 ist. 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\`

Sie können auf die Web-Benutzeroberfläche zugreifen, um die Ersteinrichtung von Unified Manager durchzuführen, wie in beschrieben"Active IQ Unified Manager wird konfiguriert".

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	`ActiveIQUnifiedManager-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:
	
	`ActiveIQUnifiedManager.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	`ActiveIQUnifiedManager-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:
	
	`ActiveIQUnifiedManager.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"`

Die `/qr` Option aktiviert den leisen Modus mit reduzierter 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, sollten Sie die Option verwenden `/qr`. Die Installation schlägt fehl, wenn die `/qn` Option auf einem Server verwendet wird, auf dem keine Pakete von Drittanbietern installiert sind.

Die `/qn` Option aktiviert den leisen Modus ohne Benutzeroberfläche. Während der Installation werden keine Benutzeroberfläche oder Details angezeigt. Sie sollten die Option nicht verwenden `/qn`, 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`

Ändern des JBoss-Passworts

Sie können das Instanzspezifische JBoss-Passwort zurücksetzen, das während der Installation festgelegt wurde. Sie können das Passwort optional zurücksetzen, falls Ihr Standort diese Sicherheitsfunktion erfordert, um die Installationseinstellung für Unified Manager zu überschreiben. Dieser Vorgang ändert auch das Passwort, das JBoss zum Zugriff auf MySQL verwendet.

Was Sie brauchen

- Sie sollten Windows-Administratorrechte für das System besitzen, auf dem Unified Manager installiert ist.
- Sie sollten das Passwort für den MySQL-Root-Benutzer haben.
- Sie sollten auf das von NetApp bereitgestellte Skript im Verzeichnis zugreifen können `password.bat`

  `C:\Program Files\NetApp\essentials\bin`.

Schritte

1. Melden Sie sich als Admin-Benutzer auf der Unified Manager-Host-Maschine an.
2. Beenden Sie mithilfe der Windows Services-Konsole die folgenden Unified Manager-Services:
   - Erwerbsservice für NetApp Active IQ (Ozie-au)
   - NetApp Active IQ Management Server-Service (OnCommandsvc)
3. Starten Sie das `password.bat` Skript, um den Kennwortänderungsprozess zu starten:

   ```
   C:\Program Files\NetApp\essentials\bin> password.bat resetJBossPassword
   ```

4. Geben Sie bei entsprechender Aufforderung das Passwort für den Benutzer MySQL Root ein.
5. Geben Sie bei Aufforderung das neue JBoss-Benutzerpasswort ein, und geben Sie es zur Bestätigung erneut ein.

   Beachten Sie, dass das Passwort zwischen 8 und 16 Zeichen lang sein muss und mindestens eine Ziffer, ein Großbuchstaben und ein Kleinbuchstaben sowie mindestens eines der folgenden Sonderzeichen enthalten muss:

   ```
   !@%^*-_=[]:<>.?/~+
   ```

6. Starten Sie nach Abschluss des Skripts die Unified Manager-Dienste über die Windows-Dienstkonsole:
   - NetApp Active IQ Management Server-Service (OnCommandsvc)
   - Erwerbsservice für NetApp Active IQ (Ozie-au)
7. Nachdem alle Services gestartet wurden, können Sie sich in der UI von Unified Manager einloggen.

Unterstützter Upgrade-Pfad für Unified Manager-Versionen

Active IQ Unified Manager unterstützt für jede Version einen bestimmten Upgrade-Pfad.

Nicht alle Versionen von Unified Manager können ein Upgrade ohne Upgrade auf neuere Versionen durchführen. Die Unified Manager Upgrades sind auf ein N-2-Modell beschränkt, d. h. ein Upgrade kann nur innerhalb der nächsten zwei Versionen auf allen Plattformen durchgeführt werden. Beispielsweise können Sie nur ein Upgrade von Unified Manager 9.12 und 9.13 auf Unified Manager 9.14 durchführen.

Wenn Sie eine Version verwenden, die vor den unterstützten Versionen liegt, muss Ihre Unified Manager Instanz zuerst auf eine der unterstützten Versionen aktualisiert und dann auf die aktuelle Version aktualisiert werden.

Wenn die installierte Version beispielsweise Unified Manager 9.9 ist und Sie auf Unified Manager 9.14 aktualisieren möchten, führen Sie eine Reihe von Upgrades aus.

Beispiel für ein Upgrade-Pfad:

1. Upgrade 9.9 → 9.11
2. Upgrade 9.11 → 9.13
3. Upgrade 9.13 → 9.14

Weitere Informationen zur Upgrade-Pfadmatrix finden Sie in diesem "Knowledge Base-Artikel (KB".

Upgrade Von Unified Manager

Sie können ein Upgrade von Unified Manager 9.12 oder 9.13 auf 9.14 durchführen, indem Sie die Installationsdatei auf die Windows-Plattform herunterladen und ausführen.

Was Sie brauchen

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

  Siehe "Hardwaresystemanforderungen".

  Siehe "Windows Software- und Installationsanforderungen".

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

  Stellen Sie sicher, dass Microsoft .NET 4.5.2 oder höher auf Ihrem System installiert ist, bevor Sie das Upgrade starten.

- MySQL Community Edition wird beim Unified Manager Upgrade automatisch aktualisiert. Wenn die auf Ihrem System installierte Version von MySQL älter als 8.0.34 ist, führt das Upgrade von MySQL durch Unified Manager automatisch ein Upgrade auf 8.0.34 durch. Sie dürfen kein eigenständiges Upgrade einer früheren Version von MySQL auf 8.0.34 ausführen.
- Sie sollten über Windows-Administratorrechte verfügen. Stellen Sie sicher, dass Ihr Benutzername nicht mit einem Ausrufezeichen "!" beginnt!`". Installation of Unified Manager might fail if the user name of user running the installation begins with "`.
- Sie sollten über gültige Zugangsdaten verfügen, um sich auf der NetApp Support Site anzumelden.

- Um Datenverlust zu vermeiden, sollten Sie ein Backup des Unified Manager-Rechners erstellt haben, falls während des Upgrades ein Problem auftritt.
- Sie sollten über ausreichend Speicherplatz verfügen, um das Upgrade durchzuführen.

  Der verfügbare Speicherplatz auf dem Installationslaufwerk sollte 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.

- Während des Upgrades werden Sie möglicherweise aufgefordert zu bestätigen, ob Sie die vorherigen Standardeinstellungen für die Aufbewahrung von Performancedaten für 13 Monate beibehalten oder in 6 Monate ändern möchten. Nach der Bestätigung werden die historischen Leistungsdaten nach 6 Monaten gelöscht.
- Vor dem Upgrade sollten Sie alle offenen Dateien oder Ordner in *<InstallDir>\JDK* und *MySQL Data Directory* schließen.
- Wenn auf Ihrem Windows-System eine aktive Virenschutzsoftware installiert ist, kann das Unified Manager-Upgrade fehlschlagen. Vor dem Upgrade von Unified Manager sollten Sie alle Virenschutzsoftware auf Ihrem System deaktivieren.

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 navigieren Sie zur Download-Seite für Unified Manager:

   "NetApp Support-Website".

2. Wählen Sie die erforderliche Version von Unified Manager aus, und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (Endbenutzer License Agreement, EULA).
3. Laden Sie die Installationsdatei für Unified Manager Windows in ein Zielverzeichnis auf dem Windows-System herunter.
4. Klicken Sie mit der rechten Maustaste, und führen Sie die ausführbare Datei des Unified Manager-Installationsprogramms (.exe) als Administrator aus.

   Unified Manager fordert Sie zur folgenden Meldung auf:

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

5. Klicken Sie auf **Ja** und dann auf **Weiter**.
6. Geben Sie das bei der Installation festgelegte MySQL8-Root-Passwort ein, und klicken Sie dann auf **Weiter**.

7. Starten Sie die Web-Benutzeroberfläche in einem neuen Fenster in einem unterstützten Webbrowser, und melden Sie sich an, um die aktualisierte Version von Unified Manager zu verwenden.
8. Wenn auf Ihrem Windows-System eine aktive Virenschutzsoftware installiert ist, stellen Sie sicher, dass Sie nach Abschluss des Upgrades die folgenden Pfade von Virenschutzprüfung manuell ausschließen:
   - Unified Manager-Datenverzeichnis
   - Unified Manager Installationsverzeichnis vorhanden
   - MySQL-Datenverzeichnis

> Führen Sie den folgenden Befehl aus, um ein stille Upgrade von Unified Manager durchzuführen:
> `ActiveIQUnifiedManager-<version\>.exe /s /v"MYSQL_PASSWORD=<password> /qn /l*v <system_drive>:\install.log"`

Upgrade von Drittanbieterprodukten

Sie können Produkte von Drittanbietern wie JRE 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.

Aktualisierung von OpenJDK

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

Was Sie brauchen

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

Sie können OpenJDK-Versionen innerhalb von Versionsfamilien aktualisieren. Sie können beispielsweise von OpenJDK 11.0.16 auf OpenJDK 11.0.18 aktualisieren, aber Sie können nicht direkt von OpenJDK 11 auf OpenJDK 12 aktualisieren.

Schritte

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

   Zum Beispiel, download `jdk-11.0.18_windows-x64_bin.zip from https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html`.

   > Zum Herunterladen der Datei ist ein Oracle-Konto erforderlich. Wenn Sie noch kein Oracle-Konto haben, gehen Sie zu Seite, um ein Konto zu "Anmeldung beim Oracle-Konto"erstellen.

3. Beenden Sie mithilfe der Windows Services-Konsole die folgenden Unified Manager-Services:

- Erwerbsservice für NetApp Active IQ (Ozie-au)
- NetApp Active IQ Management Server-Service (OnCommandsvc)

4. Erweitern Sie die `zip` Datei.
5. Kopieren Sie die Verzeichnisse und Dateien aus dem resultierenden `jdk` Verzeichnis (z. B. `jdk-11.0.18` 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 Active IQ Management Server-Service (OnCommandsvc)
   - Erwerbsservice für NetApp Active IQ (Ozie-au)

Neustart Von Unified Manager

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

Was Sie brauchen

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. Erwerbsservice für NetApp Active IQ (Ozie-au) b. NetApp Active IQ Management Server-Service (OnCommandsvc)

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 Active IQ Management Server-Service (OnCommandsvc) b. Erwerbsservice für NetApp Active IQ (Ozie-au)

Deinstallieren Von Unified Manager

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

Was Sie brauchen

- Sie müssen über Administratorrechte für Windows verfügen.
- Alle Cluster (Datenquellen) müssen vom Unified Manager-Server entfernt werden, bevor die Software deinstalliert wird.
- Sie sollten die Firewall-Regeln, die erstellt werden, manuell löschen, um MySQL-Port 3306 zu ermöglichen oder zu blockieren. Die Firewall-Regeln werden nicht automatisch gelöscht.

Schritte

1. Deinstallieren Sie Unified Manager, indem Sie eine der folgenden Optionen auswählen:
   - Wenn Sie Unified Manager aus dem Assistenten für Programme und Funktionen* deinstallieren, führen Sie die folgenden Schritte aus:
     i. Navigieren Sie zu **Systemsteuerung** > **Programm und Funktionen**.
     ii. Wählen Sie Active IQ Unified Manager, und klicken Sie auf **Deinstallieren**.
   - Wenn Sie Unified Manager von der Befehlszeile deinstallieren, führen Sie die folgenden Schritte aus:
     i. Melden Sie sich mit Administratorrechten an der Windows-Befehlszeile an.
     ii. Navigieren Sie zum Active IQ Unified Manager-Verzeichnis, 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.

2. 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, Python, Und 7zip
   - MySQL Applikationsdaten von Unified Manager
   - Anwendungsprotokolle und Inhalt des Applikationsdatenverzeichnisses

Durchführung von Konfigurations- und Administrationsaufgaben

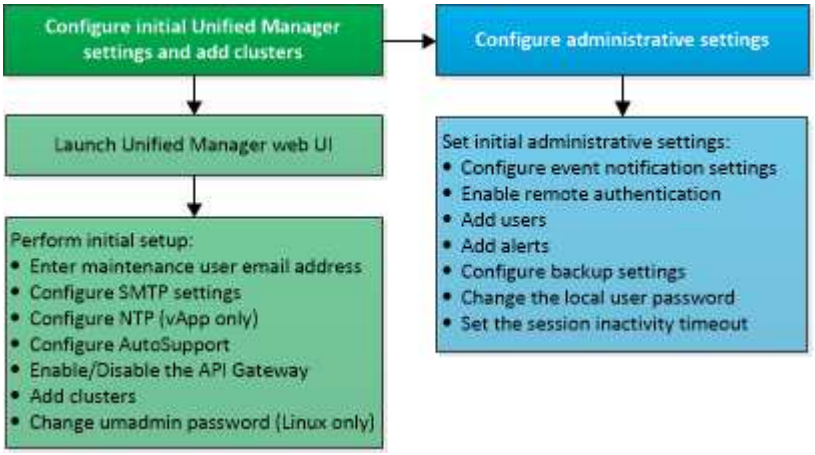
Active IQ Unified Manager wird konfiguriert

Nach der Installation von Active IQ Unified Manager (früher OnCommand 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.

Was Sie brauchen

- 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.

   Wenn Sie innerhalb einer Stunde drei aufeinanderfolgende erfolglose Versuche zur Anmeldung bei der Web-Benutzeroberfläche vornehmen, werden Sie aus dem System gesperrt und müssen sich an Ihren Systemadministrator wenden. Dies gilt nur für lokale Benutzer.

Die Ersteinrichtung der Unified Manager-Weboberfläche durchführen

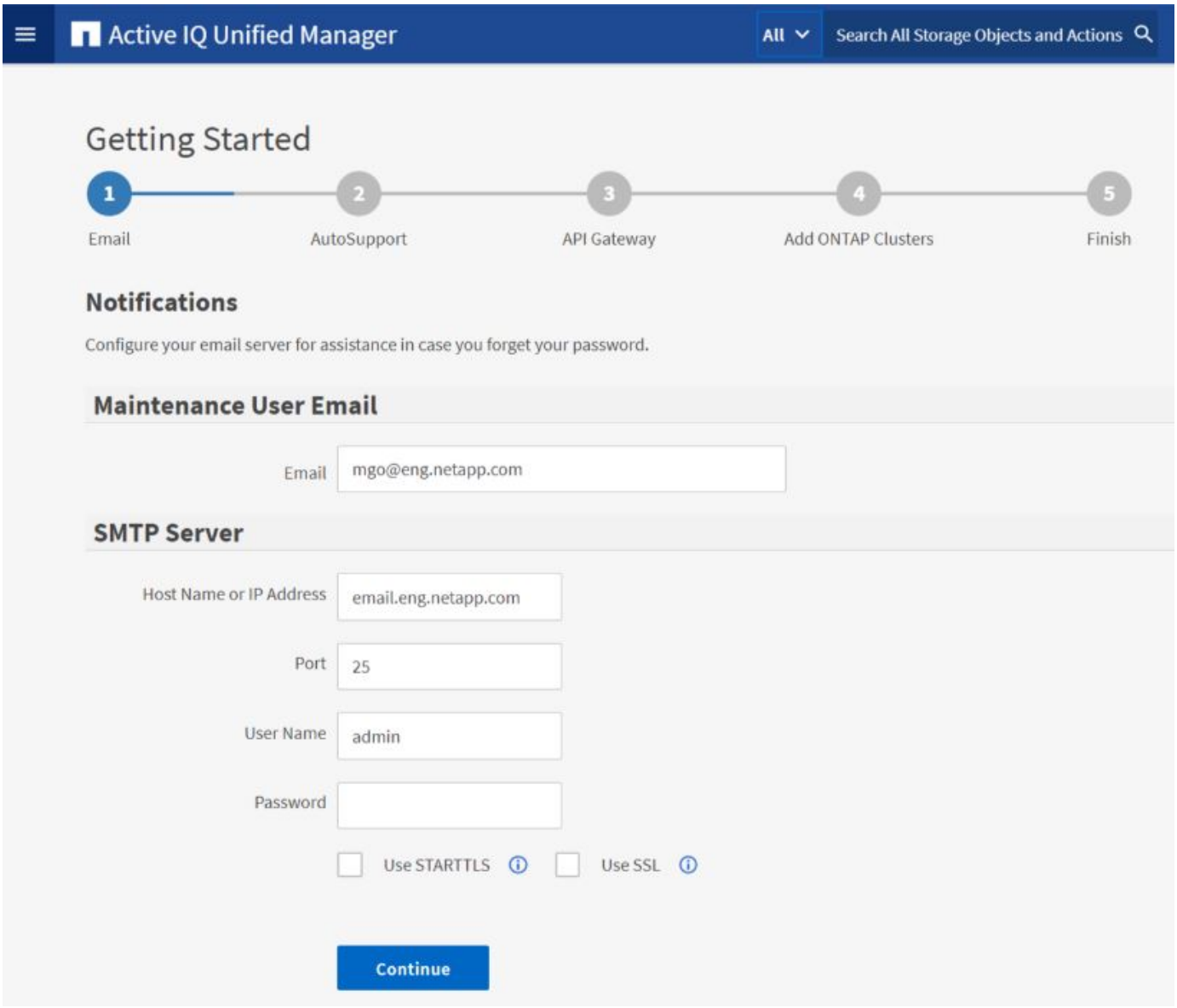
Um Unified Manager zu verwenden, müssen Sie zuerst die anfänglichen Setup-Optionen konfigurieren, einschließlich des NTP-Servers, der Wartungs-Benutzer-E-Mail-Adresse, des SMTP-Server-Hosts und des Hinzufügens von ONTAP-Clustern.

Was Sie brauchen

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

Die Seite Active IQ Unified ManagerGetting Started 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 Ihre Auswahl aus den Optionen Allgemein im linken Navigationsbereich von Unified Manager auswählen. Beachten Sie, dass die NTP-Einstellung nur für VMware Installationen gilt. Die Einstellung kann später mithilfe der Unified Manager Wartungskonsole geändert werden.

Schritte

1. Geben Sie auf der Seite Active IQ Unified Manager-Ersteinrichtung die E-Mail-Adresse des Wartungsbenutzers, den Hostnamen des SMTP-Servers und weitere SMTP-Optionen sowie den NTP-Server (nur VMware-Installationen) ein. Klicken Sie dann auf **Weiter**.

   Wenn Sie die Option **STARTTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Weiter** eine Zertifikatseite angezeigt. Überprüfen Sie die Zertifikatdetails, und akzeptieren Sie das Zertifikat, um mit den anfänglichen Setup-Einstellungen der Web-Benutzeroberfläche fortzufahren.

2. Klicken Sie auf der AutoSupport Seite auf **zustimmen und fortfahren**, um das Senden von AutoSupport Nachrichten von Unified Manager an NetAppActive IQ zu aktivieren.

   Wenn Sie einen Proxy für den Zugriff auf das Internet festlegen müssen, um AutoSupport-Inhalte zu

senden, oder wenn Sie AutoSupport deaktivieren möchten, verwenden Sie die Option **Allgemein** > **AutoSupport** von der Web-Benutzeroberfläche.

3. Ändern Sie auf Red hat- und CentOS-Systemen das umadmin-Benutzerpasswort von der standardmäßigen Zeichenfolge „`admin`“ in eine personalisierte Zeichenfolge.
4. Wählen Sie auf der Seite API-Gateway einrichten, ob Sie die API-Gateway-Funktion verwenden möchten, mit der Unified Manager die ONTAP-Cluster verwalten kann, die Sie mit ONTAP REST-APIs überwachen möchten. Klicken Sie dann auf **Weiter**.

   Sie können diese Einstellung später in der Web-Benutzeroberfläche über **Allgemein** > **Feature-Einstellungen** > **API-Gateway** aktivieren oder deaktivieren. Weitere Informationen zu den APIs finden Sie unter "Erste Schritte mit Active IQ Unified Manager REST APIs".

5. Fügen Sie die Cluster hinzu, die Unified Manager verwalten soll, und klicken Sie dann auf **Weiter**. Für jeden Cluster, den Sie verwalten möchten, müssen Sie den Host-Namen oder die Cluster-Management-IP-Adresse (IPv4 oder IPv6) sowie den Benutzernamen und die Kennwort-Anmeldedaten haben. Der Benutzer muss über die Rolle „`admin`“ verfügen.

   Dieser Schritt ist optional. Sie können Cluster später in der Web-Benutzeroberfläche von **Storage Management** > **Cluster-Setup** hinzufügen.

6. Überprüfen Sie auf der Seite Zusammenfassung, ob alle Einstellungen korrekt sind, und klicken Sie auf **Fertig stellen**.

Die Seite „erste Schritte“ wird geschlossen, und die Seite „Unified Manager Dashboard“ wird angezeigt.

Hinzufügen von Clustern

Sie können Active IQ Unified Manager ein Cluster hinzufügen, 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die folgenden Informationen haben:
  - Unified Manager unterstützt lokale ONTAP Cluster, ONTAP Select und Cloud Volumes ONTAP.
  - 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.

  - Der Cluster muss die ONTAP Version 9.1 oder höher ausführen.
  - Benutzername und Passwort für den ONTAP-Administrator

    Für dieses Konto muss die Rolle *admin* mit dem Anwendungszugriff auf *ontapi*, *Console* und *http*

eingestellt sein.

- Die Port-Nummer für die Verbindung zum Cluster mithilfe des HTTPS-Protokolls (normalerweise Port 443)
- Sie verfügen über die erforderlichen Zertifikate:

  SSL (HTTPS) Zertifikat: Dieses Zertifikat ist im Besitz von Unified Manager. Bei einer neuen Installation von Unified Manager wird ein selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt ein Upgrade auf ein Zertifikat, das von einer Zertifizierungsstelle unterzeichnet wurde, um die Sicherheit zu erhöhen. Wenn das Serverzertifikat abgelaufen ist, sollten Sie es neu generieren und Unified Manager neu starten, damit die Dienste das neue Zertifikat aufnehmen können. Weitere Informationen zur Neugenerierung von SSL-Zertifikaten finden Sie unter "Erstellen eines HTTPS-Sicherheitszertifikats".

  EMS-Zertifikat: Dieses Zertifikat ist im Besitz von Unified Manager. Es wird bei der Authentifizierung für EMS-Benachrichtigungen verwendet, die von ONTAP empfangen werden.

  Zertifikate für gegenseitige TLS-Kommunikation: Wird bei der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatbasierte Authentifizierung ist auf Grundlage der Version von ONTAP für ein Cluster aktiviert. Wenn das Cluster mit der Version ONTAP niedriger als die Version 9.5 ist, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

  Die zertifikatbasierte Authentifizierung wird für ein Cluster nicht automatisch aktiviert, wenn Sie eine ältere Version von Unified Manager aktualisieren. Allerdings können Sie die Aktivierung durch Ändern und Speichern der Cluster-Details aktivieren. Wenn das Zertifikat abgelaufen ist, sollten Sie es erneut generieren, um das neue Zertifikat zu integrieren. Weitere Informationen zum Anzeigen und Neugenerieren des Zertifikats finden Sie unter "Cluster werden bearbeitet".

  - Sie können ein Cluster über die Web-Benutzeroberfläche hinzufügen, und die zertifikatbasierte Authentifizierung wird automatisch aktiviert.
  - Sie können ein Cluster über die Unified Manager CLI hinzufügen. Die zertifikatbasierte Authentifizierung ist standardmäßig nicht aktiviert. Wenn Sie ein Cluster mit der Unified Manager CLI hinzufügen, muss das Cluster über die Unified Manager UI bearbeitet werden. Es wird angezeigt"Unterstützte CLI-Befehle von Unified Manager", wie Sie mithilfe der Unified Manager CLI einen Cluster hinzufügen.
  - Wenn die zertifikatbasierte Authentifizierung für ein Cluster aktiviert ist und Sie das Backup von Unified Manager von einem Server aus erstellen und auf einen anderen Unified Manager Server wiederherstellen. Hier wird der Hostname oder die IP-Adresse geändert, dann kann das Monitoring des Clusters fehlschlagen. Um den Ausfall zu vermeiden, bearbeiten und speichern Sie die Cluster-Details. Weitere Informationen zum Bearbeiten von Cluster-Details finden Sie unter "Cluster werden bearbeitet".

+
Cluster-Zertifikate: Dieses Zertifikat ist Eigentum von ONTAP. Sie können Unified Manager kein Cluster mit einem abgelaufenen Zertifikat hinzufügen. Wenn das Zertifikat bereits abgelaufen ist, sollten Sie es neu erstellen, bevor Sie das Cluster hinzufügen. Informationen zur Zertifikatgenerierung finden Sie im Artikel Knowledge Base (KB) "So erneuern Sie ein selbstsigniertes ONTAP-Zertifikat in der System Manager-Benutzeroberfläche" .

- 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.

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

Schritte

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

   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. Klicken Sie im Dialogfeld Host autorisieren auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.
6. Klicken Sie Auf **Ja**.

   Nachdem Sie die Cluster-Details gespeichert haben, können Sie das Zertifikat für die gegenseitige TLS-Kommunikation für ein Cluster anzeigen.

   Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, überprüft Unified Manager das Zertifikat nur, wenn das Cluster zunächst hinzugefügt wird. Unified Manager überprüft nicht das Zertifikat für jeden API-Aufruf an ONTAP.

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. 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, überprüfen Sie, ob die Uhren auf den beiden Systemen nicht synchronisiert sind und das HTTPS-Zertifikat von Unified Manager nach dem Startdatum des Clusters liegt. Sie müssen sicherstellen, dass die Uhren mit NTP oder einem ähnlichen Dienst synchronisiert werden.

Verwandte Informationen

"Installieren einer Zertifizierungsstelle, die signiert ist und ein HTTPS-Zertifikat zurückgegeben hat"

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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

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.

Was Sie brauchen

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
- Hostname oder IP-Adresse für den Trap-Ziel-Host, der den SNMP-Trap empfängt, zusammen mit der SNMP-Version, dem Outbound-Trap-Port, der Community und anderen erforderlichen SNMP-Konfigurationswerten

  Um mehrere Trap-Ziele festzulegen, trennen Sie jeden Host durch ein Komma. In diesem Fall müssen alle anderen SNMP-Einstellungen, wie Version und Outbound-Trap-Port, für alle Hosts in der Liste identisch sein.

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benachrichtigungen**.
2. Konfigurieren Sie auf der Seite Benachrichtigungen die entsprechenden Einstellungen.

   Hinweise:

   - Wenn die von-Adresse mit der Adresse „ActiveIQUnifiedManager@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.
3. Klicken Sie Auf **Speichern**.
4. Wenn Sie die Option **STARTTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Speichern** eine Zertifikatseite angezeigt. Überprüfen Sie die Zertifikatdetails, und akzeptieren Sie das Zertifikat, um die Benachrichtigungseinstellungen zu speichern.

   Sie können auf die Schaltfläche **Zertifikatdetails anzeigen** klicken, um die Zertifikatdetails anzuzeigen. Wenn das vorhandene Zertifikat abgelaufen ist, deaktivieren Sie das Kontrollkästchen **STARTTLS verwenden** oder **SSL verwenden**, speichern Sie die Benachrichtigungseinstellungen und aktivieren Sie erneut das Kontrollkästchen **STARTTLS verwenden** oder **SSL verwenden**, um ein neues Zertifikat anzuzeigen.

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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

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.

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 im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Aktivieren Sie das Kontrollkästchen für **Remote-Authentifizierung aktivieren…**.
3. Wählen Sie im Feld Authentifizierungsdienst den Diensttyp aus, und konfigurieren Sie den Authentifizierungsservice.

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-Notation) • 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. **Optional:** Fügen Sie Authentifizierungsserver hinzu, und testen Sie die Authentifizierung.
5. Klicken Sie Auf **Speichern**.

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.

Was Sie brauchen

- Sie müssen über die Anwendungsadministratorrolle verfügen.
- Das Deaktivieren verschachtelter Gruppen ist nur bei Verwendung von Active Directory anwendbar.

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 im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Aktivieren Sie das Kontrollkästchen für **Suche nach verschachtelter Gruppe 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.

Was Sie brauchen

- Sie müssen die Remote-Authentifizierung aktiviert haben.
- Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. 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, dann ist der Name der Basisunterscheidungder **cn=ou,dc=Domain,dc=com**.
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, dann ist der Name der Basisunterscheidungder **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, dann ist der Name der Basisunterscheidungder **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.

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.

Was Sie brauchen

- 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 über die Anwendungsadministratorrolle verfügen.

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 im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Aktivieren oder Deaktivieren der Option * Sichere Verbindung verwenden*:

Ihr Ziel ist	Dann tun Sie das…
Aktivieren Sie sie	a. Wählen Sie die Option * Sichere Verbindung verwenden* aus. 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.
Deaktivieren	a. Deaktivieren Sie 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.

3. 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.

Was Sie brauchen

- 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 über die Anwendungsadministratorrolle verfügen.

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 im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Klicken Sie Auf **Authentifizierung Testen**.
3. Geben Sie im Dialogfeld Testbenutzer den Benutzernamen und das Kennwort des Remote-Benutzers oder des Benutzernamens der Remote-Gruppe ein, und klicken Sie dann auf **Test**.

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

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.

Was Sie brauchen

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

Sie können eine Warnmeldung direkt auf der Seite Ereignisdetails erstellen, nachdem Sie ein Ereignis empfangen haben. Zusätzlich können Sie eine Warnung auf der Seite „Alarmkonfiguration“ erstellen, wie hier beschrieben.

Schritte

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

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

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

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

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

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

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

   Sie können auch Benutzer über SNMP-Traps benachrichtigen.

7. Klicken Sie Auf **Speichern**.

Beispiel für das Hinzufügen einer Meldung

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

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

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

Schritte

1. Klicken Sie auf **Name**, und geben Sie **HealthTest** in das Feld **Alarmname** ein.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
   a. Geben Sie in das Feld **Name enthält abc** ein, um die Volumes anzuzeigen, deren Name „`abc`“ enthält.
   b. Wählen Sie[All Volumes whose name contains 'abc'] im Bereich „Verfügbare Ressourcen“ die Option **++** aus, und verschieben Sie sie in den Bereich „Ausgewählte Ressourcen“.
   c. Klicken Sie auf **exclude**, und geben Sie **xyz** in das Feld **Name enthält** ein, und klicken Sie dann 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 **sample@domain.com** in das Feld Diese Benutzer benachrichtigen ein.
6. Wählen Sie **alle 15 Minuten**, um den Benutzer alle 15 Minuten zu benachrichtigen.

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

Ändern des lokalen Benutzerpassworts

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

Was Sie brauchen

Sie müssen als lokaler Benutzer angemeldet sein.

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 Benutzerpassworts für die Wartung 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**.

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.

Einstellen des Timeout für die Inaktivität der Sitzung

Sie können für Unified Manager den Wert für Inaktivitätszeitüberschreitung festlegen, damit die Sitzung nach einer bestimmten Zeit automatisch beendet wird. Standardmäßig ist das Timeout auf 4,320 Minuten (72 Stunden) eingestellt.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Diese Einstellung betrifft alle angemeldeten Benutzersitzungen.

Diese Option ist nicht verfügbar, wenn Sie die SAML-Authentifizierung (Security Assertion Markup Language) aktiviert haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Funktionseinstellungen**.
2. Geben Sie auf der Seite **Feature Settings** das Inaktivitätszeitlimit an, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Haben Sie keine Zeitüberschreitung gesetzt, so dass die Sitzung nie automatisch geschlossen wird	Bewegen Sie im Fenster **Inaktivität Timeout** den Schieberegler nach links (aus) und klicken Sie auf **Apply**.
Legen Sie eine bestimmte Anzahl von Minuten als Zeitwert fest	Bewegen Sie im Fenster **Inaktivität Timeout** die Schieberegler-Taste nach rechts (ein), geben Sie den Wert für Inaktivität in Minuten an und klicken Sie auf **Apply**.

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.

Was Sie brauchen

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

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 „`Unified Manager`“ 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

Wenn Active IQ Unified Manager zum ersten Mal installiert wird, wird ein HTTPS-Standardzertifikat installiert. Sie können ein neues HTTPS-Sicherheitszertifikat generieren, das das vorhandene Zertifikat ersetzt.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Es kann mehrere Gründe geben, das Zertifikat neu zu generieren, z. B. wenn Sie bessere Werte für Distinguished Name (DN) haben möchten oder wenn Sie eine höhere Schlüsselgröße oder einen längeren Ablaufzeitraum wünschen oder wenn das aktuelle Zertifikat abgelaufen ist.

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. Beim erneuten Generieren von Zertifikaten können Sie die Schlüsselgröße und die Gültigkeitsdauer des Schlüssels festlegen. Wenn Sie die Option aus

der Wartungskonsole verwenden `Reset Server Certificate`, wird ein neues HTTPS-Zertifikat erstellt, das 397 Tage gültig ist. Dieses Zertifikat hat einen RSA-Schlüssel der Größe 2048 Bit.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikat erneut erstellen**.

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

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

Ihr Ziel ist	Tun Sie das…
Generieren Sie das Zertifikat mit den aktuellen Werten neu	Klicken Sie auf die Option **regenerieren mit aktuellen Zertifikatattributen**.

Ihr Ziel ist	Tun Sie das…
Generieren Sie das Zertifikat mithilfe anderer Werte	Klicken Sie auf die Option **Aktuellen Zertifikatattributen aktualisieren**. Die Felder allgemeiner Name und Alternative Namen verwenden die Werte aus dem vorhandenen Zertifikat, wenn Sie keine neuen Werte eingeben. Der „`Common Name`“ sollte auf den FQDN des Hosts gesetzt werden. Die anderen Felder erfordern keine Werte, Sie können aber Werte eingeben, beispielsweise FÜR E-MAIL, FIRMA, ABTEILUNG, Stadt, Bundesland und Land, wenn diese Werte im Zertifikat ausgefüllt werden sollen. Sie können auch aus der verfügbaren SCHLÜSSEGRÖSSE (der Schlüsselalgorithmus lautet „`RSA`“.) und DER GÜLTIGKEITSDAUER auswählen.

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

- Die zulässigen Werte für die Schlüsselgröße sind `2048`, `3072` und `4096`.
- Die Gültigkeitsdauer beträgt mindestens 1 Tag bis maximal 36500 Tage.

Auch wenn eine Gültigkeitsdauer von 36500 Tagen zulässig ist, wird empfohlen, eine Gültigkeitsdauer von nicht mehr als 397 Tagen oder 13 Monaten zu verwenden. Denn wenn Sie eine Gültigkeitsdauer von mehr als 397 Tagen auswählen und planen, eine CSR für dieses Zertifikat zu exportieren und es von einer bekannten Zertifizierungsstelle unterschrieben zu lassen, wird die Gültigkeit des von der Zertifizierungsstelle zurückgegebenen signierten Zertifikats auf 397 Tage reduziert.

- 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, wird im Feld Alternative Namen nur das verwendet, was Sie in das Feld eingeben. Wenn das Zertifikat leer gelassen wird, hat das resultierende Zertifikat überhaupt kein Feld alternativer Namen.

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.

Was Sie brauchen

Die virtuelle Appliance wird eingeschaltet.

Sie sind als Maintenance-Benutzer bei der Wartungskonsole angemeldet.

Sie können die virtuelle Maschine auch von vSphere 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.

Was Sie brauchen

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

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 den folgenden Befehl eingeben:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Ändern Sie den Hostnamen mit dem 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:

   ```
   systemctl restart NetworkManager.service
   ```

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. Starten Sie Unified Manager neu, indem Sie den folgenden Befehl eingeben, nachdem Sie die Änderung Ihres Host-Namens abgeschlossen und überprüft haben:

   ```
   systemctl start mysqld ocie ocieau
   ```

Aktivieren und Deaktivieren des richtlinienbasierten Storage-Managements

Ab Unified Manager 9.7 können Sie Storage-Workloads (Volumes und LUNs) auf Ihren ONTAP Clustern bereitstellen und diese Workloads auf Basis zugewiesener Performance-Service-Level managen. Diese Funktion ähnelt dem Erstellen von Workloads in ONTAP System Manager und dem Anbinden von QoS-Richtlinien. Bei Anwendung mit Unified Manager können Sie Workloads jedoch über alle Cluster bereitstellen und managen, von denen Ihre Unified Manager Instanz überwacht wird.

Sie müssen über die Anwendungsadministratorrolle verfügen.

Diese Option ist standardmäßig aktiviert, Sie können sie jedoch deaktivieren, wenn Sie Workloads nicht über Unified Manager bereitstellen und managen möchten.

Wenn diese Option aktiviert ist, werden viele neue Elemente in der Benutzeroberfläche angezeigt:

Neuer Inhalt	Standort
Eine Seite für die Bereitstellung neuer Workloads	Verfügbar über **Allgemeine Aufgaben** > **Provisioning**
Eine Seite zum Erstellen von Service-Level-Richtlinien für die Performance	Verfügbar über **Einstellungen** > **Richtlinien** > **Leistungsstufen**
Eine Seite, um Richtlinien zur Performance-Storage-Effizienz zu erstellen	Erhältlich über **Einstellungen** > **Richtlinien** > **Storage-Effizienz**
Panels zur Beschreibung Ihrer aktuellen Workload-Performance und Workload-IOPS	Verfügbar über das Dashboard

Weitere Informationen zu diesen Seiten und zu dieser Funktion finden Sie in der Online-Hilfe des Produkts.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Funktionseinstellungen**.
2. Deaktivieren oder aktivieren Sie auf der Seite **Feature Settings** die richtlinienbasierte Speicherverwaltung, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren Sie das richtlinienbasierte Storage-Management	Bewegen Sie im Fenster **Policy-based Storage Management** die Schieberegler-Taste nach links.
Richtlinienbasiertes Storage-Management	Bewegen Sie im Fenster **Policy-based Storage Management** die Schieberegler-Taste nach rechts.

Konfiguration des Unified Manager Backups

Sie können die Backup-Fähigkeit in Unified Manager über eine Reihe von Konfigurationsschritten konfigurieren, die auf den Host-Systemen und mit der Wartungskonsole durchgeführt werden.

Informationen zu den Konfigurationsschritten finden Sie unter "Managen von Backup- und Restore-Vorgängen".

Funktionseinstellungen verwalten

Auf der Seite „Funktionseinstellungen“ können Sie bestimmte Funktionen in Active IQ Unified Manager aktivieren und deaktivieren. Dazu gehört auch die Erstellung und Verwaltung von Speicherobjekten auf Basis von Richtlinien, die Aktivierung von API-Gateway und Anmelde-Banner, das Hochladen von Skripten zur Verwaltung von Warnmeldungen, das Timing einer Web-UI-Sitzung nach Inaktivität und das Deaktivieren des Empfangs von Active IQ Plattform-Ereignissen.

Die Seite Funktionseinstellungen ist nur für Benutzer mit Anwendungsadministratorrolle verfügbar.

Informationen zum Hochladen von Skripten finden Sie unter "Aktivieren und Deaktivieren des Hochladen von Skripten".

Aktivieren eines richtlinienbasierten Storage-Managements

Die Option **richtlinienbasiertes Storage Management** ermöglicht Storage-Management basierend auf Service Level Objectives (SLOs). Diese Option ist standardmäßig aktiviert.

Nach der Aktivierung dieser Funktion können Sie Storage-Workloads auf den ONTAP Clustern bereitstellen, die Ihrer Active IQ Unified Manager Instanz hinzugefügt werden, und die Workloads anhand der zugewiesenen Performance-Service-Level und Storage-Effizienz-Richtlinien managen.

Sie können diese Funktion über **Allgemein** > **Feature-Einstellungen** > **Policy-based Storage Management** aktivieren oder deaktivieren. Bei Aktivierung dieser Funktion stehen folgende Seiten für Betrieb und Überwachung zur Verfügung:

- Provisionierung (Provisionierung von Storage-Workloads)
- **Richtlinien** > **Leistungs-Service-Level**
- **Richtlinien** > **Storage-Effizienz**
- Von Performance Service Level verwaltete Workloads auf der Seite Cluster-Einrichtung
- Workload Performance Panel auf dem **Dashboard**

Sie können die Bildschirme verwenden, um Performance Service Level und Storage-Effizienz-Richtlinien zu erstellen und Storage Workloads bereitzustellen. Kunden können auch Storage-Workloads überwachen, die den zugewiesenen Performance-Service-Leveln entsprechen, Der Bereich Workload-Performance und IOPS für Workloads ermöglicht Ihnen zudem, die Gesamtkapazität, verfügbare und genutzte Kapazität und Performance (IOPS) der Cluster im gesamten Datacenter basierend auf den auf ihnen bereitgestellten Storage-Workloads zu bewerten.

Nach Aktivierung dieser Funktion können Sie die Rest-APIs von Unified Manager ausführen, um einige dieser Funktionen aus der **Menüleiste** > **Hilfe-Schaltfläche** > **API-Dokumentation** > **Storage-Anbieter** Kategorie auszuführen. Alternativ können Sie den Hostnamen oder die IP-Adresse sowie die URL für den Zugriff auf die REST-API-Seite im Format https://<hostname>/docs/API/ eingeben

Weitere Informationen zu den APIs finden Sie unter "Erste Schritte mit Active IQ Unified Manager REST APIs".

Aktivieren des API-Gateways

Mit der API-Gateway-Funktion kann Active IQ Unified Manager als eine einzige Kontrollebene verwendet werden, über die Sie diverse ONTAP-Cluster managen können, ohne sich dabei individuell anmelden zu müssen.

Sie können diese Funktion über die Konfigurationsseiten aktivieren, die beim ersten Anmelden bei Unified Manager angezeigt werden. Alternativ können Sie diese Funktion über **Allgemein** > **Feature-Einstellungen** > **API-Gateway** aktivieren oder deaktivieren.

Unified Manager REST-APIs unterscheiden sich von den ONTAP REST-APIs. Nicht alle Funktionen der ONTAP REST APIs können über die Unified Manager REST-APIs verfügbar sein. Wenn jedoch für Sie

bestimmte geschäftliche Anforderungen beim Zugriff auf ONTAP APIs zum Management bestimmter Funktionen gelten, die nicht mit Unified Manager offengelegt werden, können Sie die API Gateway-Funktion aktivieren und die ONTAP-APIs ausführen. Das Gateway fungiert als Proxy, um die API-Anforderungen zu Tunneln, indem die Header- und Body-Anfragen im gleichen Format wie in den ONTAP-APIs beibehalten werden. Sie können Ihre Unified Manager Anmeldedaten verwenden und die spezifischen APIs ausführen, um auf die ONTAP Cluster zuzugreifen und diese zu managen, ohne die individuellen Cluster-Anmeldedaten zu übergeben. Unified Manager übernimmt als zentrale Managementstelle für die Ausführung der APIs auf den ONTAP Clustern, die von Ihrer Unified Manager Instanz gemanagt werden. Die Antwort der APIs ist die gleiche wie die Antwort, die von den jeweiligen ONTAP REST APIs zurückgegeben wird, die direkt von ONTAP ausgeführt werden.

Nachdem Sie diese Funktion aktiviert haben, können Sie die Unified Manager REST-APIs aus der **Menüleiste** > **Hilfe-Schaltfläche** > **API-Dokumentation** > **Gateway**-Kategorie ausführen. Alternativ können Sie den Hostnamen oder die IP-Adresse und die URL für den Zugriff auf die REST-API-Seite im Format eingeben `https://<hostname>/docs/api/`

Weitere Informationen zu den APIs finden Sie unter "Erste Schritte mit Active IQ Unified Manager REST APIs".

Festlegen des Inaktivitätszeitlimits

Sie können den Wert für die Inaktivität-Zeitüberschreitung für Active IQ Unified Manager angeben. Nach einer Inaktivität der angegebenen Zeit wird die Anwendung automatisch abgemeldet. Diese Option ist standardmäßig aktiviert.

Sie können diese Funktion deaktivieren oder die Uhrzeit über **Allgemein** > **Funktionseinstellungen** > **Inaktivität Timeout** ändern. Wenn Sie diese Funktion aktivieren, sollten Sie im Feld **ABMELDEN NACH** das Zeitlimit für Inaktivität (in Minuten) angeben, nach dem sich das System automatisch abmeldet. Der Standardwert ist 4320 Minuten (72 Stunden).

Diese Option ist nicht verfügbar, wenn Sie die SAML-Authentifizierung (Security Assertion Markup Language) aktiviert haben.

Aktivieren von Active IQ Portal-Ereignissen

Sie können angeben, ob Sie Active IQ-Portalereignisse aktivieren oder deaktivieren möchten. Mit dieser Einstellung kann das Active IQ-Portal zusätzliche Ereignisse über die Systemkonfiguration, die Verkabelung usw. erkennen und anzeigen. Diese Option ist standardmäßig aktiviert.

Wenn Sie diese Funktion aktivieren, zeigt Active IQ Unified Manager Ereignisse an, die vom Active IQ-Portal erkannt wurden. Diese Ereignisse werden durch Regelwerke für AutoSupport-Meldungen erstellt, die von allen überwachten Storage-Systemen generiert werden. Diese Ereignisse unterscheiden sich von anderen Unified Manager Ereignissen und sie identifizieren Vorfälle oder Risiken im Zusammenhang mit Systemkonfiguration, Verkabelung, Best Practice und Verfügbarkeitsproblemen.

Sie können diese Funktion über **Allgemein** > **Feature-Einstellungen** > **Active IQ Portal Events** aktivieren oder deaktivieren. Bei Sites ohne externen Netzwerkzugriff müssen Sie die Regeln manuell von **Speicherverwaltung** > **Event-Setup** > **Upload-Regeln** hochladen.

Diese Funktion ist standardmäßig aktiviert. Durch Deaktivieren dieser Funktion wird verhindert, dass Active IQ-Ereignisse auf Unified Manager erkannt oder angezeigt werden. Wenn diese Funktion deaktiviert ist, kann Unified Manager die Active IQ Ereignisse auf einem Cluster bei einer vordefinierten Zeit von 00:15 für diese

Cluster-Zeitzone empfangen.

Aktivieren und Deaktivieren von Sicherheitseinstellungen zur Einhaltung der Compliance

Mit der Schaltfläche **Anpassen** im Fenster **Sicherheits-Dashboard** der Seite Eigenschaften-Einstellungen können Sie die Sicherheitsparameter für die Compliance-Überwachung in Unified Manager aktivieren oder deaktivieren.

Die auf dieser Seite aktivierten oder deaktivierten Einstellungen regeln den Compliance-Status der Cluster und Storage VMs in Unified Manager. Auf der Grundlage der Auswahl sind die entsprechenden Spalten in der **Security: All Clusters** Ansicht der Cluster Inventory Seite und der **Security: All Storage VMs** Ansicht der Storage VMs Inventarseite sichtbar.

Diese Einstellungen können nur von Benutzern mit Administratorrolle bearbeitet werden.

Die Sicherheitskriterien für Ihre ONTAP-Cluster, Storage-VMs und Volumes werden anhand der Empfehlungen im geprüft"Security Hardening Guide for NetApp ONTAP 9". Im Bereich Sicherheit auf dem Dashboard und auf der Seite Sicherheit wird der Standard-Sicherheitskonformitätsstatus Ihrer Cluster, Storage-VMs und Volumes angezeigt. Zudem werden Sicherheitsereignisse generiert und Aktionen des Managements für die Cluster und Storage VMs mit Sicherheitsverletzungen aktiviert.

Anpassen der Sicherheitseinstellungen

Gehen Sie wie folgt vor, um die Einstellungen für das Compliance-Monitoring nach Bedarf für Ihre ONTAP-Umgebung anzupassen:

Schritte

1. Klicken Sie Auf **Allgemein > Funktionseinstellungen > Sicherheits-Dashboard > Anpassen**. Das Popup-Fenster **Einstellungen für das Sicherheits-Dashboard anpassen** wird angezeigt.

   Die von Ihnen aktivieren oder deaktivieren Sicherheitsparameter können sich direkt auf die Standardsicherheitsansichten, -Berichte und -geplanten Berichte auf den Bildschirmen Cluster- und Storage-VMs auswirken. Wenn Sie einen Excel-Bericht von diesen Bildschirmen hochgeladen haben, bevor Sie die Sicherheitsparameter ändern, sind die heruntergeladenen Excel-Berichte möglicherweise fehlerhaft.

2. Um die benutzerdefinierten Einstellungen für Ihre ONTAP-Cluster zu aktivieren oder zu deaktivieren, wählen Sie unter **Cluster** die erforderliche allgemeine Einstellung aus. Informationen zu den Optionen zum Anpassen der Cluster-Compliance finden Sie unter "Cluster-Compliance-Kategorien".
3. Um die benutzerdefinierten Einstellungen für Ihre Speicher-VMs zu aktivieren oder zu deaktivieren, wählen Sie unter **Storage VM** die erforderliche allgemeine Einstellung aus. Informationen zu den Optionen zum Anpassen der Storage VM-Compliance finden Sie unter "Compliance-Kategorien für Storage-VMs".

AutoSupport- und Authentifizierungseinstellungen werden angepasst

Im Abschnitt **AutoSupport-Einstellungen** können Sie angeben, ob HTTPS-Transport zum Senden von AutoSupport-Nachrichten von ONTAP verwendet werden soll.

Im Abschnitt **Authentifizierungseinstellungen** können Sie die Warnmeldungen von Unified Manager für den standardmäßigen ONTAP-Administrator aktivieren.

Aktivieren und Deaktivieren des Hochladen von Skripten

Die Möglichkeit, Skripts in Unified Manager hochzuladen und sie auszuführen, ist standardmäßig aktiviert. Wenn Ihr Unternehmen diese Aktivität aus Sicherheitsgründen nicht zulassen möchte, können Sie diese Funktion deaktivieren.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Funktionseinstellungen**.
2. Deaktivieren oder aktivieren Sie auf der Seite **Feature Settings** das Skript, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren von Skripten	Bewegen Sie im Bereich **Skript-Upload** die Schieberegler-Taste nach links.
Skripte aktivieren	Bewegen Sie im Bereich **Skript-Upload** die Schieberegler-Taste nach rechts.

Anmeldebanner hinzufügen

Durch das Hinzufügen eines Anmeldebanners kann Ihr Unternehmen alle Informationen anzeigen, z. B. wer Zugriff auf das System hat und die Nutzungsbedingungen während der Anmeldung und beim Abmelden.

Jeder Benutzer, wie z. B. Storage-Operatoren oder -Administratoren, kann dieses Popup-Banner für die Anmeldung, Anmeldung und Sitzungszeitüberschreitung anzeigen.

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 Rolle „Anwendungsadministrator“ in der Web-Benutzeroberfläche, 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.

Zugriff auf die Wartungskonsole

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

Was Sie brauchen

Sie müssen Unified Manager installiert und konfiguriert haben.

Nach 15 Minuten Inaktivität meldet die Wartungskonsole sie aus.

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

Schritt

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

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

Das Menü der Unified Manager-Wartungskonsole wird angezeigt.

Zugriff auf die Wartungskonsole über die vSphere VM-Konsole

Wenn die Benutzeroberfläche von Unified Manager nicht ausgeführt wird oder Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie die Wartungskonsole aufrufen, um die virtuelle Appliance neu zu konfigurieren.

Was Sie brauchen

- Sie müssen der Wartungbenutzer sein.
- Die virtuelle Appliance muss eingeschaltet sein, um auf die Wartungskonsole zugreifen zu können.

Schritte

1. Suchen Sie in vSphere Client die virtuelle Unified Manager Appliance.
2. Klicken Sie auf die Registerkarte **Konsole**.
3. Klicken Sie innerhalb des Konsolenfensters, um sich anzumelden.
4. Melden Sie sich mit Ihrem Benutzernamen und Passwort an der Wartungskonsole an.

   Nach 15 Minuten Inaktivität meldet die Wartungskonsole sie aus.

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)
  a. Support/Diagnose
  b. Serverzertifikat Zurücksetzen
  c. Externer Daten-Provider
  d. Backup Restore
  e. Konfiguration Des Leistungsintervalls
  f. Deaktivieren Sie die SAML-Authentifizierung
  g. Anwendungsports Anzeigen/Ändern
  h. Debug-Protokollkonfiguration
  i. Kontrolle des Zugriffs auf den MySQL-Port 3306
  j. Beenden

Sie wählen die Nummer aus der Liste aus, um auf die spezifische Menüoption zuzugreifen. Zum Beispiel wählen Sie für die Sicherung und Wiederherstellung *4*.

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.

Wenn Unified Manager auf einem Linux- oder Microsoft-Windows-System installiert ist, steht in diesem Menü nur die Option „`Restore from a Unified Manager Backup`“ zur Verfügung.

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).

- **NTP Service ändern**

  Wechselt zwischen den `ntp` und - `systemd-timesyncd`Diensten.

- **Wiederherstellen aus einem Unified Manager 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, das Sie zur Fehlerbehebung an den technischen Support senden können.

Folgende Menüoptionen stehen zur Verfügung:

- **Lichtunterstützungspaket Generieren**

  Ermöglicht Ihnen die Erstellung eines schlanken Supportpakets, das nur 30 Tage Protokolle und Konfigurationsdatenbankdatensätze enthält - es schließt Leistungsdaten, Erfassungsdateien und Server Heap Dump aus.

- * Unterstützungspaket Generieren*

  Mit dieser Funktion können Sie ein komplettes Supportpaket (7-Zip-Datei) mit Diagnoseinformationen im Home-Verzeichnis des Diagnosebenutzers erstellen. Wenn Ihr System mit dem Internet verbunden ist, können Sie auch das Support Bundle auf NetApp hochladen.

  Die Datei enthält 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 oder im Lightweight Support Bundle 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 **Allgemein** > **HTTPS Zertifikate** > **HTTPS-Zertifikat regenerieren** klicken.

- **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.

- **Wiederherstellung Der Sicherung**

  Weitere Informationen finden Sie unter "Managen von Backup- und Restore-Vorgängen".

- **Konfiguration Des Leistungsintervalls**

  Bietet eine Option für die Konfiguration, wie häufig Unified Manager Performance-statistische Daten aus Clustern erfasst. Das Standard-Erfassungsintervall beträgt 5 Minuten.

  Sie können dieses Intervall in 10 oder 15 Minuten ändern, wenn Sie feststellen, dass Sammlungen von großen Clustern nicht rechtzeitig abgeschlossen werden.

- **Anwendungsports Anzeigen/Ändern**

  Bietet eine Option zum Ändern der Standardports, die Unified Manager für HTTP- und HTTPS-Protokolle verwendet, falls dies für die Sicherheit erforderlich ist. Die Standardports sind 80 für HTTP und 443 für HTTPS.

- **Zugriff auf MySQL-Port 3306** steuern

  Steuert den Hostzugriff auf den standardmäßigen MySQL-Port 3306. Aus Sicherheitsgründen ist der Zugriff über diesen Port nur auf localhost beschränkt, während eine Neuinstallation von Unified Manager auf Linux-, Windows- und VMware vSphere-Systemen durchgeführt wird. Mit dieser Option können Sie die Sichtbarkeit dieses Ports zwischen dem localhost und den Remote-Hosts umschalten. Wenn dieser Port nur für localhost in Ihrer Umgebung aktiviert ist, können Sie diesen Port auch Remote-Hosts zur Verfügung stellen. Wenn Sie diese Option für alle Hosts aktivieren, können Sie den Zugriff dieses Ports auf localhost beschränken. Wenn der Zugriff zuvor auf Remote-Hosts aktiviert wurde, bleibt die Konfiguration in einem Upgrade-Szenario erhalten. Sie sollten die Firewall-Einstellungen auf Windows-Systemen überprüfen, nachdem Sie die Portsichtbarkeit aktiviert haben, und die Firewall-Einstellungen deaktivieren, wenn die Einstellungen so konfiguriert sind, dass der Zugriff auf MySQL-Port 3306 eingeschränkt wird.

- **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.

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.

Was Sie brauchen

- 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.

Ändern der Ports Unified Manager verwendet für HTTP- und HTTPS-Protokolle

Die Standard-Ports, die Unified Manager für HTTP- und HTTPS-Protokolle verwendet, können nach der Installation geändert werden, falls dies zur Sicherheit erforderlich ist. Die Standardports sind 80 für HTTP und 443 für HTTPS.

Was Sie brauchen

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

> Es gibt einige Ports, die als unsicher, wenn Sie die Mozilla Firefox oder Google Chrome Browser. Fragen Sie im Browser nach, bevor Sie eine neue Portnummer für HTTP- und HTTPS-Datenverkehr zuweisen. Wenn Sie einen unsicheren Anschluss auswählen, kann das System nicht zugänglich gemacht werden. Dies erfordert, dass Sie sich an den Kundendienst wenden, um eine Lösung zu finden.

Die Instanz von Unified Manager wird automatisch neu gestartet, nachdem Sie den Port geändert haben. Stellen Sie also sicher, dass dies ein guter Zeitpunkt ist, um das System für kurze Zeit herunterzufahren.

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 **Anwendungsports anzeigen/ändern** ein, und drücken Sie dann die Eingabetaste.
3. Geben Sie bei der entsprechenden Aufforderung das Wartungs-Benutzerpasswort erneut ein.
4. Geben Sie die neuen Portnummern für die HTTP- und HTTPS-Ports ein, und drücken Sie dann die Eingabetaste.

Wenn Sie eine Portnummer leer lassen, wird der Standardport für das Protokoll zugewiesen.

Sie werden gefragt, ob Sie die Ports ändern und Unified Manager jetzt neu starten möchten.

5. Geben Sie **y** ein, um die Ports zu ändern und Unified Manager neu zu starten.
6. Beenden Sie die Wartungskonsole.

Nach dieser Änderung müssen Benutzer die neue Portnummer in die URL einfügen, um auf die Unified Manager-Webbenutzeroberfläche zuzugreifen, z. B. https://host.company.com:1234, https://12.13.14.15:1122, oder https://[2001:db8:0:1]:2123.

Hinzufügen von Netzwerkschnittstellen

Sie können neue Netzwerkschnittstellen hinzufügen, wenn Sie den Netzwerkverkehr trennen müssen.

Was Sie brauchen

Sie müssen die Netzwerkschnittstelle der virtuellen Appliance mit vSphere hinzugefügt haben.

Die virtuelle Appliance muss eingeschaltet sein.

Dieser Vorgang kann nicht ausgeführt werden, wenn Unified Manager auf Red hat Enterprise Linux oder unter Microsoft Windows installiert ist.

Schritte

1. Wählen Sie im Hauptmenü der vSphere-Konsole die Option **Systemkonfiguration** > **Betriebssystem neu starten** aus.

   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 Verzeichnis nicht genügend Speicherplatz zur Unterstützung von Unified Manager zugewiesen `/opt/netapp/data` haben, wenn Sie den Linux-Host ursprünglich eingerichtet und Unified Manager dann installiert haben, können Sie nach der Installation Festplattenspeicher hinzufügen, indem Sie den Speicherplatz im Verzeichnis erhöhen `/opt/netapp/data`.

Was Sie brauchen

Sie müssen Root-Benutzerzugriff auf die Red hat Enterprise Linux oder CentOS Linux Maschine haben, auf der Unified Manager installiert ist.

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:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Erstellen Sie einen temporären Sicherungsordner (z.B.) mit ausreichend Speicherplatz, `/backup-data` um die Daten im aktuellen Verzeichnis zu enthalten `/opt/netapp/data`.
4. Kopieren Sie den Inhalt und die Berechtigungskonfiguration des vorhandenen `/opt/netapp/data` Verzeichnisses in das Sicherungsdatenverzeichnis:

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

5. Wenn SE Linux aktiviert ist:

   a. Rufen Sie den SE Linux-Typ für Ordner im vorhandenen Ordner ab `/opt/netapp/data`:

      ```
      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 den Befehl chcon aus, um den Linux-Typ SE für das Sicherungsverzeichnis festzulegen:

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

6. Inhalt des Verzeichnisses entfernen `/opt/netapp/data`:

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

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

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

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

   ```
   ls -ltr /opt/netapp/ | grep 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, dass der Kontext für das `/opt/netapp/data` Verzeichnis weiterhin auf mysqld_db_t gesetzt ist:

   a. `touch /opt/netapp/data/abc`

   b. `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. Löschen Sie die Datei abc, damit diese externe Datei zukünftig keinen Datenbankfehler verursacht.
11. Kopieren Sie den Inhalt von Backup-Daten zurück in das erweiterte `/opt/netapp/data` Verzeichnis:

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

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

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

13. Starten Sie den MySQL-Dienst:

    ```
    systemctl start mysqld
    ```

14. Nachdem der MySQL-Dienst gestartet wurde, starten sie die ocie- und ocieau-Dienste in der folgenden Reihenfolge:

    ```
    systemctl start ocie ocieau
    ```

15. Nachdem alle Dienste gestartet wurden, löschen Sie 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 vergrößern müssen, können Sie nach der Installation Kapazität hinzufügen, indem Sie über die Unified Manager-Wartungskonsole Festplattenspeicher erweitern.

Was Sie brauchen

- 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.

Wir empfehlen, dass Sie Ihre virtuelle Maschine sichern, bevor Sie die Größe der virtuellen Laufwerke erhöhen.

Schritte

1. Wählen Sie im vSphere-Client die virtuelle Unified Manager-Maschine aus, und fügen Sie den Daten dann zusätzliche Festplattenkapazität hinzu `disk 3`. Details finden Sie in der VMware Dokumentation.

   In seltenen Fällen verwendet die Unified Manager-Bereitstellung „`Hard Disk 2`“ für die Datenfestplatte statt „`Hard Disk 3`“. Wenn dies bei Ihrer Bereitstellung der Fall ist, erhöhen Sie den Speicherplatz, je nachdem, welcher Datenträger größer ist. Die Datenfestplatte hat immer mehr Speicherplatz als die andere Festplatte.

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 vergrößern** 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.

Was Sie brauchen

Sie müssen über Administratorrechte für Windows verfügen.

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"

Verwalten des Benutzerzugriffs

Sie können Rollen erstellen und Funktionen zuweisen, um den Benutzerzugriff auf Active IQ Unified Manager zu steuern. Sie können Benutzer identifizieren, die über die erforderlichen Funktionen für den Zugriff auf ausgewählte Objekte in Unified Manager verfügen. Nur Benutzer mit diesen Rollen und Funktionen können die Objekte in Unified Manager managen.

Benutzer hinzufügen

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

Was Sie brauchen

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

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Klicken Sie auf der Seite 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**.

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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Datenbankbenutzer ermöglichen die Integration in Workflow Automation und den Zugriff auf Berichtsspezifische Datenbankansichten. Datenbankbenutzer haben keinen Zugriff auf die Unified Manager

Web-UI oder die Wartungskonsole und können keine API-Aufrufe ausführen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Klicken Sie auf der Seite Benutzer auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld Benutzer hinzufügen in der Dropdown-Liste **Typ** die Option **Datenbankbenutzer** aus.
4. Geben Sie einen Namen und ein Kennwort für den Datenbankbenutzer ein.
5. Wählen Sie in der Dropdown-Liste **Rolle** die entsprechende Rolle aus.

Ihr Unternehmen	Wählen Sie diese Rolle aus
Verbindung von Unified Manager mit Workflow Automation	Integrationsschema
Zugriff auf Berichtsdaten und andere Datenbankansichten	Berichtschema

6. 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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

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 im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Wählen Sie auf der Benutzerseite 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**.

Anzeigen von Benutzern

Sie können die Seite Benutzer verwenden, um eine 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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritt

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

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.

Was Sie brauchen

- 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 über die Anwendungsadministratorrolle verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Wählen Sie auf der Seite 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.

Was RBAC ist

RBAC (rollenbasierte Zugriffssteuerung) bietet die Möglichkeit, zu steuern, wer Zugriff auf verschiedene Funktionen und Ressourcen im Active IQ 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 starten, für den bestimmte Privileges erforderlich sind, fordert der Verwaltungsserver Sie auf, sich anzumelden. Zum Beispiel müssen Sie sich mit dem Zugriff auf das Anwendungsadministratorkonto anmelden, um Administratorkonten zu erstellen.

Definitionen der Benutzertypen

Ein Benutzertyp gibt die Art des Kontos an, das der Benutzer besitzt und umfasst Remote-Benutzer, Remote-Gruppen, lokale Benutzer, Datenbankbenutzer und Wartungbenutzer. Jeder dieser Typen hat seine eigene Rolle, die von einem Benutzer mit der Rolle „Administrator“ zugewiesen wird.

Unified Manager-Benutzertypen sind wie folgt:

- **Benutzer der Wartung**

  Erstellt während der Erstkonfiguration von Unified Manager. Der Wartungsbenutzer erstellt dann weitere Benutzer und weist Rollen zu. Der Benutzer der Wartung ist außerdem der einzige Benutzer, der Zugriff auf die Wartungskonsole hat. Wenn Unified Manager auf einem Red hat Enterprise Linux- oder CentOS-System installiert ist, erhält der Wartungbenutzer den Benutzernamen „`umadmin`.“.

- **Lokaler Benutzer**

  Greift auf die Unified Manager-Benutzeroberfläche zu und führt Funktionen basierend auf der Rolle durch, die der Wartungsbenutzer oder ein Benutzer mit der Anwendungsadministratorrolle angegeben hat.

- **Remote-Gruppe**

  Eine Gruppe von Benutzern, die mit den auf dem Authentifizierungsserver gespeicherten Anmeldeinformationen auf die Benutzeroberfläche von Unified Manager zugreifen. Der Name dieses Kontos muss mit dem Namen einer auf dem Authentifizierungsserver gespeicherten Gruppe übereinstimmen. Allen Benutzern innerhalb der Remote-Gruppe wird über ihre individuellen Benutzeranmeldeinformationen der Zugriff auf die Unified Manager-Benutzeroberfläche gewährt. Remote-Gruppen können Funktionen entsprechend ihren zugewiesenen Rollen ausführen.

- **Remote-Benutzer**

  Greift über die auf den Authentifizierungsserver gespeicherten Anmeldeinformationen auf die Unified Manager-UI zu. Ein Remote-Benutzer führt Funktionen basierend auf der Rolle aus, die der Wartungsbenutzer oder ein Benutzer mit der Anwendungsadministratorrolle angegeben hat.

- **Datenbankbenutzer**

  Hat schreibgeschützten Zugriff auf Daten in der Unified Manager-Datenbank, hat keinen Zugriff auf die Unified Manager-Webschnittstelle oder die Wartungskonsole und kann keine API-Aufrufe ausführen.

Definitionen von Benutzerrollen

Der Wartungsbenutzer oder der Anwendungsadministrator weist jedem Benutzer eine Rolle zu. Jede Rolle enthält bestimmte Berechtigungen. Der Umfang der Aktivitäten, die

Sie in Unified Manager ausführen können, hängt von der Ihnen zugewiesenen Rolle ab und welchen Berechtigungen die Rolle enthält.

Unified Manager enthält die folgenden vordefinierten Benutzerrollen:

- **Betreiber**

  Anzeige von Storage-Systeminformationen und anderen von Unified Manager erfassten Daten, einschließlich Verläufe und Kapazitätstrends Mit dieser Rolle kann der Speicherbetreiber Notizen zu den Ereignissen anzeigen, zuweisen, bestätigen, auflösen und hinzufügen.

- * Storage Administrator*

  Konfiguration von Storage-Managementvorgängen in Unified Manager Diese Rolle ermöglicht es dem Storage-Administrator, Schwellenwerte zu konfigurieren und Alarme sowie andere für das Storage-Management spezifische Optionen und Richtlinien zu erstellen.

- **Anwendungsadministrator**

  Konfiguriert Einstellungen, die in keinem Zusammenhang mit dem Storage-Management stehen. Diese Rolle ermöglicht das Management von Benutzern, Sicherheitszertifikaten, Datenbankzugriff und Verwaltungsoptionen, einschließlich Authentifizierung, SMTP, Networking und AutoSupport.

  Wenn Unified Manager auf Linux-Systemen installiert wird, heißt der erste Benutzer mit der Anwendungsadministratorrolle automatisch „`umadmin`“.

- **Integrationsschema**

  Diese Rolle bietet schreibgeschützten Zugriff auf Unified Manager Datenbankansichten für die Integration von Unified Manager mit OnCommand Workflow Automation (WFA).

- **Schema Melden**

  Diese Rolle ermöglicht einen schreibgeschützten Zugriff auf Reporting und andere Datenbankansichten direkt aus der Unified Manager Datenbank. Folgende Datenbanken stehen zur Verfügung:

  - netapp_Modell_Ansicht
  - netapp_Performance
  - Okum
  - Ocum_Report
  - Ocum_Report_birt
  - opm
  - Skalemonitor

Unified Manager Benutzer-Rollen und -Funktionen

Anhand der Ihnen zugewiesenen Benutzerrolle können Sie festlegen, welche Vorgänge Sie in Unified Manager ausführen können.

In der folgenden Tabelle sind die Funktionen aufgeführt, die die einzelnen Benutzerrollen ausführen können:

Funktion	Operator	Storage-Administrator	Applikationsadministrator	Integrationsschema	Berichtschema
Anzeigen von Speichersysteminformationen	•	•	•	•	•
Andere Daten wie Verläufe und Kapazitätstrends anzeigen	•	•	•	•	•
Ereignisse anzeigen, zuweisen und lösen	•	•	•		
Anzeigen von Storage-Serviceobjekten, z. B. SVM-Zuordnungen und Ressourcenpools	•	•	•		
Anzeigen von Schwellenwertrichtlinien	•	•	•		
Management von Storage-Serviceobjekten wie SVM-Zuordnungen und Ressourcenpools		•	•		
Definieren von Warnmeldungen		•	•		
Optionen für das Storage Management managen		•	•		

Funktion	Operator	Storage-Administrator	Applikationsadministrator	Integrationsschema	Berichtschema
Storage Management-Richtlinien managen		•	•		
Benutzer managen			•		
Management von Verwaltungsoptionen			•		
Definieren Sie Schwellenwertrichtlinien			•		
Datenbankzugriff managen			•		
Managen Sie die Integration in WFA und erhalten Sie Zugriff auf die Datenbankansichten				•	
Planen und Speichern von Berichten		•	•		
Führen Sie „`Fix IT`“-Vorgänge aus Management Actions aus		•	•		
Schreibgeschützter Zugriff auf Datenbankansichten					•

Verwalten von SAML-Authentifizierungseinstellungen

Nachdem Sie die Remote-Authentifizierungseinstellungen konfiguriert haben, können Sie

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

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

Anforderungen an Identitätsanbieter

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

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

Unterstützte Verschlüsselungsstandards

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

Validierte Identitätsanbieter

- Shibboleth
- Active Directory Federation Services (ADFS)

ADFS-Konfigurationsanforderungen

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

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

- Sie müssen die Authentifizierungsmethode auf „`Forms Authentication`“ setzen, oder Benutzer erhalten möglicherweise einen Fehler beim Abmelden von Unified Manager. Führen Sie hierzu folgende Schritte aus:
  a. Öffnen Sie die ADFS-Verwaltungskonsole.
  b. Klicken Sie in der linken Strukturansicht auf den Ordner Authentication Policies.

c. Klicken Sie unter Aktionen auf der rechten Seite auf Globale primäre Authentifizierungsrichtlinie bearbeiten.

d. Setzen Sie die Intranet-Authentifizierungsmethode auf „`Forms Authentication`“ anstatt auf die Standardauthentifizierung „`Windows Authentication`“.

- In einigen Fällen wird die Anmeldung über das IdP abgelehnt, wenn das Unified Manager-Sicherheitszertifikat CA-signiert ist. Es gibt zwei Problemumgehungen zur Lösung dieses Problems:
  - Befolgen Sie die Anweisungen im Link, um die Widerrufs-Prüfung auf dem ADFS-Server für verkettete CA-Zertifikat zugeordnete abhängige Partei zu deaktivieren:

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

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

Sonstige Konfigurationsanforderungen

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

Aktivieren der SAML-Authentifizierung

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

Was Sie brauchen

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

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

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

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

Schritte

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

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

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

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

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

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

5. Klicken Sie Auf **Speichern**.

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

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

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.

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

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

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

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

Was Sie brauchen

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

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

Schritte

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

Server mit dem IdP zu verbinden.

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

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

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

5. Klicken Sie auf **OK**.

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.

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 einen neuen Vertrauenseintrag hinzu, der sich `saml_sp_metadata.xml` auf dem aktualisierten Unified Manager-Server befindet. 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 die `attribute-filter.xml` Dateien und `relying-party.xml`. 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.

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

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

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

Schritte

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

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

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

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.

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

Deaktivieren der SAML-Authentifizierung über die Wartungskonsole

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

Was Sie brauchen

Sie müssen als Wartungbenutzer Zugriff auf die Wartungskonsole haben.

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.

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.

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

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 bei der Web-UI von Unified Manager anmelden können.

- Sie müssen über die Anwendungsadministratorrolle verfügen, um die SAML-Konfiguration zu erstellen oder zu ändern.
- 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 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.

Informationen zur Aktivierung der Fernauthentifizierung, zum Einrichten von Authentifizierungsdiensten und zum Hinzufügen von Authentifizierungsseviern finden Sie im vorherigen Abschnitt unter **Konfigurieren von Unified Manager zum Senden von Benachrichtigungen**.

Bearbeiten von Authentifizierungsservern

Sie können den Port ändern, den der Unified Manager-Server für die Kommunikation mit Ihrem Authentifizierungsserver verwendet.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Aktivieren Sie 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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Wenn Sie einen Authentifizierungsserver löschen, können Remote-Benutzer oder -Gruppen des Authentifizierungsservers nicht mehr auf Unified Manager zugreifen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Wählen Sie 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 kommunizieren kann, damit 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.

Audit-Protokollierung

Sie können erkennen, ob die Audit-Protokolle unter Verwendung von Audit-Protokollen kompromittiert wurden. Alle von einem Benutzer durchgeführten Aktivitäten werden überwacht und in den Audit-Protokollen protokolliert. Die Audits werden für alle Benutzerschnittstellen und öffentlich exponierte APIs' Funktionalitäten von Active IQ Unified Manager durchgeführt.

Mit dem **Audit Log: File View** können Sie alle in Ihrem Active IQ Unified Manager verfügbaren Audit-Log-Dateien anzeigen und darauf zugreifen. Die Dateien im Audit Log: File View werden basierend auf ihrem Erstellungsdatum aufgelistet. In dieser Ansicht werden Informationen über das gesamte Überwachungsprotokoll angezeigt, das von der Installation oder dem Upgrade auf die im System vorhandenen Protokolle erfasst wird. Wenn Sie in Unified Manager eine Aktion ausführen, werden die Informationen aktualisiert und stehen in den Protokollen zur Verfügung. Der Status jeder Protokolldatei wird mit dem Attribut „`File Integrity Status`“ erfasst, das aktiv überwacht wird, um Manipulation oder Löschung der Protokolldatei zu erkennen. Die Audit-Protokolle können einen der folgenden Status haben, wenn die Audit-Protokolle im System verfügbar sind:

Status	Beschreibung
AKTIV	Datei, in der Protokolle aktuell protokolliert werden.
NORMAL	Datei, die inaktiv, komprimiert und im System gespeichert ist.

Status	Beschreibung
MANIPULIERT	Datei, die von einem Benutzer kompromittiert wurde, der die Datei manuell bearbeitet hat.
MANUELL_LÖSCHEN	Datei, die von einem autorisierten Benutzer gelöscht wurde.
ROLLOVER_DELETE	Datei, die aufgrund von Rolling Off auf der Grundlage Rolling Configuration Policy gelöscht wurde.
UNEXPECTED_DELETE	Datei, die aus unbekannten Gründen gelöscht wurde.

Die Seite „Prüfprotokoll“ enthält die folgenden Befehlsschaltflächen:

- Konfigurieren
- Löschen
- Download

Mit der Schaltfläche **DELETE** können Sie alle in der Ansicht Audit Logs aufgeführten Audit-Protokolle löschen. Sie können ein Audit-Protokoll löschen und optional einen Grund angeben, die Datei zu löschen, was in Zukunft hilft, ein gültiges Löschen zu bestimmen. Die SPALTE GRUND enthält den Grund und den Namen des Benutzers, der den Löschvorgang durchgeführt hat.

Das Löschen einer Protokolldatei führt zum Löschen der Datei aus dem System, der Eintrag in der DB-Tabelle wird jedoch nicht gelöscht.

Sie können die Audit-Protokolle von Active IQ Unified Manager mit der Schaltfläche **DOWNLOAD** im Bereich Audit-Protokolle herunterladen und die Audit-Log-Dateien exportieren. Die mit „`NORMAL`“ oder „`MANIPULED`“ markierten Dateien werden in einem komprimierten Format heruntergeladen `.gzip`.

Die Audit-Log-Dateien werden regelmäßig archiviert und zur Referenz in der Datenbank gespeichert. Vor der Archivierung werden die Audit-Protokolle digital signiert, um die Sicherheit und Integrität zu gewährleisten.

Wenn ein komplettes AutoSupport Bundle generiert wird, enthält das Support Bundle sowohl archivierte als auch aktive Audit-Log-Dateien. Wenn aber ein Light Support Bundle erzeugt wird, enthält es nur die aktiven Audit-Protokolle. Die archivierten Prüfprotokolle sind nicht enthalten.

Audit-Protokolle werden konfiguriert

Sie können die Schaltfläche **Konfigurieren** im Bereich Audit Logs verwenden, um die Rolling Policy für Audit Log-Dateien zu konfigurieren und auch die Remote-Protokollierung für die Audit-Protokolle zu aktivieren.

Sie können die Werte in den AUFBEWAHRUNGSTAGEN **MAX-DATEIGRÖSSE** und **AUDIT-LOGBUCH** entsprechend der gewünschten Menge und Häufigkeit der Daten festlegen, die Sie im System speichern möchten. Der Wert im Feld **GESAMTE LOGGRÖSSE DES AUDITS** ist die Größe der gesamten Audit-Log-Daten im System. Die Roll-Over-Richtlinie wird durch die Werte im Feld **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** und **TOTAL AUDIT LOG SIZE** bestimmt. Wenn die Größe des Backups des Revisionsprotokolls den in **GESAMT-AUDIT-LOG-GRÖSSE** konfigurierten Wert erreicht, wird die zuerst archivierte Datei gelöscht.

Das bedeutet, dass die älteste Datei gelöscht wird. Der Dateieintrag ist jedoch weiterhin in der Datenbank verfügbar und wird als „`Rollover Delete`“ markiert. Der **AUDIT LOG RETENTION DAYS**-Wert gilt für die Anzahl der Tage, an denen die Audit Log-Dateien aufbewahrt werden. Jede Datei, die älter als der in diesem Feld eingestellte Wert ist, wird über gerollt.

Schritte

1. Klicken Sie Auf **Prüfprotokolle** > **Konfigurieren**.
2. Geben Sie die Werte in den * MAX-DATEIGRÖSSEN*, **GESAMT-AUDIT-LOG-GRÖSSE** und **AUDIT-LOG-AUFBEWAHRUNGSTAGE** ein.

   Wenn Sie die Fernprotokollierung aktivieren möchten, wählen Sie die Option **Remote Logging aktivieren**.

Aktivieren der Fernprotokollierung von Audit-Protokollen

Aktivieren Sie das Kontrollkästchen **Remote-Protokollierung aktivieren** im Dialogfeld Audit-Protokolle konfigurieren, um die Remote-Audit-Protokollierung zu aktivieren. Mit dieser Funktion können Sie Überwachungsprotokolle an einen Remote Syslog-Server übertragen. Auf diese Weise können Sie Ihre Audit-Protokolle verwalten, wenn es Platzbeschränkungen gibt.

Die Remote-Protokollierung von Audit-Protokollen bietet ein manipulationssicheres Backup, falls die Audit-Log-Dateien auf dem Active IQ Unified Manager Server manipuliert werden.

Schritte

1. Aktivieren Sie im Dialogfeld **Audit Logs konfigurieren** das Kontrollkästchen **Remote Logging aktivieren**.

   Zusätzliche Felder zum Konfigurieren der Remote-Protokollierung werden angezeigt.

2. Geben Sie den **HOSTNAME** und den **PORT** des Remoteserver ein, mit dem Sie eine Verbindung herstellen möchten.
3. Klicken Sie im Feld **SERVER CA ZERTIFIKAT** auf **DURCHSUCHEN**, um ein öffentliches Zertifikat des Zielservers auszuwählen.

   Das Zertifikat sollte im Format hochgeladen werden `.pem`. Dieses Zertifikat sollte vom Ziel-Syslog-Server abgerufen werden und sollte nicht abgelaufen sein. Das Zertifikat sollte den ausgewählten „`Hostname`“ als Teil des Attributs (SAN) enthalten `SubjectAltName`.

4. Geben Sie die Werte für die folgenden Felder ein: **CHARSET**, **VERBINDUNGS-TIMEOUT**, **VERBINDUNGSVERZÖGERUNG**.

   Für diese Felder sollten die Werte in Millisekunden angegeben werden.

5. Wählen Sie das erforderliche Syslog-Format und die TLS-Protokollversion in den Feldern **FORMAT** und **PROTOKOLL** aus.
6. Aktivieren Sie das Kontrollkästchen **Client Authentication** aktivieren, wenn für den Ziel-Syslog-Server eine zertifikatbasierte Authentifizierung erforderlich ist.

   Sie müssen das Clientauthentifizierungszertifikat herunterladen und auf den Syslog-Server hochladen, bevor Sie die Konfiguration des Überwachungsprotokolls speichern. Andernfalls schlägt die Verbindung fehl. Je nach Typ des Syslog-Servers müssen Sie möglicherweise einen Hash des Client-Authentifizierungszertifikats erstellen.

Beispiel: Syslog-ng erfordert, dass ein <hash> des Zertifikats mit dem Befehl erstellt `openssl x509 -noout -hash -in cert.pem` wird, und dann sollten Sie das Client-Authentifizierungszertifikat symbolisch mit einer Datei verknüpfen, die nach der <hash> .0 benannt ist.

7. Klicken Sie auf **Speichern**, um die Verbindung mit Ihrem Server zu konfigurieren und die Fernprotokollierung zu aktivieren.

   Sie werden zur Seite Audit Logs weitergeleitet.

   Der Wert **Connection Timeout** kann sich auf die Konfiguration auswirken. Wenn die Konfiguration länger als der definierte Wert reagiert, kann dies zu einem Konfigurationsfehler aufgrund eines Verbindungsfehlers führen. Um eine erfolgreiche Verbindung herzustellen, erhöhen Sie den Wert **Connection Timeout** und versuchen Sie die Konfiguration erneut.

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 „Anwendungsadministrator“ 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, dann ist der Name der Basisunterscheidungder **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, dann ist der Name der Basisunterscheidungder **cn=ou,dc=Domain,dc=com**.

- Verwenden Sie Secure Connection

  Gibt an, dass Secure LDAP zur Kommunikation mit LDAP-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, dann ist der Name der Basisunterscheidungder **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.

> Die Werte, die Sie für die Attribute *Member*, *User Object Class* und *Group Object Class* eingeben, sollten dieselben sein wie die in Ihren Active Directory-, OpenLDAP- und LDAP-Konfigurationen hinzugefügten Werte. Andernfalls kann die Authentifizierung fehlschlagen.

- 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.

  - Hinzufügung

    Ermöglicht das Hinzufügen eines Authentifizierungsservers.

  Wenn der neue 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.

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.

Was Sie brauchen

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

Durch das Anzeigen des Zertifikats können Sie den Inhalt eines neu erstellten Zertifikats überprüfen oder die entsprechenden Alt-Namen (SAN) anzeigen, auf die Sie auf Unified Manager zugreifen können.

Schritt

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.

   Das HTTPS-Zertifikat wird oben auf der Seite angezeigt

Wenn Sie ausführlichere Informationen zum Sicherheitszertifikat als auf der Seite HTTPS-Zertifikat anzeigen müssen, können Sie das Verbindungszertifikat in Ihrem Browser anzeigen.

Herunterladen einer Anforderung zum Signieren eines HTTPS-Zertifikats

Sie können eine Zertifizierungssignierungsanforderung für das aktuelle HTTPS-Sicherheitszertifikat herunterladen, so dass Sie die Datei einer Zertifizierungsstelle zum Signieren zur Verfügung stellen 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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikatsignierungsanforderung herunterladen**.
3. Speichern Sie die `<hostname>.csr` Datei.

Sie können die Datei einer Zertifizierungsstelle zum Signieren bereitstellen und dann das signierte Zertifikat installieren.

Installieren einer Zertifizierungsstelle, die signiert ist und ein HTTPS-Zertifikat zurückgegeben hat

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.

Was Sie brauchen

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 über die Anwendungsadministratorrolle verfügen.

Wenn die Gültigkeit des Zertifikats, für das ein CSR erstellt wurde, mehr als 397 Tage beträgt, wird die Gültigkeit von der Zertifizierungsstelle vor dem Signieren und Zurücksenden des Zertifikats auf 397 Tage reduziert

Schritte

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

   Weitere Informationen finden Sie unter "Installieren eines HTTPS-Zertifikats, das mit externen Tools generiert wurde".

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-----
```

Installieren eines HTTPS-Zertifikats, das mit externen Tools generiert wurde

Sie können Zertifikate installieren, die selbst signiert sind oder CA-signiert sind und mit einem externen Tool wie OpenSSL, BoringSSL, LetsEncrt generiert werden.

Sie sollten den privaten Schlüssel zusammen mit der Zertifikatskette laden, da diese Zertifikate extern öffentlich-private Schlüsselpaare sind. Die zulässigen Schlüssel-Paar-Algorithmen sind „RSA“ und „EC“. Die Option **HTTPS-Zertifikat installieren** ist auf der Seite HTTPS-Zertifikate im Abschnitt Allgemein verfügbar. Die Datei, die Sie hochladen, sollte das folgende Eingabeformat aufweisen.

1. Privater Schlüssel des Servers, der zum Active IQ Unified Manager-Host gehört

2. Zertifikat des Servers, das mit dem privaten Schlüssel übereinstimmt
3. Zertifikat der CAS in umgekehrter Reihenfolge bis zum Root, die zum Signieren des obigen Zertifikats verwendet werden

Format zum Laden eines Zertifikats mit einem EC-Schlüsselpaar

Die zulässigen Kurven sind „`prime256v1`“ und „`secp384r1`“. Beispiel eines Zertifikats mit einem extern generierten EC-Paar:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----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-----
```

Format zum Laden eines Zertifikats mit einem RSA-Schlüsselpaar

Die zulässigen Schlüsselgrößen für das RSA-Schlüsselpaar, das zum Hostzertifikat gehört, sind 2048, 3072 und 4096. Zertifikat mit einem extern generierten **RSA-Schlüsselpaar**:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----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-----
```

Nachdem das Zertifikat hochgeladen wurde, sollten Sie die Active IQ Unified Manager-Instanz neu starten, damit die Änderungen wirksam werden.

Überprüft beim Hochladen extern generierter Zertifikate

Das System führt Prüfungen beim Hochladen eines Zertifikats durch, das mit externen Tools erstellt wurde. Wenn eine der Prüfungen fehlschlägt, wird das Zertifikat abgelehnt. Es gibt auch eine Validierung für die Zertifikate, die aus der CSR innerhalb des Produkts erzeugt werden, und für Zertifikate, die mit externen Tools generiert werden.

- Der private Schlüssel in der Eingabe wird anhand des Hostzertifikats in der Eingabe validiert.
- Der allgemeine Name (CN) im Hostzertifikat wird mit dem FQDN des Hosts überprüft.
- Der allgemeine Name (CN) des Host-Zertifikats sollte nicht leer oder leer sein und nicht auf localhost gesetzt werden.
- Das Startdatum der Gültigkeit darf nicht in der Zukunft liegen und das Gültigkeitsdatum des Zertifikats sollte nicht in der Vergangenheit liegen.
- Wenn Intermediate CA oder CA vorhanden ist, sollte das Startdatum des Zertifikats nicht in der Zukunft liegen und das Gültigkeitsdatum sollte nicht in der Vergangenheit liegen.

Der private Schlüssel in der Eingabe sollte nicht verschlüsselt werden. Wenn private Schlüssel verschlüsselt sind, werden sie vom System abgelehnt.

Beispiel 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Beispiel 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Beispiel 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Wenn die Zertifikatinstallation fehlschlägt, lesen Sie den Knowledge Base-Artikel (KB): "ActiveIQ Unified Manager kann ein extern generiertes Zertifikat nicht installieren"

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 Anfrage zum Signieren von Zertifikaten herunterladen, ein neues selbstsigniertes HTTPS-Zertifikat erstellen oder ein neues HTTPS-Zertifikat installieren.

Wenn Sie kein neues selbstsigniertes 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. Ihr Browser fordert Sie auf, die Datei <hostname>.csr zu speichern, damit Sie die Datei einer 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 neuen selbstsignierten 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.

- **SCHLÜSSELGRÖSSE (SCHLÜSSELALGORITHMUS: RSA)**

  Der Schlüsselalgorithmus ist auf RSA festgelegt. Sie können eine der Schlüsselgrößen wählen: 2048, 3072 oder 4096 Bit. Die Standardschlüsselgröße ist auf 2048 Bit eingestellt.

- **GÜLTIGKEITSZEITRAUM**

  Die standardmäßige Gültigkeitsdauer beträgt 397 Tage. Wenn Sie ein Upgrade von einer früheren Version durchgeführt haben, wird die vorherige Zertifikatsgültigkeit möglicherweise nicht geändert.

Weitere Informationen finden Sie unter "HTTPS-Zertifikate werden generiert".

Überwachung und Management von Storage

Einführung in Active IQ Unified Manager

Mit Active IQ Unified Manager (ehemals OnCommand Unified Manager) überwachen und managen Sie den Zustand und die Performance Ihrer ONTAP Storage-Systeme über eine einzige Benutzeroberfläche.

Unified Manager bietet folgende Funktionen:

- Bestandsaufnahme, Monitoring und Benachrichtigungen für Systeme, die mit der ONTAP Software installiert sind
- Dashboard zum Anzeigen des Kapazitäts-, Sicherheits- und Performance-Zustands 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, sowie eine Schaltfläche „Beheben von Ereignissen“, damit Sie das Problem sofort beheben können.
- Integration in OnCommand Workflow Automation zur Ausführung automatisierter Sicherungs-Workflows
- Möglichkeit zum Erstellen neuer Workloads wie beispielsweise LUNs oder Dateifreigabe direkt über Unified Manager und Zuweisen eines Performance Service Levels zum Definieren der Performance- und Storage-Ziele für Benutzer, die auf die Applikation über diesen Workload zugreifen

Einführung in das Active IQ Unified Manager Monitoring des Systemzustands

Active IQ Unified Manager (ehemals OnCommand Unified Manager) hilft Ihnen, eine große Anzahl von Systemen mit ONTAP Software über eine zentrale Benutzeroberfläche zu überwachen. Die Unified Manager Serverinfrastruktur bietet Skalierbarkeit, Unterstützbarkeit sowie verbesserte Monitoring- und Benachrichtigungsfunktionen.

Zu den wichtigsten Funktionen von Unified Manager gehören Monitoring-, Warnfunktionen-, Management der Verfügbarkeit und Kapazität von Clustern, Management der Sicherungsfunktionen und Bündelung von Diagnosedaten sowie der Versand 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.

Physische und logische Kapazität

Unified Manager nutzt die Konzepte von physischem und logischem Speicherplatz für ONTAP Storage-Objekte.

- Physische Kapazität: Physischer Speicherplatz bezieht sich auf die physischen Blöcke des Storage, der im Volume verwendet wird. „Genutzte physische Kapazität“ ist in der Regel kleiner als die logische genutzte Kapazität, da Storage-Effizienzfunktionen wie Deduplizierung und Komprimierung reduziert werden.
- Logische Kapazität: Logischer Speicherplatz bezeichnet den nutzbaren Speicherplatz (die logischen Blöcke) in einem Volume. Logischer Speicherplatz bezeichnet die Art und Weise, wie theoretischer Speicherplatz verwendet werden kann, ohne dabei die Folgen der Deduplizierung oder Komprimierung berücksichtigen zu müssen. Der „logische Platz“ ist der verwendete physische Speicherplatz plus die Einsparungen durch Storage-Effizienzfunktionen (wie Deduplizierung und Komprimierung), die konfiguriert wurden. Diese Messung erscheint oft größer als die physisch genutzte Kapazität, da diese nicht auf die Datenkomprimierung und andere Reduzierungen des physischen Speicherplatzes zurückführt. Somit kann die logische Gesamtkapazität über dem bereitgestellten Speicherplatz liegen.

Kapazitätsmesseinheiten

Unified Manager berechnet die Storage-Kapazität auf der Grundlage von binären Einheiten von 1024 (2^{10}) Byte. In ONTAP 9.10.0 und früher wurden diese Einheiten als KB, MB, GB, TB und PB angezeigt. Ab ONTAP 9.10.1 werden sie im Unified Manager als KiB, MiB, gib, tib und PiB angezeigt.

Die für den Durchsatz verwendeten Einheiten betragen für alle ONTAP-Versionen weiterhin Kilobyte pro Sekunde (Kbit/s), Megabyte pro Sekunde (MB/s), Gigabyte pro Sekunde (GB/s) oder Terabyte pro Sekunde (Tbit/s) usw.

In Unified Manager für ONTAP 9.10.0 und früher angezeigte Kapazitätseinheit	Im Unified Manager für ONTAP 9.10.1 wird die Kapazitätseinheit angezeigt	Berechnung	Wert in Byte
KB	KiB	1024	1024 Byte
MB	MIB	1024 * 1024	1.048.576 Byte
GB	Gib	1024 * 1024 * 1024	1.073.741.824 Byte
TB	TIB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 Byte

Einführung in das Active IQ Unified Manager Performance-Monitoring

Active IQ Unified Manager (ehemals OnCommand Unified Manager) bietet Funktionen für das Performance-Monitoring sowie 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.

Verwendung von Unified Manager REST-APIs

Mithilfe von Active IQ Unified Manager KÖNNEN Sie ÜBER REST-APIs Informationen zum Monitoring und Management Ihrer Storage-Umgebung abrufen. APIs ermöglichen außerdem die Bereitstellung und das Management von Storage-Objekten basierend auf Richtlinien.

Sie können ONTAP-APIs auch auf allen von ONTAP gemanagten Clustern ausführen. Verwenden Sie dazu das von Unified Manager unterstützte API-Gateway.

Weitere Informationen zu Unified Manager REST-APIs finden Sie unter "Erste Schritte mit Active IQ Unified Manager REST APIs".

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.

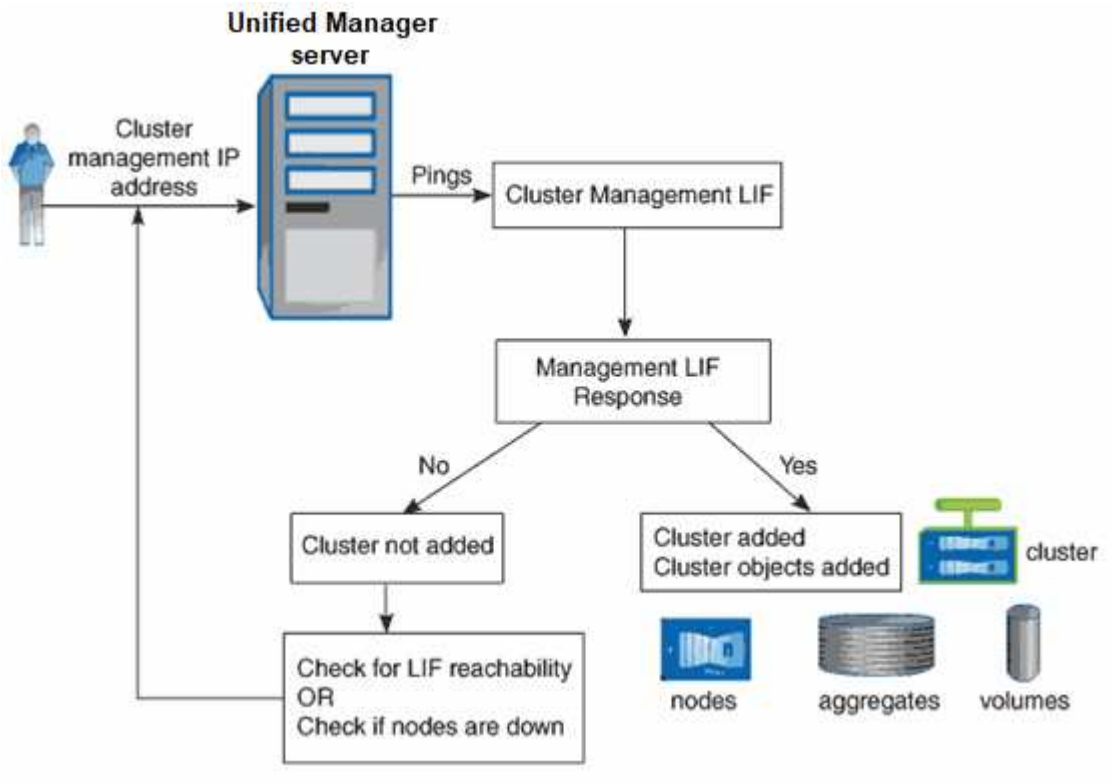
Unified Manager sammelt Cluster-Informationen, speichert die Daten in der Datenbank und analysiert die Daten, um zu prüfen, ob es Cluster-Probleme gibt.

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 Active IQ Unified Manager:



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.

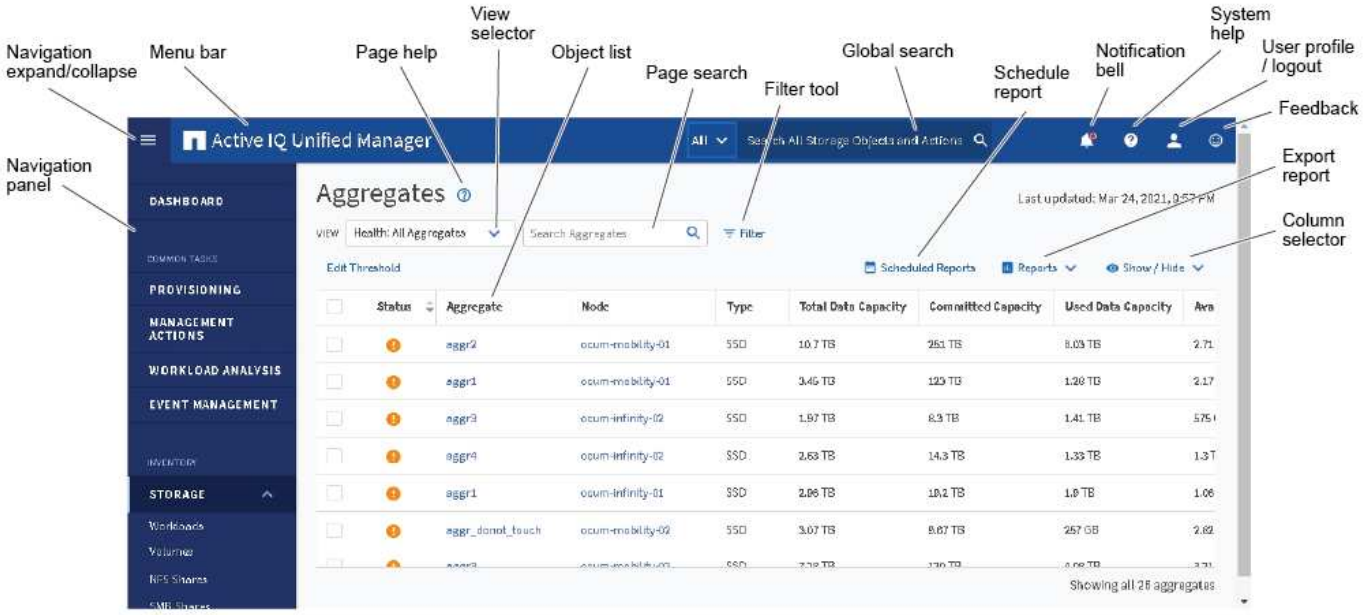
Sie können eine bevorzugte Ansicht auswählen und ggf. die Aktionsschaltflächen verwenden. Ihre Bildschirmkonfiguration wird in einem Arbeitsbereich gespeichert, sodass alle Funktionen verfügbar sind, die Sie benötigen, wenn Sie Unified Manager starten. Wenn Sie jedoch von einer Ansicht zur anderen navigieren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

Typische Fensterlayouts

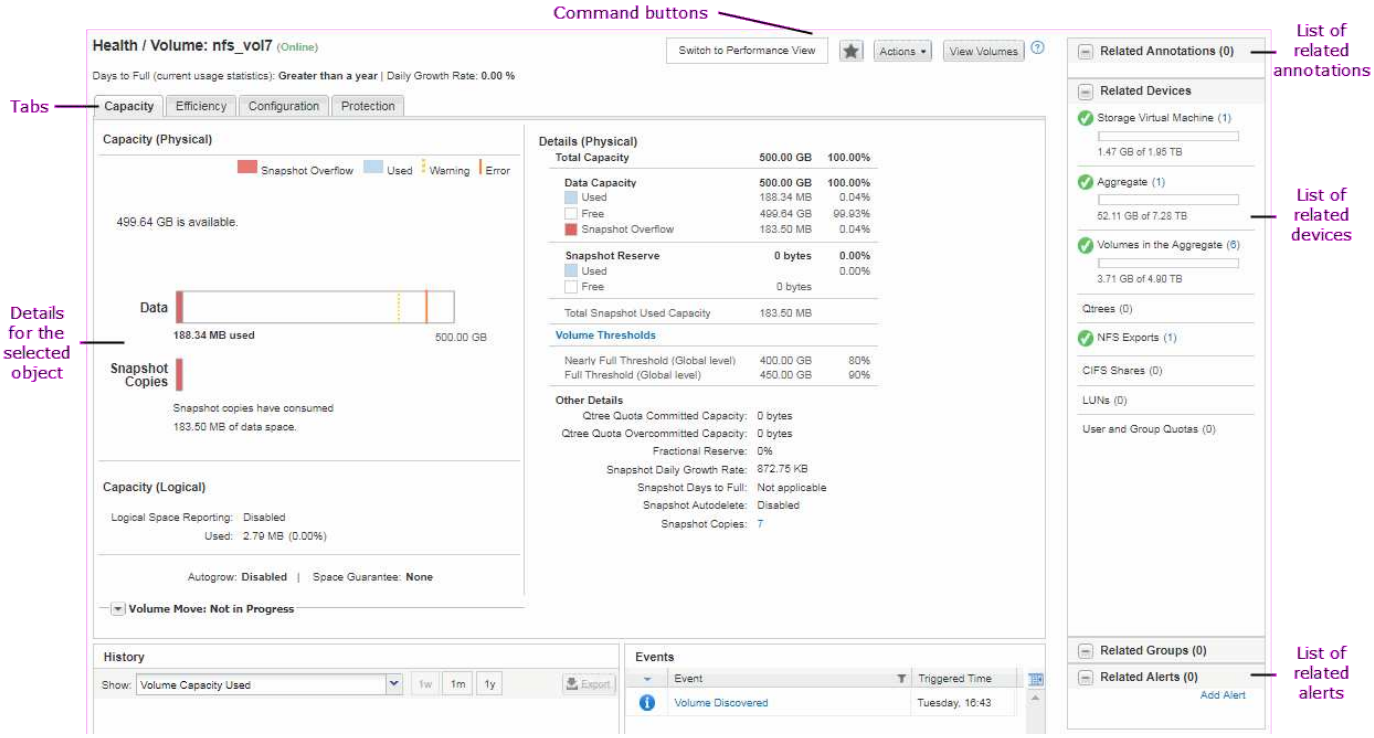
Das Verständnis der typischen Fensterlayouts hilft Ihnen, Active IQ Unified Manager effektiv zu nutzen und zu navigieren. Die meisten Unified Manager-Fenster ähneln einem von zwei allgemeinen Layouts: Objektliste oder Details. Die empfohlene Bildschirmeinstellung beträgt mindestens 1280 x 1024 Pixel.

Nicht jedes Fenster enthält jedes Element in den folgenden Diagrammen.

Layout des Fensters Objektliste



Layout des Fensters „Objektdetails“



Anpassung des Fensterlayouts

Active IQ Unified Manager ermöglicht Ihnen das Anpassen des Layouts für Informationen auf den Storage- und Netzwerk-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) für diese Spalte angezeigt.

- **Filterung**

  Sie können auf das Filtersymbol () klicken, um Filter anzuwenden, um die Anzeige von Informationen auf den Speicher- und Netzwerkobjektseiten so anzupassen, dass nur die Einträge angezeigt werden, die den angegebenen Bedingungen entsprechen. Sie wenden Filter im Fensterbereich Filter an.

  Im Bereich Filter können Sie die meisten Spalten anhand der ausgewählten Optionen filtern. In der Ansicht „Systemzustand: Alle Volumes“ können Sie z. B. im Bereich „Filter“ alle Volumes anzeigen, die offline sind, indem Sie die entsprechende Filteroption unter Status auswählen.

  Kapazitätsbezogene Spalten in jeder Liste zeigen immer Kapazitätsdaten in entsprechenden Einheiten an, abgerundet auf zwei Dezimalstellen. Dies gilt auch beim Filtern von Kapazitätspalten. Wenn Sie beispielsweise den Filter in der Spalte „Gesamtkapazität Daten“ in der Ansicht „Systemzustand: Alle Aggregate“ verwenden, um Daten größer als 20.45 GB zu filtern, wird die tatsächliche Kapazität von 20.454 GB als 20.45 GB angezeigt. 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 % in der Ansicht Systemzustand: Alle Aggregate verwenden, um Daten größer 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.

- **Ausblenden oder Anzeigen der Spalten**

  Sie können auf das Spaltenanzeigungssymbol (**ein-/ausblenden**) klicken, um auszuwählen, welche Spalten angezeigt werden sollen. Sobald Sie die entsprechenden Spalten ausgewählt haben, können Sie sie mit der Maus neu ordnen.

- **Suchen**

  Mit dem Suchfeld können Sie nach bestimmten Objektattributen suchen, um die Liste der Elemente auf der Bestandsseite zu verfeinern. Zum Beispiel können Sie „Cloud“ eingeben, um die Liste der Volumes auf der Seite „Volumes Inventory“ zu verfeinern, um alle Volumes anzuzeigen, in denen das Wort „Cloud“ enthalten ist.

- **Daten exportieren**

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

Verwenden der Unified Manager-Hilfe

Die Hilfe enthält Informationen zu allen in Active IQ Unified Manager enthaltenen Funktionen. Über das Inhaltsverzeichnis, den Index oder das Suchtool finden Sie Informationen zu den Funktionen und deren Verwendung.

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.

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

  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**.

Suche nach Speicherobjekten

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

Was Sie brauchen

- Sie müssen eine der folgenden Rollen haben, um diese Aufgabe auszuführen: Operator, Anwendungsadministrator oder Speicheradministrator.
- Eine gültige Suche muss mindestens drei Zeichen enthalten.

Wenn Sie den Dropdown-Menüwert „Alle“ verwenden, zeigt die globale Suche die Gesamtzahl der Ergebnisse in allen Objektkategorien an; für jede Objektkategorie sind maximal 25 Suchergebnisse verfügbar. Sie können einen bestimmten Objekttyp aus dem Dropdown-Menü 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
- Storage-VMs
- Aggregate
- Volumes

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

Durch die Eingabe eines Workload-Namens werden eine Liste der Workloads unter der entsprechenden Kategorie Volumes oder LUNs angezeigt.

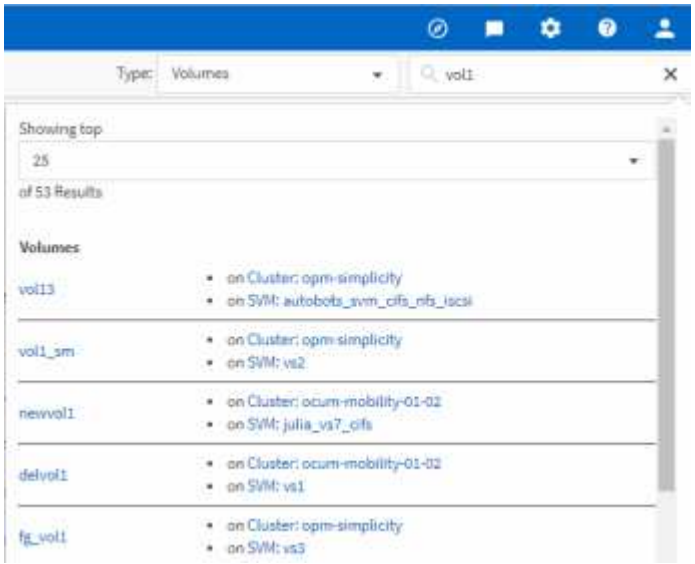
Sie können auf ein beliebiges Objekt in den Suchergebnissen klicken, um zur Seite Gesundheitsdetails für das Objekt zu navigieren. Wenn für ein Objekt keine direkte Integritätsseite vorhanden ist, wird die Seite Systemzustand des übergeordneten Objekts angezeigt. Beispiel: Bei der Suche nach einer bestimmten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

Ports und LIFs sind in der globalen Suchleiste nicht durchsuchbar.

Schritte

1. Wählen Sie einen Objekttyp aus dem Menü 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 ist im Dropdown-Feld 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.



Exportieren von Speicherdaten als Berichte

Sie können Storage-Daten in verschiedenen Ausgabeformaten exportieren und dann die exportierten Daten verwenden, um Berichte zu erstellen. Wenn z. B. 10 kritische Ereignisse nicht behoben wurden, können Sie die Daten von der Seite „Ereignismanagement-Bestand“ exportieren, um einen Bericht zu erstellen, und den Bericht anschließend an Administratoren senden, die die Probleme beheben können.

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Exportieren…	Tun Sie das…
Details zum Storage-Objektbestand	Klicken Sie im linken Navigationsmenü auf **Storage** oder **Network** und wählen Sie dann ein Speicherobjekt aus. Wählen Sie eine der vom System bereitgestellten Ansichten oder eine beliebige benutzerdefinierte Ansicht aus, die Sie erstellt haben.
Details zur QoS-Richtliniengruppe	Klicken Sie im linken Navigationsmenü auf **Storage** > **QoS Policy Groups**.
Details zur Storage-Kapazität und zum Sicherungsverlauf	Klicken Sie auf **Storage** > **Aggregate** oder **Storage** > **Volumes** und wählen Sie dann ein einzelnes Aggregat oder Volume aus.
Veranstaltungsdetails	Klicken Sie im linken Navigationsmenü auf **Ereignisverwaltung**.
Storage Objekt: Top 10 Performance-Details	Klicken Sie auf **Storage** > **Cluster** > **Performance:All Clusters**, 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 **Berichte** (oder auf einigen UI-Seiten auf die Schaltfläche **Exportieren**).
3. Klicken Sie **Download CSV**, **Download PDF** oder **Excel herunterladen** um die Exportanfrage zu bestätigen.

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

   Die Datei wird heruntergeladen.

4. Öffnen Sie die Datei in der entsprechenden Anwendung.

Verwandte Informationen

"„Systemzustand“/„Cluster Inventory“-Seite"

"Planen eines Berichts"

Inhalt der Bestandsseite wird gefiltert

Sie können die Daten auf den Inventarseiten in Unified Manager filtern, um Daten anhand spezifischer 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, um nur die Daten anzuzeigen, in denen Sie interessiert sind.

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 rechts neben der Schaltfläche Filter die Anzahl der angewendeten Filter angezeigt.

Es werden drei Filterparameter unterstützt.

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

Die Felder Spalte, Operator und Wert sind für jeden Filter erforderlich. Die verfügbaren Filter spiegeln die filterbaren Spalten auf der aktuellen Seite wider. 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 die Schaltfläche **Filter**. Das Filterfenster wird angezeigt.
2. Klicken Sie auf die linke Dropdown-Liste und wählen Sie ein Objekt aus, z. B. *Cluster* oder einen Performance-Zähler.
3. Klicken Sie auf die mittlere Dropdown-Liste, und wählen Sie den gewünschten Operator aus.
4. Wählen Sie in der letzten Liste einen Wert aus oder geben Sie einen Wert ein, um den Filter für dieses Objekt abzuschließen.
5. Um einen anderen 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.
6. Klicken Sie Auf **Filter Anwenden**. Die Filteroptionen werden auf das Raster angewendet und die Anzahl der Filter wird rechts neben der Schaltfläche Filter angezeigt.

7. Verwenden Sie den Filterbereich, um einzelne Filter zu entfernen, indem Sie auf das Papierkorb-Symbol rechts neben dem zu entfernenden Filter klicken.
8. 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, schließt sich das Filterfenster, wendet Ihre Filter an und zeigt die Anzahl der angewendeten Filter an ( ).

Anzeigen aktiver Ereignisse über die Benachrichtigunglocke

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

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

Hinweis: Wenn ein Cluster nicht erreichbar ist, zeigt Unified Manager diese Informationen auf dieser Seite an. Sie können detaillierte Informationen über ein Cluster anzeigen, das nicht erreichbar ist, indem Sie auf die Schaltfläche **Details** klicken. Mit dieser Aktion wird die Seite Ereignisdetails geöffnet. Auf dieser Seite werden auch Probleme mit der Skalenüberwachung, z. B. wenig Speicherplatz oder RAM auf der Management Station, angezeigt.

Schritte

1. Klicken Sie in der Menüleiste auf .
2. Um Details zu einem der aktiven Ereignisse anzuzeigen, klicken Sie auf den Ereignistext-Link, z. B. „2 Kapazität“ oder „4 Leistung“.

Monitoring und Management von Clustern über das Dashboard

Das Dashboard bietet auf einen Blick kumulative Informationen über den aktuellen Zustand Ihrer überwachten ONTAP-Systeme. Das Dashboard bietet „`Panels`“, mit denen Sie die Gesamtkapazität, die Performance und den Sicherheitszustand der von Ihnen überwachten Cluster bewerten können.

Außerdem gibt es bestimmte ONTAP Probleme, die Sie direkt über die Benutzeroberfläche von Unified Manager beheben können, anstatt ONTAP System Manager oder die ONTAP CLI verwenden zu müssen.

Oben im Dashboard können Sie auswählen, ob in den Bedienfeldern Informationen für alle überwachten Cluster oder für einen einzelnen Cluster angezeigt werden. Sie können beispielsweise den Status aller Cluster anzeigen und anschließend bei Bedarf detaillierte Informationen zu einzelnen Clustern abrufen.

Einige der unten aufgeführten Felder werden möglicherweise nicht auf der Seite angezeigt, je nach Ihrer Konfiguration.

Bedienfelder	Beschreibung
Managementaktionen	Wenn Unified Manager eine einzelne Lösung für ein Problem diagnostizieren und bestimmen kann, werden diese Auflösungen in diesem Fenster mit der Schaltfläche **Fix IT** angezeigt.
Kapazität	Zeigt die Gesamt- und genutzte Kapazität für die lokale Tier- und Cloud-Ebene sowie die Anzahl der Tage an, bis die lokale Kapazität das obere Limit erreicht.
Performance-Kapazität	Zeigt den Performance-Kapazitätswert für jedes Cluster und die Anzahl der Tage an, bis die Performance-Kapazität das obere Limit erreicht.
Workload-IOPS	Zeigt die Gesamtzahl der Workloads an, die derzeit in einem bestimmten IOPS-Bereich ausgeführt werden.
Workload-Performance	Zeigt die Gesamtzahl der konformen und nicht konformen Workloads an, die jedem definierten Performance-Service-Level zugewiesen sind.
Sicherheit	Zeigt die Anzahl an kompatiblen oder nicht kompatiblen Clustern an, die Anzahl an konformen bzw. nicht kompatiblen SVMs sowie die Anzahl der verschlüsselten Volumes.
Darstellt	Zeigt die Anzahl der Storage-VMs an, die durch eine SVM-DR-Beziehung gesichert sind, Volumes, die durch SnapMirror Beziehungen geschützt sind, Volumes durch Snapshots geschützt und durch MetroCluster geschützte Cluster.
Nutzungsübersicht	Zeigt die Cluster an, sortiert nach den höchsten IOPS, dem höchsten Durchsatz (MB/s) oder der höchsten genutzten physischen Kapazität.

Dashboard-Seite

Die Seite Dashboard verfügt über „Bereiche“, in denen die allgemeine Kapazität, Performance und der Sicherheitszustand der von Ihnen überwachten Cluster angezeigt wird. Diese Seite enthält außerdem ein Fenster „Management Actions“, in dem Korrekturen aufgeführt sind, die Unified Manager zur Behebung bestimmter Ereignisse durchführen kann.

Die meisten Felder zeigen auch die Anzahl der aktiven Ereignisse in dieser Kategorie sowie die Anzahl der neuen Ereignisse an, die in den letzten 24 Stunden hinzugefügt wurden. Anhand dieser Informationen können Sie entscheiden, welche Cluster Sie möglicherweise weiter analysieren müssen, um Ereignisse zu lösen. Wenn Sie auf die Ereignisse klicken, werden die wichtigsten Ereignisse angezeigt und es wird ein Link zur Seite „Ereignismanagement“ angezeigt, die gefiltert wurde, um die aktiven Ereignisse in dieser Kategorie anzuzeigen.

Oben im Dashboard können Sie auswählen, ob in den Bedienfeldern Informationen für alle überwachten Cluster („Alle Cluster“) oder für einen einzelnen Cluster angezeigt werden. Sie können beispielsweise den Status aller Cluster anzeigen und anschließend bei Bedarf detaillierte Informationen zu einzelnen Clustern abrufen.

Einige der unten aufgeführten Felder werden basierend auf Ihrer Konfiguration auf dem Dashboard angezeigt.

Bereich „Verwaltungsaktionen“

Es gibt bestimmte Probleme, die Unified Manager sorgfältig analysieren und eine singuläre Lösung anbieten kann. Wenn verfügbar, werden diese Auflösungen in diesem Fenster mit der Schaltfläche **Fix IT** oder **Fix All** angezeigt. Diese Probleme können Sie sofort von Unified Manager beheben, anstatt ONTAP System Manager oder die ONTAP CLI zu verwenden. Um alle Probleme anzuzeigen, klicken Sie auf unter"Behebung von ONTAP Problemen direkt über Unified Manager", um weitere Informationen zu erhalten.

Kapazität Panel

Bei der Anzeige aller Cluster zeigt dieses Feld die physisch genutzte Kapazität (nach Anwendung der Speichereffizienzeinsparungen) und die physisch verfügbare Kapazität (ohne Berücksichtigung der potenziellen Speichereffizienzeinsparungen) für jeden Cluster an. Die Anzahl der Tage, bis die Festplatten voraussichtlich voll sind. Das Datenreduzierungsverhältnis (ohne Snapshot Kopien) basiert auf konfigurierten ONTAP Storage-Effizienzeinstellungen. Außerdem werden die genutzte Kapazität für alle konfigurierten Cloud-Tiers aufgelistet. Durch Klicken auf das Balkendiagramm gelangen Sie zur Seite „Aggregates Inventory“ für den Cluster. Wenn Sie auf den Text „Tage bis zum vollen“ klicken, wird eine Meldung angezeigt, die das Aggregat mit der geringsten Anzahl an verbleibenden Kapazitätstagen identifiziert. Klicken Sie auf den Aggregatnamen, um weitere Details zu erhalten.

Wenn Sie sich ein einzelnes Cluster anzeigen lassen, werden in diesem Bereich die genutzte physische Kapazität und physische verfügbare Kapazität für Datenaggregate angezeigt, die nach den einzelnen Festplattentypen auf der lokalen Tier und für die Cloud-Tier sortiert sind. Wenn Sie auf das Balkendiagramm für einen Festplattentyp klicken, gelangen Sie zur Seite Volume Inventory für die Volumes, die diesen Festplattentyp verwenden.

Bereich Performance-Kapazität

Bei der Anzeige aller Cluster zeigt dieses Feld den Performance-Kapazitätswert für jedes Cluster (durchschnittlich über die vorherige 1 Stunde) und die Anzahl der Tage an, bis die Performance-Kapazität die Obergrenze erreicht (basierend auf der täglichen Wachstumsrate). Durch Klicken auf das Balkendiagramm gelangen Sie zur Seite „Nodes-Inventar“ für dieses Cluster. Auf der Seite Nodes-Inventar wird die Performancskapazität angezeigt, die über die letzten 72 Stunden Durchschnitt lag. Wenn Sie auf den Text „Tage bis zum vollen“ klicken, wird eine Meldung angezeigt, in der der Node mit der geringsten Anzahl an verbleibenden Performance-Kapazitätstagen identifiziert wird. Klicken Sie auf den Node-Namen, um weitere Details anzuzeigen.

Wenn Sie ein einzelnes Cluster anzeigen, werden in diesem Bereich die Werte der verwendeten Cluster-Performance-Kapazität, der IOPS-Gesamtwert und der Gesamtdurchsatz (MB/s) angezeigt. Die Anzahl der

Tage, bis die drei Kennzahlen ihre Obergrenze erreichen sollen.

Workload-IOPS-Bereich

Wenn Sie sich ein einzelnes Cluster anzeigen lassen, wird in diesem Bereich die Gesamtzahl der Workloads angezeigt, die derzeit in einem bestimmten IOPS-Bereich ausgeführt werden, und die Anzahl der einzelnen Festplattentypen wird angezeigt, wenn Sie den Mauszeiger über das Diagramm bewegen.

Bereich „Workload Performance“

In diesem Fenster wird die Gesamtzahl der konformen und nicht konformen Workloads angezeigt, die jeder PSL-Richtlinie (Performance Service Level) zugewiesen sind. Außerdem wird die Anzahl der Workloads angezeigt, denen keine PSL zugewiesen ist. Durch Klicken auf ein Balkendiagramm gelangen Sie zu den Workloads, die dieser Richtlinie zugeordnet sind, auf der Seite Workloads. Wenn Sie auf das folgende Balkendiagramm klicken, gelangen Sie zu den Workloads, die dieser Richtlinie zugeordnet sind, die den entsprechenden Anforderungen nicht gerecht werden.

Sicherheitstafel

Das Sicherheitsfenster zeigt je nach aktueller Ansicht den allgemeinen Sicherheitsstatus aller Cluster oder eines einzelnen Clusters an. In diesem Fenster wird Folgendes angezeigt:

- Eine Liste der Sicherheitsereignisse, die in den letzten 24 Stunden eingehen. Klicken Sie auf eine Veranstaltung, um die Details auf der Seite „Veranstaltungsdetails“ anzuzeigen
- Cluster-Sicherheitsstatus (Anzahl konformer und nicht konformer Cluster)
- Der Sicherheitsstatus der Storage-VM (Anzahl konformer und nicht konformer Storage VMs)
- Status der Volume-Verschlüsselung (Anzahl der verschlüsselten Volumes)
- Der Anti-Ransomware-Status des Volumes (Anzahl Volumes mit aktivierter oder deaktivierter Anti-Ransomware-Lösung)

Sie können auf die Balkendiagramme der Compliance-konformen und nicht konformen Cluster, Storage-VMS, verschlüsselten und nicht verschlüsselten Volumes und den Status für nicht-Ransomware-Volumes klicken, um zu den jeweiligen Seiten zu gelangen und die Sicherheitsinformationen für gefilterte Cluster, Storage-VMs und Volumes anzuzeigen.

Die Compliance basiert auf der "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9". Klicken Sie auf den Rechtspfeil oben im Bedienfeld, um die Sicherheitsinformationen für alle Cluster auf der Seite Sicherheit anzuzeigen. Weitere Informationen finden Sie unter "Anzeigen des detaillierten Sicherheitsstatus für Cluster und Storage-VMs".

Data Protection Panel

In diesem Fenster wird die Zusammenfassung der Datensicherung für ein einzelnes oder alle Cluster in einem Rechenzentrum angezeigt. Sie zeigt die Gesamtzahl der Datensicherungsereignisse, MetroCluster-Ereignisse und die Anzahl der aktiven Ereignisse an, die in den letzten 24 Stunden in ONTAP angesprochen wurden. Wenn Sie auf den Link der einzelnen Veranstaltungen klicken, gelangen Sie zur Seite Veranstaltungsdetails. Sie können auf den Link * Alle anzeigen* klicken, um alle aktiven Schutzereignisse auf der Seite Ereignisverwaltung Inventar anzuzeigen. Das Fenster zeigt:

- Die Anzahl der Volumes in einem Cluster oder alle Cluster in einem durch Snapshot Kopien geschützten Datacenter.
- Die Anzahl der Volumes in einem Cluster oder alle Cluster in einem durch SnapMirror Beziehungen

geschützten Datacenter. Für SnapMirror Beziehungen wird die Anzahl der Volumes im Quell-Cluster berücksichtigt.

- Die Anzahl der Cluster oder alle Cluster in einem durch MetroCluster-Konfiguration geschützten Datacenter über IP oder FC
- Die Anzahl der Volume-Beziehungen mit der SnapMirror Recovery Point Objective (RPO)-Verzögerung basierend auf dem lag-Status.

Sie können mit der Maus die entsprechenden Zählungen und Legenden anzeigen. Sie können auf den Rechtspfeil oben im Bedienfeld klicken, um die Details für einen einzelnen oder alle Cluster auf der Datenschutzseite anzuzeigen. Sie können außerdem auf klicken:

- Die Balkendiagramme für nicht geschützte Volumes und durch Snapshot-Kopien geschützte Volumes sind, werden zur Seite „Volumes“ und zur Ansicht der Details angezeigt.
- Die Balkendiagramme für die durch MetroCluster-Konfiguration geschützten oder nicht geschützten Cluster werden angezeigt, um zur Seite Cluster zu gelangen und die Details anzuzeigen.
- Die Balkendiagramme für alle Beziehungen gehen zur Seite „Beziehungen“, auf der die Details nach dem Quellcluster gefiltert werden.

Weitere Informationen finden Sie unter "Anzeigen des Volume-Sicherungsstatus".

Das Fenster „Verwendungsübersicht“

Bei der Anzeige aller Cluster können Sie Cluster nach den höchsten IOPS, dem höchsten Durchsatz (MB/s) oder der am höchsten genutzten physischen Kapazität anzeigen.

Bei der Anzeige eines einzelnen Clusters können Sie Workloads nach den höchsten IOPS, dem höchsten Durchsatz (MB/s) oder der am höchsten genutzten logischen Kapazität anzeigen.

Verwandte Informationen

"Behebung von Problemen durch automatische Problembehebung mit Unified Manager"

"Anzeigen von Informationen zu Performance-Ereignissen"

"Performance-Management mithilfe von Performance-Kapazität und verfügbaren IOPS-Informationen"

"Seite „Volume/Health Details“"

"Performance-Ereignisanalyse und -Benachrichtigung"

"Beschreibung der Ereignistypen"

"Quellen von Leistungsereignissen"

"Verwalten von Zielen für die Cluster-Sicherheit"

"Monitoring der Cluster-Performance über die Startseite des Performance Cluster"

"Überwachung der Performance mithilfe der Seiten „Performance Inventory“ (Performance-Bestandsaufnahme"

Direktes Management von ONTAP Problemen oder Funktionen über Unified Manager

Bestimmte ONTAP Probleme können behoben oder bestimmte ONTAP Funktionen direkt über die Benutzeroberfläche von Unified Manager verwaltet werden, anstatt ONTAP System Manager oder die ONTAP CLI verwenden zu müssen. Die Option „`MManagement Actions`“ enthält Korrekturen an einer Reihe von ONTAP Problemen, die Unified Manager Ereignisse ausgelöst haben.

Sie können Probleme direkt auf der Seite „Management Actions“ beheben, indem Sie im linken Navigationsbereich die Option **Management Actions** auswählen. Managementaktionen können auch über das Fenster „Management Actions“ auf der Seite „Dashboard“, „Ereignisdetails“ und „Workload Analysis“ im linken Navigationsmenü aufgerufen werden.

Es gibt bestimmte Probleme, die Unified Manager sorgfältig analysieren und eine singuläre Lösung anbieten kann. Bei bestimmten ONTAP Funktionen wie dem Monitoring gegen Ransomware führt Unified Manager interne Prüfungen durch und empfiehlt bestimmte Aktionen. Wenn verfügbar, werden diese Auflösungen in Management Actions mit der Schaltfläche **Fix IT** angezeigt. Klicken Sie auf die Schaltfläche **Fix IT**, um das Problem zu beheben. Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Unified Manager sendet ONTAP-Befehle an das Cluster, um den angeforderten Fix zu erstellen. Nach Abschluss der Fehlerbehebung ist das Ereignis veraltet.

Einige Verwaltungsaktionen ermöglichen es Ihnen, das gleiche Problem auf mehreren Speicherobjekten mit der Schaltfläche * alles beheben. Zum Beispiel kann es 5 Volumen geben, die das Ereignis „Volume Space Full“ haben, das durch Klicken auf die Aktion * alles* Management für „Enable Volume Autogrow“ behoben werden könnte. Mit einem Klick können Sie dieses Problem auf 5 Volumes beheben.

Informationen zu ONTAP-Problemen und "Welche Probleme können mit Unified Manager behoben werden" -Funktionen, die Sie mit automatischer Problembehebung managen können, finden Sie unter .

Welche Optionen habe ich, wenn ich die Schaltfläche „alles beheben“ oder „Alle beheben“ sehe

Auf der Seite „Management Actions“ finden Sie die Schaltfläche **Fix IT** oder **Fix All**, um Probleme zu beheben, über die Unified Manager über ein Ereignis benachrichtigt wurde.

Wir empfehlen, dass Sie auf die Schaltflächen klicken, um ein Problem zu beheben, falls erforderlich. Wenn Sie jedoch nicht sicher sind, dass Sie das Problem wie von Unified Manager empfohlen lösen möchten, können Sie die folgenden Aktionen durchführen:

Was möchten Sie tun?	Aktion
Unified Manager hat das Problem für alle ermittelten Objekte behoben.	Klicken Sie auf die Schaltfläche * Alle beheben.
Beheben Sie das Problem derzeit nicht für eines der identifizierten Objekte, und verbergen Sie diese Verwaltungsaktion, bis das Ereignis erneut angesprochen wird.	Klicken Sie auf den Pfeil nach unten und klicken Sie auf **Alle verwerfen**.

Was möchten Sie tun?	Aktion
Beheben Sie das Problem nur bei einigen der identifizierten Objekte.	Klicken Sie auf den Namen der Management-Aktion, um die Liste zu erweitern und alle einzelnen **Fix IT** -Aktionen anzuzeigen.dann folgen Sie den Schritten, um einzelne Management-Aktionen zu beheben oder zu verfehlen.

Was möchten Sie tun?	Aktion
Lassen Sie das Problem mit Unified Manager beheben.	Klicken Sie auf die Schaltfläche **Fix it**.
Beheben Sie das Problem derzeit nicht und verbergen Sie diese Verwaltungsaktion, bis das Ereignis erneut angesprochen wird.	Klicken Sie auf den Abwärtspfeil und klicken Sie auf **Abweisen**.
Zeigen Sie die Details für dieses Ereignis an, damit Sie das Problem besser verstehen können.	• Klicken Sie auf die Schaltfläche **Fix it** und prüfen Sie die Fehlerbehebung, die im resultierenden Dialogfeld angewendet wird. • Klicken Sie auf den Abwärtspfeil und klicken Sie auf **Ereignisdetails anzeigen**, um die Seite Ereignisdetails anzuzeigen. Klicken Sie dann auf einer dieser Seiten auf **Fix it**, wenn Sie das Problem beheben möchten.
Zeigen Sie die Details für dieses Speicherobjekt an, damit Sie das Problem besser verstehen.	Klicken Sie auf den Namen des Speicherobjekts, um Details auf der Seite Performance Explorer oder Health Details anzuzeigen.

In einigen Fällen wird der Fix in der nächsten 15-minütigen Konfigurationsabfrage reflektiert. In anderen Fällen kann es bis zu viele Stunden dauern, bis die Konfigurationsänderung überprüft und das Ereignis veraltet ist.

Um die Liste der abgeschlossenen oder laufenden Management-Aktionen anzuzeigen, klicken Sie auf das Filtersymbol und wählen Sie **abgeschlossen** oder **in Bearbeitung** aus.

Fix Alle Operationen laufen seriell, so dass, wenn Sie das **in progress** Panel sehen, einige Objekte den Status **in progress** haben, während andere den Status **terminiert** haben; das heißt, sie warten noch auf die Implementierung.

Anzeigen des Status der Verwaltungsaktionen, die Sie beheben möchten

Sie können den Status aller Verwaltungsaktionen anzeigen, die Sie auf der Seite „Verwaltungsaktionen“ ausgewählt haben. Die meisten Aktionen werden relativ schnell als **abgeschlossen** angezeigt, nachdem Unified Manager den ONTAP-Befehl an das Cluster sendet. Einige Aktionen, wie zum Beispiel das Verschieben eines Volumes, können jedoch länger dauern.

Auf der Seite „Management Actions“ stehen drei Filter zur Verfügung:

- **Abgeschlossen** zeigt sowohl erfolgreich abgeschlossene Management-Aktionen als auch fehlgeschlagene. **Fehlgeschlagene** Aktionen geben einen Grund für den Fehler, so dass Sie das Problem manuell beheben können.
- **In progress** zeigt sowohl die Management-Aktionen, die durchgeführt werden, als auch die, die geplant sind, umzusetzen.
- **Empfohlen** zeigt alle Management-Aktionen an, die derzeit für alle überwachten Cluster aktiv sind.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Management Actions**. Alternativ dazu klicken Sie ⋮ oben im Bereich **Management Actions** auf dem **Dashboard** und wählen die Ansicht aus, die Sie sehen möchten.

   Die Seite Verwaltungsaktionen wird angezeigt.

2. Sie können im Feld **Beschreibung** auf das Caret-Symbol neben der Verwaltungsaktion klicken, um Details zum Problem und den Befehl anzuzeigen, mit dem das Problem behoben wird.
3. Um Aktionen anzuzeigen, die **fehlgeschlagen** sind, Sortieren Sie in der Spalte **Status** in der Ansicht **abgeschlossen** nach. Für diesen Zweck können Sie das **Filter** Werkzeug verwenden.
4. Wenn Sie weitere Informationen zu einer fehlgeschlagenen Verwaltungsaktion anzeigen möchten oder wenn Sie sich entscheiden, eine empfohlene Verwaltungsaktion zu beheben, können Sie im erweiterten Bereich auf **Ereignisdetails anzeigen** klicken, nachdem Sie neben der Verwaltungsaktion auf das Caret-Symbol geklickt haben. Auf dieser Seite steht ein **Fix it** Button zur Verfügung.

Welche Probleme können mit Unified Manager behoben werden

Mit der Funktion zur automatischen Korrektur von Active IQ Unified Manager lassen sich bestimmte ONTAP Probleme beheben oder bestimmte ONTAP Funktionen wie die Ransomware-Überwachung effektiv über Unified Manager managen.

In dieser Tabelle werden die ONTAP-Probleme oder Funktionen beschrieben, die Sie direkt über die Schaltfläche **Fix IT** oder **Fix All** auf der Web-Benutzeroberfläche von Unified Manager verwalten können.

Name und Beschreibung des Events	Managementaktion	Operation „Fix It“
Volume-Speicherplatz Voll Das Volume ist fast nicht mehr Platz vorhanden und es hat den Schwellenwert für die Kapazitäten erreicht. Dieser Schwellenwert ist standardmäßig auf 90 % der Volume-Größe eingestellt.	Aktivieren Sie Autogrow	Unified Manager ermittelt, dass Volume Autogrow nicht für dieses Volume konfiguriert ist, sodass es diese Funktion aktiviert, damit das Volume bei Bedarf die Kapazität erweitert.
Inodes Voll Dieses Volume hat keine Inodes und kann keine neuen Dateien akzeptieren.	Erhöhen Sie die Anzahl von Inodes auf dem Volumen	Erhöht die Anzahl der Inodes auf dem Volumen um 2 Prozent.

Name und Beschreibung des Events	Managementaktion	Operation „Fix It“
Richtlinie Für Storage-Tier Wurde Nicht Stimmt Überein Das Volume verfügt über viele inaktive Daten und die aktuelle Tiering-Richtlinie wird auf „nur Snapshots“ oder „keine“ gesetzt.	Aktivieren Sie automatisches Cloud Tiering	Da sich das Volume bereits auf einer FabricPool befindet, wird die Tiering-Richtlinie in „automatisch“ geändert, sodass inaktive Daten in die kostengünstigere Cloud-Tier verschoben werden.
Nichtübereinkommen Bei Storage Tier Erkannt Auf dem Volume befinden sich viele inaktive Daten, die sich jedoch nicht auf einem Cloud-fähigen Storage Tier (FabricPool) befinden.	Storage-Tier von Volumes ändern	Das Volume wird auf Cloud-fähige Storage-Tier verschoben und die Tiering-Richtlinie auf „automatisch“ gesetzt, um inaktive Daten auf die Cloud-Tier zu verschieben.
Überwachungsprotokoll Deaktiviert Das Prüfprotokoll ist für die Storage-VM nicht aktiviert	Aktivieren der Audit-Protokollierung für die Storage-VM	Aktiviert die Protokollierung von Prüfungen auf der Storage-VM. Beachten Sie, dass für die Storage-VM bereits ein lokaler oder ein Remote-Audit-Protokollverzeichnis konfiguriert sein muss.
Anmelde-Banner Deaktiviert Das Login-Banner für den Cluster sollte aktiviert sein, um die Sicherheit zu erhöhen, indem Zugriffsbeschränkungen klar werden.	Setzen Sie das Anmeldebanner für den Cluster ein	Setzt das Cluster-Anmeldebanner auf „`Zugriff beschränkt auf autorisierte Benutzer`“.
Anmelde-Banner Deaktiviert Das Login-Banner für die Storage-VM sollte aktiviert sein, um die Sicherheit zu erhöhen, indem Zugriffsbeschränkungen klar werden.	Setzen Sie das Anmeldebanner für die Storage-VM ein	Legt den Storage VM Login Banner auf „Access Restricted to Authorized Users“ fest.
SSH verwendet unsichere Chiffren Chiffren mit dem Suffix „-cbc“ werden als unsicher betrachtet.	Entfernen Sie unsichere Chiffren aus dem Cluster	Entfernt die unsicheren Chiffren - wie aes192-cbc und aes128-cbc — aus dem Cluster.

Name und Beschreibung des Events	Managementaktion	Operation „Fix It“
SSH verwendet unsichere Chiffren Chiffren mit dem Suffix „-cbc“ werden als unsicher betrachtet.	Entfernen Sie unsichere Chiffren aus der Storage-VM	Entfernt die unsicheren Chiffren - wie aes192-cbc und aes128-cbc — von der Storage-VM.
AutoSupport HTTPS-Transport deaktiviert Das Transportprotokoll zum Senden von AutoSupport Meldungen an den technischen Support sollte verschlüsselt sein.	Legen Sie HTTPS als Transportprotokoll für AutoSupport Meldungen fest	Legt HTTPS als Transportprotokoll für AutoSupport Meldungen auf dem Cluster fest.
Überschreitung Des Schwellenwerts Für Das Cluster-Load-Ungleichgewicht Zeigt an, dass der Lastausgleich zwischen den Nodes im Cluster nicht ausgeglichen ist. Dieses Ereignis wird generiert, wenn die verwendete Performance-Abweichung zwischen den Nodes mehr als 30 % beträgt.	Lastausgleich für Cluster-Workloads	Unified Manager ermittelt, welches Volume am besten von einem Node zum anderen verschoben werden soll, um das Ungleichgewicht zu verringern und dann das Volume zu verschieben.
Unterschreiten Des Schwellenwerts Für Die Clusterkapazität Zeigt an, dass der Kapazitätsausgleich zwischen den Aggregaten im Cluster nicht möglich ist. Dieses Ereignis wird erzeugt, wenn die verwendete Kapazitätsabweichung zwischen Aggregaten mehr als 70 % beträgt.	Ausgewogene Cluster-Kapazität	Unified Manager erkennt das optimale Volume für die Verschiebung von einem Aggregat zu einem anderen, um das Ungleichgewicht zu verringern und dann das Volume zu verschieben.
Nicht Genutzte Performance-Kapazität Schwellenwert Zeigt an, dass die Last auf dem Node überausgelastet werden kann, wenn die Auslastung nicht um mindestens einen hochaktiven Workload reduziert wird. Dieses Ereignis wird generiert, wenn die genutzte Node-Performance-Kapazität für mehr als 12 Stunden mehr als 100 % beträgt.	Begrenzen Sie die hohe Last auf dem Node	Unified Manager ermittelt das Volume mit den höchsten IOPS und wendet eine QoS-Richtlinie auf Basis des erwarteten historischen IOPS-Spitzenniveaus an, um die Last auf dem Node zu verringern.

Name und Beschreibung des Events	Managementaktion	Operation „Fix It“
Schwellenwert Für Dynamische Ereigniswarnung Überschritten Zeigt an, dass der Node aufgrund der ungewöhnlich hohen Auslastung einiger Workloads bereits überlastet ist.	Verringern Sie die Überlastung in einem Node	Unified Manager ermittelt das Volume mit den höchsten IOPS und wendet eine QoS-Richtlinie auf Basis des erwarteten historischen IOPS-Spitzenniveaus an, um die Last auf dem Node zu verringern.
Übernahme ist nicht möglich Der Failover ist derzeit deaktiviert, sodass während eines Ausfalls oder Neubootens der Zugriff auf die Ressourcen des Node unterbrochen wird, bis der Node wieder verfügbar ist.	Aktivieren Sie Node-Failover	Unified Manager sendet den entsprechenden Befehl, um Failover auf allen Knoten im Cluster zu aktivieren.
Option cf.takeover.on_Panic IST AUS konfiguriert Die nodeshell Option "cf.takeover.on_Panic" wird auf **aus** gesetzt, was bei HA-konfigurierten Systemen zu einem Problem führen könnte.	Aktivieren Sie die Übernahme in Panikzustand	Unified Manager sendet den entsprechenden Befehl an den Cluster, um diese Einstellung in **ein** zu ändern.
Deaktivieren Sie die nodeshell Option snapmirror.enable Die alte nodeshell Option "snapmirror.enable" steht auf **on**, was nach dem Upgrade auf ONTAP 9.3 oder höher ein Problem beim Booten verursachen kann.	Setzen Sie die option snapmirror.enable auf aus	Unified Manager sendet den entsprechenden Befehl an den Cluster, um diese Einstellung in **aus** zu ändern.
Telnet ist aktiviert Weist auf ein potenzielles Sicherheitsproblem hin, da Telnet unsicher ist und Daten unverschlüsselt weiterleitet.	Deaktivieren Sie Telnet	Unified Manager sendet den entsprechenden Befehl an das Cluster, um Telnet zu deaktivieren.

Name und Beschreibung des Events	Managementaktion	Operation „Fix It“
Konfiguration des Anti-Ransomware-Lernens für Storage-VMs Regelmäßige Überprüfungen auf Cluster mit Lizenzen für Anti-Ransomware-Monitoring Validierung, ob eine Storage VM nur NFS- oder SMB-Volumes in einem solchen Cluster unterstützt	Versetzen Sie Storage VMs in einen `learning` Modus zum Schutz vor Ransomware	Unified Manager gibt über die Cluster-Managementkonsole Anti-Ransomware Monitoring `learning` für die Storage VMs an. Das Ransomware-Monitoring auf allen neuen Volumes, die auf der Storage-VM erstellt wurden, wird automatisch in den Learning-Modus versetzt. Im Rahmen dieses Enablement lernt ONTAP das Aktivitätsmuster auf den Volumes und erkennt Anomalien aufgrund potenzieller bösartiger Angriffe.
Konfiguration des Anti-Ransomware-Lernens für Volumes Regelmäßige Überprüfungen auf Cluster mit Lizenzen für Anti-Ransomware-Monitoring Validierung, ob ein Volume nur NFS- oder SMB-Services in einem solchen Cluster unterstützt	Volumes in den Modus für das Ransomware-Monitoring versetzen `learning`	Unified Manager legt über die Cluster-Managementkonsole fest, dass Anti-Ransomware-Monitoring `learning` für die Volumes erfolgt. Im Rahmen dieses Enablement lernt ONTAP das Aktivitätsmuster auf den Volumes und erkennt Anomalien aufgrund potenzieller bösartiger Angriffe.
Volume-Anti-Ransomware aktivieren Regelmäßige Überprüfungen auf Cluster mit Lizenzen für Anti-Ransomware-Monitoring Er erkennt, ob sich die Volumes mehr als 45 Tage lang im Anti-Ransomware-Monitoring befinden, und ermittelt, ob `learning` sie in den aktiven Modus versetzt werden sollen.	Volumes in den Modus für das Ransomware-Monitoring versetzen `active`	Unified Manager setzt über die Cluster-Managementkonsole ein Anti-Ransomware-Monitoring auf `active` den Volumes. Im Rahmen dieses Enablement lernt ONTAP das Aktivitätsmuster auf den Volumes kennen, erkennt Anomalien aufgrund potenzieller bösartiger Angriffe und erstellt Warnmeldungen zu Datensicherungsmaßnahmen.

Name und Beschreibung des Events	Managementaktion	Operation „Fix It“
Deaktivieren Sie die Anti-Ransomware des Volumes Regelmäßige Überprüfungen auf Cluster mit Lizenzen für Anti-Ransomware-Monitoring Erkennt sich wiederholende Benachrichtigungen während der aktiven Anti-Ransomware-Überwachung auf den Volumes (so werden beispielsweise mehrere Warnungen vor potenziellen Ransomware-Angriffen über 30 Tage zurückgegeben).	Deaktivieren Sie das Anti-Ransomware-Monitoring auf Volumes	Unified Manager deaktiviert das Ransomware-Monitoring auf den Volumes über die Cluster Management-Konsole.

Management-Aktionen über Skripte überschreiben

Sie können benutzerdefinierte Skripts erstellen und sie zu Warnungen zuordnen, um bestimmte Aktionen für bestimmte Ereignisse durchzuführen. Sie können nicht die Standardverwaltungsaktionen auswählen, die ihnen auf der Seite „Managementaktionen“ oder auf dem Unified Manager-Dashboard zur Verfügung stehen.

Wenn Sie bestimmte Aktionen für einen Ereignistyp ausführen möchten und diese nicht als Teil der von Unified Manager bereitgestellten Management Action-Funktion beheben möchten, können Sie ein benutzerdefiniertes Skript für die spezifische Aktion konfigurieren. Sie können das Skript dann mit einer Warnung für diesen Ereignistyp verknüpfen und sich um solche Ereignisse individuell kümmern. In diesem Fall werden Management-Aktionen für diesen spezifischen Ereignistyp auf der Seite „Management Actions“ oder auf dem Unified Manager Dashboard nicht generiert.

Verwalten von Clustern

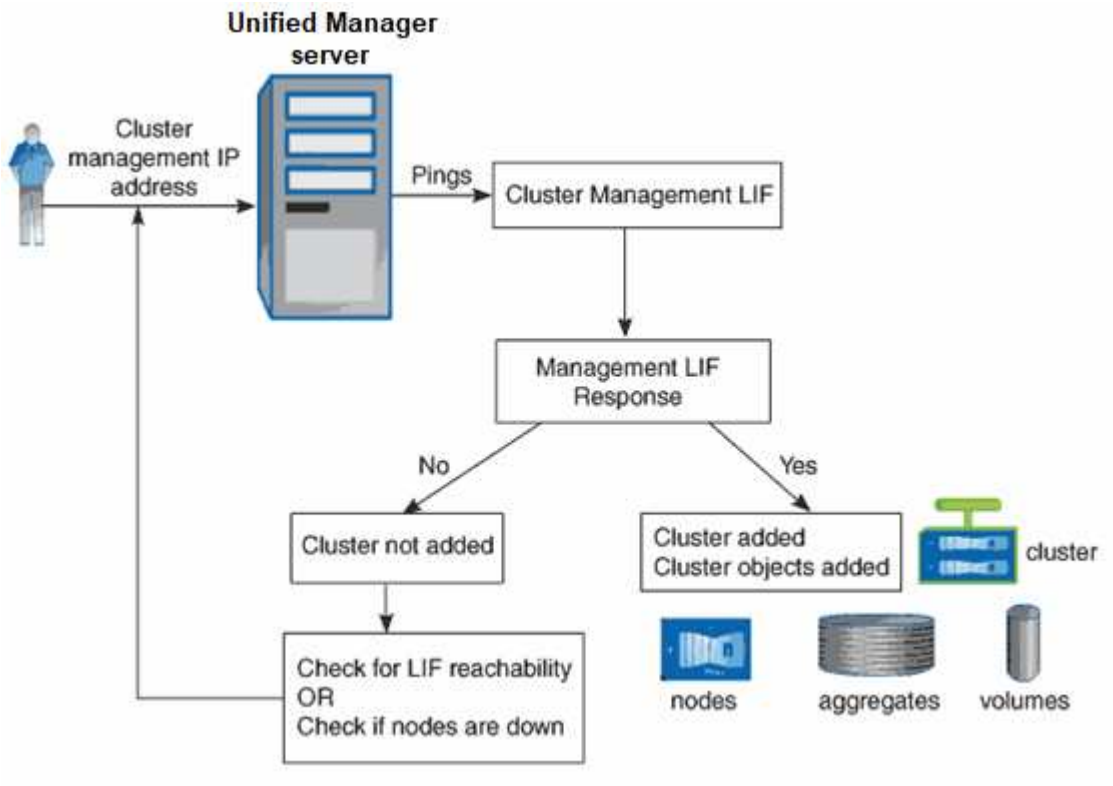
ONTAP-Cluster können mit Unified Manager gemanagt werden, um Cluster zu überwachen, hinzuzufügen, zu bearbeiten und zu entfernen.

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

Mithilfe der Seite Cluster Setup 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.

Was Sie brauchen

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

Schritt

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

   Es werden alle Cluster in der Storage-Umgebung angezeigt, die von Unified Manager gemanagt werden. Die Liste der Cluster ist nach der Spalte mit dem Schweregrad des Erfassungsstatus sortiert. Sie können auf eine Spaltenüberschrift klicken, um die Cluster nach unterschiedlichen Spalten zu sortieren.

Hinzufügen von Clustern

Sie können Active IQ Unified Manager ein Cluster hinzufügen, 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.

Was Sie brauchen

- Sie müssen über die Anwendungsadministratorrolle oder die Speicheradministratorrolle verfügen.
- Sie müssen die folgenden Informationen haben:
  - Unified Manager unterstützt lokale ONTAP Cluster, ONTAP Select und Cloud Volumes ONTAP.
  - 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*, *Console* und *http* eingestellt sein.
  - Sie müssen die Port-Nummer kennen, um eine Verbindung zum Cluster mithilfe des HTTPS-Protokolls (normalerweise Port 443) herzustellen.
  - Der Cluster muss die ONTAP Version 9.1 oder höher ausführen.
  - 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 verfügen über die erforderlichen Zertifikate:

    SSL (HTTPS) Zertifikat: Dieses Zertifikat ist im Besitz von Unified Manager. Bei einer neuen Installation von Unified Manager wird ein selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt ein Upgrade auf ein Zertifikat, das von einer Zertifizierungsstelle unterzeichnet wurde, um die Sicherheit zu erhöhen. Wenn das Serverzertifikat abgelaufen ist, sollten Sie es neu generieren und Unified Manager neu starten, damit die Dienste das neue Zertifikat aufnehmen können. Weitere Informationen zur Neugenerierung von SSL-Zertifikaten finden Sie unter "Erstellen eines HTTPS-Sicherheitszertifikats".

    EMS-Zertifikat: Dieses Zertifikat ist im Besitz von Unified Manager. Es wird bei der Authentifizierung für EMS-Benachrichtigungen verwendet, die von ONTAP empfangen werden.

    Zertifikate für gegenseitige TLS-Kommunikation: Wird bei der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatbasierte Authentifizierung ist auf Grundlage der Version von ONTAP für ein Cluster aktiviert. Wenn das Cluster mit der Version ONTAP niedriger als die Version 9.5 ist, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

    Die zertifikatbasierte Authentifizierung wird für ein Cluster nicht automatisch aktiviert, wenn Sie eine ältere Version von Unified Manager aktualisieren. Allerdings können Sie die Aktivierung durch Ändern und Speichern der Cluster-Details aktivieren. Wenn das Zertifikat abgelaufen ist, sollten Sie es erneut generieren, um das neue Zertifikat zu integrieren. Weitere Informationen zum Anzeigen und

Neugenerieren des Zertifikats finden Sie unter "Cluster werden bearbeitet".

- Sie können ein Cluster über die Web-Benutzeroberfläche hinzufügen, und die zertifikatbasierte Authentifizierung wird automatisch aktiviert.
- Sie können ein Cluster über die Unified Manager CLI hinzufügen. Die zertifikatbasierte Authentifizierung ist standardmäßig nicht aktiviert. Wenn Sie ein Cluster mit der Unified Manager CLI hinzufügen, muss das Cluster über die Unified Manager UI bearbeitet werden. Es wird angezeigt"Unterstützte CLI-Befehle von Unified Manager", wie Sie mithilfe der Unified Manager CLI einen Cluster hinzufügen.
- Wenn die zertifikatbasierte Authentifizierung für ein Cluster aktiviert ist und Sie das Backup von Unified Manager von einem Server aus erstellen und auf einen anderen Unified Manager Server wiederherstellen. Hier wird der Hostname oder die IP-Adresse geändert, dann kann das Monitoring des Clusters fehlschlagen. Um den Ausfall zu vermeiden, bearbeiten und speichern Sie die Cluster-Details. Weitere Informationen zum Bearbeiten von Cluster-Details finden Sie unter "Cluster werden bearbeitet".
- Auf Cluster-Ebene fügt die Active IQ-Schnittstelle zwei neue Benutzergruppen-Einträge für die Authentifizierungsmethode „cert“ hinzu.

+
Cluster-Zertifikate: Dieses Zertifikat ist Eigentum von ONTAP. Sie können Unified Manager kein Cluster mit einem abgelaufenen Zertifikat hinzufügen. Wenn das Zertifikat bereits abgelaufen ist, sollten Sie es neu erstellen, bevor Sie das Cluster hinzufügen. Informationen zur Zertifikatgenerierung finden Sie im Artikel Knowledge Base (KB) "So erneuern Sie ein selbstsigniertes ONTAP-Zertifikat in der System Manager-Benutzeroberfläche" .

- 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. Informationen zur Liste der unterstützten Knotenanzahl finden Sie im "Unified Manager Best Practices-Leitfaden".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Cluster-Setup**.
2. Klicken Sie auf der Seite Cluster Setup auf **Hinzufügen**.
3. Geben Sie im Dialogfeld Cluster hinzufügen die Werte nach Bedarf an, und klicken Sie dann auf **Absenden**.
4. Klicken Sie im Dialogfeld Host autorisieren auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.
5. Klicken Sie Auf **Ja**.

   Nachdem Sie die Cluster-Details gespeichert haben, können Sie das Zertifikat für die gegenseitige TLS-Kommunikation für ein Cluster anzeigen.

   Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, überprüft Unified Manager das Zertifikat nur, wenn das Cluster zunächst hinzugefügt wird. Unified Manager überprüft nicht das Zertifikat für jeden API-Aufruf an ONTAP.

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. 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.

Verwandte Informationen

"Benutzer hinzufügen"

"Anzeigen der Cluster-Liste und der Details"

"Installieren einer Zertifizierungsstelle, die signiert ist und ein HTTPS-Zertifikat zurückgegeben hat"

Cluster werden bearbeitet

Sie können die Einstellungen eines vorhandenen Clusters, z. B. Host-Name oder IP-Adresse, Benutzername, Passwort und Port, über das Dialogfeld Cluster bearbeiten ändern.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle oder die Speicheradministratorrolle verfügen.

Ab Unified Manager 9.7 können Cluster nur mit HTTPS hinzugefügt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Cluster-Setup**.
2. Wählen Sie auf der Seite **Cluster Setup** den Cluster aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Cluster bearbeiten** die Werte nach Bedarf. + Wenn Sie die Details für einen zu Unified Manager hinzugefügten Cluster geändert haben, können Sie die Zertifikatdetails für die gegenseitige TLS-Kommunikation basierend auf der ONTAP-Version anzeigen. Weitere Informationen zur ONTAP-Version finden Sie unter "Zertifikate für die gegenseitige TLS-Kommunikation". + Sie können die Zertifikatsdetails anzeigen, indem Sie auf **Zertifikatdetails** klicken. Wenn das Zertifikat abgelaufen ist, klicken Sie auf die Schaltfläche **regenerieren**, um das neue Zertifikat einzubauen.
4. Klicken Sie Auf **Absenden**.

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

Verwandte Informationen

"Benutzer hinzufügen"

"Anzeigen der Cluster-Liste und der Details"

Cluster werden entfernt

Sie können ein Cluster mithilfe der Seite Cluster-Setup aus Unified Manager entfernen. Beispielsweise können Sie ein Cluster entfernen, wenn die Cluster-Erkennung ausfällt oder wenn Sie ein Storage-System stilllegen möchten.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle oder die Speicheradministratorrolle verfügen.

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 **Storage-Management** > **Cluster-Setup**.
2. Wählen Sie auf der Seite Cluster Setup den Cluster aus, den Sie entfernen möchten, und klicken Sie auf **Entfernen**.
3. Klicken Sie im Dialogfeld **Datenquelle entfernen** auf **Entfernen**, um die Anforderung zum Entfernen zu bestätigen.

Verwandte Informationen

"Benutzer hinzufügen"

"Anzeigen der Cluster-Liste und der Details"

Cluster-Erkennung neu ermitteln

Sie können ein Cluster manuell auf der Seite Cluster Setup neu finden, um die neuesten Informationen über den Systemzustand, den Monitoring-Status und den Performance-Status des Clusters abzurufen.

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 **Storage-Management** > **Cluster-Setup**.
2. Klicken Sie auf der Seite **Cluster Setup** auf **Wiederentdecken**.

   Unified Manager erkennt das ausgewählte Cluster erneut und zeigt den neuesten Zustand und Performance-Status an.

Verwandte Informationen

"Anzeigen der Cluster-Liste und der Details"

Monitoring der virtuellen VMware Infrastruktur

Active IQ Unified Manager bietet einen Einblick in die Virtual Machines (VMs) in Ihrer virtuellen Infrastruktur und ermöglicht Monitoring und Fehlerbehebung von Storage- und Performance-Problemen in Ihrer virtuellen Umgebung. Mit dieser Funktion können Sie alle Latenzprobleme in Ihrer Storage-Umgebung ermitteln oder ein gemeldeter Performance-Ereignis auf Ihrem vCenter Server durchführen.

Eine typische Implementierung einer virtuellen Infrastruktur auf ONTAP setzt auf verschiedene Komponenten, die auf Computing-, Netzwerk- und Storage-Ebenen verteilt sind. Alle Performance-Einbußen bei einer VM-Applikation können aufgrund einer Kombination aus Latenzen auftreten, die bei den verschiedenen Komponenten auf den jeweiligen Ebenen auftreten. Diese Funktion ist nützlich für Storage- und vCenter Server-Administratoren und IT-Generalisten, die ein Performance-Problem in einer virtuellen Umgebung analysieren und verstehen müssen, welche Komponente das Problem aufgetreten ist.

Sie können jetzt über das vCenter-Menü im VMware-Abschnitt auf den vCenter Server zugreifen. In der Vorschau jeder aufgeführten virtuellen Maschine befindet sich der **VCENTER SERVER**-Link in der TOPOLOGIEANSICHT, über den der vCenter Server in einem neuen Browser gestartet wird. Sie können den vCenter Server auch mit der Schaltfläche **Expand Topology** starten und auf die Schaltfläche **View in vCenter** klicken, um die Datastores in vCenter Server anzuzeigen.

Unified Manager stellt das zugrunde liegende Untersystem einer virtuellen Umgebung in einer topologischen Übersicht vor, um zu ermitteln, ob beim Computing-Node, Netzwerk oder Storage ein Latenzproblem aufgetreten ist. Die Ansicht zeigt außerdem das spezifische Objekt, das aufgrund der Performance-Verzögerung Korrekturmaßnahmen ergreifen und das zugrunde liegende Problem lösen kann.

Eine auf ONTAP Storage implementierte virtuelle Infrastruktur umfasst folgende Objekte:

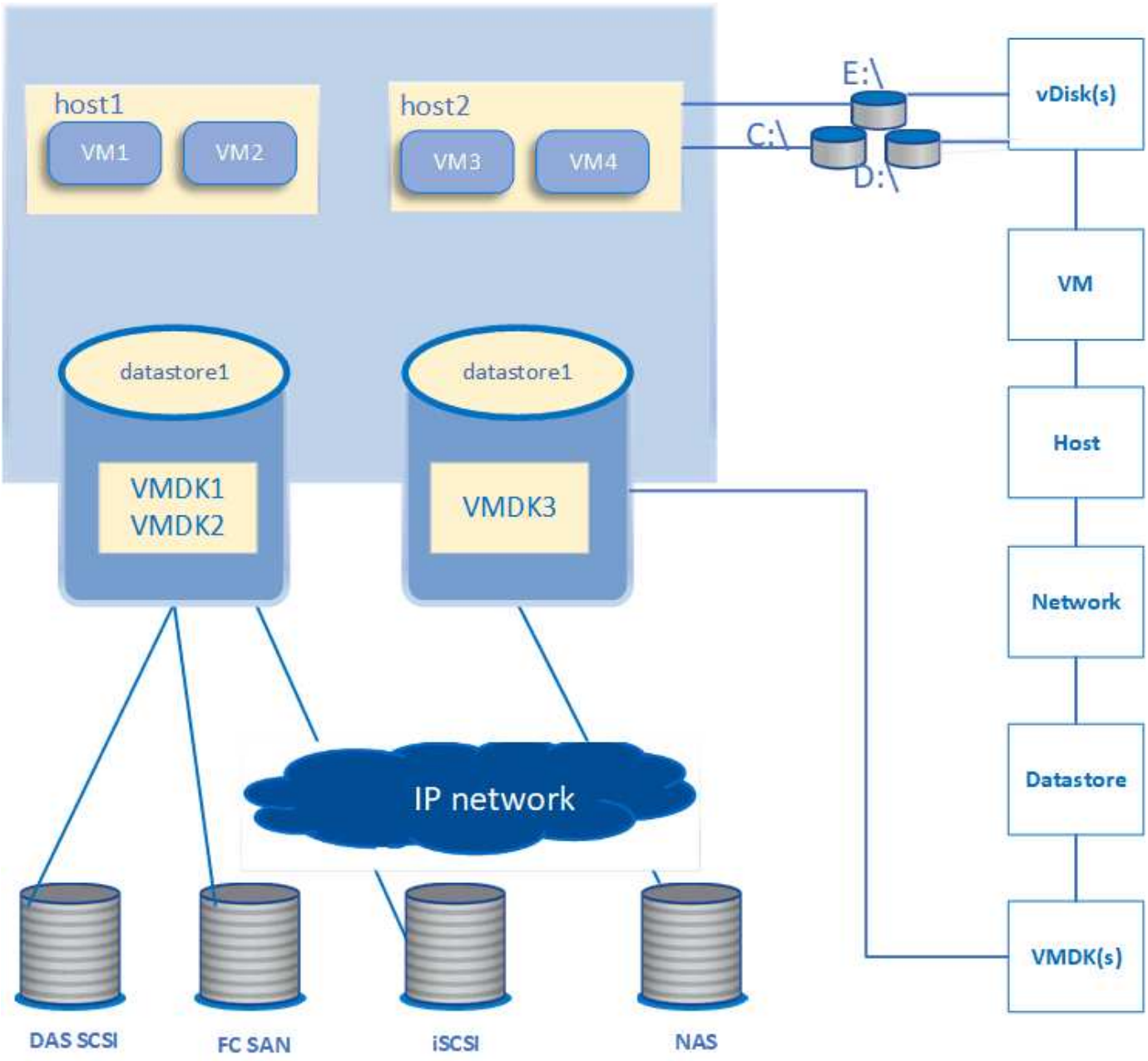
- VCenter Server: Eine zentrale Kontrollebene zum Management von VMware VMs, ESXi Hosts und allen zugehörigen Komponenten in einer virtuellen Umgebung Weitere Informationen zu vCenter Server finden Sie in der VMware-Dokumentation.
- Host: Ein physisches oder virtuelles System, auf dem ESXi ausgeführt wird, die Virtualisierungssoftware von VMware, und hostet die VM.
- Datastore: Datastores sind virtuelle Speicherobjekte, die mit den ESXi-Hosts verbunden sind. Datastores sind verwaltbare Storage-Einheiten von ONTAP, beispielsweise LUNs oder Volumes, die als Repository für VM-Dateien, wie Log-Dateien, Skripte, Konfigurationsdateien und virtuelle Festplatten, verwendet werden. Sie sind über eine SAN- oder IP-Netzwerkverbindung mit den Hosts in der Umgebung verbunden. Datastores außerhalb von ONTAP, die vCenter Server zugeordnet sind, werden auf Unified Manager nicht

unterstützt oder angezeigt.

- VM: Eine virtuelle VMware Maschine.
- Virtuelle Laufwerke: Virtuelle Laufwerke auf Datastores, die zu den VMs gehören und über eine Erweiterung als VMDK verfügen. Die Daten eines virtuellen Laufwerks werden auf der entsprechenden VMDK gespeichert.
- VMDK: Eine virtuelle Maschine im Datenspeicher, die Speicherplatz für virtuelle Laufwerke bereitstellt. Für jedes virtuelle Laufwerk gibt es eine entsprechende VMDK.

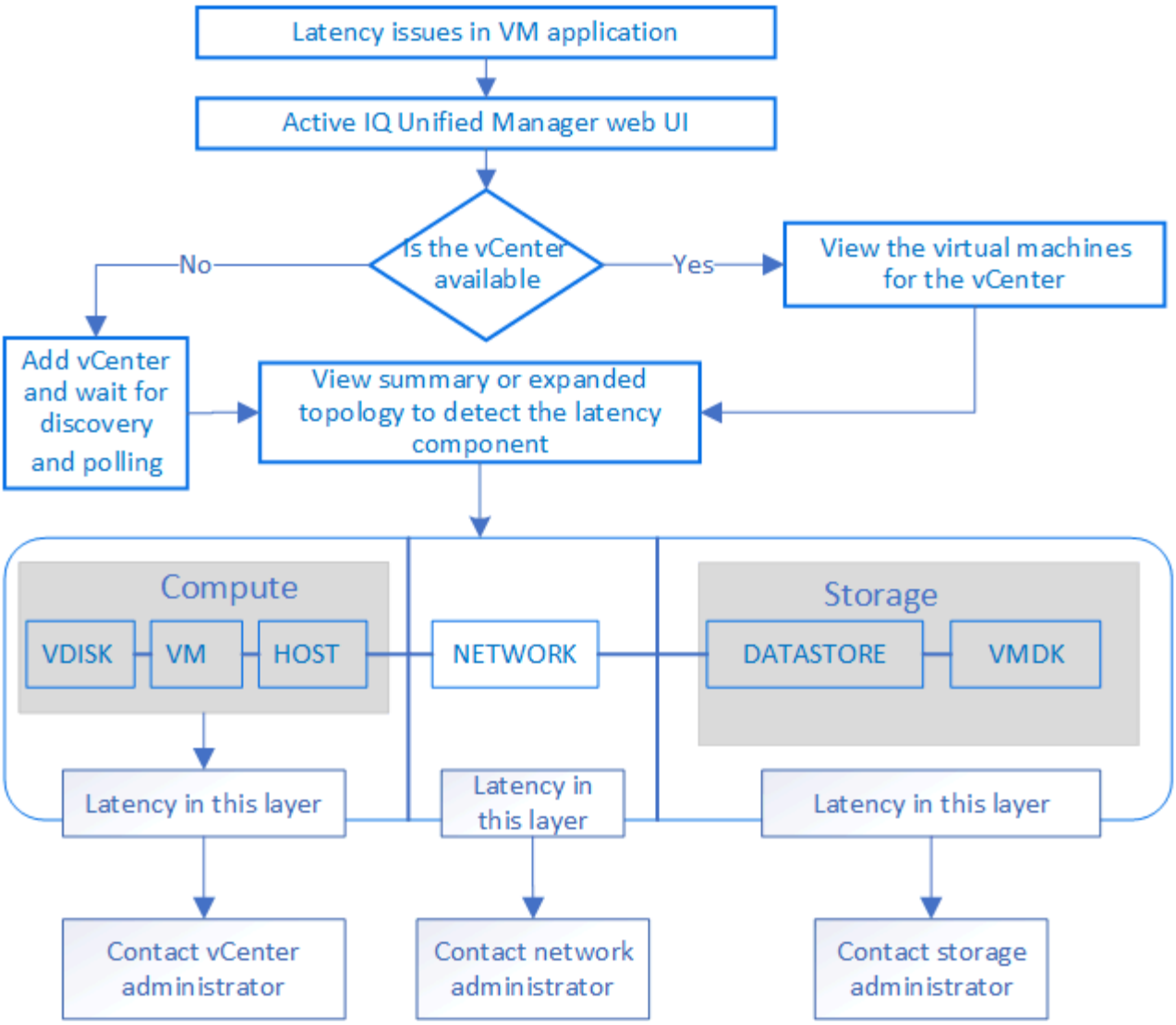
Diese Objekte werden in einer VM-Topologieansicht dargestellt.

VMware Virtualisierung auf ONTAP



Benutzer-Workflow

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



Was nicht unterstützt wird

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

  Beispiel: Angenommen, Cluster A verfügt über Datenspeicher A. Datenspeicher A wird über eine Datenschnittstelle mit derselben IP-Adresse x.x.x.x exportiert und VM A wird auf diesem Datenspeicher erstellt. In ähnlicher Weise verfügt Cluster B über Datenspeicher B. der Datenspeicher B wird über eine Daten-LIF mit derselben IP-Adresse x.x.x.x exportiert und VM B wird auf Datenspeicher B erstellt. Um kann den Datenspeicher A für die Topologie von VM A weder dem entsprechenden ONTAP Volume/LUN zuordnen noch VM B zuordnen

- Nur NAS- und SAN-Volumes (iSCSI und FCP für VMFS) werden als Datenspeicher unterstützt, virtuelle

Volumes (VVols) werden nicht unterstützt.

- Es werden nur virtuelle iSCSI-Festplatten unterstützt. Virtuelle Festplatten mit NVMe- und SATA-Typen werden nicht unterstützt.
- In den Ansichten können Sie keine Berichte zur Analyse der Leistung der verschiedenen Komponenten erstellen.
- Für die Disaster Recovery (DR) Einrichtung der Storage Virtual Machine (Storage VM), die nur für eine virtuelle Infrastruktur in Unified Manager unterstützt wird, muss die Konfiguration manuell in vCenter Server geändert werden, um auf die aktiven LUNs in Switchover- und Switchback-Szenarien zu verweisen. Ohne manuelle Eingriffe sind ihre Datenspeicher nicht mehr zugänglich.

Anzeigen und Hinzufügen von vCenter Server

Um die Performance der Virtual Machines (VMs) anzuzeigen und zu beheben, müssen die zugehörigen vCenter Server in Ihrer Active IQ Unified Manager Instanz hinzugefügt werden.

Was Sie brauchen

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

- Sie kennen die vCenter Server-Namen.
- Sie kennen die IP-Adresse von vCenter Server und verfügen über die erforderlichen Anmeldedaten. Die Anmeldedaten müssen ein vCenter Server-Administrator oder ein Root-Benutzer mit schreibgeschütztem Zugriff auf vCenter Server sein.
- Der vCenter Server, den Sie hinzufügen möchten, führt vSphere 6.5 oder höher aus.

  Unified Manager für VMware ESXi und vCenter Server wird auf Englisch und Japanisch unterstützt.

- Die Datenerfassungseinstellung in vCenter Server wird auf die Statistikebene von gesetzt *`Level 3`*, wodurch die erforderliche Kennzahlenerhebung für alle überwachten Objekte sichergestellt wird. Die Intervalldauer sollte *`5 minutes`* , und die Speicherdauer sollte sein *`1 day`*.

  Weitere Informationen finden Sie im Abschnitt „`Data Collection Levels`“ der Dokumentation zu vSphere Monitoring and Performance Guide_.

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

Bei jedem hinzugefügten und erkannten vCenter Server erfasst Unified Manager die Konfigurationsdaten wie

z. B. die Angaben zu vCenter Server und ESXi Server, die ONTAP-Zuordnung, die Datenspeicherdetails und die Anzahl der gehosteten VMs. Es sammelt weiter die Leistungskennzahlen der Komponenten.

Schritte

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

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

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

      Nach erfolgreicher Ermittlung wird ein Serverzertifikat angezeigt, mit dem Sie akzeptieren können.

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

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

   Beim Hinzufügen von vCenter Server können Sie die folgenden Status anzeigen: Die Performance- und Latenzdaten der entsprechenden VMs können jedoch bis zu eine Stunde dauern, nachdem Sie vCenter Server hinzugefügt haben, um sich exakt wiederspiegeln zu können.

   - Grün: „Normal“, was darauf hinweist, dass vCenter Server erkannt wurde und Leistungskennzahlen erfolgreich erfasst wurden
   - Gelb: „Warnung“ (z. B. wenn die Statistikebene für vCenter Server nicht auf 3 oder höher eingestellt wurde, um Statistiken für jedes Objekt zu erhalten)
   - Orange: "Fehler" (zeigt alle internen Fehler an, wie Ausnahme, Fehler bei der Erfassung von Konfigurationsdaten oder vCenter Server nicht erreichbar) Sie können auf das Spaltenanzeigesymbol (**Anzeigen/Ausblenden**) klicken, um die Statusmeldung für einen vCenter Server-Status anzuzeigen und das Problem zu beheben.

3. Falls vCenter Server nicht erreichbar ist oder sich die Anmeldeinformationen geändert haben, bearbeiten Sie die vCenter Server-Details, indem Sie **vCenter** > **Bearbeiten** wählen.
4. Nehmen Sie die erforderlichen Änderungen auf der Seite **Edit VMware vCenter Server** vor.
5. Klicken Sie Auf **Speichern**.

VCenter Server Datenerfassung beginnt

VCenter Server erfasst in Echtzeit 20-Sekunden-Performance-Datenproben und liefert bis zu 5-Minuten-Proben. Der Zeitplan für die Erfassung von Performance-Daten in Unified Manager basiert auf den Standardeinstellungen von vCenter Server. Unified Manager verarbeitet die 5-minütigen Muster von vCenter

Server und berechnet einen stündlichen Durchschnitt der IOPS und Latenz für die virtuellen Festplatten, VMs und Hosts. Bei Datastores berechnet Unified Manager einen stündlichen Durchschnitt der IOPS und Latenz anhand von ONTAP Proben. Diese Werte stehen am Anfang der Stunde zur Verfügung. Die Leistungskennzahlen sind nicht unmittelbar nach dem Hinzufügen von vCenter Server verfügbar und sind nur verfügbar, wenn die nächste Stunde beginnt. Die Abfrage der Leistungsdaten beginnt mit dem Abschluss eines Zyklus der Erfassung von Konfigurationsdaten.

Für das Abrufen der Konfigurationsdaten von vCenter Server folgt Unified Manager demselben Zeitplan wie beim Erfassen von Cluster-Konfigurationsdaten. Informationen zum Konfigurations- und Performance-Datenerfassungsplan von vCenter Server finden Sie unter „Aktivitäten zur Clusterkonfiguration und Erfassung von Performancedaten“.

Verwandte Informationen

"Aktivitäten zur Cluster-Konfiguration und zur Datenerfassung für die Performance"

VCenter Server wird entfernt

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

Durch das Entfernen eines vCenter Servers werden auch alle virtuellen Maschinen (VMs) gelöscht, die auf diesem vCenter gehostet werden, sowie die zugehörigen Konfigurationsdaten. Nachdem der vCenter Server entfernt wurde, wird er zusammen mit den zugehörigen Objekten und historischen Daten nicht mehr überwacht. Diese Änderungen werden auf den Seiten vCenter und des virtuellen Maschineninventars übernommen.

Was Sie brauchen

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

- Sie verfügen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“.
- Sie sollten die vCenter-Servernamen und die zugehörigen IP-Adressen kennen.

Schritte

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

Monitoring von Virtual Machines

Um Latenzproblem der Virtual Machine (VM)-Applikationen zu beheben, müssen Sie möglicherweise die VMs überwachen, um die Ursache zu analysieren und zu beheben. Die VMs sind verfügbar, wenn ihr vCenter Server und die ONTAP Cluster, die den VM Storage hosten, zu Unified Manager hinzugefügt werden.

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

des Datenspeichers und des Hosts werden angezeigt. Bei einer VM, die mehrere Datastores unterstützt, zeigt das Raster die Kennzahlen des Datenspeichers mit der schlechtesten Latenz an. Dabei ist ein Sternchen (*) für weitere Datenspeicher vorhanden. Wenn Sie auf das Symbol klicken, werden die Metriken des zusätzlichen Datastores angezeigt. Einige dieser Spalten sind nicht zum Sortieren und Filtern verfügbar.

Um eine VM und deren Details anzuzeigen, muss die Erkennung (Abfrage oder Kennzahlensammlung) des ONTAP Clusters abgeschlossen sein. Wenn das Cluster aus Unified Manager entfernt wird, ist die VM nach dem nächsten Erkennungszyklus nicht mehr verfügbar.

Auf dieser Seite können Sie auch die detaillierte Topologie einer VM anzeigen und die zugehörigen Komponenten anzeigen, beispielsweise den Host, das virtuelle Laufwerk und den damit verbundenen Datastore. Die Topologieansicht zeigt die zugrunde liegenden Komponenten in ihrer jeweiligen Ebene in der folgenden Reihenfolge an: **Virtual Disk** > **VM** > **Host** > **Netzwerk** > **Datastore** > **VMDK**.

Ermitteln Sie den I/O-Pfad und die Latenzen auf Komponentenebene anhand eines topologischen Aspekts und ermitteln, ob Storage die Ursache des Performance-Problems ist. In der Übersichtsansicht der Topologie wird der I/O-Pfad angezeigt und die Komponente mit IOPS- und Latenzproblemen hervorgehoben, damit Sie die Schritte zur Fehlerbehebung bestimmen können. Es besteht außerdem die Möglichkeit, eine erweiterte Ansicht der Topologie, in der jede Komponente separat dargestellt wird, sowie eine größere Latenz der Komponente. Sie können eine Komponente auswählen, um den durch die Ebenen markierten E/A-Pfad zu bestimmen.

Anzeigen der zusammenfassenden Topologie

Zur Ermittlung von Performance-Problemen durch Anzeige der VMs in einer zusammengefassten Topologie:

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

   VCenter Server ermöglichen Sonderzeichen (z. B. %, &, *, €, #, @, !, \, /, :, *, ?, "`, <, >, ;, ') im Namen von vSphere Einheiten wie VM, Cluster, Datenspeicher, Ordner, Oder Datei. Der VMware vCenter Server und ESX/ESXi Server entweichen keine Sonderzeichen, die in den Anzeigenamen verwendet werden. Wenn der Name jedoch in Unified Manager verarbeitet wird, wird er anders angezeigt. Beispielsweise wird in Unified Manager eine VM mit dem Namen als `%$VC_AIQUM_clone_191124%` in vCenter Server angezeigt `%25$VC_AIQUM_clone_191124%25`. Sie müssen dieses Problem notieren, wenn Sie eine VM mit einem Namen mit Sonderzeichen abfragen.

3. Den Status der VM überprüfen. Die VM-Status werden vom vCenter Server abgerufen. Folgende Status stehen zur Verfügung. Weitere Informationen zu diesen Status finden Sie in der VMware-Dokumentation.
   - Normal
   - Warnung
   - Alarm
   - Nicht überwacht
   - Unbekannt
4. Klicken Sie auf den nach-unten-Pfeil neben der VM, um eine zusammenfassende Ansicht der Topologie der Komponenten auf Computing-, Netzwerk- und Storage-Ebenen anzuzeigen. Der Node mit Latenzproblemen ist hervorgehoben. Die Zusammenfassung zeigt die schlechteste Latenz der

Komponenten an. Wenn eine VM beispielsweise mehr als ein virtuelles Laufwerk hat, zeigt diese Ansicht das virtuelle Laufwerk an, das die schlechteste Latenz aller virtuellen Laufwerke hat.

5. Um die Latenz und den Durchsatz des Datastore über einen bestimmten Zeitraum zu analysieren, klicken Sie oben im Datastore-Objektsymbol auf die Schaltfläche **Workload Analyzer**. Sie rufen die Seite Workload Analysis auf. Dort können Sie einen Zeitbereich auswählen und die Performance-Diagramme des Datastores anzeigen. Weitere Informationen zur Workload-Analyse finden Sie unter *Fehlerbehebung von Workloads mithilfe des Workload Analyzer*.

Anzeigen der erweiterten Topologie

Sie können die einzelnen Komponenten separat anzeigen, indem Sie die erweiterte Topologie der VM anzeigen.

Schritte

1. Klicken Sie in der Topologieübersicht auf **Expand Topology**. Die detaillierte Topologie jeder Komponente lässt sich separat mit den Latenzzahlen für jedes Objekt anzeigen. Wenn in einer Kategorie mehrere Nodes vorhanden sind, zum Beispiel mehrere Nodes im Datastore oder VMDK, ist der Node mit der schlechtesten Latenz rot markiert.
2. Um den IO-Pfad eines bestimmten Objekts zu überprüfen, klicken Sie auf das Objekt, um den IO-Pfad und die entsprechende Zuordnung anzuzeigen. Um beispielsweise die Zuordnung eines virtuellen Laufwerks anzuzeigen, klicken Sie auf das virtuelle Laufwerk, um die markierte Zuordnung zur jeweiligen VMDK anzuzeigen. Im Fall einer Performance-Verzögerung dieser Komponenten können Sie mehr Daten von ONTAP erfassen und das Problem beheben.

Metriken werden nicht für VMDKs gemeldet. In der Topologie werden nur die VMDK-Namen angezeigt, nicht Metriken.

Verwandte Informationen

"Fehlerbehebung bei Workloads mit der Workload Analyzer"

Anzeige virtueller Infrastrukturen in Disaster-Recovery-Setups

Sie können die Konfigurations- und Performance-Kennzahlen der Datastores anzeigen, die in einer MetroCluster Konfiguration oder in einer Storage Virtual Machine (Storage VM) Disaster Recovery (SVM DR)-Einrichtung gehostet werden.

Bei Unified Manager können Sie die NAS-Volumes oder LUNs in einer MetroCluster-Konfiguration anzeigen, die als Datastores in vCenter Server verbunden sind. Die in einer MetroCluster-Konfiguration gehosteten Datenspeicher werden in der gleichen topologischen Ansicht dargestellt wie ein Datenspeicher in einer Standardumgebung.

Sie können auch die NAS-Volumes oder LUNs in einer Storage-VM-Disaster-Recovery-Konfiguration anzeigen, die den Datastores in vCenter Server zugeordnet sind.

Anzeigen von Datastores in der MetroCluster-Konfiguration

Beachten Sie die folgenden Voraussetzungen vor dem Anzeigen von Datastores in einer MetroCluster Konfiguration:

- Bei einem Switchover und einem Wechsel zurück sollte die Erkennung der primären und sekundären Cluster des HA-Paars und der vCenter Server abgeschlossen sein.

- Die primären und sekundären Cluster des HA-Paars und vCenter Server müssen durch Unified Manager gemanagt werden.
- Die erforderliche Einrichtung muss auf ONTAP und vCenter Server abgeschlossen sein. Weitere Informationen finden Sie in der Dokumentation zu ONTAP und vCenter.

  "ONTAP 9 Dokumentationszentrum"

Führen Sie die folgenden Schritte zum Anzeigen von Datastores aus:

1. Klicken Sie auf der Seite **VMWARE** > **Virtuelle Maschinen** auf die VM, die den Datenspeicher hostet. Klicken Sie auf den Link **Workload Analyzer** oder den Datastore-Objekt. Im Standardszenario, wenn der primäre Standort, der das Volume oder LUN hostet, wie erwartet funktioniert, sehen Sie die Vserver Cluster Details des primären Standorts.
2. Bei einem Ausfall und einer fortlaufenden Umschaltung auf den sekundären Standort verweist der Datastore auf die Performance-Kennzahlen des Volume oder der LUN im sekundären Cluster. Dies spiegelt sich nach dem nächsten Cluster-Zyklus wider und die Ermittlung von Vserver (Akquisition) ist abgeschlossen.
3. Nach dem erfolgreichen Wechsel zurück gibt der Datastore-Link die Performance-Metriken des Volume oder der LUN im primären Cluster wieder. Dies spiegelt sich nach dem nächsten Cluster-Zyklus wieder und die Vserver Erkennung ist abgeschlossen.

Anzeigen von Datenspeichern in der Konfiguration der Disaster Recovery von Storage-VM

Beachten Sie die folgenden Voraussetzungen, bevor Sie Datastores in einer Disaster-Recovery-Konfiguration einer Storage-VM anzeigen:

- Bei einem Switchover und einem Wechsel zurück sollte die Erkennung der primären und sekundären Cluster des HA-Paars und der vCenter Server abgeschlossen sein.
- Peers sollten die Cluster an der Quelle und am Ziel sowie die Storage VM-Experten von Unified Manager managen.
- Die erforderliche Einrichtung muss auf ONTAP und vCenter Server abgeschlossen sein.
  - Für NAS-Datastores (NFS und VMFS) im Katastrophenfall beinhalten die Schritte das Einrichten der sekundären Storage VM, die Überprüfung der Daten-LIFs und -Routen, die Einrichtung verlorener Verbindungen auf dem vCenter Server und das Starten der VMs.

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

  - Für SAN-Datastores (iSCSI und FC für VMFS) formatiert vCenter Server die gemountete LUN in einem VMFS-Format. Bei einem Notfall besteht das darin, die sekundäre Storage-VM zu erstellen und die Daten-LIFs und -Routen zu überprüfen. Wenn sich die iSCSI-Ziel-IPs von den primären LIFs unterscheiden, müssen sie manuell hinzugefügt werden. Die neuen LUNs sollten als Geräte unter dem iSCSI-Adapter des Speicheradapters des Hosts verfügbar sein. Danach sollten neue VMFS Datastores mit den neuen LUNs erstellt und die alten VMs mit neuen Namen registriert werden. Die VMs müssen betriebsbereit sein.

    Im Falle einer Wiederherstellung sollten die Daten zwischen den Volumes synchronisiert werden. Neue VMFS Datastores sollten erneut mit den LUNs erstellt werden und die alten, mit neuen Namen registrierten VMs.

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

"ONTAP 9 Dokumentationszentrum"

Führen Sie die folgenden Schritte zum Anzeigen von Datastores aus:

1. Klicken Sie auf der Seite **VMWARE** > **Virtuelle Maschinen** auf den VM-Bestand, der den Datenspeicher hostet. Klicken Sie auf den Link zum Datastore-Objekt. In dem Standardszenario sehen Sie die Performance-Daten der Volumes und LUNs in der primären Storage-VM.
2. Bei einem Ausfall und einer fortlaufenden Umschaltung auf die sekundäre Storage-VM verweist der Datastore auf die Performance-Kennzahlen des Volumes oder der LUN in der sekundären Storage-VM. Dies spiegelt sich nach dem nächsten Cluster-Zyklus wider und die Ermittlung von Vserver (Akquisition) ist abgeschlossen.
3. Nach dem erfolgreichen Wechsel wieder gibt der Datastore-Link die Performance-Kennzahlen des Volume oder der LUN in der primären Storage-VM wieder. Dies spiegelt sich nach dem nächsten Cluster-Zyklus wieder und die Vserver Erkennung ist abgeschlossen.

Nicht unterstützte Szenarien

- Beachten Sie bei einer MetroCluster-Konfiguration die folgenden Einschränkungen:
  - Cluster nur in den `NORMAL` Zuständen und `SWITCHOVER` werden aufgenommen. Andere Staaten wie `PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK`, und `NOT_REACHABLE` werden nicht unterstützt.
  - Wenn das primäre Cluster ausfällt, kann das sekundäre Cluster nicht erkannt werden, sofern nicht Automatic Switch over (ASO) aktiviert ist und die Topologie weiterhin auf das Volume oder die LUN im primären Cluster verweist.
- Beachten Sie bei einer Storage-VM-Konfiguration für die Disaster Recovery folgende Einschränkung:
  - Eine Konfiguration mit Site Recovery Manager (SRM) oder Storage Replication Adapter (SRA), die für eine SAN-Storage-Umgebung aktiviert ist, wird nicht unterstützt.

Bereitstellung und Management von Workloads

Die aktive Managementfunktion von Active IQ Unified Manager bietet Performance-Service-Level, Richtlinien für Storage-Effizienz und APIs von Storage-Providern für Provisionierung, Monitoring und Management von Storage-Workloads in einem Datacenter.

Unified Manager bietet diese Funktion standardmäßig. Sie können es über **Storage Management** > **Feature-Einstellungen** deaktivieren, wenn Sie diese Funktion nicht nutzen möchten.

Wenn diese Option aktiviert ist, können Sie Workloads auf den ONTAP Clustern bereitstellen, die von Ihrer Instanz von Unified Manager gemanagt werden. Es können Richtlinien wie z. B. Performance Service Levels und Storage-Effizienz-Richtlinien für die Workloads zugewiesen und die Storage-Umgebung basierend auf diesen Richtlinien gemanagt werden.

Diese Funktion ermöglicht folgende Funktionen:

- Automatisches Erkennen von Storage-Workloads auf den zusätzlichen Clustern für eine einfache Evaluierung und Implementierung von Storage-Workloads
- Bereitstellung von NAS-Workloads, die NFS- und CIFS-Protokolle unterstützen

- Bereitstellen von SAN-Workloads, die iSCSI- und FCP-Protokolle unterstützen
- Unterstützung für NFS- und CIFS-Protokolle auf demselben File Share
- Management von Performance Service Levels und Richtlinien für Storage-Effizienz
- Zuweisung von Performance Service Levels und Storage-Effizienz-Richtlinien für Storage Workloads

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

Sie können folgende Funktionen ausführen, indem Sie folgende Optionen verwenden:

- Anzeige von Speicher-Workloads auf der Seite **Storage** > **Workloads**
- Erstellen Sie Storage-Workloads auf der Seite „Workloads bereitstellen“
- Erstellung und Management von Performance-Service-Levels anhand von Richtlinien
- Erstellung und Management von Storage-Effizienz-Richtlinien aus Richtlinien
- Weisen Sie Storage-Workloads Richtlinien über die Seite Workloads zu

Verwandte Informationen

"Richtlinienbasiertes Storage-Management"

Workload-Überblick

Ein Workload repräsentiert die I/O-Vorgänge (Input/Output, I/O) eines Storage-Objekts, z. B. eines Volumes oder einer LUN. Die Art der Storage-Bereitstellung basiert auf den erwarteten Workload-Anforderungen. Workload-Statistiken werden von Active IQ Unified Manager nur nachverfolgt, nachdem der Datenverkehr zum und vom Storage-Objekt erfolgt ist. Beispielsweise sind die IOPS-Werte und die Latenzwerte von Workloads verfügbar, nachdem Benutzer eine Datenbank oder E-Mail-Applikation verwenden.

Auf der Seite Workloads wird eine Zusammenfassung der Storage Workloads der von Unified Manager gemanagten ONTAP Cluster angezeigt. Das Tool liefert auf einen Blick kumulative Informationen über Storage Workloads, die dem Performance-Service-Level entsprechen, und die nicht konformen Storage Workloads. Außerdem können Sie die Gesamtkapazität, die verfügbare und die genutzte Kapazität und Performance (IOPS) der Cluster im Datacenter bewerten.

> Es wird empfohlen, die Anzahl der Storage Workloads zu bewerten, die nicht dem Performance-Service-Level entsprechen, nicht verfügbar sind oder nicht durch ein Performance-Service-Level gemanagt werden, und die erforderlichen Maßnahmen zu ergreifen, um die Konformität, Kapazitätsauslastung und IOPS zu gewährleisten.

Die Seite Workloads enthält die folgenden zwei Abschnitte:

- Übersicht Workloads: Übersicht über die Anzahl der Storage Workloads auf den durch Unified Manager gemanagten ONTAP Clustern
- Datacenter-Überblick: Bietet einen Überblick über die Kapazität und IOPS der Storage Workloads im Datacenter. Die relevanten Daten werden auf der Rechenzentrumsebene und für den Einzelnen angezeigt.

Übersicht über Workloads

Der Abschnitt Workloads im Überblick bietet einen Überblick über alle gesammelten Informationen zu den Storage Workloads. Der Status der Storage-Workloads wird auf Grundlage von zugewiesenen und nicht zugewiesenen Performance-Service-Leveln angezeigt.

- **Assigned**: Für Storage Workloads, denen Performance Service Levels zugewiesen wurden, werden die folgenden Status gemeldet:
  - **Konform**: Performance von Storage Workloads basiert auf den ihnen zugewiesenen Performance-Service-Leveln. Wenn die Storage-Workloads die im zugehörigen Performance-Service-Level definierte Schwellenwert erreichen, sind sie als „`konform`“ gekennzeichnet. Die entsprechenden Workloads sind in blau gekennzeichnet.
  - **Nicht konform**: Storage Workloads sind beim Performance-Monitoring mit „`nicht konform`“ gekennzeichnet, wenn die Latenz der Storage Workloads den im zugehörigen Performance Service Level definierten Schwellwert überschreitet. Die nicht konformen Workloads sind orange gekennzeichnet.
  - **Nicht verfügbar**: Speicher-Workloads werden als „`nicht verfügbar`“ markiert, wenn sie offline sind oder wenn das entsprechende Cluster nicht erreichbar ist. Die nicht verfügbaren Workloads sind rot markiert.
- **Nicht zugewiesen**: Speicher-Workloads, denen kein Performance-Service-Level zugewiesen ist, werden als „`nicht zugewiesen`“ gemeldet. Die Nummer wird über das Informationssymbol angezeigt.

Die Gesamtzahl der Workloads ergibt sich aus der Summe der zugewiesenen und nicht zugewiesenen Workloads.

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

Im Unterabschnitt Performance by Performance Service Levels wird die Gesamtzahl der verfügbaren Storage Workloads angezeigt:

- Entsprechend jeder Art von Performance Service Level
- Für die es eine Diskrepanz zwischen den zugewiesenen und den empfohlenen Leistungsservicestufen gibt

Bereich „Datacenter Overview“

Der Abschnitt mit der Übersicht des Datacenters stellt die verfügbare und genutzte Kapazität sowie die IOPS für alle Cluster im Datacenter grafisch dar. Mithilfe dieser Daten sollten Sie die Kapazität und IOPS der Storage Workloads managen. Im Abschnitt werden auch die folgenden Informationen für Storage-Workloads in allen Clustern angezeigt:

- Die verfügbare Gesamtkapazität und genutzte Kapazität aller Cluster in Ihrem Datacenter
- Die insgesamt verfügbaren, verfügbaren und genutzten IOPS für alle Cluster im Datacenter
- Die verfügbare und genutzte Kapazität basiert auf dem jeweiligen Performance Service Level
- Die verfügbaren und verwendeten IOPS basierend auf dem jeweiligen Performance Service Level
- Der gesamte Speicherplatz und die IOPS, die von den Workloads verwendet werden, denen kein Performance Service Level zugewiesen ist

Wie Kapazität und Performance des Rechenzentrums auf Basis von Performance Service Levels berechnet wird

Die genutzte Kapazität und IOPS werden hinsichtlich der insgesamt genutzten Kapazität und Performance aller Storage-Workloads im Cluster abgerufen.

Die verfügbaren IOPS werden auf Basis der erwarteten Latenz und der empfohlenen Performance-Service-Level auf den Nodes berechnet. Es enthält die verfügbaren IOPS für alle Performance-Service-Level, deren erwartete Latenz kleiner als oder gleich der eigenen erwarteten Latenz ist.

Die verfügbare Kapazität wird auf Grundlage der erwarteten Latenz und der empfohlenen Performance-Service-Level für Aggregate berechnet. Sie beinhaltet die verfügbare Kapazität aller Performance-Service-Level, deren erwartete Latenz kleiner als oder gleich der eigenen erwarteten Latenz ist.

Anzeigen von Workloads

Wenn Sie Unified Manager Cluster hinzufügen, werden die Storage-Workloads jedes Clusters automatisch erkannt und auf der Seite Workloads angezeigt.

Unified Manager beginnt mit der Analyse der Workloads auf Empfehlung (Empfohlene PSLs) erst, nachdem I/O-Vorgänge für die Storage-Workloads gestartet wurden.

FlexGroup Volumes und zugehörige Komponenten sind nicht enthalten.

Workload-Überblick

Auf der Seite „Workload Overview“ wird eine Übersicht über die Workloads im Datacenter sowie eine Übersicht über Speicherplatz und Performance im Datacenter angezeigt.

- **Workloads Übersicht** Panel: Zeigt die Gesamtzahl der Workloads und die Anzahl der Workloads mit oder ohne PSLs an, die ihnen zugewiesen sind. Der Aufbruch der Workload-Anzahl für jede PSL wird ebenfalls angezeigt. Wenn Sie auf die Zählwerte klicken, gelangen Sie zur Ansicht **Alle Workloads** mit den gefilterten Workloads. Sie können auch die Anzahl der Workloads anzeigen, die der Systemempfehlung nicht entsprechen, und ihnen die vom System empfohlenen PSLs zuweisen, indem Sie auf die Schaltfläche **System-Recommended PSLs** klicken.
- **Data Center Overview** Panel: Zeigt den verfügbaren und genutzten Speicherplatz (tib) und die Leistung (IOPS) des Rechenzentrums an. Es wird außerdem ein Aufbruch des verfügbaren und genutzten Speicherplatzes (tib) und der Performance (IOPS) aller Workloads unter den einzelnen PSL angezeigt.

Ansicht aller Workloads

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

Für die neu erkannten Storage-Workloads, für die es keine I/O-Vorgänge gab, lautet der Status „`Warten auf I/O`“. Nachdem der I/O-Betrieb auf den Storage Workloads gestartet wurde, startet Unified Manager die Analyse und ändert sich der Workload-Status in „`Learning…`“. Nach Abschluss der Analyse (innerhalb von 24 Stunden nach Beginn der I/O-Vorgänge) werden die empfohlenen PSLs für die Storage-Workloads angezeigt.

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

- Hinzufügen oder Bereitstellen von Storage Workloads
- Liste der Workloads anzeigen und filtern
- Weisen Sie Storage-Workloads PSLs zu
- Systemempfehlungen bewerten und Workloads zuweisen

- Weisen Sie SEPs Storage Workloads zu

Hinzufügen oder Bereitstellen von Storage Workloads

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

Schritte

1. Klicken Sie Auf **Storage > Workloads > Alle Workloads > Erstellen**.
2. Workloads erstellen. Weitere Informationen finden Sie unter "Bereitstellung und Management von Workloads".

Anzeigen und Filtern von Workloads

Im Bildschirm Alle Workloads können Sie alle Workloads in Ihrem Datacenter anzeigen oder anhand der zugehörigen PSLs oder Namen nach bestimmten Storage Workloads suchen. Über das Filtersymbol können Sie spezifische Bedingungen für Ihre Suche eingeben. Sie können unterschiedliche Filterbedingungen suchen, z. B. nach dem Host-Cluster oder der Storage-VM. Die Option **Capacity Total** ermöglicht das Filtern nach der Gesamtkapazität der Workloads (nach MB). In diesem Fall kann jedoch die Anzahl der zurückgegebenen Workloads variieren, da die Gesamtkapazität auf Byte-Ebene verglichen wird.

Für jeden Workload werden Informationen wie das Host-Cluster und die Speicher-VM zusammen mit den zugewiesenen PSL und SEP angezeigt.

Auf der Seite können Sie auch die Performance-Details eines Workloads anzeigen. Sie können detaillierte Informationen über die IOPS, Kapazität und Latenz des Workloads anzeigen, indem Sie auf die Schaltfläche **Spalten auswählen / Reihenfolge** klicken und bestimmte Spalten auswählen, die angezeigt werden sollen. In der Spalte „Performance View“ werden die durchschnittlichen und Spitzen-IOPS für einen Workload angezeigt. Durch Klicken auf das Symbol für die Workload-Analyse wird die detaillierte IOPS-Analyse angezeigt.

Analyse der Performance- und Kapazitätskriterien für einen Workload

Die Schaltfläche **Analyse Workload** im Pop-up * IOPS-Analyse* führt Sie zur Seite Workload-Analyse, auf der Sie einen Zeitbereich auswählen und die Latenz-, Durchsatz- und Kapazitätstrends für den ausgewählten Workload anzeigen können. Weitere Informationen zum Workload Analyzer finden Sie unter "Fehlersuche bei Workloads mithilfe der Workload Analyzer".

Sie können Leistungsinformationen über einen Workload anzeigen, um bei der Fehlerbehebung zu helfen, indem Sie auf das Balkendiagramm-Symbol in der Spalte **Performance View** klicken. Um Performance- und Kapazitätsdiagramme auf der Seite Workload Analysis anzuzeigen, um das Objekt zu analysieren, klicken Sie auf die Schaltfläche **Workload analysieren**.

Weitere Informationen finden Sie unter "Welche Daten werden vom Workload Analyzer angezeigt".

Zuweisung von Richtlinien zu Workloads

Sie können Storage-Workloads auf der Seite Alle Workloads mit verschiedenen Navigationsoptionen Storage Efficiency Policies (SEPs) und Performance Service Levels (PSLs) zuweisen.

Zuweisen von Richtlinien zu einem einzelnen Workload

Sie können eine PSL oder eine SEP oder beide für einen einzelnen Workload zuweisen. Führen Sie hierzu

folgende Schritte aus:

1. Wählen Sie den Workload aus.
2. Klicken Sie auf das Bearbeiten-Symbol neben der Zeile und dann auf **Bearbeiten**.

   Die Felder **zugewiesene Performance Service Level** und **Storage Efficiency Policy** sind aktiviert.
3. Wählen Sie die erforderliche PSL oder SEP oder beides aus.
4. Klicken Sie auf das Häkchen-Symbol, um die Änderungen anzuwenden.

Sie können auch einen Workload auswählen und auf **Mehr Aktionen** klicken, um die Richtlinien zuzuweisen.

Zuweisung von Richtlinien zu mehreren Storage Workloads

Sie können eine PSL oder eine SEP mehreren Storage Workloads zuweisen. Führen Sie hierzu folgende Schritte aus:

1. Aktivieren Sie die Kontrollkästchen für die Workloads, denen die Richtlinie zugewiesen werden soll, oder wählen Sie alle Workloads in Ihrem Datacenter aus.
2. Klicken Sie Auf **Weitere Aktionen**.
3. Wählen Sie zum Zuweisen einer PSL * Performance Service Level zuweisen* aus. Wählen Sie für die Zuweisung eines SEP * Storage-Effizienz-Policy zuweisen* aus. Es wird ein Popup-Fenster angezeigt, in dem Sie die Richtlinie auswählen können.
4. Wählen Sie die entsprechende Richtlinie aus und klicken Sie auf **Anwenden**. Es werden die Anzahl der Workloads angezeigt, denen die Richtlinien zugewiesen sind. Die Workloads, in denen Richtlinien nicht zugewiesen sind, werden ebenfalls mit der Ursache aufgeführt.

Das Anwenden von Richtlinien auf große Workloads kann je nach Anzahl der ausgewählten Workloads eine gewisse Zeit in Anspruch nehmen. Sie können auf die Schaltfläche **Ausführen im Hintergrund** klicken und mit anderen Aufgaben fortfahren, während der Vorgang im Hintergrund ausgeführt wird. Wenn die Massenzuweisung abgeschlossen ist, können Sie den Status des Abschlusses anzeigen. Wenn Sie eine PSL auf mehrere Workloads anwenden, können Sie keine andere Anforderung auslösen, wenn der vorherige Auftrag der Massenzuweisung ausgeführt wird.

Zuweisen von systemempfohlenen PSLs zu Workloads

Sie können den Speicher-Workloads in einem Rechenzentrum, das keine PSLs zugewiesen hat, systemempfohlene PSLs zuweisen, oder die zugewiesenen PSLs stimmen nicht mit der Systemempfehlung überein. Um diese Funktionalität zu nutzen, klicken Sie auf die Schaltfläche **System Empfohlene PSLs**. Es müssen keine spezifischen Workloads ausgewählt werden.

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

Es gibt spezielle Schlüsselwörter, nach denen Unified Manager im Workload-Namen sucht, um die Systemanalysen außer Kraft zu setzen und eine andere PSL für den Workload zu empfehlen. Wenn die Arbeitslast die Buchstaben “ora” im Namen hat, wird das **Extreme Performance**PSL empfohlen. Und wenn der Workload die Buchstaben “vm” im Namen hat, wird das **Performance**PSL empfohlen.

Siehe auch den Artikel der Knowledge Base (KB) "ActiveIQ Unified Manager „Assign System Recommended Performance Service Level“ ist nicht an einen hochgradig variablen Workload angepasst"

Bereitstellen von Dateifreigabe-Volumes

Sie können Dateifreigabe-Volumes erstellen, die CIFS/SMB- und NFS-Protokolle unterstützen, auf einem vorhandenen Cluster und auf der Seite Storage Virtual Machine (Storage VM) für Bereitstellungs-Workloads.

Was Sie brauchen

- Die Storage-VM muss Platz haben, um das Dateifreigabvolume bereitzustellen.
- Auf Ihrer Storage VM sollten entweder oder beide SMB- und NFS-Services aktiviert werden.
- Für die Auswahl und Zuweisung des Performance Service Level (PSL) und der Storage Efficiency Policy (SEP) für den Workload müssen die Richtlinien erstellt werden, bevor Sie mit der Erstellung des Workloads beginnen.

Schritte

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

   Basierend auf den von der Storage-VM unterstützten SMB- und NFS-Services ist die NAS-Option im Abschnitt „Hostinformationen“ aktiviert.

3. Weisen Sie im Abschnitt Speicher und Optimierung die Speicherkapazität und PSL zu und optional einen SEP für den Workload.

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

4. Aktivieren Sie das Kontrollkästchen **Leistungsgrenzen erzwingen**, wenn Sie die PSL durchsetzen möchten, die Sie dem Workload zugewiesen haben.

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

   Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird die PSL nicht auf den Workload angewendet, und der Status des Workloads auf dem Dashboard wird als nicht zugewiesen angezeigt.

5. Wählen Sie die Option **NAS**.

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

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

6. Geben Sie bei NFS-Dateifreigabedatenvolumes die IP-Adresse des Hosts oder Netzwerks an, um auf das Dateifreigabvolume zuzugreifen. Sie können kommagetrennte Werte für mehrere Hosts eingeben.

   Beim Hinzufügen der Host-IP-Adresse wird eine interne Überprüfung ausgeführt, um die Hostdetails mit der Storage-VM zu übereinstimmen und die Exportrichtlinie für diesen Host zu erstellen. Im Fall einer bestehenden Richtlinie wird sie zudem wiederverwendet. Wenn mehrere NFS Shares für denselben Host erstellt wurden, wird für alle File Shares eine verfügbare Exportrichtlinie für denselben Host mit übereinstimmenden Regeln verwendet. Die Funktion, Regeln für einzelne Richtlinien festzulegen oder Richtlinien neu zu verwenden, indem bestimmte Richtlinienschlüssel bereitgestellt werden, ist verfügbar, wenn Sie die NFS-Freigabe über APIs bereitstellen.

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

   Der Workload wird der Liste der Storage Workloads hinzugefügt.

Bereitstellung von LUNs

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

Was Sie brauchen

- Die Storage-VM muss Platz für die Bereitstellung der LUN haben.
- ISCSI und FCP müssen auf der Storage VM aktiviert sein, auf der Sie die LUN erstellen.
- Für die Auswahl und Zuweisung des Performance Service Level (PSL) und der Storage Efficiency Policy (SEP) für den Workload müssen die Richtlinien erstellt werden, bevor Sie mit der Erstellung des Workloads beginnen.

Schritte

1. Fügen Sie auf der Seite **Workloads bereitstellen** den Namen des Workloads hinzu, den Sie erstellen möchten, und wählen Sie dann den Cluster aus der Liste verfügbar aus.

   Basierend auf dem ausgewählten Cluster filtert das Feld **STORAGE VM** die verfügbaren Storage VMs für diesen Cluster.

2. Wählen Sie die Storage VM aus der Liste aus, die die iSCSI- und FCP-Services unterstützt.

   Je nach Ihrer Auswahl ist die SAN-Option im Abschnitt Hostinformationen aktiviert.

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

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

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

   Durch die Zuweisung einer PSL zu einem Workload wird sichergestellt, dass das Aggregat, auf dem der Workload erstellt wird, die in der jeweiligen Richtlinie definierten Performance- und Kapazitätsziele unterstützen kann. Wenn einem Workload beispielsweise die PSL „Extreme Performance“ zugewiesen wird, sollte das Aggregat, auf dem der Workload bereitgestellt werden soll, die Performance- und Kapazitätsziele der Richtlinie „Extreme Performance“ unterstützen, z. B. SSD Storage.

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

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

   Wenn Sie eine neue Initiatorgruppe erstellen während Sie die LUN bereitstellen, müssen Sie bis zum nächsten Erkennungszyklus (bis zu 15 Minuten) warten, um sie zu verwenden. Daher wird empfohlen, eine vorhandene Initiatorgruppe aus der Liste der verfügbaren Initiatorgruppen zu verwenden.

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

8. Klicken Sie Auf **Speichern**.

   Die LUN wird der Liste der Storage Workloads hinzugefügt.

Performance Service Level

Mit einem Performance Service Level (PSL) können Sie die Performance- und Speicherziele für einen Workload definieren. Sie können eine PSL einem Workload beim ersten Erstellen des Workloads zuweisen oder anschließend den Workload bearbeiten.

Das Management und die Überwachung von Storage-Ressourcen basieren auf Service Level Objectives (SLOs). Sie werden über Service-Level-Agreements definiert, die auf der erforderlichen Performance und Kapazität basieren. In Unified Manager beziehen sich SLOs auf die PSL-Definitionen der Applikationen, die auf NetApp Storage ausgeführt werden. Storage-Services werden nach der Performance und Auslastung der zugrunde liegenden Ressourcen differenziert. Ein PSL ist eine Beschreibung der Speicherserviceziele. Ein

PSL ermöglicht es dem Storage-Provider, die Performance- und Kapazitätsziele für den Workload festzulegen. Wenn Sie eine PSL für einen Workload zuweisen, wird der entsprechende Workload auf ONTAP durch seine Performance- und Kapazitätsziele verwaltet. Jede PSL unterliegt Spitzenwerten, erwarteten und absoluten IOPS-Minimums sowie der erwarteten Latenz.

Unified Manager verfügt über die folgenden PSLs:

- **System-Defined**: Unified Manager bietet einige vordefinierte Richtlinien, die nicht geändert werden können. Folgende vordefinierte PSLs sind verfügbar:

  - Höchste Performance
  - Performance
  - Wert

    Die Extreme Performance, Performance und Value PSLs sind für die meisten gängigen Storage-Workloads im Datacenter anwendbar.

  Unified Manager bietet außerdem drei Performance-Service-Level für Datenbankapplikationen. Diese extrem hochperformanten PSLs unterstützen sprunghafte IOPS und eignen sich für Datenbankapplikationen mit höchsten Durchsatzanforderungen.

  - Extreme für Datenbank-Logs
  - Extreme für gemeinsam genutzte Datenbank-Daten
  - Extreme für Datenbankdaten
- **Benutzerdefiniert**: Wenn die vordefinierten Leistungsservicelevel Ihren Anforderungen nicht entsprechen, können Sie neue PSLs erstellen, die Ihren Anforderungen entsprechen. Weitere Informationen finden Sie unter "Erstellen und Bearbeiten von Performance Service Levels".
- **Beyond Extreme**: Die Beyond Extreme PSLs sind die vom System empfohlenen PSLs, die für Workloads empfohlen werden, die IOPS höher als Extreme erfordern. Die Workloads werden intern auf Basis ihrer IOPS, Kapazität und Latenz analysiert. Für jede dieser Workloads wird auf dem Bildschirm **Storage > Workloads > Alle Workloads** ein Wert über die extreme PSL hinaus empfohlen. Sie können die PSLs auf die Workloads anwenden, um eine optimale Leistung zu gewährleisten.

  Die IOPS-Parameter für die Workloads werden je nach Workload-Verhalten dynamisch generiert und im Format an den Namen des Beyond Extreme PSL angehängt `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`. Wenn das System beispielsweise feststellt, dass ein Workload den Spitzenwert und den erwarteten IOPS als `37929` bzw. aufweist `106345`, wird das für den Workload erzeugte Beyond Extreme PSL mit dem Namen benannt `Beyond Extreme 106345 37929`. Obwohl diese PSLs vom System empfohlen werden, werden diese PSLs beim Zuweisen zu Workloads als Typ gekennzeichnet `User-defined`.

Verwalten von Workloads durch Zuweisen von PSLs

Sie können über die Seite **Richtlinien** > **Performance Service Levels** und über die APIs des Speicheranbieters auf PSLs zugreifen. Das Management von Storage-Workloads durch die Zuweisung von PSLs ist praktisch, da Storage-Workloads nicht individuell gemanagt werden müssen. Alle Änderungen können auch verwaltet werden, indem eine andere PSL neu zugewiesen wird, anstatt sie einzeln zu verwalten. Mit Unified Manager lassen sich PSLs auf Basis interner Bewertungen und Empfehlungen auf Basis der Workloads zuweisen.

Informationen zum Zuweisen von vom System empfohlenen PSLs zu Workloads finden Sie unter "Zuweisen von systemempfohlenen PSLs zu Workloads"

Auf der Seite Leistungsstufen werden die verfügbaren PSL-Richtlinien aufgelistet und Sie können sie hinzufügen, bearbeiten und löschen.

Eine PSL, die systemdefiniert oder einem Workload zugewiesen ist, kann nicht geändert werden. Eine PSL, die einem Workload zugewiesen ist, kann nicht gelöscht werden, oder es ist die einzige verfügbare PSL.

Auf dieser Seite werden die folgenden Informationen angezeigt:

Feld	Beschreibung
Name	Name der PSL.
Typ	Gibt an, ob die Richtlinie systemdefiniert oder benutzerdefiniert ist.
Erwartete IOPS/TB	Mindestanzahl an IOPS, die eine Applikation für ein LUN oder File-Share durchführen soll Der erwartete IOPS gibt die erwarteten IOPS-Minimum an, die basierend auf der zugewiesenen Storage-Objektgröße zugewiesen wurden.
Max. IOPS/TB	Maximale Anzahl an IOPS, die eine Applikation für ein LUN oder File Share durchführen kann IOPS-Maximum gibt die maximal möglichen IOPS an, die zugewiesen werden. Diese Angabe basiert auf der zugewiesenen Größe des Storage-Objekts oder der verwendeten Größe des Storage-Objekts. IOPS-Spitzenlasten basieren auf einer Zuweisungsrichtlinie. Die Zuweisungsrichtlinie ist entweder zugewiesener Speicherplatz oder belegter Speicherplatz. Wenn die Zuweisungsrichtlinie auf zugewiesenen Speicherplatz festgelegt ist, wird die IOPS-Spitzenwert basierend auf der Größe des Storage-Objekts berechnet. Wenn die Zuweisungsrichtlinie auf usbelegten Speicherplatz festgelegt wird, wird die IOPS-Spitzenwert unter Berücksichtigung der Storage-Effizienz basierend auf der Datenmenge berechnet, die im Storage-Objekt gespeichert ist. Standardmäßig ist die Zuordnungsrichtlinie auf used-space festgelegt.

Feld	Beschreibung
Absolutes IOPS-Minimum	Die absoluten MindestIOPS-Werte werden als Überschreiben verwendet, wenn die erwarteten IOPS kleiner als dieser Wert sind. Die Standardwerte der systemdefinierten PSLs sind: • Extreme Performance: Falls IOPS >= 6144/TB erwartet werden, dann absolute Minimum-IOPS = 1000 • Performance: Falls erwartete IOPS >= 2048/TB und < 6144/TB, dann absolutes Minimum IOPS = 500 • Wert: Falls erwartete IOPS >= 128/TB und < 2048/TB, dann absolutes Minimum IOPS = 75 Die Standardwerte der systemdefinierten Datenbank-PSLs sind: • Extreme für Datenbank-Logs: Wenn IOPS >= 22528 erwartet werden, dann absolute Minimum IOPS = 4000 • Extreme für gemeinsam genutzte Datenbank-Daten: Wenn erwartete IOPS >= 16384, dann absolute Minimum IOPS = 2000 • Extreme für Datenbankdaten: Wenn IOPS erwartet werden >= 12288, dann absolute Minimum IOPS = 2000 Der höhere Wert der absoluten MindestIOPS für benutzerdefinierte PSLs kann maximal 75000 beträgt. Der untere Wert wird wie folgt berechnet: 1000/erwartete Latenz
Erwartete Latenz	Erwartete Latenz für Storage-IOPS in Millisekunden pro Vorgang (ms/op)
Kapazität	Verfügbare und genutzte Gesamtkapazität in den Clustern.
Workloads	Anzahl der Speicher-Workloads, denen das PSL zugewiesen wurde.

Informationen darüber, wie die IOPS-Spitzenwerte und die erwarteten IOPS dazu beitragen, eine konsistent differenzierte Performance auf ONTAP Clustern zu erzielen, finden Sie in folgendem KB-Artikel: "Was ist Performance-Budgetierung?"

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

Beachten Sie, dass wenn Workloads den erwarteten Latenzwert für 30 % der Zeit während der vorherigen Stunde überschreiten, generiert Unified Manager eines der folgenden Ereignisse, um Sie über ein potenzielles Performance-Problem zu benachrichtigen:

- Workload-Volume-Latenzschwellenwert, der gemäß Definition in der Performance-Service-Level-Richtlinie nicht eingehalten wird
- Workload-LUN-Latenzschwellenwert, der gemäß Definition in der Performance-Service-Level-Richtlinie nicht eingehalten wird

Vielleicht möchten Sie den Workload analysieren, um zu sehen, was zum möglicherweise die höheren Latenzwerte führt.

Weitere Informationen finden Sie unter den folgenden Links:

- "Volume-Ereignisse"
- "Was passiert, wenn eine Performance-Richtlinie nicht eingehalten wird"
- "Unified Manager verwendet Workload-Latenz zur Identifizierung von Performance-Problemen"
- "Was sind Performance-Ereignisse"

Systemdefinierte PSLs

Die folgende Tabelle enthält Informationen zu den systemdefinierten PSLs:

Performance Service Level	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/OP)	IOPS-Spitzenwert	IOPS erwartet	Absolutes IOPS-Minimum
Höchste Performance	Sorgt für einen extrem hohen Durchsatz bei sehr niedriger Latenz Ideal für latenzkritische Applikationen	1	12288	6144	1000
Performance	Hoher Durchsatz bei niedriger Latenz Ideal für Datenbanken und virtualisierte Applikationen	2	4096	2048	500

Performance Service Level	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/OP)	IOPS-Spitzenwert	IOPS erwartet	Absolutes IOPS-Minimum
Wert	Bietet hohe Storage-Kapazität und mittlerer Latenz Ideal für Applikationen mit hoher Kapazität wie E-Mail, Web-Inhalte, Dateifreigaben und Backup-Ziele	17	512	128	75
Extreme für Datenbank-Logs	Bietet maximalen Durchsatz bei geringster Latenz. Ideal für Datenbankapplikationen, die Datenbankprotokolle unterstützen Diese PSL bietet den höchsten Durchsatz, da Datenbankprotokolle extrem sprunghafte Anstiege bieten und die Protokollierung ständig erforderlich ist.	1	45056	22528	4000

Performance Service Level	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/OP)	IOPS-Spitzenwert	IOPS erwartet	Absolutes IOPS-Minimum
Extreme für gemeinsam genutzte Datenbank-Daten	Sehr hoher Durchsatz bei geringster Latenz. Ideal für Daten von Datenbankapplikationen, die in einem gemeinsamen Datenspeicher gespeichert, aber datenbankübergreifend verwendet werden	1	32768	16384	2000
Extreme für Datenbankdaten	Bietet hohen Durchsatz bei geringster Latenz. Ideal für Daten von Datenbankapplikationen, z. B. Datenbanktabellen und Metadaten	1	24576	12288	2000

Erstellen und Bearbeiten von Performance Service Levels

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

Was Sie brauchen

- Sie müssen über die Anwendungsadministratorrolle verfügen.
- Der Name der Leistungsstufe muss eindeutig sein, und Sie können die folgenden reservierten Schlüsselwörter nicht verwenden:

  `Prime`, `Extreme`, `Performance`, `Value`, `Unassigned`, `Learning`, , `Idle` `Default` und `None`.

Sie erstellen und bearbeiten benutzerdefinierte Performance-Service-Level über die Seite Performance-

Service-Level, indem Sie die Service-Level-Ziele definieren, die Sie für die Applikationen benötigen, die auf den Storage zugreifen.

Ein Performance-Service-Level kann nicht geändert werden, wenn er derzeit einem Workload zugewiesen ist.

Schritte

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

An…	Führen Sie die folgenden Schritte aus…
Erstellen Sie ein neues Performance Service Level	Klicken Sie Auf **Hinzufügen**.
Bearbeiten eines vorhandenen Performance-Service-Levels	Wählen Sie einen vorhandenen Performance Service Level aus, und klicken Sie dann auf **Bearbeiten**.

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

3. Passen Sie den Performance Service Level an, indem Sie die Leistungsziele festlegen, und klicken Sie dann auf **Absenden**, um den Performance Service Level zu speichern.

Sie können das neue oder geänderte Performance Service Level auf Workloads (LUNs, NFS File Shares, CIFS Shares) auf der Seite Workloads oder bei der Bereitstellung eines neuen Workloads anwenden.

Management Von Richtlinien Zur Storage-Effizienz

Mit einer Storage-Effizienz-Richtlinie (SEP) können Sie die Storage-Effizienz-Merkmale eines Workloads definieren. Sie können einem Workload bei der ersten Erstellung des Workloads einen SEP zuweisen oder anschließend den Workload bearbeiten.

Storage-Effizienz beinhaltet Technologien wie Thin Provisioning, Deduplizierung und Datenkomprimierung, die die Storage-Auslastung erhöhen und die Storage-Kosten senken. Bei der Erstellung von SEPs können Sie diese platzsparenden Technologien entweder einzeln oder gemeinsam nutzen, um eine maximale Storage-Effizienz zu erzielen. Wenn Sie die Richtlinien Ihren Storage-Workloads zuordnen, werden ihnen die angegebenen Richtlinieneinstellungen zugewiesen. Mit Unified Manager können Sie systemdefinierte und benutzerdefinierte SEPs zuweisen, um die Speicherressourcen in Ihrem Rechenzentrum zu optimieren.

Unified Manager bietet zwei systemdefinierte SEPs: High und Low. Diese SEPs gelten für die meisten Storage-Workloads in einem Datacenter. Sie können jedoch eigene Richtlinien erstellen, wenn die systemdefinierten SEPs Ihre Anforderungen nicht erfüllen.

Sie können einen SEP, der systemdefiniert ist oder der derzeit einem Workload zugewiesen ist, nicht ändern. Eine SEP, die einem Workload zugewiesen ist, kann nicht gelöscht werden oder ist sie das einzige verfügbare SEP.

Auf der Seite Storage Efficiency Policies werden die verfügbaren SEPs aufgelistet und Sie können benutzerdefinierte SEPs hinzufügen, bearbeiten und löschen. Auf dieser Seite werden die folgenden

Informationen angezeigt:

Feld	Beschreibung
Name	Name der SEP.
Typ	Gibt an, ob die Richtlinie systemdefiniert oder benutzerdefiniert ist.
Space Reserve	Gibt an, ob es sich um Thin Provisioning oder Thick Provisioning für das Volume handelt:
Deduplizierung	Gibt an, ob die Deduplizierung für den Workload aktiviert ist: • Inline: Deduplizierung wird während des Verschreibens auf den Workload durchgeführt • Hintergrund: Deduplizierung findet im Workload statt • Deaktivieren: Die Deduplizierung ist für den Workload deaktiviert
Komprimierung	Gibt an, ob die Datenkomprimierung für den Workload aktiviert ist: • Inline: Datenkomprimierung wird während des Verschreibens auf den Workload ausgeführt • Hintergrund: Datenkomprimierung findet im Workload statt • Deaktivieren: Für den Workload ist die Datenkomprimierung deaktiviert
Workloads	Anzahl an Storage Workloads, denen SEP zugewiesen wurde

Richtlinien zum Erstellen einer individuellen Richtlinie zur Storage-Effizienz

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

Sie können den SEP, der Workloads zugewiesen ist, auf der Seite Alle Workloads und auf der Seite Volume / Health Details anzeigen. Sie können das Datenreduzierungsverhältnis auf Cluster-Ebene (ohne Snapshot-Kopien) basierend auf diesen Storage-Effizienzfunktionen im Fenster „Kapazität“ im Dashboard und in der Ansicht „Kapazität: Alle Cluster“ anzeigen.

Erstellung und Bearbeitung von Storage-Effizienz-Richtlinien

Wenn die System-definierten Storage-Effizienzrichtlinien nicht Ihren Workload-Anforderungen entsprechen, können Sie Ihre eigenen Storage-Effizienzrichtlinien

erstellen, die für Ihre Workloads optimiert sind.

Was Sie brauchen

- Sie müssen über die Anwendungsadministratorrolle verfügen.
- Der Name der Storage Efficiency Policy muss eindeutig sein. Sie können die folgenden reservierten Schlüsselwörter nicht verwenden:

  `High`, `Low`, `Unassigned`, `Learning`, `Idle`, `Default`, und `None`.

Sie können benutzerdefinierte Storage-Effizienz-Richtlinien über die Seite Storage-Effizienz-Richtlinien erstellen und bearbeiten, indem Sie die Merkmale definieren, die Sie für die Applikationen benötigen, die auf den Storage zugreifen.

Sie können eine Storage-Effizienz-Richtlinie nicht ändern, wenn sie derzeit einem Workload zugewiesen ist.

Schritte

1. Wählen Sie im linken Navigationsbereich unter **Einstellungen Richtlinien** > **Storage-Effizienz** aus.
2. Klicken Sie auf der Seite **Storage Efficiency Policies** auf die entsprechende Schaltfläche, je nachdem, ob Sie eine neue Storage Efficiency Policy erstellen möchten oder ob Sie eine vorhandene Storage Efficiency Policy bearbeiten möchten.

An…	Führen Sie die folgenden Schritte aus…
Erstellen Sie eine neue Storage-Effizienz-Richtlinie	Klicken Sie Auf **Hinzufügen**
Bearbeiten Sie eine vorhandene Richtlinie zur Storage-Effizienz	Wählen Sie eine vorhandene Richtlinie zur Storage-Effizienz aus, und klicken Sie auf **Bearbeiten**

   Die Seite zum Hinzufügen oder Bearbeiten einer Richtlinie für die Storage-Effizienz wird angezeigt.

3. Passen Sie die Storage-Effizienz-Richtlinie an, indem Sie die Merkmale der Storage-Effizienz angeben. Klicken Sie dann auf **Absenden**, um die Storage-Effizienz-Richtlinie zu speichern.

Sie können die neue oder geänderte Storage-Effizienzrichtlinie auf Workloads (LUNs, NFS File Shares, CIFS Shares) auf der Seite Workloads oder bei der Bereitstellung eines neuen Workloads anwenden.

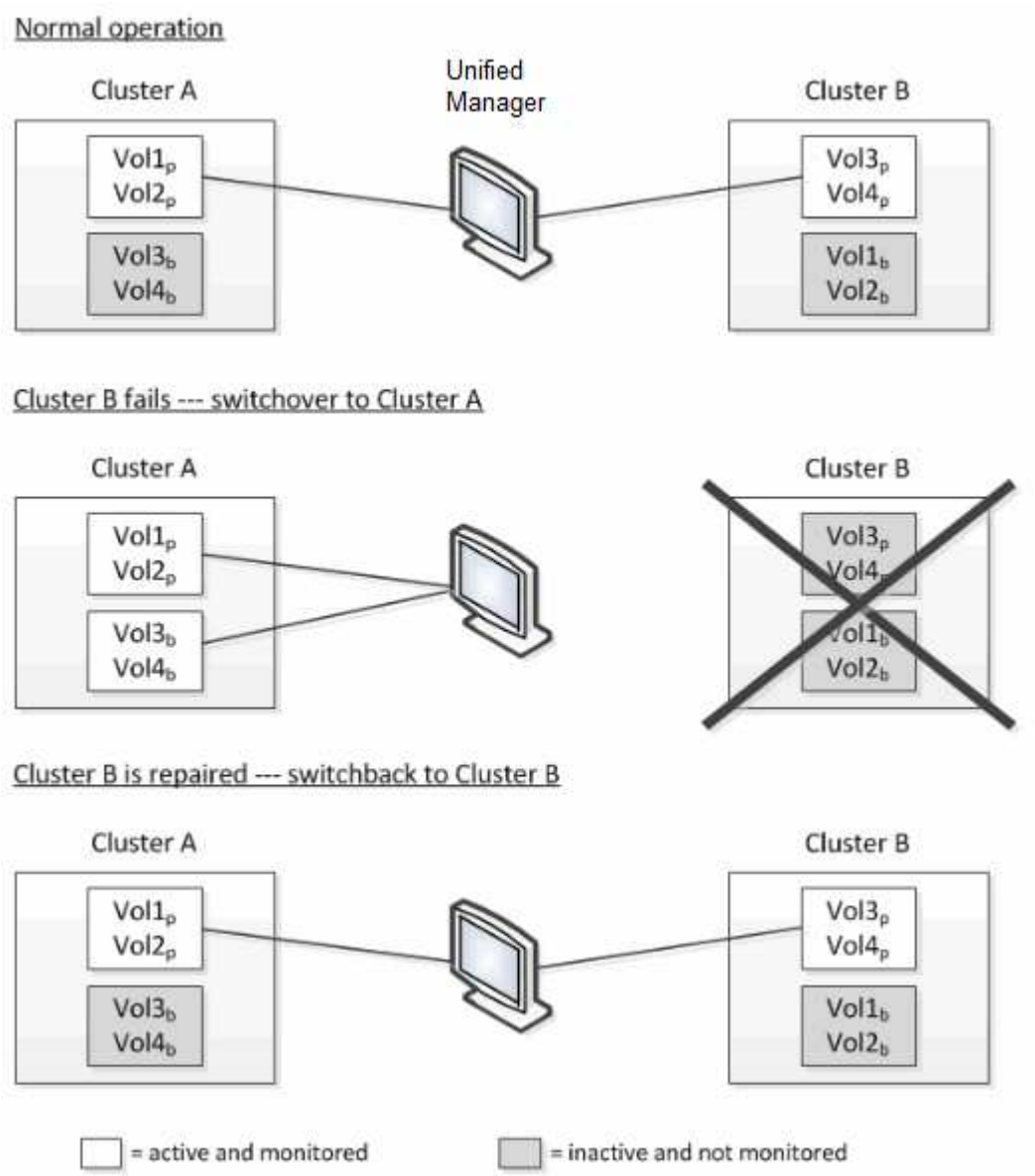
Verwalten und Überwachen von MetroCluster Konfigurationen

Die Monitoring-Unterstützung für MetroCluster-Konfigurationen in der Unified Manager Web-Benutzeroberfläche ermöglicht es Ihnen, nach Verbindungsproblemen in Ihren MetroCluster-over-FC- und IP-Konfigurationen zu suchen. Durch die frühzeitige Erkennung eines Verbindungsproblem können Sie Ihre MetroCluster-Konfigurationen effektiv verwalten.

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 erfolgt ist und VOL3 für Cluster A aktiv geworden ist

Cluster-Konnektivitätsstatus-Definitionen für MetroCluster über FC-Konfiguration

Die Konnektivität zwischen den Clustern in einer MetroCluster über FC-Konfiguration kann einen der folgenden Status aufweisen: Optimal, beeinträchtigt oder ausgefallen. Wenn Sie 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.	
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 für Datenspiegelung für MetroCluster über FC

MetroCluster over FC-Konfigurationen ermöglichen Datenspiegelung und zusätzliche Fähigkeit, Failover zu initiieren, wenn ein kompletter Standort nicht mehr verfügbar ist. Der Status der Datenspiegelung zwischen den Clustern in einer MetroCluster-over-FC-Konfiguration kann entweder Normal oder Spiegelung nicht verfügbar sein. 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.	

Status Datenspiegelung	Beschreibung	Wird angezeigt
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. Hier erfahren Sie, wie Sie Konnektivitätsprobleme in durch MetroCluster geschützten Clustern über FC- und MetroCluster over IP-Konfigurationen überwachen.

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

- **Speicherung** > **Cluster** > **Schutz: Ansicht MetroCluster**
- **Schutz** > **Beziehungen** > **Beziehung: MetroCluster** Ansicht

Unified Manager verwendet Systemzustandsmeldungen, um den Status der Komponenten und die Konnektivität in der MetroCluster-Konfiguration anzugeben.

Was Sie brauchen

- Der Active IQ Unified Manager muss sowohl die lokalen als auch die Remote-Cluster in einer MetroCluster Konfiguration hinzugefügt werden.
- Wenn in einer Konfiguration von MetroCluster over IP ein Mediator unterstützt werden soll, sollte der Mediator konfiguriert und dem Cluster durch die entsprechende API hinzugefügt werden.
- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Überwachen von Konnektivitätsproblemen in der MetroCluster-over-FC-Konfiguration

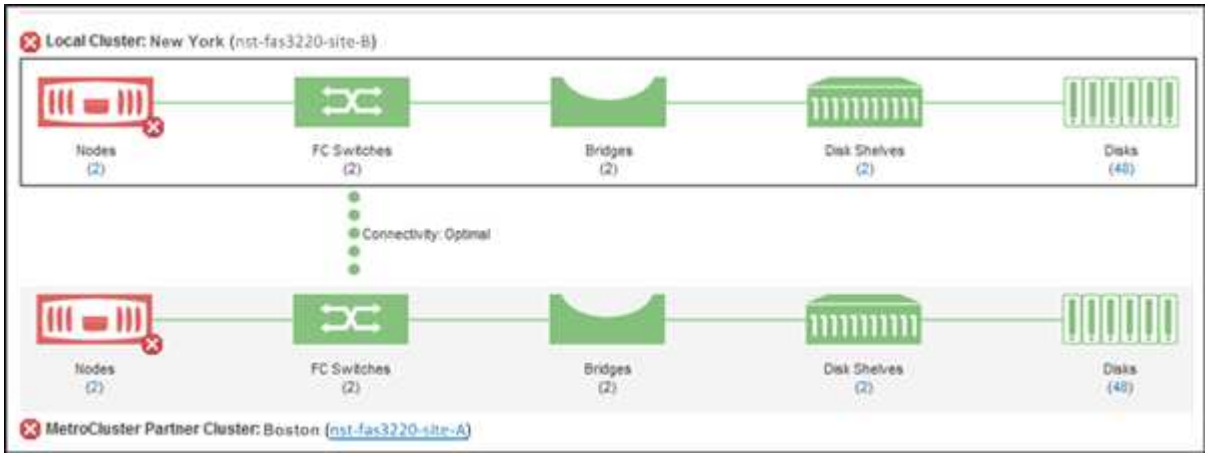
Bei Clustern in einer MetroCluster-over-FC-Konfiguration werden die Konnektivitätsdiagramme auf der Seite **Cluster / Health**-Details angezeigt. Auszuführende Schritte:

Schritte

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

   Eine Liste aller überwachten Cluster wird angezeigt.

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



Die Topologie der MetroCluster-Konfiguration wird im entsprechenden Cluster-Objektbereich angezeigt. Sie können die auf der Seite Cluster/Health 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.

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.

Weitere Informationen zum Bestimmen des Clusterzustands finden Sie unter "Ermitteln des Clusterzustands in der MetroCluster-over-FC-Konfiguration".

Überwachen von Konnektivitätsproblemen in der MetroCluster-over-IP-Konfiguration

Bei Clustern in einer MetroCluster-over-IP-Konfiguration werden die Konnektivitätskarten auf der Seite **Cluster** angezeigt. Auszuführende Schritte:

Schritte

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

   Eine Liste aller überwachten Cluster wird angezeigt.

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

   Sie können die Topologie der Quell- und Spiegelstandorte sowie den Mediator, sofern vorhanden, für die

Verbindung anzeigen. Sie können folgende Informationen anzeigen:

- Konnektivität über die Standorte hinweg
- Falls überhaupt, auf beiden Seiten Probleme mit dem Systemzustand und der Verfügbarkeit
- Mediatorbezogene Probleme
- Probleme bei der Replizierung.

> Folgende Status werden gemeldet: Kritisch (), Fehler (✕) oder Normal (✓)!. Sie können den Replizierungsstatus der aggregierten Daten der primären und gespiegelten Daten in derselben Topologie anzeigen.

In der folgenden Abbildung sehen Sie, dass die Verbindung zwischen den Standorten zwischen den Quell- und Ziel-Clustern nicht verfügbar ist und der Mediator zwischen ihnen nicht konfiguriert ist.

4. Klicken Sie auf das Statussymbol. Es wird eine Meldung mit der Fehlerdefinition angezeigt. Wenn ein Ereignis für das Problem in Ihrer MetroCluster over IP-Konfiguration aufgeworfen wurde, können Sie in der Meldung auf die Schaltfläche **Ereignis anzeigen** klicken und die Ereignisdetails anzeigen. Wenn Sie das Problem und das Ereignis behoben haben, wird das Statussymbol in dieser Topologie zu Normal (✓).
5. Weitere Konfigurationsdetails können Sie im Abschnitt **MetroCluster Übersicht** und **Schutz** auf der Registerkarte **Konfiguration** der Detailseite **Cluster / Gesundheit** einsehen.

> Nur bei einer MetroCluster-over-IP-Konfiguration können Sie die Clustertopologie auf der Seite **Cluster** anzeigen lassen. Bei Clustern in einer MetroCluster-über-FC-Konfiguration wird die Topologie auf der Registerkarte **MetroCluster-Konnektivität** auf der Seite **Cluster / Systemzustand**-Details angezeigt.

Verwandte Informationen

- "„Cluster/Systemzustand“-Details"
- Informationen zur Ansicht **Beziehung:MetroCluster** finden Sie unter "Monitoring der MetroCluster Konfigurationen".
- Informationen zu **Beziehung: Letzte 1 Monat Transferstatus** Ansicht, siehe "Beziehung: Letzte 1 Monat Transfer Status Ansicht".

- Für Informationen über **Beziehung: Letzte 1 Monat Transfer Rate** Ansicht, siehe "Beziehung: Letzte 1 Monat Transferrate Ansicht".
- Für Informationen über **Beziehung: Alle Beziehungen** Ansicht, siehe "Beziehung: Ansicht aller Beziehungen".

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.

Unified Manager überwacht mit Systemzustandsmeldungen den Status der Komponenten und die Konnektivität in der MetroCluster-Konfiguration.

Was Sie brauchen

Der lokale und der Remote-Cluster in der MetroCluster Konfiguration müssen Unified Manager hinzugefügt werden

Anzeigen der Replizierung für MetroCluster über IP-Konfigurationen

Bei MetroCluster-over-IP-Konfigurationen wird der Datenreplizierungsstatus in der Topologieansicht für einen durch MetroCluster over IP geschützten Cluster aus den folgenden Ansichten im linken Navigationsbereich von Unified Manager angezeigt:

- **Speicherung** > **Cluster** > **Schutz: Ansicht MetroCluster**
- **Schutz** > **Beziehungen** > **Beziehung: MetroCluster** Ansicht

Weitere Informationen finden Sie unter "Überwachen Sie Konnektivitätsprobleme in MetroCluster über IP".

Anzeigen der Replizierung für MetroCluster über FC-Konfigurationen

Befolgen Sie diese Schritte, um alle Probleme in der Datenreplizierung für die MetroCluster-over-FC-Konfiguration zu ermitteln.

Schritte

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

   Eine Liste der überwachten Cluster wird angezeigt.

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

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

Sie können die auf der Seite Cluster/Health Details angezeigten Informationen verwenden, um alle Replikationsprobleme zu beheben. 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.

Verwandte Informationen

"„Cluster/Systemzustand“-Details"

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. Benutzer mit der Anwendungsadministratorrolle können Warnungen konfigurieren, die die angegebenen Empfänger über die Quota-Ereignisse der Benutzer- oder Benutzergruppe benachrichtigen.

Sie können die Kontingentgrenze entweder mit ONTAP System Manager oder mit der ONTAP CLI festlegen.

Anzeigen von Benutzer- und Benutzergruppenkontingenten

Auf der Seite Storage VM/Health Details 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.

Was Sie brauchen

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

Schritte

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

Verwandte Informationen

"Benutzer hinzufügen"

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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Richtlinien auf der Seite Regeln zur Erstellung von Benutzer- und Gruppenkontingente-E-Mail-Adresse geprüft haben.

Sie müssen die Regeln für Quota-E-Mail-Adressen definieren und in der Reihenfolge eingeben, in der sie ausgeführt werden sollen. Wenn Sie zum Beispiel die E-Mail-Adresse abc@xyz.com verwenden möchten, um Benachrichtigungen über Quotenverletzungen für abc zu erhalten und die E-Mail-Adresse dl-€GROUP@ für alle anderen Gruppen zu verwenden, müssen die Regeln in der folgenden Reihenfolge aufgeführt sein:

- Wenn (BENUTZER == 'abc') dann abc@xyz.com
- Wenn (@ GROUP == *) dann dl-€GRUPPE DOMÄNE

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 im linken Navigationsbereich auf **Allgemein** > **Quota Email Rules**.
2. Geben Sie die Regel basierend auf Ihren Kriterien ein.
3. Klicken Sie auf **Validieren**, um die Syntax der Regel zu validieren.

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

4. Klicken Sie Auf **Speichern**.
5. Überprüfen Sie, ob die von Ihnen erstellte E-Mail-Adresse auf der Seite Storage **VM / Health** 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).

Was Sie brauchen

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

Schritte

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

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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen die überprüft haben "Richtlinien zur Erstellung von Regeln".

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 **Storage** > **SVMs**.
2. Wählen Sie in der Ansicht **Systemzustand: Alle Storage VMs** eine SVM aus und klicken Sie dann auf die Registerkarte **Benutzer- und Gruppenquoten**.
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.

Wenn…	Dann…
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 Quotas mit der Datei an `/etc/quotas`. 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 in der Ansicht Systemzustand: Alle Storage VMs verwenden, um das Format der E-Mail-Benachrichtigung zu konfigurieren, die bei Auftreten eines quota-bezogenen 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 ist dies die E-Mail-Adresse, die die Seite 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 (`valid variableoperator *`) dann `email ID@domain name`

  Wenn ein Schlüsselwort ist und in Kleinbuchstaben ist. 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 (`valid variableoperator `string`) dann `email ID@domain name`

  Wenn es sich um ein Schlüsselwort handelt und klein geschrieben wird. Der Operator kann entweder oder == enthalten. 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.

Fehlerbehebung

Mithilfe von Informationen zur Fehlerbehebung können Sie Probleme identifizieren und beheben, die bei Verwendung von Unified Manager auftreten.

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 vergrößern müssen, können Sie nach der Installation Kapazität hinzufügen,

indem Sie über die Unified Manager-Wartungskonsole Festplattenspeicher erweitern.

Was Sie brauchen

- 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.

Wir empfehlen, dass Sie Ihre virtuelle Maschine sichern, bevor Sie die Größe der virtuellen Laufwerke erhöhen.

Schritte

1. Wählen Sie im vSphere-Client die virtuelle Unified Manager-Maschine aus, und fügen Sie den Daten dann zusätzliche Festplattenkapazität hinzu `disk 3`. Details finden Sie in der VMware Dokumentation.

   In seltenen Fällen verwendet die Unified Manager-Implementierung „Festplatte 2“ für die Datenfestplatte statt „Festplatte 3“. Wenn dies bei Ihrer Bereitstellung der Fall ist, erhöhen Sie den Speicherplatz, je nachdem, welcher Datenträger größer ist. Die Datenfestplatte hat immer mehr Speicherplatz als die andere Festplatte.

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 Verzeichnis nicht genügend Speicherplatz zur Unterstützung von Unified Manager zugewiesen `/opt/netapp/data` haben, wenn Sie den Linux-Host ursprünglich eingerichtet und Unified Manager dann installiert haben, können Sie nach der Installation Festplattenspeicher hinzufügen, indem Sie den Speicherplatz im Verzeichnis erhöhen `/opt/netapp/data`.

Was Sie brauchen

Sie müssen Root-Benutzerzugriff auf die Red hat Enterprise Linux oder CentOS Linux Maschine haben, auf der Unified Manager installiert ist.

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. Stoppen Sie den Unified Manager-Service und die zugehörige MySQL-Software in der angezeigten Reihenfolge: `systemctl stop ocieau ocie mysqld`

3. Erstellen Sie einen temporären Sicherungsordner (z.B.) mit ausreichend Speicherplatz, `/backup-data` um die Daten im aktuellen Verzeichnis zu enthalten `/opt/netapp/data`.
4. Kopieren Sie den Inhalt und die Berechtigungskonfiguration des vorhandenen `/opt/netapp/data` Verzeichnisses in das Sicherungsdatenverzeichnis:

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

5. Wenn SE Linux aktiviert ist:

   a. Rufen Sie den SE Linux-Typ für Ordner im vorhandenen Ordner ab `/opt/netapp/data`:

      ```
      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 den Befehl aus `chcon`, um den SE Linux-Typ für das Backup-Verzeichnis festzulegen:

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

6. Inhalt des Verzeichnisses entfernen `/opt/netapp/data`:

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

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

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

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

   ```
   ls -ltr /opt/netapp/ | grep 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, dass der Kontext für das `/opt/netapp/data` Verzeichnis weiterhin auf mysqld_db_t gesetzt ist:

   a. `touch /opt/netapp/data/abc`

b. `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. Löschen Sie die Datei `abc`, damit diese externe Datei in Zukunft keinen Datenbankfehler verursacht.
11. Kopieren Sie den Inhalt von `backup-data` zurück in das erweiterte `/opt/netapp/data` Verzeichnis:

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

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

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

13. Starten Sie den MySQL-Dienst:

```
systemctl start mysqld
```

14. Nachdem der MySQL-Dienst gestartet wurde, starten sie die ocie- und ocieau-Dienste in der folgenden Reihenfolge:

```
systemctl start ocie ocieau
```

15. Nachdem alle Dienste gestartet wurden, löschen Sie 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.

Was Sie brauchen

Sie müssen über Administratorrechte für Windows verfügen.

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"

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.

Was Sie brauchen

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

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

Sie sollten das Erfassungsintervall nur ändern, wenn dies aufgrund eines Problems 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-Einrichtung 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.

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.

Änderung der Zeitdauer, bei der Unified Manager Ereignis- und Performance-Daten aufbewahrt werden

Standardmäßig speichert Unified Manager Ereignisdaten und Performance-Daten für 6 Monate für alle überwachten Cluster. Nach diesem Zeitpunkt werden ältere Daten automatisch gelöscht, um Platz für neue Daten zu schaffen. Dieser Zeitrahmen eignet sich für die meisten Konfigurationen gut. Sehr große Konfigurationen mit vielen Clustern und Nodes müssen möglicherweise den Aufbewahrungszeitraum verkürzen, um einen optimalen Betrieb von Unified Manager zu erzielen.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

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

Unified Manager sammelt Performance-Statistiken alle 5 Minuten. Die Statistiken von 5 Minuten werden jeden Tag in Performance-Statistiken von Stunden zusammengefasst. Es speichert 30 Tage Verlaufsdaten zu 5 Minuten und fasst 6 Monate zusammengefasster Performance-Daten auf Stundenbasis (standardmäßig).

Sie sollten die Aufbewahrungsdauer nur reduzieren, wenn Ihnen der Speicherplatz knapp wird oder wenn Backup- und andere Vorgänge sehr lange dauern. Die Verringerung des Aufbewahrungszeitraums hat folgende Auswirkungen:

- Alte Performance-Daten werden nach Mitternacht aus der Unified Manager-Datenbank gelöscht.
- Alte Ereignisdaten werden sofort aus der Unified Manager-Datenbank gelöscht.
- Ereignisse vor dem Aufbewahrungszeitraum können in der Benutzeroberfläche nicht mehr angezeigt werden.
- Standorte in der UI, an denen stündliche Performance-Statistiken angezeigt werden, sind vor dem Aufbewahrungszeitraum leer.
- Wenn der Aufbewahrungszeitraum des Ereignisses die Aufbewahrungsdauer der Leistungsdaten überschreitet, wird unter dem Leistungsschieber eine Meldung angezeigt, die darauf hinweist, dass ältere Performanceereignisse möglicherweise keine Sicherungsdaten in den zugehörigen Diagrammen haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Richtlinien** > **Datenspeicherung**.
2. Wählen Sie auf der Seite **Datenspeicherung** das Schieberegler-Tool im Bereich Ereignisspeicherung oder -Speicherung aus, und verschieben Sie es auf die Anzahl der Monate, in denen Daten gespeichert werden sollen, und klicken Sie auf **Speichern**.

Unbekannter Authentifizierungsfehler

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

Ursache

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

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

Korrekturmaßnahmen

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

Der Benutzer wurde nicht gefunden

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

Ursache

Dieses Problem kann auftreten, wenn der Benutzer im AD-Server oder LDAP-Server existiert und wenn Sie den Distinguished Base-Namen auf einen falschen Wert gesetzt haben.

Korrekturmaßnahmen

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Geben Sie die entsprechenden Informationen für den Basisnamen ein.
3. Klicken Sie Auf **Speichern**.

Problem beim Hinzufügen von LDAP über andere Authentifizierungsdienste

Wenn Sie andere als den Authentifizierungsdienst auswählen, behalten die Benutzer- und Gruppenobjektklasse 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:

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

Wenn die Objektklasse und die Objektklasse des LDAP-Benutzers positixAccount bzw. positixGroup sind, führen Sie die folgenden Schritte aus:

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

Wenn die ersten beiden Problemumgehungen nicht zutreffen, rufen Sie die `option-set` API auf, und setzen Sie die `auth.ldap.userObjectClass` Optionen und `auth.ldap.groupObjectClass` auf die richtigen Werte.

Verwalten von Ereignissen und Meldungen

Verwalten von Ereignissen

Ereignisse unterstützen Sie bei der Erkennung von Problemen in den überwachten Clustern.

Was sind die Active IQ Plattform-Ereignisse

Unified Manager kann Ereignisse anzeigen, die von der Active IQ Plattform erkannt wurden. Diese Ereignisse werden durch Regelwerke gegen AutoSupport Meldungen erstellt, die von allen Storage-Systemen, die von Unified Manager überwacht werden, generiert werden.

Weitere Informationen finden Sie unter "Generieren von Active IQ-Plattformereignissen".

Unified Manager prüft automatisch auf eine neue Regeldatei und lädt nur eine neue Datei herunter, wenn neuere Regeln vorliegen. Bei Sites ohne externen Netzwerkzugriff müssen Sie die Regeln manuell von **Speicherverwaltung** > **Event-Setup** > **Upload-Regeln** hochladen.

Diese Active IQ Ereignisse überschneiden sich nicht mit bestehenden Unified Manager Ereignissen, und sie ermitteln Vorfälle oder Risiken bei Systemkonfiguration, Verkabelung, Best Practices und Verfügbarkeitsproblemen.

Weitere Informationen zum Aktivieren von Plattformereignissen finden Sie unter "Aktivieren von Active IQ Portal-Ereignissen". Weitere Informationen zum Hochladen von Regeldateien finden Sie unter "Eine neue Datei für Active IQ-Regeln wird hochgeladen".

NetApp Active IQ ist ein Cloud-basierter Service, der prädiktive Analysen und proaktiven Support bietet, um den Betrieb von Storage-Systemen in der gesamten NetApp Hybrid Cloud zu optimieren. Weitere Informationen finden Sie unter "NetApp Active IQ" .

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. Beispielsweise zeigt das Informationsereignis „FlexGroup-Komponenten-Raumstatus alles OK“ an, dass das Fehlerereignis „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

Die folgenden ONTAP EMS-Ereignisse werden dem Unified Manager automatisch 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 von Unified Manager
Zugriff auf Cloud-Tier für Aggregatverschiebung verweigert	arl.netra.ca.check.failed	Aggregat	Fehler
Beim Storage Failover wurde der Zugriff auf Cloud-Tier für Aggregatverschiebung verweigert	gb.netra.ca.check.failed	Aggregat	Fehler
Resync der FabricPool-Spiegelreplikation abgeschlossen	wafl.ca.resync.complete	Cluster	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 von Unified Manager
Cloud AWS IAMRoleNotFound	Cloud.aws.iamRoleNotFound	Knoten	Fehler
Unlösbar Für Cloud Tier Host	Objstore.Host.unlösbar	Knoten	Fehler
Cloud Tier Intercluster-Netzwerkschnittstelle Nicht Aktiv	objstore.interclusterlifDown	Knoten	Fehler
Anforderung Einer Signatur Für Die Cloud-Ebene Mit Nicht Übereinstimmung	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 von Unified Manager
Max. CIFS-Verbindung überschritten	Nblade.cifsMaxOpenSameFile	SVM	Fehler
Max. Anzahl der CIFS-Verbindung pro Benutzer überschritten	Nblade.cifsMaxSessPerUsrConn	SVM	Fehler
CIFS NetBIOS-Name-Konflikt	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 von Unified Manager
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.inc.sav	Datenmenge	Warnung
Logischer Speicherplatz Des Volume Voll	monitor.vol.full.inc.sav	Datenmenge	Fehler
Logischer Speicherplatz Des Volume Ist Normal	monitor.vol.one.ok.inc.sav	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
Timeout für den Vorgang der WAFL-READDIR-Datei	wafl.readdir.exist	Datenmenge	Fehler

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.

Was Sie brauchen

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.

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 **Storage-Management** > **Event-Setup**.
2. Klicken Sie auf der Seite Event Setup auf die Schaltfläche **EMS-Ereignisse abonnieren**.
3. Geben Sie im Dialogfeld EMS-Ereignisse abonnieren den Namen des EMS-Ereignisses von ONTAP ein, für das Sie abonnieren möchten.

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

   "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.

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.

Was passiert, wenn ein Ereignis empfangen wird

Wenn Unified Manager ein Ereignis empfängt, wird es auf der Seite Dashboard, auf der Seite Ereignismanagement-Inventar, auf den Registerkarten Zusammenfassung und Explorer der Seite Cluster/Performance und auf der objektspezifischen Bestandsseite (z. B. auf der Seite Volumes/Integritätsbestand) angezeigt.

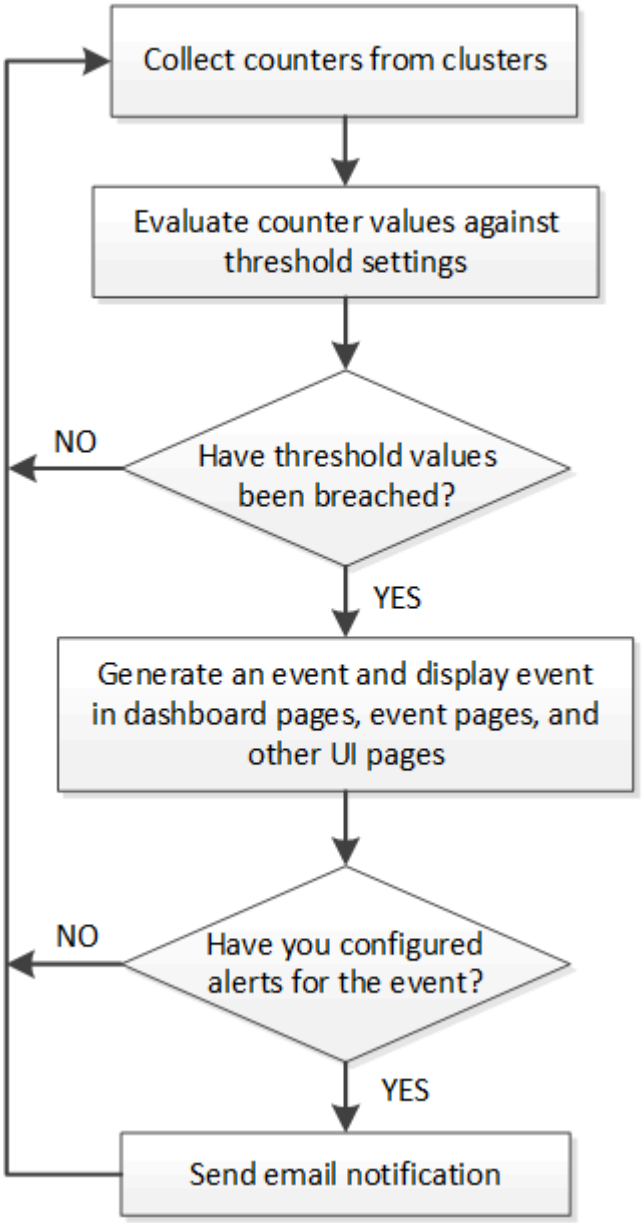
Wenn Unified Manager mehrere kontinuierliche Vorkommnisse derselben Clusterkomponente erkennt, werden

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 Alarmkonfiguration 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.



Anzeigen von Ereignissen und 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.

Was Sie brauchen

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

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 **Ereignisverwaltung**.

   Standardmäßig werden in der Ansicht Alle aktiven Ereignisse die neuen und bestätigten (aktiven) Ereignisse angezeigt, die in den letzten 7 Tagen mit einem Level der Auswirkung von Vorfall oder Risiko generiert wurden.

2. Wenn Sie eine bestimmte Kategorie von Ereignissen anzeigen möchten, z. B. Kapazitätsereignisse oder Performanceereignisse, klicken Sie auf **Ansicht** und wählen Sie im Menü der Ereignistypen aus.
3. Klicken Sie auf den Ereignisnamen, dessen Details angezeigt werden sollen.

   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.

Was Sie brauchen

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

Schritte

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

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

2. Wählen Sie im 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.

Was Sie brauchen

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

Sie können mehrere Ereignisse gleichzeitig bestätigen und beheben.

Sie können keine Informationsereignisse bestätigen.

Schritte

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

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

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

3. **Optional**: Fügen Sie im Bereich **Notizen und Updates** einen Hinweis dazu, 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.

Was Sie brauchen

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

Schritte

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

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

Deaktivieren unerwünschter Ereignisse

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.

Was Sie brauchen

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

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

Wenn Sie ein Ereignis für ein Objekt deaktivieren (z. B. das `vol offline` Ereignis), und später das Ereignis aktivieren, generiert Unified Manager keine neuen Ereignisse für Objekte, die offline gingen, während das Ereignis im Status deaktiviert war. Unified Manager generiert ein neues Ereignis nur, wenn nach der erneuten Aktivierung des Ereignisses eine Änderung im Objektstatus vorhanden ist.

Schritte

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

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren von Ereignissen	a. Klicken Sie Auf **Deaktivieren**. b. Wählen Sie im Dialogfeld Ereignisse deaktivieren den Schweregrad 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. Stellen Sie sicher, dass die deaktivierten Ereignisse in der Listenansicht der Seite Event Setup angezeigt werden.
Aktivieren von Ereignissen	a. Aktivieren Sie das Kontrollkästchen für das Ereignis oder die Ereignisse, die Sie aktivieren möchten. b. Klicken Sie Auf **Aktivieren**.

Behebung von Problemen mithilfe der automatischen Problembehebung in Unified Manager

Es gibt bestimmte Ereignisse, die Unified Manager gründlich diagnostizieren und eine einzige Lösung mit der Schaltfläche * Fix IT* bereitstellen kann. Wenn verfügbar, werden diese Auflösungen im Dashboard, auf der Seite Ereignisdetails und aus der Auswahl Workload Analysis im linken Navigationsmenü angezeigt.

Die meisten Ereignisse haben eine Vielzahl von möglichen Auflösungen, die auf der Seite Ereignisdetails angezeigt werden, so dass Sie die beste Lösung mit ONTAP System Manager oder der ONTAP CLI implementieren können. Eine Aktion **Beheben Sie es** ist verfügbar, wenn Unified Manager festgestellt hat, dass es eine einzige Lösung gibt, um das Problem zu beheben, und dass es mit einem ONTAP CLI-Befehl behoben werden kann.

Schritte

1. Um Ereignisse anzuzeigen, die über das **Dashboard** behoben werden können, klicken Sie auf **Dashboard**.
2. Um Probleme zu beheben, die Unified Manager beheben kann, klicken Sie auf die Schaltfläche **Fix IT**. Um ein Problem zu beheben, das auf mehreren Objekten vorhanden ist, klicken Sie auf die Schaltfläche * Alle beheben*.

Informationen zu Problemen, die durch automatische Problembehebung behoben werden können, finden Sie unter "Welche Probleme können mit Unified Manager behoben werden".

Aktivieren und Deaktivieren der Active IQ-Ereignisberichterstellung

Ereignisse auf der Active IQ-Plattform werden standardmäßig in der Benutzeroberfläche von Unified Manager generiert und angezeigt. Wenn diese Ereignisse zu „laut“ sind oder Sie diese Ereignisse nicht in Unified Manager anzeigen möchten, können Sie die Erzeugung dieser Ereignisse deaktivieren. Sie können sie zu einem späteren Zeitpunkt aktivieren, wenn Sie den Empfang dieser Benachrichtigungen fortsetzen möchten.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Wenn Sie diese Funktion deaktivieren, wird Active IQ-Plattformereignisse sofort von Unified Manager nicht mehr empfangen.

Wenn Sie diese Funktion aktivieren, beginnt Unified Manager gemäß der Zeitzone des Clusters kurz nach Mitternacht mit dem Empfang von Active IQ Plattformereignissen. Die Startzeit hängt ab, wenn Unified Manager AutoSupport Meldungen von jedem Cluster empfängt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Funktionseinstellungen**.
2. Deaktivieren oder aktivieren Sie auf der Seite **Feature Settings** Active IQ-Plattformereignisse, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren von Active IQ-Plattformereignissen	Bewegen Sie im Fenster **Active IQ Portal Ereignisse** die Schieberegler-Taste nach links.
Aktivieren von Active IQ-Plattformereignissen	Bewegen Sie im Fenster **Active IQ Portal Ereignisse** die Schieberegler-Taste nach rechts.

Eine neue Datei für Active IQ-Regeln wird hochgeladen

Unified Manager prüft automatisch auf eine neue Active IQ-Datei (Events, Regeln) und lädt eine neue Datei herunter, wenn neuere Regeln vorhanden sind. In Sites ohne externen Netzwerkzugriff müssen Sie die Regeldatei jedoch manuell hochladen.

Active IQ-Regeln werden auch als sichere Config Advisor-Regeln (CA) bezeichnet.

Wenn Sie Unified Manager auf eine bestimmte Version an einem Standort ohne Netzwerkverbindung installieren oder aktualisieren, stehen die gebündelten Active IQ-Regeln automatisch für den Upload zur Verfügung. Wir empfehlen jedoch, etwa einmal pro Monat eine neue Regeldatei von der NetApp Support Site herunterzuladen, um sicherzustellen, dass aktualisierte Ereignisse generiert werden und Ihre Storage-Systeme weiterhin optimal funktionieren.

Was Sie brauchen

- Die Ereignisberichte für das Active IQ Portal müssen aktiviert sein. Diese Funktion ist standardmäßig aktiviert. Weitere Informationen finden Sie unter "Aktivieren von Active IQ Portal-Ereignissen".
- Sie müssen die Regeldatei von der NetApp Support-Website herunterladen.

  Die Regeldatei befindet sich unter: https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

Schritte

1. Navigieren Sie auf einem Computer mit Netzwerkzugriff zur NetApp-Support-Website, und laden Sie die aktuelle Regeldatei herunter `.zip`.

   Das Paket der Paketregeln umfasst das regelRepository, die Datenquellen und einen NetApp KB-Artikel.

   > Auf Windows-Systemen wird der NetApp-KB-Artikel nicht standardmäßig mit dem Installer gebündelt, wenn er keine Netzwerkverbindung hat. Sie können die Datei *Secure_rules.zip* von der Support-Website herunterladen und hochladen, um den KB-Artikel für alle Regeln anzuzeigen.

2. Übertragen Sie die Regeldatei auf einige Medien, die Sie in den sicheren Bereich bringen können, und kopieren Sie sie dann in ein System im sicheren Bereich.
3. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Event-Setup**.
4. Klicken Sie auf der Seite **Event Setup** auf die Schaltfläche **Regeln hochladen**.
5. Navigieren Sie im Dialogfeld **Upload Rules** zu der heruntergeladenen Regeldatei, wählen Sie sie aus und `.zip` klicken Sie auf **Upload**.

   Dieser Vorgang kann einige Minuten dauern.

Die Regeldatei wird auf dem Unified Manager-Server entpackt. Nachdem die gemanagten Cluster nach Mitternacht eine AutoSupport-Datei generiert haben, überprüft Unified Manager die Cluster anhand der Regeldatei und erzeugt bei Bedarf neue Risiken und Vorfälle.

Weitere Informationen finden Sie in diesem Knowledge Base-Artikel (KB): "Wie man AIQCASecure Regeln manuell in Active IQ Unified Manager aktualisiert".

Generieren von Active IQ-Plattformereignissen

Ereignisse und Risiken auf Active IQ Plattformen werden wie in der folgenden Abbildung dargestellt in Unified Manager Ereignisse konvertiert.

Wie Sie sehen, wird die auf der Active IQ-Plattform kompilierte Regeldatei aktuell, Cluster-AutoSupport-Meldungen werden täglich generiert und Unified Manager aktualisiert die Liste der Ereignisse täglich.

Ereignisse auf der Active IQ Plattform werden aufgelöst

Störungen und Risiken von Active IQ Plattformen ähneln anderen Ereignissen von Unified Manager, da sie anderen Benutzern zur Lösung zugewiesen werden können und denselben verfügbaren Status aufweisen. Wenn Sie jedoch diese Art von Ereignissen mithilfe der Schaltfläche **Fix IT** lösen, können Sie die Auflösung innerhalb von Stunden

überprüfen.

In dem folgenden Diagramm sind die Maßnahmen aufgeführt, die Sie ergreifen müssen (in Grün) und die Aktion, die Unified Manager beim Beheben von Ereignissen übernimmt, die über die Active IQ Plattform generiert wurden.

Wenn Sie eine manuelle Behebung des Problems durchführen, müssen Sie sich bei System Manager oder der Befehlszeilenschnittstelle von ONTAP anmelden, um das Problem zu beheben. Sie können das Problem nur überprüfen, nachdem das Cluster eine neue AutoSupport Meldung um Mitternacht generiert hat.

Wenn Sie eine halbautomatische Auflösung mit der **Fix IT**-Taste durchführen, können Sie überprüfen, ob die Fehlerbehebung innerhalb von Stunden erfolgreich war.

Konfigurieren von Einstellungen für die Ereignisaufbewahrung

Sie können die Anzahl der Monate angeben, die ein Ereignis im Unified Manager-Server beibehalten wird, bevor es automatisch gelöscht wird.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Die Aufbewahrung von Ereignissen über 6 Monate kann die Serverleistung beeinträchtigen und wird nicht empfohlen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Datenspeicherung**.
2. Wählen Sie auf der Seite **Datenspeicherung** den Schieberegler im Bereich Ereignisaufbewahrung aus, und verschieben Sie ihn auf die Anzahl der Monate, die Ereignisse beibehalten werden sollen, und klicken Sie auf **Speichern**.

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 „Objektwartung gestartet“ auf der Seite „Ereignisverwaltung Bestand“ veröffentlicht. Dieses Ereignis wird automatisch veraltet, wenn das Wartungsfenster endet.

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

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

Planen eines Wartungsfensters zum Deaktivieren der Cluster-Ereignisbenachrichtigungen

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

Was Sie brauchen

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

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

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

Schritte

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

   Das Kalenderfenster wird angezeigt.

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

   Die Meldung „geplant“ wird neben dem Schieberegler angezeigt.

Wenn die Startzeit erreicht ist, wechselt das Cluster in den Wartungsmodus und ein Ereignis „Objektwartung 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.

Was Sie brauchen

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

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

Schritte

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

Ihr Ziel ist	Führen Sie diesen Schritt aus…
Ändern Sie den Zeitrahmen für ein geplantes Wartungsfenster	a. Klicken Sie neben dem Schieberegler auf den Text „geplant“. 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 „aktiv“ neben dem Schieberegler. 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.

Was Sie brauchen

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

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

Schritte

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

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

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

   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.

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.

Schritt

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 **Ereignisverwaltung**. b. Klicken Sie im Fensterbereich Filter auf der Seite „Inventar der Ereignisverwaltung“ 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, Ereignis oder Upgrade) verbunden, die Ihnen dabei hilft, Ereignisse zu priorisieren, die umgehend Korrekturmaßnahmen erfordern.

- **Vorfall**

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

- **Risiko**

  Ein Risiko ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster nicht mehr Daten für den Client bereitstellt, und nicht mehr genügend Speicherplatz zum Speichern von Daten vorhanden ist. Ereignisse mit Risikoeinwirkung können zu Serviceunterbrechungen führen. Möglicherweise ist eine Korrekturmaßnahme erforderlich.

- **Veranstaltung**

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

- **Upgrade**

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

Beschreibung der Bereiche für Ereignisauswirkungen

Ereignisse werden in sechs Auswirkungsbereiche unterteilt (Verfügbarkeit, Kapazität, Konfiguration, Performance, Schutz, Und Sicherheit) damit Sie sich auf die Arten von

Ereignissen konzentrieren können, für die Sie verantwortlich sind.

- **Verfügbarkeit**

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

- * Kapazität*

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

- **Konfiguration**

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

- **Leistung**

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

- **Schutz**

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

- **Sicherheit**

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

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

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.

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. Oben in diesem Abschnitt befindet sich der Zeit- und Datumsbereich, in dem ein Ereignis erkannt und zuletzt analysiert wurde. Bei aktiven Ereignissen (neu oder bestätigt) wird die zuletzt analysierte Zeit 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. Weitere Informationen finden Sie unter "Arten von Workloads, die von Unified Manager überwacht werden".

> 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 zu den dynamischen Leistungsschwellenwerten finden Sie unter "Analyse von Ereignissen aus dynamischen Leistungsschwellenwerten".

Informationen zum Einordnen der Workloads durch Unified Manager und zum Bestimmen 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 "Messwerte für die Workload-Performance".

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 Schreib MB/s 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.

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 Explorers wird ein Änderungssymbol () angezeigt , um das Datum und die Uhrzeit anzuzeigen, zu der die Änderung erkannt wurde.

Sie können die Performance-Diagramme auf den Seiten des Performance Explorers und auf der Seite Workload Analysis 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 Normalzustand zurück und alle Ereignisse, die durch diese Spitzen verursacht werden, 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.

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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Aggregat herabgestuft (ocumEvtAggregateRaidStateDegradiert)	Dar	Aggregat	Warnung
Cloud Tier teilweise erreichbar (ocumEventCloudTierPartiallyAbnehmbar)	Dar	Aggregat	Warnung
Cloud Tier nicht erreichbar (ocumEventCloudTiernicht erreichbar)	Dar	Aggregat	Fehler
Cloud-Tier-Zugriff für Aggregatverschiebung verweigert *(arlNetraCaCheckFailed)	Dar	Aggregat	Fehler
Zugriff auf Cloud-Ebene für Aggregatverschiebung während Storage Failover *(gbNetraCaCheckFailed) verweigert	Dar	Aggregat	Fehler
MetroCluster Aggregat links hinter(ocumEvtMetroClusterAggregateLeftBehind)	Dar	Aggregat	Fehler
MetroCluster Aggregatspiegelung mit herabgestufter(occumEvtMetroClusterAggregateMirrorDegradiert)	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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Aggregieren Sie Tage bis voll (ocumEvtAggregateTagenUntilFullSoon)	Dar	Aggregat	Fehler
Aggregat überengagiert (ocumEvtAggregateOverwockt)	Dar	Aggregat	Fehler
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
Unterschreitster kritischer Schwellenwert für MB/s des Aggregats (ocumAggregateMbpsVorfall)	Vorfall	Aggregat	Kritisch
MB/s Aggregat Warnung: Unterschreitster Schwellenwert (ocumAggregateMbpsWarnung)	Dar	Aggregat	Warnung
Unterschreiten der kritischen Latenzzeit für das Aggregat (ocumAggregateLatencyVorfall)	Vorfall	Aggregat	Kritisch
Warnung: Aggregatlatenz - nicht erreichenem Schwellenwert (okumAggregateLatencyWarnung)	Dar	Aggregat	Warnung
Verwendete Aggregat-Performance-Kapazität, kritischer Schwellenwert verletzt (ocumAggregatePerfkapazitätVerwendungVorfall)	Vorfall	Aggregat	Kritisch
Verwendete Aggregat-Performance-Kapazität, Warnschwellenwert nicht erreicht (ocumAggregatePerfkapazitätVerwendWarnung)	Dar	Aggregat	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreiten der Aggregatauslastung zum kritischen Schwellenwert (okumAggregateUtilizationVorfall)	Vorfall	Aggregat	Kritisch
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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Cluster-Überwachung fehlgeschlagen (ocumEvtClusterMonitoringFailed)	Dar	Cluster	Warnung
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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Cluster-Benutzerpasswort geändert *(cluster.passwd.changed)	Ereignis	Cluster	Informationsdaten

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unausgeglichene Cluster-Kapazität – Schwellenwert überschritten (ocumConformanceNodeImbalanceWarnung)	Dar	Cluster	Warnung
Cluster-Cloud-Tier-Planung (ClusterCloudTierPlanningWarnung)	Dar	Cluster	Warnung
Resync der FabricPool-Spiegelreplikation abgeschlossen *(WaflCaResyncComplete)	Ereignis	Cluster	Warnung
FabricPool-Bereich fast voll * (FabricPool Nearvoll)	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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
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
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
Unterschreiten Schwellenwert Für Das Lastwucht Des Clusters()	Dar	Cluster	Warnung
Unterschreitster Cluster-IOPS-Schwellenwert (OktumClusterIopsVorfall)	Vorfall	Cluster	Kritisch
Unterschreitster Cluster IOPS-Warnungsschwellenwert (ocumClusterIopsWarnung)	Dar	Cluster	Warnung
Cluster-MB/s – kritischer Schwellenwert überschritten (ocumClusterMbpsVorfall)	Vorfall	Cluster	Kritisch
Cluster MB/s Warnschwellenwert nicht erreicht (ocumClusterMbpsWarnung)	Dar	Cluster	Warnung
Nicht verbundenes dynamischer Schwellenwert (ocumClusterDynamicEventWarnung)	Dar	Cluster	Warnung

Impact Area: Security

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
AutoSupport HTTPS-Transport deaktiviert (ocumClusterASUPHttpsConfigurations deaktiviert)	Dar	Cluster	Warnung
Protokollweiterleitung nicht verschlüsselt (ocumClusterAuditLogunverschlüsselt)	Dar	Cluster	Warnung
Lokaler Admin-Standardbenutzer aktiviert (ocumClusterDefaultAdminaktiviert)	Dar	Cluster	Warnung
FIPS-Modus deaktiviert (ocumClusterFipsdeaktiviert)	Dar	Cluster	Warnung
Login Banner deaktiviert (ocumClusterLoginBannerdeaktiviert)	Dar	Cluster	Warnung
Login Banner geändert (ocumClusterLoginBannerChanged)	Dar	Cluster	Warnung
Log-Forwarding-Ziele geändert(ocumLogForwardDestinationsChanged)	Dar	Cluster	Warnung
NTP-Servernamen geändert(ocumNtpServerNamesChanged)	Dar	Cluster	Warnung
NTP-Server-Anzahl ist niedrig (securityConfigNTPServerCountLowRisk)	Dar	Cluster	Warnung
Cluster-Peer-Kommunikation nicht verschlüsselt (ocumClusterPeerVerschlüsselungdeaktiviert)	Dar	Cluster	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
SSH verwendet unsichere Chiffren (ocumClusterSSHInSecure)	Dar	Cluster	Warnung
Telnet-Protokoll aktiviert (ocumClusterTelnetEnabled)	Dar	Cluster	Warnung
Passwörter einiger ONTAP-Benutzerkonten verwenden die weniger sichere MD5-Hash-Funktion (ocumClusterMD5PasswordHashUsed).	Dar	Cluster	Warnung
Cluster verwendet selbstsigniertes Zertifikat (ocumClusterSelfSignedZertifikat)	Dar	Cluster	Warnung
Cluster-Remote-Shell ist aktiviert (ocumClusterRshdeaktiviert)	Dar	Cluster	Warnung
Cluster Certificate About to Expire (ocumEvtClusterCertificateAboutToExpire)	Dar	Cluster	Warnung
Cluster-Zertifikat abgelaufen (ocumEvtClusterCertificateExpired)	Dar	Cluster	Fehler

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
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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
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 Netzwerkschnittstelle (LIF)

Ereignisse an der Netzwerkschnittstelle liefern Informationen zum Status Ihrer Netzwerkschnittstelle (LIFs), 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: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Status der Netzwerkschnittstelle aus (ocumEvtLifStatusDown)	Dar	Schnittstelle	Fehler
FC/FCoE-Netzwerkschnittstelle Status ausgefallen (occumEvtFCLifStatus aus)	Dar	Schnittstelle	Fehler
Network Interface Failover nicht möglich (ocumEvtLifFailoverNotMögliche)	Dar	Schnittstelle	Warnung
Netzwerkschnittstelle nicht am Home Port (ocumEvtLifNotAtHomePort)	Dar	Schnittstelle	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Network Interface Route nicht konfiguriert (nicht zutreffend)	Ereignis	Schnittstelle	Informationsdaten

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Netzwerkschnittstelle MB/s kritischer Schwellenwert überschritten (ocumNetworkLifMbpsVorfall)	Vorfall	Schnittstelle	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Netzwerkschnittstelle MB/s Warnschwellenwert verletzt(OccumNetworkLifMbpsWarnung)	Dar	Schnittstelle	Warnung
FC-Netzwerkschnittstelle MB/s kritischer Schwellenwert überschritten (ocumFcpLifMbpsVorfall)	Vorfall	Schnittstelle	Kritisch
FC-Netzwerkschnittstelle MB/s Warnschwellenwert verletzt(OccumFcpLifMbpsWarnung)	Dar	Schnittstelle	Warnung
NVMf FC-Netzwerkschnittstelle MB/s Critical Threshold Überlaufen(ocumNvmfcLifMbpsVorfall)	Vorfall	Schnittstelle	Kritisch
NVMf FC-Netzwerkschnittstelle MB/s Warnschwellenwert verletzt(ocumNvmfcLifMbpsWarnung)	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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN zerstört * (lunDestroy)	Ereignis	LUN	Informationsdaten
LUN zugeordnet mit nicht unterstütztem Betriebssystem in igroup(igroupUnsupportedOsType)	Vorfall	LUN	Warnung
Einzel aktiv Pfad für den Zugriff auf LUN(occumEvtLunSingleActivePath)	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
Kein Pfad zum LUN-Zugriff von einem Knoten im HA-Paar (ocumEvtLunNodePathStatusDown)	Dar	LUN	Fehler

Impact Area: Kapazität

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unzureichender Speicherplatz für LUN Snapshot Kopie (ocumEvtLunSnapshotmöglich)	Dar	Datenmenge	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN zugeordnet mit nicht unterstütztem Betriebssystem in igroup(igroupUnsupportedOsType)	Dar	LUN	Warnung

Impact Area: Performance

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreiten kritischer Schwellenwert für LUN-IOPS (OktumLunIopsVorfall)	Vorfall	LUN	Kritisch
Unterschreitr. LUN IOPS-Warnungsschwellenwert (ocumLunIopsWarnung)	Dar	LUN	Warnung
LUN MB/s Critical Threshold unchoccumLunMbpsIncident (ocumLunMbpsIncident)	Vorfall	LUN	Kritisch
LUN MB/s Warnschwellenwert nicht eingehalten(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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
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 (ocumLunLatenzMbpsVorfall)	Vorfall	LUN	Kritisch
LUN-Latenz und MB/s Warnschwellenwert nicht eingehalten(ocumLunenzMbpsWarnung)	Dar	LUN	Warnung
LUN-Latenz und Aggregat-Performance-Kapazität verwendet kritische Schwellenwert verletzt(ocumLunenzaggregatPerformance-AggregatePerformance-KapazitätenUsedVorfall)	Vorfall	LUN	Kritisch
LUN-Latenz und verwendete Aggregat-Performance-Kapazität Warnschwellenwert nicht erreicht (ocumLunenzAggregatePerformance-KapazitätenUsedWarnung)	Dar	LUN	Warnung
LUN-Latenz und aggregierte Auslastung kritischer Schwellenwert überschritten (ocumLunenzAggregateUtilizationVorfall)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN-Latenz und Aggregat-Auslastung Warnschwellenwert nicht erreicht (ocumLunenzAggregateUtilizationWarnung)	Dar	LUN	Warnung
LUN-Latenz und Node-Performance-Kapazität verwendet kritischen Schwellenwert überschritten (ocumLunLatenzenNodePerformance-kapazitätBenutzerfall)	Vorfall	LUN	Kritisch
Verwendete LUN-Latenz und Node-Performance-Kapazität – Warnschwellenwert nicht erreicht (ocumLunLatencyNodePerformance-kapazitätUsedWarnung)	Dar	LUN	Warnung
LUN-Latenz und verwendete Node-Performance-Kapazität – Takeover Critical Threshold Rected (ocumLunenzyAggregatePerfkapazitätUseTakeoverIncident)	Vorfall	LUN	Kritisch
Verwendete LUN-Latenz und Node-Performance-Kapazität - Überschreiten Warnungsschwellenwert (ocumLunenzAggregatePerfkapazitätUseTakeoverWarning)	Dar	LUN	Warnung
LUN-Latenz und Node-Auslastung – kritischer Schwellenwert – nicht erreicht (ocumLunLatenzenNodeUtilizationVorfall)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
LUN-Latenz und Node-Auslastung Warnung nicht erreichender Schwellenwert (ocumLunenzNodeUtilizationWarnung)	Dar	LUN	Warnung
QoS LUN Max. IOPS Warnschwellenwert nicht erreicht (ocumQosLunMaxIopsWarnung)	Dar	LUN	Warnung
QoS LUN Max. MB/s Warnschwellenwert verletzt(ocumQosLunMaxMbpsWarnung)	Dar	LUN	Warnung
Workload-LUN-Latenzschwellenwert, der gemäß Definition in der Performance-Service-Level-Richtlinie überschritten wird (ocumConformanceLatencyWarnung)	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
Management Server Disk Space Fast Full (ocumEvtUnifiedManagerDiskSpaceNearFast Full)	Dar	Management Station	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Freier Speicherplatz auf dem Verwaltungsserver voll (ocumEvtUnifiedManagerDiskSpaceFull)	Vorfall	Management Station	Kritisch
Management Server, auf dem der Speicher gering ist (ocumEvtUnifiedManagerMemoryLow)	Dar	Management Station	Warnung
Management Server fast nicht genügend Arbeitsspeicher (ocumEvtUnifiedManagerMemoryAlmostOut)	Vorfall	Management Station	Kritisch
Größe der MySQL-Log-Datei erhöht; Neustart erforderlich (ocumEvtMystqlLogFileSizeWarnung)	Vorfall	Management Station	Warnung
Die Zuweisung der Größe des gesamten Prüfprotokolls ist „Jetzt voll“	Dar	Management Station	Warnung
Syslog-Server-Zertifikat – Informationen zum Ablauf	Dar	Management Station	Warnung
Syslog Server-Zertifikat Abgelaufen	Dar	Management Station	Fehler
Audit Log-Datei Manipuliert	Dar	Management Station	Warnung
Audit Log-Datei Gelöscht	Dar	Management Station	Warnung
Syslog-Server-Verbindungsfehler	Dar	Management Station	Fehler
Syslog Server-Konfiguration Geändert	Ereignis	Management Station	Warnung

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 Bridges. So können Sie auf potenzielle Probleme in einer MetroCluster-over-FC-Konfiguration 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
Brücke nicht erreichbar(OktEvtBridgeheUnerreichbar)	Vorfall	MetroCluster-Brücke	Kritisch
Brückentemperatur anormal (occumEvtBridgeTemperatureAbnormal)	Vorfall	MetroCluster-Brücke	Kritisch

Veranstaltungen für MetroCluster-Konnektivität

Konnektivitätsereignisse bieten Informationen über die Konnektivität zwischen den Komponenten eines Clusters und zwischen den Clustern in MetroCluster über FC und MetroCluster über IP-Konfigurationen, 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.

In beiden Konfigurationen übliche Ereignisse

Diese Konnektivitätsereignisse sind sowohl für MetroCluster über FC als auch für MetroCluster über IP-Konfigurationen üblich.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Alle Links zwischen MetroCluster Partnern ausgefallen(occumEvtMetroClusterAllLinksBetweenPartnerDown)	Vorfall	MetroCluster Beziehung	Kritisch
MetroCluster Partner nicht über Peering-Netzwerk erreichbar(ocumEvtMetroClusterPartnerNotErreichbarkeit oberhalb von Netzwerk)	Vorfall	MetroCluster Beziehung	Kritisch
Betroffene MetroCluster Disaster Recovery-Funktion (ocumEvtMetroClusterDRStatusImpacted)	Dar	MetroCluster Beziehung	Kritisch
MetroCluster Konfiguration umgeschaltet(ocumEvtMetroClusterDRStatusImpacted)	Dar	MetroCluster Beziehung	Warnung

Konfiguration von MetroCluster over FC

Diese Ereignisse betreffen MetroCluster über FC-Konfigurationen.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Alle Inter-Switch Links Down(ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Vorfall	MetroCluster-Inter-Switch-Verbindung	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
FC-SAS Bridge zu Storage Stack Link Down (ocumEvtBridgeSasPortDown)	Vorfall	MetroCluster Bridge-Stack-Verbindung	Kritisch
MetroCluster Konfiguration teilweise umgeschaltet(ocumEvtMetroClusterDRStatusPartially ImpACTED)	Dar	MetroCluster Beziehung	Fehler
Knoten zu FC Switch Alle FC-VI Interconnect Links Down (ocumEvtMccNodeSwitchFcviLinksDown)	Vorfall	MetroCluster-Node-Switch-Verbindung	Kritisch
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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
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

Konfiguration von MetroCluster over IP

Diese Ereignisse betreffen MetroCluster über IP-Konfigurationen.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
MetroCluster IP-Verbindungsstatus der intersite ist ausgefallen (mcIntersitectureityStatusDown)	Dar	MetroCluster Beziehung	Kritisch
MetroCluster-IP Node zu Switch-Offline-Verbindung (mcIpPortStatusOffline)	Dar	Knoten	Fehler

Ereignisse auf dem MetroCluster-Switch

MetroCluster Switch-Ereignisse für MetroCluster-over-FC-Konfigurationen bieten Ihnen Informationen zum Status der MetroCluster-Switches, 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: 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
NVMe Namespace MB/s Critical Threshold Undurchbrochen (ocumNvmeNamespaceMbpsVorfall)	Vorfall	Namespace	Kritisch
NVMe Namespace MB/s Warnschwellenwert nicht eingehalten (ocumNvmeNamespaceMbpsWarnung)	Dar	Namespace	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
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 MB/s kritischer Schwellenwert – nicht überschritten (ocumNvmeNamespaceLatenzenMbpsVorfall)	Vorfall	Namespace	Kritisch
NVMe Namespace-Latenz und MB/s Warnschwellenwert nicht eingehalten (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
Cloud AWS IAMRoleNotFound * (ocumCloudAwsIamRoleNotFound)	Dar	Knoten	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unlösbar für Cloud Tier Host * (ocumObjstoreHostUnlösbar)	Dar	Knoten	Fehler
Cloud Tiering Intercluster-Netzwerkschnittstelle * (ocumObjstoreInterClusterLifDown)	Dar	Knoten	Fehler
Einer der NFSv4 Pools erschöpft * (nbladeNfsv4PoolEXhaust)	Vorfall	Knoten	Kritisch
Unmatch Cloud Tier Signature *(osbosnatureMismatch) anfordern	Dar	Knoten	Fehler

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
Node-MB/s – kritischer Schwellenwert überschritten (ocumNodeMbpsVorfall)	Vorfall	Knoten	Kritisch
Knoten MB/s Warnschwellenwert überschritten(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-Kapazität verwendet kritischen Schwellenwert verletzt (OktumNodePerftätNutzungVorfall)	Vorfall	Knoten	Kritisch
Verwendete Node-Performance-Kapazität, Warnschwellenwert nicht erreicht (ocumNodePerfkapazitätUsedWarnung)	Dar	Knoten	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Verwendete Node-Performance-Kapazität – Übernahme durch kritischen Schwellenwert überschritten (OktumNodePerftätNutzungTakeoverVorfall)	Vorfall	Knoten	Kritisch
Verwendete Node-Performance-Kapazität – Überschreitung der Warnschwelle (nicht erreicht wegen Performance-Performance-Performance-Kapazitäts-UseTakeoverWarning)	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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Nicht genutzter Performance-Kapazitätsschwellenwert (OktumNodeÜberschreitung Warnung)	Dar	Knoten	Warnung
Nicht behebener dynamischer Knotenschwellenwert (ocumNodeDynamicEvent Warnung)	Dar	Knoten	Warnung

Impact Area: Security

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Advisory ID: NTAP-<__Advisory ID_>(ocumx)	Dar	Knoten	Kritisch

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
Port MB/s kritischer Schwellenwert überschritten (ocumNetworkPortMbpsVorfall)	Vorfall	Port	Kritisch
Netzwerk-Port MB/s Warnschwellenwert nicht eingehalten (ocumNetworkPortMbpsWarnung)	Dar	Port	Warnung
MB/s kritischer Schwellenwert für FCP-Port überschritten (ocumFcpPortMbpsVorfall)	Vorfall	Port	Kritisch
MB/s-Warnschwellenwert für FCP-Port überschritten(ocumFcpPortMbpsWarnung)	Dar	Port	Warnung
Auslastung des Netzwerkports – kritischer Schwellenwert – unterlaufen (NetzwerkPortUtilizationVorfall)	Vorfall	Port	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Warnung über Netzwerk-Port-Auslastung, nicht überschritten (OktumNetzwerkPortUtilizationWarnung)	Dar	Port	Warnung
Unterschreitender Schwellenwert für die FCP-Port-Auslastung (ocumFcpPortUtilizationVorfall)	Vorfall	Port	Kritisch
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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
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

SnapMirror Beziehungsereignisse geben Ihnen Informationen zum Status Ihrer asynchronen und synchronen SnapMirror Beziehungen, sodass Sie mögliche Probleme überwachen können. Asynchrone SnapMirror Beziehungsereignisse werden sowohl für Storage VMs als auch für Volumes generiert, synchrone SnapMirror Beziehungsereignisse werden jedoch nur für Volume-Beziehungen erstellt. Es gibt keine Ereignisse für zusammengehörige Volumes, die Teil der Disaster-Recovery-Beziehungen für Storage VMs sind. 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.

Die Ereignisse der SnapMirror Beziehungen werden für Storage VMs generiert, die durch die Disaster Recovery von Storage VM gesichert sind, jedoch nicht für einzelne Objektbeziehungen.

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
Spiegelreplikation – Fehler (occumEvtSnapMirrorRelationshipLagerFehler)	Dar	SnapMirror Beziehung	Fehler
Spiegelreplikation Verzögerung Warnung(occumEvtSnapMirrorRelationshipLagerWarnung)	Dar	SnapMirror Beziehung	Warnung
Resync der Spiegelreplikation fehlgeschlagen(OccumEvtSnapmirrorRelationshipResyncFailed)	Dar	SnapMirror Beziehung	Fehler
Synchronous Replication Out of Sync * (syncSnapmirrorRelationshipOutofsync)	Dar	SnapMirror Beziehung	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Synchrone Replizierung wiederhergestellt * (syncSnapmirrorRelationshipInSync)	Ereignis	SnapMirror Beziehung	Informationsdaten
Synchronous Replication Auto Resync failed * (Synchronisieren von SnapmirrorRelationshipAutoSyncRetryFailed)	Dar	SnapMirror Beziehung	Fehler
ONTAP Mediator wird auf dem Cluster hinzugefügt (SnapmirrorMediatorHinzugefügt)	Ereignis	Cluster	Informationsdaten
ONTAP Mediator wird aus dem Cluster entfernt (SnapmirrorMediatorRemoved)	Ereignis	Cluster	Informationsdaten
ONTAP Mediator ist vom Cluster nicht erreichbar (SnapmirrorMediatornicht erreichbar)	Dar	Mediator	Warnung
Zugriff auf ONTAP Mediator ist über das Cluster nicht möglich (SnapmirrorMediatorMiskonfiguriert)	Dar	Mediator	Fehler
ONTAP Mediator Connectivity wurde neu eingerichtet, neu synchronisiert und bereit für SnapMirror Active Sync (snapmirrorMediatorInQuorum)	Ereignis	Mediator	Informationsdaten

Ereignisse für asynchrone Spiegelung und Vault Beziehungen

Die Beziehungsereignisse von Asynchronous Mirror und Vault liefern Ihnen Informationen zum Status Ihrer asynchronen SnapMirror- und Vault-Beziehungen, damit Sie das System auf potenzielle Probleme überwachen können. Ereignisse für asynchrone Mirror- und Vault-Beziehungen werden sowohl für Volume- als auch für Storage VM-

Sicherungsbeziehungen unterstützt. Aber für das Disaster Recovery von Storage VM werden nicht nur Vault-Beziehungen unterstützt. Ereignisse sind nach Impact Area gruppiert und umfassen den Ereignis- und Trap-Namen, den Impact-Level, den Quelltyp und den Schweregrad.

Aufprallbereich: Schutz

Die Ereignisse zu SnapMirror und Vault Beziehungen werden auch für Storage VMs generiert, die durch die Disaster Recovery von Storage VM geschützt sind, jedoch nicht für einzelne Objektbeziehungen.

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Asynchroner Spiegel und Vault ungesund (OktMirrorVaultRelationshipUngesund)	Dar	SnapMirror Beziehung	Warnung
Asynchrones Spiegeln und Vault broken-off(ocumEvtMirrorVaultRelationshipSteateBrokenoff)	Dar	SnapMirror Beziehung	Fehler
Asynchrone Spiegelung und Vault Initialisieren fehlgeschlagen (OktEvtMirrorVaultRelationshierInitialisierenFailed)	Dar	SnapMirror Beziehung	Fehler
Asynchrones Spiegeln und Vault-Update fehlgeschlagen (ocumEvtMirrorVaultRelationshipUpdatefehlgeschlagen)	Dar	SnapMirror Beziehung	Fehler
Asynchronous Mirror und Vault lag Fehler (ocumEvtMirrorVaultRelationshipLagerFehler)	Dar	SnapMirror Beziehung	Fehler
Asynchronous Mirror und Vault lag Warnung(OccumEvtMirrorVaultRelationshipLagerWarnung)	Dar	SnapMirror Beziehung	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Resync für asynchronen Spiegel und Vault fehlgeschlagen (OcumEvtMirrorVaultRelationshipResyncFailed)	Dar	SnapMirror Beziehung	Fehler

Das Ereignis „SnapMirror Update Failure“ wird vom Active IQ Portal (Config Advisor) angehoben.

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
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
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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Anormaler Strombereich (ocumEvtShelfAktuellesAbnormal)	Dar	Storage Shelf	Warnung
Anormale Temperatur(OkumEvtShelfTemperatureAbnormal)	Dar	Storage Shelf	Warnung

Ereignisse von Storage-VM

Ereignisse der Storage-VM (Storage Virtual Machine, auch als SVM bekannt) bieten Ihnen Informationen zum Status Ihrer Storage-VMs (SVMs), 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.

Ein Sternchen (*) identifiziert EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Impact Area: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Storage VM CIFS Service Down (ocumEvtVserverCifsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM CIFS-Service nicht konfiguriert (nicht zutreffend)	Ereignis	SVM	Informationsdaten
Versuche, nicht vorhandene CIFS Share zu verbinden *(nbladeCifsNoPrivShare)	Vorfall	SVM	Kritisch
CIFS NetBIOS Namenskonflikt * (nbladeCifsNbNameConflict)	Dar	SVM	Fehler
CIFS Shadow Copy Operation fehlgeschlagen *(cifsShadowCopyFailure)	Dar	SVM	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Viele CIFS-Verbindungen * (nbladeCifsManyAuths)	Dar	SVM	Fehler
Max. CIFS-Verbindung überschritten * (nbladeCifsMaxOpenSameFile)	Dar	SVM	Fehler
Max. Anzahl der CIFS-Verbindung pro Benutzer überschritten *(nbladeCifsMaxSessPerusrConn)	Dar	SVM	Fehler
SVM FC/FCoE Service-Down (ocumEvtVserverFcServiceStatusDown)	Vorfall	SVM	Kritisch
SVM iSCSI Service-Down(ocumEvtVserverIscsiServiceStatusDown)	Vorfall	SVM	Kritisch
Storage VM NFS Service Down(ocumEvtVserverNfsServiceStatusDown)	Vorfall	SVM	Kritisch
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
Storage VM angehalten (ocumEvtVserverDown)	Dar	SVM	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
AV-Server zu beschäftigt, um neue Scananforderung zu akzeptieren *(nbladeVscanConnBackPressure)	Dar	SVM	Fehler
Keine AV-Server-Verbindung für Virus Scan *(nbladeVscanNoScannerConn)	Vorfall	SVM	Kritisch
Kein AV-Server registriert *(nbladeVscanNoRegdScanner)	Dar	SVM	Fehler
Keine Responsive AV-Serververbindung *(nbladeVscanConnInaktiv)	Ereignis	SVM	Informationsdaten
Nicht autorisierter Benutzerversuch für AV-Server *(nbladeVscanBadUserPrivAccess)	Dar	SVM	Fehler
Virus von AV Server gefunden *(nbladeVscanVirusDetected)	Dar	SVM	Fehler

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
SVM MB/s Critical Threshold ToctusctusSvmMbpsVorfall)	Vorfall	SVM	Kritisch
SVM MB/s Warnschwellenwert überschritten (ocumSvmMbpsWarnung)	Dar	SVM	Warnung
Unterschreiten kritischen Schwellenwert für SVM-Latenz (ocumSvmLatencyVorfall)	Vorfall	SVM	Kritisch
Unterschreitung – SVM-Latenzschwellenwert (ocumSvmLatencyWarnung)	Dar	SVM	Warnung

Impact Area: Security

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Audit Log deaktiviert(ocumVserverAuditLogdeaktiviert)	Dar	SVM	Warnung
Login Banner deaktiviert(ocumVserverLoginBannerdeaktiviert)	Dar	SVM	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
SSH verwendet unsichere Chiffren (ocumVserverSSHInSecure)	Dar	SVM	Warnung
Login Banner geändert(ocumVserverLoginBannerChanged)	Dar	SVM	Warnung
Anti-Ransomware-Überwachung von Storage-VMs ist deaktiviert (antiErlöserSvmStatedeaktiviert)	Dar	SVM	Warnung
Das Anti-Ransomware-Monitoring für Storage VMs ist aktiviert (Learning Mode) (antiBefreiwareSvmStateDryrun).	Ereignis	SVM	Informationsdaten
Storage VM geeignet für die Ransomware-Überwachung (Learning Mode) (ocumEvtSvmArwCandidate)	Ereignis	SVM	Informationsdaten

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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
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
Volume Efficiency Operation Error(ocumEvtVolumeEfficiency OperationError)	Dar	Datenmenge	Fehler
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

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume Qtree Kontingent fast überengagiert (ocumEvtVolumeQtreeQuotaAlmostÜberengagiert)	Dar	Datenmenge	Warnung
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 *(flexGroupKonstitutionenHaveInodesIssues)	Dar	Datenmenge	Fehler

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
FlexGroup-Komponenten inodes Status alles OK *(flexGroupConstitutionenInodesStatusAllOK)	Ereignis	Datenmenge	Informationsdaten
Fehler bei der WAFL-Volume-AutoSize * (WaflVolAutoSizeFail)	Dar	Datenmenge	Fehler
Automatische WAFL-Volume-Größe abgeschlossen * (WaflVolAutoSizeDone)	Ereignis	Datenmenge	Informationsdaten
FlexGroup Volumen ist über 80% ausgelastet*	Vorfall	Datenmenge	Fehler
FlexGroup Volumen ist über 90% ausgelastet*	Vorfall	Datenmenge	Kritisch
Volume Storage-Effizienz-Anomalie (ocumVolumeAbnormalStorageEffizienzWarnung)	Dar	Datenmenge	Warnung
Volume Snapshot-Reserve wird nicht genutzt (VolumeSnaphotReserveUnderutilizedWarnung)	Ereignis	Datenmenge	Warnung
Volume Snapshot Reserve wird nicht genutzt (VolumeSnaphotReserveUnderutilizedCleared)	Ereignis	Datenmenge	Warnung

Impact Area: Konfiguration

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volumen umbenannt(nicht zutreffend)	Ereignis	Datenmenge	Informationsdaten

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
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. MB/s Warnschwellenwert überschritten(ocumQosVolumeMaxMbpsWarnung)	Dar	Datenmenge	Warnung
QoS Volume Max. IOPS/TB Warnschwellenwert nicht erreicht (ocumQosVolumeMaxIopsPerTbWarnung)	Dar	Datenmenge	Warnung
Überschreitung des Workload-Volume-Latenzschwellenwerts gemäß Definition der Performance-Service-Level-Richtlinie (ocumConformanceLatency Warning)	Dar	Datenmenge	Warnung
Unterschreiten des kritischen Schwellenwerts für Volume-IOPS (OktumVolumeIopsVorfall)	Vorfall	Datenmenge	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Unterschreitr. Volume IOPS-Warnungsschwellenwert (ocumVolumeIopsWarnung)	Dar	Datenmenge	Warnung
Unterschreiten kritischen Schwellenwert für Volume-MB/s (ocumVolumeMbpsVorfall)	Vorfall	Datenmenge	Kritisch
Volume MB/s Warnschwellenwert überschritten(OccumVolumeMbpsWarnung)	Dar	Datenmenge	Warnung
Volume-Latenz – kritischer Schwellenwert überschritten (ocumVolumeLatenzIncident)	Vorfall	Datenmenge	Kritisch
Schwellenwert für Volume-Latenzwarnung 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
Volume-Latenz und IOPS – kritischer Schwellenwert – nicht erreicht (ocumVolumeLatencyIopsVorfall)	Vorfall	Datenmenge	Kritisch

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Nicht erreichender Volume-Latenz und IOPS-Warnungsschwellenwert (ocumVolumeLatencyIops Warnung)	Dar	Datenmenge	Warnung
Volume-Latenz und MB/s kritischer Schwellenwert – nicht überschritten (ocumVolumeLatencyMbpsVorfall)	Vorfall	Datenmenge	Kritisch
Volume-Latenz und MB/s Warnschwellenwert nicht eingehalten (ocumVolumeLatencyMbpsWarnung)	Dar	Datenmenge	Warnung
Volume-Latenz und Aggregat-Performance-Kapazität eingesetzt. Kritischer Schwellenwert ist nicht erreicht (ocumVolumeLatencyAggregatePerformance-KapazitätenUsedVorfall)	Vorfall	Datenmenge	Kritisch
Volume-Latenz und verwendete Aggregat-Performance-Kapazität Warnschwellenwert nicht erreicht (ocumVolumeLatencyAggregatePerformance-KapazitätenUsedWarnung)	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-Kapazität verwendet kritischer Schwellenwert – nicht erreicht (ocumVolumeLatencyNodePerformance-kapazitätBenutzerfall)	Vorfall	Datenmenge	Kritisch
Verwendete Volume-Latenz und Node-Performance-Kapazität – Warnschwellenwert nicht erreicht (ocumVolumeLatencyNodePerformance-kapazitätUsedWarnung)	Dar	Datenmenge	Warnung
Verwendete Volume-Latenz und Node-Performance-Kapazität – Überschreiten kritischer Schwellenwert (ocumVolumeLatencyAggregatePerfkapazitätUseTakeoverIncident)	Vorfall	Datenmenge	Kritisch
Verwendete Volume-Latenz und Node-Performance-Kapazität – Überschreitung der Schwellenwertverletzungen (ocumVolumeLatencyAggregatePerfkapazitätUseTakeoverWarning)	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

Impact Area: Security

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume-Anti-Ransomware-Überwachung ist aktiviert (aktiv-Modus) (antiBefreieVolumeaktiviert)	Ereignis	Datenmenge	Informationsdaten
Volume-Anti-Ransomware-Überwachung ist deaktiviert (antiBefreieVolumeSpeicherdeaktiviert)	Dar	Datenmenge	Warnung
Volume-Anti-Ransomware-Überwachung ist aktiviert (Learning Mode) (antiBefreieVolumeStateDryrun)	Ereignis	Datenmenge	Informationsdaten
Volume Anti-Ransomware Monitoring ist angehalten (Learning Mode) (antiBefreiwareVolumeStateDryrunPen)	Dar	Datenmenge	Warnung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume-Anti-Ransomware-Überwachung ist angehalten (aktiver Modus) (antiBefreieVolumeSpeicherErd)	Dar	Datenmenge	Warnung
Anti-Ransomware-Monitoring auf Volume wird deaktiviert (AntiErlöserVolumeSpeicherErsternInProgress)	Dar	Datenmenge	Warnung
Aktivitäten durch Ransomware (CallHomeBefreiwareActivitySeen)	Vorfall	Datenmenge	Kritisch
Volume geeignet für die Anti-Ransomware-Überwachung (Lernmodus) (ocumEvtVolumeArwCandidate)	Ereignis	Datenmenge	Informationsdaten
Volume geeignet für die Anti-Ransomware-Überwachung (aktiver Modus) (ocumVolumeSuitedForActiveAntiBefreiwareDetection)	Dar	Datenmenge	Warnung
Volume weist eine laute Anti-Ransomware-Warnung auf (antiBefreiwareFeatureNoisyVolume)	Dar	Datenmenge	Warnung

Impact-Bereich: Datensicherung

Ereignisname (Trap-Name)	Auswirkungen	Typ der Quelle	Schweregrad
Volume verfügt über unzureichenden lokalen Snapshot-Schutz (VolumeLackLocalProtectionWarnung)	Dar	Datenmenge	Warnung
Volume verfügt über unzureichenden lokalen Snapshot-Schutz (VolumeLackLocalProtectionCleared)	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 „Lagerbestand für das Ereignismanagement“ und die Seite „Ereignisdetails“ verwenden, um alle Ereignisse zu überwachen. Über das Dialogfeld „Benachrichtigungseinstellungen“ können Sie Benachrichtigungen konfigurieren. Mithilfe der Seite Event Setup können Sie Ereignisse deaktivieren bzw. aktivieren.

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 „Anwendungsadministrator“ 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 „ActiveIQUnifiedManager@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.

- **Start/TLS verwenden**

  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. Um mehrere Trap-Ziele festzulegen, trennen Sie jeden Host durch ein Komma.

  Alle anderen SNMP-Einstellungen, z. B. „Version“ und „Outbound Port“, müssen für alle Hosts in der Liste identisch sein.

- * 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.

Weitere Informationen zu SNMP-Objekten und -Traps finden Sie "Active IQ Unified Manager MIB"auf der NetApp-Support-Website.

Inventarseite des Ereignismanagements

Auf der Seite „Ereignismanagement-Bestand“ können Sie eine Liste aktueller Ereignisse und ihrer Eigenschaften anzeigen. Sie können Aufgaben wie Quittieren, Auflösen und Zuweisen von Ereignissen durchführen. Sie können auch eine Meldung für bestimmte Ereignisse hinzufügen.

Die Informationen auf dieser Seite werden automatisch alle 5 Minuten 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.

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.

- **Berichte**

  Ermöglicht das Exportieren von Details der aktuellen Ereignisansicht in eine kommagetrennte Datei (.csv) oder ein PDF-Dokument.

- **Spaltenauswahl Ein-/Ausblenden**

  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 wird die Ansicht Alle aktiven Ereignisse angezeigt, um die neuen und bestätigten Ereignisse für die letzten sieben Tage mit einem Level der Auswirkung von Vorfall oder Risiko anzuzeigen.

- **Auslösezeit**

  Die Zeit, zu der das Ereignis generiert wurde.

- **Severity**

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

- **Bundesland**

  Der Ereignisstatus: Neu, bestätigt, aufgelöst oder veraltet.

- **Impact Level**

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

- **Aufprallbereich**

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

- **Name**

  Der Ereignisname. Sie können den Namen auswählen, um die Seite Ereignisdetails für dieses Ereignis anzuzeigen.

- **Quelle**

  Der Name des Objekts, auf dem das Ereignis aufgetreten ist. Sie können den Namen auswählen, um die Seite mit den Angaben zu Systemzustand und Performance für das Objekt anzuzeigen.

  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.

- **Quelltyp**

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

- * Zugewiesen Zu*

  Der Name des Benutzers, dem das Ereignis zugeordnet ist.

- **Event Ursprung**

  Ob das Ereignis aus dem "Active IQ Portal" oder direkt aus "Active IQ Unified Manager" stammt.

- **Anmerkungsname**

  Der Name der Anmerkung, die dem Speicherobjekt zugewiesen 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.

Eine Beschreibung der hier angezeigten Komponenten finden Sie unter *Cluster-Komponenten und darüber, warum sie sich in Konflikt befinden können*.

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 Information ( ).

- **Impact Level**

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

- **Aufprallbereich**

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

- **Quelle**

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

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

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

- **Quellanmerkungen**

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

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

- **Quellgruppen**

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

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

- **Quelltyp**

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

- * Auf Cluster*

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

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

- **Betroffene Objekte Zählen**

  Die Anzahl der vom Ereignis betroffenen Objekte.

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

  Dieses Feld wird nur für Performanceereignisse angezeigt.

- * Betroffene Volumen*

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

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

- * Ausgelöste Richtlinie*

  Der Name der Schwellenwertrichtlinie, die das Ereignis ausgegeben hat.

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

  Dieses Feld wird nur für Performanceereignisse angezeigt.

- **Regel-Id**

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

- * Bestätigt durch*

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

- * Gelöst von*

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

- * Zugewiesen zu*

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

- **Warnmeldungseinstellungen**

  Die folgenden Informationen über Meldungen werden angezeigt:

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

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

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

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

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

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

  Deaktivierte Warnmeldungen werden nicht angezeigt.

- **Letzte Benachrichtigung Gesendet**

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

- **Senden nach**

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

- **Vorheriger Skriptlauf**

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

Der Abschnitt „Empfohlene Maßnahmen“ wird angezeigt

Der Abschnitt „Empfohlene Maßnahmen“ auf der Seite „Veranstaltungsdetails“ enthält mögliche Gründe für das Ereignis und schlägt einige Maßnahmen vor, damit Sie versuchen können, das Ereignis selbst zu lösen. Die vorgeschlagenen Maßnahmen

werden auf Grundlage der Art des Ereignisses oder des Schwellenwerts, die nicht eingehalten wurden, angepasst.

Dieser Bereich wird nur für bestimmte Ereignistypen angezeigt.

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

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

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

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

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

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.

Seite „Ereignis-Einrichtung“

Auf der Seite Event Setup werden die Liste der deaktivierten Ereignisse angezeigt und Informationen wie den zugehörigen Objekttyp und den Schweregrad des Ereignisses bereitgestellt. Sie können auch Aufgaben wie Deaktivieren oder Aktivieren von Ereignissen global ausführen.

Sie können diese Seite nur aufrufen, wenn Sie die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ 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.

- **Regeln Hochladen**

  Startet das Dialogfeld „Regeln hochladen“, in dem Sites ohne externen Netzwerkzugriff die Datei „Active IQ-Regeln“ manuell auf Unified Manager hochladen können. Die Regeln werden auf Cluster AutoSupport Meldungen ausgeführt, um Ereignisse für die Systemkonfiguration, Verkabelung, Best Practice und Verfügbarkeit zu generieren, die von der Active IQ Plattform definiert wurden.

- **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.

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 „Anwendungsadministrator“ 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 oder den Schwellenwert, der gegen das Ereignis verstoßen wurde, sowie 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.

Nachstehend finden Sie eine Beispiel-E-Mail für eine Warnmeldung:

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.

Was Sie brauchen

- Sie müssen Benachrichtigungseinstellungen wie die Benutzer-E-Mail-Adresse, den SMTP-Server und den

SNMP-Trap-Host konfiguriert haben, damit der Active IQ Unified Manager-Server diese Einstellungen verwenden kann, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.

- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Meldung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie ein Skript auf der Grundlage des Ereignisses ausführen möchten, müssen Sie das Skript mithilfe der Seite „Skripte“ zu Unified Manager hinzugefügt haben.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können eine Warnmeldung direkt auf der Seite Ereignisdetails erstellen, nachdem Sie ein Ereignis empfangen haben. Zusätzlich können Sie eine Warnung auf der Seite „Alarmkonfiguration“ erstellen, wie hier beschrieben.

Schritte

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

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

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

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

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

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

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

   Sie können auch Benutzer über SNMP-Traps benachrichtigen.

7. Klicken Sie Auf **Speichern**.

Beispiel für das Hinzufügen einer Meldung

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

- Alarmname: HealthTest
- Ressourcen: Enthält alle Volumes, deren Name "abc" enthält und schließt alle Volumes aus, deren Name "xyz" enthält
- Ereignisse: Umfasst alle kritischen Systemzustandsereignisse
- Aktionen: Enthält "sample@domain.com", ein "Test"-Skript, 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 **`HealthTest`** in das Feld **Alert Name** ein.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
   a. Geben Sie **`abc`** in das Feld **Name enthält** ein, um die Volumes anzuzeigen, deren Name „abc“ enthält.
   b. Wählen Sie[All Volumes whose name contains 'abc'] im Bereich „Verfügbare Ressourcen“ die Option **++** aus, und verschieben Sie sie in den Bereich „Ausgewählte Ressourcen“.
   c. Klicken Sie auf **exclude**, und geben Sie **`xyz`** in das Feld **Name enthält** ein, und klicken Sie dann auf **Add**.
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 **actions**, und geben Sie **`sample@domain.com`** in das Feld Diese Benutzer benachrichtigen ein.
6. Wählen Sie **alle 15 Minuten**, um den Benutzer alle 15 Minuten zu benachrichtigen.

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

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.

  Wenn Sie eine Ressourcenkategorie auswählen, z. B. **<<All User or Group Quotas>>**, erhalten Sie Warnungen für alle Objekte in dieser Kategorie.

  > Das Auswählen eines Clusters als Ressource wählt nicht automatisch die Speicherobjekte innerhalb dieses Clusters aus. Wenn Sie beispielsweise eine Meldung für alle kritischen Ereignisse für alle Cluster erstellen, erhalten Sie Warnmeldungen nur für Cluster-kritische Ereignisse. Für kritische Ereignisse in Nodes, Aggregaten usw. werden keine Warnmeldungen ausgegeben.

- Schweregrad des Ereignisses

  Sie sollten entscheiden, ob ein Ereignis eines bestimmten Schweregrades (kritisch, Fehler, Warnung) die Warnmeldung auslösen soll und, falls ja, welchen Schweregrad.

- Ausgewählte Ereignisse

  Wenn Sie eine Meldung basierend auf dem generierten Ereignistyp hinzufügen, sollten Sie entscheiden, für welche Ereignisse eine Meldung erforderlich ist.

  Wenn Sie einen Ereignisschwergrad auswählen, jedoch keine einzelnen Ereignisse auswählen (wenn Sie die Spalte „Ausgewählte Ereignisse“ leer lassen), erhalten Sie Benachrichtigungen für alle Ereignisse in der Kategorie.

- 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.

Was Sie brauchen

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

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 **Storage-Management** > **Alarm-Setup**.
2. Klicken Sie auf der Seite **Alarm-Setup** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
4. 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 **`latency`** ein, und klicken Sie dann auf den Pfeil, um alle übereinstimmenden Ereignisse auszuwählen.
   c. Geben Sie im Feld Ereignisname enthält **`iops`** ein, und klicken Sie dann auf den Pfeil, um alle übereinstimmenden Ereignisse auszuwählen.
   d. Geben Sie im Feld Ereignisname enthält **`mbps`** ein, 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, um SNMP-Traps auszugeben und ein Skript auszuführen.
8. Klicken Sie 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.

Was Sie brauchen

- 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 über die Anwendungsadministratorrolle verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Alarm-Setup**.
2. Wählen Sie auf der Seite **Alarmeinstellungen** 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.

Aktivieren und Deaktivieren von Warnmeldungen für gelöste und veraltete Ereignisse

Für alle Ereignisse, die Sie für das Senden von Warnungen konfiguriert haben, wird eine Warnmeldung gesendet, wenn diese Ereignisse alle verfügbaren Status durchlaufen: Neu, bestätigt, behoben und veraltet. Wenn Sie keine Benachrichtigungen für Ereignisse erhalten möchten, während diese in den Status „aufgelöst“ und „veraltet“ verschoben werden, können Sie eine globale Einstellung konfigurieren, um diese Warnmeldungen zu unterdrücken.

Was Sie brauchen

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

Standardmäßig werden keine Warnmeldungen für Ereignisse gesendet, wenn sie in den Status „aufgelöst“ und „veraltet“ verschoben werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Alarm-Setup**.
2. Führen Sie auf der Seite **Alarm Setup** eine der folgenden Aktionen durch, indem Sie das Schieberegler neben dem Element **Warnungen für gelöste und veraltete Ereignisse** verwenden:

An…	Tun Sie das…
Das Senden von Warnmeldungen wird unterbrochen, wenn Ereignisse aufgelöst oder veraltet sind	Schieben Sie den Regler nach links
Beginnen Sie mit dem Senden von Warnungen, wenn Ereignisse aufgelöst oder veraltet sind	Bewegen Sie den Schieberegler nach rechts

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.

Was Sie brauchen

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

Die Alarme für Disaster-Recovery-Ziel-Volumes lassen sich deaktivieren, indem Volumes mit dem Namen der Ziel-SVM ausgeschlossen werden. Dies ist möglich, da die Kennung für Volume-Ereignisse den SVM-Namen und den Volume-Namen im Format „<svm_Name>:/<Volume_Name>“ enthält.

Das folgende Beispiel zeigt, wie Warnungen für Volume „vol1“ auf der primären SVM „vs1“ erstellt werden, schließt jedoch die Warnmeldung aus, die auf einem Volume mit demselben Namen auf SVM „vs1-dr“ generiert wird.

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 **Volume** aus der Dropdown-Liste aus, und geben Sie **`vol1`** in das Feld **Name enthält** ein, um die Volumes anzuzeigen, deren Name "vol1" enthält.
   b. Wählen Sie **<<All Volumes whose name contains 'vol1'>>** aus dem Bereich **Verfügbare Ressourcen** und verschieben Sie es in den Bereich **Ausgewählte Ressourcen**.
3. Wählen Sie die Registerkarte **exclude**, wählen Sie **Volume**, geben Sie **`vs1-dr`** in das Feld **Name enthält** ein und klicken Sie dann auf **Add**.

   Ausgeschlossen ist die Warnmeldung, die für Volume „vol1“ auf SVM „vs1-dr“ generiert wird.
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**.

Anzeigen von Meldungen

Sie können die Liste der Warnungen, die für verschiedene Ereignisse erstellt wurden, auf der Seite „Alarm-Setup“ 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.

Was Sie brauchen

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

Schritt

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

   Die Liste der Warnungen wird auf der Seite „Alarmkonfiguration“ 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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Alarm-Setup**.
2. Wählen Sie auf der Seite **Alarm Setup** die Warnmeldung aus, die Sie bearbeiten möchten, 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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Alarm-Setup**.
2. Wählen Sie auf der Seite **Warnmeldungseinstellungen** 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 „Alarmkonfiguration“ anzeigen.

Seite „Alarmkonfiguration“

Auf der Seite „Alarm-Setup“ wird eine Liste von Warnungen angezeigt und Informationen zu Name, Status, Benachrichtigungsmethode und Benachrichtigungshäufigkeit angezeigt. Sie können auf dieser Seite auch Warnmeldungen hinzufügen, bearbeiten, entfernen, aktivieren oder deaktivieren.

Sie müssen über die Rolle „Anwendungsadministrator“ 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.

- **Warnungen für gelöste und veraltete Ereignisse**

  Ermöglicht das Aktivieren oder Deaktivieren des Sendens von Warnungen, wenn Ereignisse in den Status „gelöst“ oder „veraltet“ verschoben werden. Dies kann Benutzern helfen, unnötige Benachrichtigungen zu erhalten.

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 Warnung aktiviert () oder deaktiviert ( ) ist .

- **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 „Anwendungsadministrator“ 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. Zum Beispiel können Sie alle Volumes ausschließen, deren Name den "xyz"-String 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 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.

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

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 Ausschließen 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.

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

Verwandte Informationen

"Aktivieren und Deaktivieren der Fähigkeit zum Hochladen von Skripten"

Funktionsweise von Skripten mit Warnmeldungen

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

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

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

Das Skript verwendet die folgenden Argumente zur Ausführung:

- `-eventID`

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

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

Beispiel zum Abrufen von Argumenten aus Skripts

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

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

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

Skripte werden hinzugefügt

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

Was Sie brauchen

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

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

  - Für Perl-Skripte muss Perl auf dem Unified Manager-Server installiert sein. Bei VMware-Installationen

wird Perl 5 standardmäßig installiert und Skripte werden nur das unterstützen, was Perl 5 unterstützt. Wenn Perl nach Unified Manager installiert wurde, müssen Sie den Unified Manager-Server neu starten.

- Bei PowerShell Skripten muss auf dem Windows Server die entsprechende PowerShell Ausführungsrichtlinie festgelegt werden, damit die Skripte ausgeführt werden können.

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

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

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

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

Schritte

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

Verwandte Informationen

"Aktivieren und Deaktivieren der Fähigkeit zum Hochladen von Skripten"

Skripte werden gelöscht

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

Was Sie brauchen

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

Schritte

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

Skriptausführung wird getestet

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

Was Sie brauchen

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

Schritte

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

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

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

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

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.

Alle Befehle müssen mit dem Befehl und einem gültigen Benutzernamen und Passwort für die Authentifizierung vorangehen `um cli login`.

Wenn Sie den Befehl *um Run* ausführen, stellen Sie sicher, dass Ihr Konto über den Zugriff auf die Anwendung *Console* verfügt.

CLI-Befehl	Beschreibung	Ausgabe
`um cli login -u <username> [-p <password>]`	Melden Sie sich bei der CLI an. Wegen der Auswirkungen auf die Sicherheit sollten Sie nur den Benutzernamen nach der Option „-U“ eingeben. Wenn Sie auf diese Weise verwendet werden, werden Sie zur Eingabe des Passworts aufgefordert, und das Passwort wird nicht in der Historie oder Prozesstabelle erfasst. Die Sitzung läuft nach drei Stunden ab dem Zeitpunkt der Anmeldung ab. Danach muss sich der Benutzer erneut anmelden.	Zeigt die entsprechende Meldung an.
`um cli logout`	Melden Sie sich über die CLI ab.	Zeigt die entsprechende Meldung an.
`um help`	Zeigt alle Unterbefehle der ersten Ebene an.	Zeigt alle Unterbefehle der ersten Ebene an.
`um run cmd [ -t <timeout> ] <cluster> <command>`	Die einfachste Methode, einen Befehl auf einem oder mehreren Hosts auszuführen. Hauptsächlich wird verwendet für Alert Scripting um ONTAP zu erhalten oder eine Operation durchzuführen. Das optionale Argument für die Zeitüberschreitung setzt eine maximale Zeitgrenze (in Sekunden), damit der Befehl auf dem Client ausgeführt werden kann. Der Standardwert ist 0 (ewig warten).	Nach Erhalt bei ONTAP.
`um run query <sql command>`	Führt eine SQL-Abfrage aus. Es sind nur Abfragen erlaubt, die aus der Datenbank gelesen werden. Aktualisierungsvorgänge, Einfügevorgänge oder Löschvorgänge werden nicht unterstützt.	Die Ergebnisse werden in tabellarischer Form angezeigt. Wenn ein leerer Satz zurückgegeben wird, oder wenn ein Syntaxfehler oder eine fehlerhafte Anforderung vorliegt, wird die entsprechende Fehlermeldung angezeigt.

CLI-Befehl	Beschreibung	Ausgabe
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Fügt der Liste der gemanagten Speichersysteme eine Datenquelle hinzu. Eine Datenquelle beschreibt, wie Verbindungen zu Speichersystemen hergestellt werden. Beim Hinzufügen einer Datenquelle müssen die Optionen -U (Benutzername) und -P (Passwort) angegeben werden. Die Option -t (Protocol) gibt das Protokoll an, das zur Kommunikation mit dem Cluster verwendet wird (http oder https). Wenn das Protokoll nicht angegeben wird, werden beide Protokolle versucht, die Option -p (Port) gibt den Port an, der zur Kommunikation mit dem Cluster verwendet wird. Wenn der Port nicht angegeben wird, wird versucht, den Standardwert des entsprechenden Protokolls zu verwenden. Dieser Befehl kann nur vom Storage-Admin ausgeführt werden.	Fordert den Benutzer auf, das Zertifikat anzunehmen, und druckt die entsprechende Meldung.
`um datasource list [ <datasource-id>]`	Zeigt die Datenquellen für verwaltete Speichersysteme an.	Zeigt die folgenden Werte im Tabellenformat an: `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message.`
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	Ändert eine oder mehrere Datenquellenoptionen. Kann nur vom Storage-Administrator ausgeführt werden.	Zeigt die entsprechende Meldung an.
`um datasource remove <datasource-id>`	Entfernt die Datenquelle (Cluster) aus Unified Manager.	Zeigt die entsprechende Meldung an.
`um option list [ <option> .. ]`	Listet alle Optionen auf, die Sie mit dem Befehl Set konfigurieren können.	Zeigt die folgenden Werte im Tabellenformat an: `Name, Value, Default Value, and Requires Restart.`

CLI-Befehl	Beschreibung	Ausgabe
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	Legt eine oder mehrere Optionen fest. Der Befehl kann nur vom Storage-Admin ausgeführt werden.	Zeigt die entsprechende Meldung an.
`um version`	Zeigt die Softwareversion von Unified Manager an.	`Version ("9.6")`
`um lun list [-q] [ -ObjectType <object-id>]`	Führt die LUNs nach dem Filtern auf das angegebene Objekt auf. -q ist für alle Befehle geeignet, keine Kopfzeile anzuzeigen. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, Oder svm. Beispiel: **`um lun list -cluster 1`** In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Mit dem Befehl werden alle LUNs im Cluster mit der ID 1 aufgeführt.	Zeigt die folgenden Werte im Tabellenformat an: `ID and LUN path.`
`um svm list [-q] [ -ObjectType <object-id>]`	Führt die Storage-VMs nach dem Filtern nach dem angegebenen Objekt auf. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, Oder svm. Beispiel: **`um svm list -cluster 1`** In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Storage VMs innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an: `Name and Cluster ID.`

CLI-Befehl	Beschreibung	Ausgabe
`um qtree list [-q] [ -ObjectType <object-id>]`	Führt die qtrees nach dem Filtern auf dem angegebenen Objekt auf. -q ist für alle Befehle geeignet, keine Kopfzeile anzuzeigen. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, Oder svm. Beispiel: **`um qtree list -cluster 1`** In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Mit dem Befehl werden alle qtrees im Cluster mit der ID 1 aufgelistet.	Zeigt die folgenden Werte im Tabellenformat an: `Qtree ID and Qtree Name.`
`um disk list [-q] [-ObjectType <object-id>]`	Listet die Festplatten nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node oder Cluster sein. Beispiel: **`um disk list -cluster 1`** In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Festplatten im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `ObjectType and object-id`.
`um cluster list [-q] [-ObjectType <object-id>]`	Listet die Cluster nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster, lun, sein Qtree, Volume, Kontingent oder svm. Beispiel: **`um cluster list -aggr 1`** In diesem Beispiel ist "-aggr" der objectType und "1" die objectId. Der Befehl listet das Cluster auf, zu dem das Aggregat mit der ID 1 gehört.	Zeigt die folgenden Werte im Tabellenformat an: `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.`

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 oder Cluster sein. Beispiel: **`um cluster node list -cluster 1`** In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Nodes im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Name and Cluster ID`.
`um volume list [-q] [-ObjectType <object-id>]`	Listet die Volumes nach dem Filtern auf dem angegebenen Objekt auf. Objekttyp kann lun, qtree, Cluster, Volume, Kontingent, svm oder Aggregat: Beispiel: **`um volume list -cluster 1`** In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Volumes im Cluster mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Volume ID and Volume Name`.
`um quota user list [-q] [-ObjectType <object-id>]`	Listet die Quota-Benutzer nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann qtree, Cluster, Volume, Kontingent oder svm sein. Beispiel: **`um quota user list -cluster 1`** In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Kontingentbenutzer innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `ID, Name, SID and Email`.

CLI-Befehl	Beschreibung	Ausgabe
`um aggr list [-q] [-ObjectType <object-id>]`	Führt die Aggregate nach dem Filtern auf das angegebene Objekt auf. Objekttyp kann Disk, aggr, Node, Cluster oder Volume sein. Beispiel: **`um aggr list -cluster 1`** In diesem Beispiel ist "-Cluster" der objectType und "1" die objectId. Der Befehl listet alle Aggregate innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an `Aggr ID, and Aggr Name`.
`um event ack <event-ids>`	Bestätigt ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event resolve <event-ids>`	Löst ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event assign -u <username> <event-id>`	Weist einem Benutzer ein Ereignis zu.	Zeigt die entsprechende Meldung an.
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Listet die vom System oder Benutzer generierten Ereignisse auf. Filtern von Ereignissen nach Quelle, Status und IDs	Zeigt die folgenden Werte im Tabellenformat an `Source, Source type, Name, Severity, State, User and Timestamp`.
`um backup restore -f <backup_file_path_and_name>`	Stellt eine Sicherung einer MySQL-Datenbank mithilfe von .7z-Dateien wieder her.	Zeigt die entsprechende Meldung an.

Beschreibung der Skriptfenster und Dialogfelder

Auf der Seite Skripts können Sie Skripte zu Unified Manager hinzufügen.

Seite „Skripte“

Auf der Seite Skripts können Sie Ihre benutzerdefinierten Skripte zu Unified Manager hinzufügen. Sie können diese Skripte mit Warnmeldungen verknüpfen, um die automatische Neukonfiguration von Speicherobjekten zu ermöglichen.

Auf der Seite Skripts 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 „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

- **Wählen Sie Skriptdatei**

  Ermöglicht die Auswahl eines Skripts für die Warnmeldung.

- **Beschreibung**

  Hier können Sie eine Beschreibung für das Skript angeben.

Überwachung und Management der Cluster-Performance

Einführung in das Active IQ Unified Manager Performance-Monitoring

Active IQ Unified Manager (ehemals OnCommand Unified Manager) bietet Funktionen für das Performance-Monitoring sowie 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 Netzwerkschnittstellen (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.
- Identifiziert die QoS-Richtlinien (Quality of Service) und Performance Service Level Richtlinien (PSLs), die auf Ihre Volumes und LUNs angewendet werden.
- 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

Diese Abschnitte enthalten Informationen zu den beiden Benutzeroberflächen, die Active IQ 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 diesen Abschnitten 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-UI von Unified Manager angezeigt werden.

Wartungskonsole

Die Unified Manager-Wartungskonsole ermöglicht Administratoren das Überwachen, Diagnostizieren und behandeln von Betriebssystemproblemen, Problemen mit dem Versionsaktualisierung, Problemen mit dem Benutzerzugriff und Netzwerkproblemen im Zusammenhang mit dem Unified Manager-Server selbst. Wenn die Web-UI von Unified Manager nicht verfügbar ist, stellt die Wartungskonsole die einzige Zugriffsmöglichkeit auf Unified Manager dar.

Sie können diese Informationen für den Zugriff auf die Wartungskonsole verwenden, um Probleme im Zusammenhang mit der Funktionsweise des Unified Manager-Servers zu beheben.

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 180 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 180 Tage lang aufbewahrt.

Aktivität	Zeitintervall	Beschreibung
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, die älter als 180 Tage sind, und dynamische Schwellenwerte, die älter als 180 Tage sind.
Datenbeschnitt	Jeden Tag nach 3:30 Uhr	Löscht aus der Datenbank alle Leistungsdaten von einer Stunde, die älter als 180 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.

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.

- 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 Datenkontinuitätssammlung erforderlich ist, um mehr als eine Stunde historische Daten zu erfassen, sehen Sie eine Bannermeldung für diesen Cluster oben im Bereich Benachrichtigungen.

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-Seite
- Seiten für Storage- und Netzwerkobjektbestand
- Detailseiten von Storage-Objekten (einschließlich Performance-Explorer)
- Konfigurations- und Setup-Seiten
- Ereignisseiten

Melden Sie sich bei der UI an

Sie können sich über einen unterstützten Webbrowser bei der Benutzeroberfläche von Unified Manager anmelden.

Was Sie brauchen

- Der Webbrowser muss die Mindestanforderungen erfüllen.

  Die Interoperabilitäts-Matrix unter "mysupport.netapp.com/matrix" enthält eine vollständige Liste der unterstützten Browser-Versionen.

- Sie müssen die IP-Adresse oder URL des Unified Manager-Servers haben.

Sie werden automatisch nach 1 Stunde Inaktivität von der Sitzung abgemeldet. Dieser Zeitrahmen kann unter **Allgemein** > **Funktionseinstellungen** konfiguriert werden.

Schritte

1. Geben Sie die URL in Ihrem Webbrowser ein. Dabei handelt es sich um die URL der IP-Adresse oder um den vollqualifizierten Domänennamen (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. . 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 Dashboard 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.

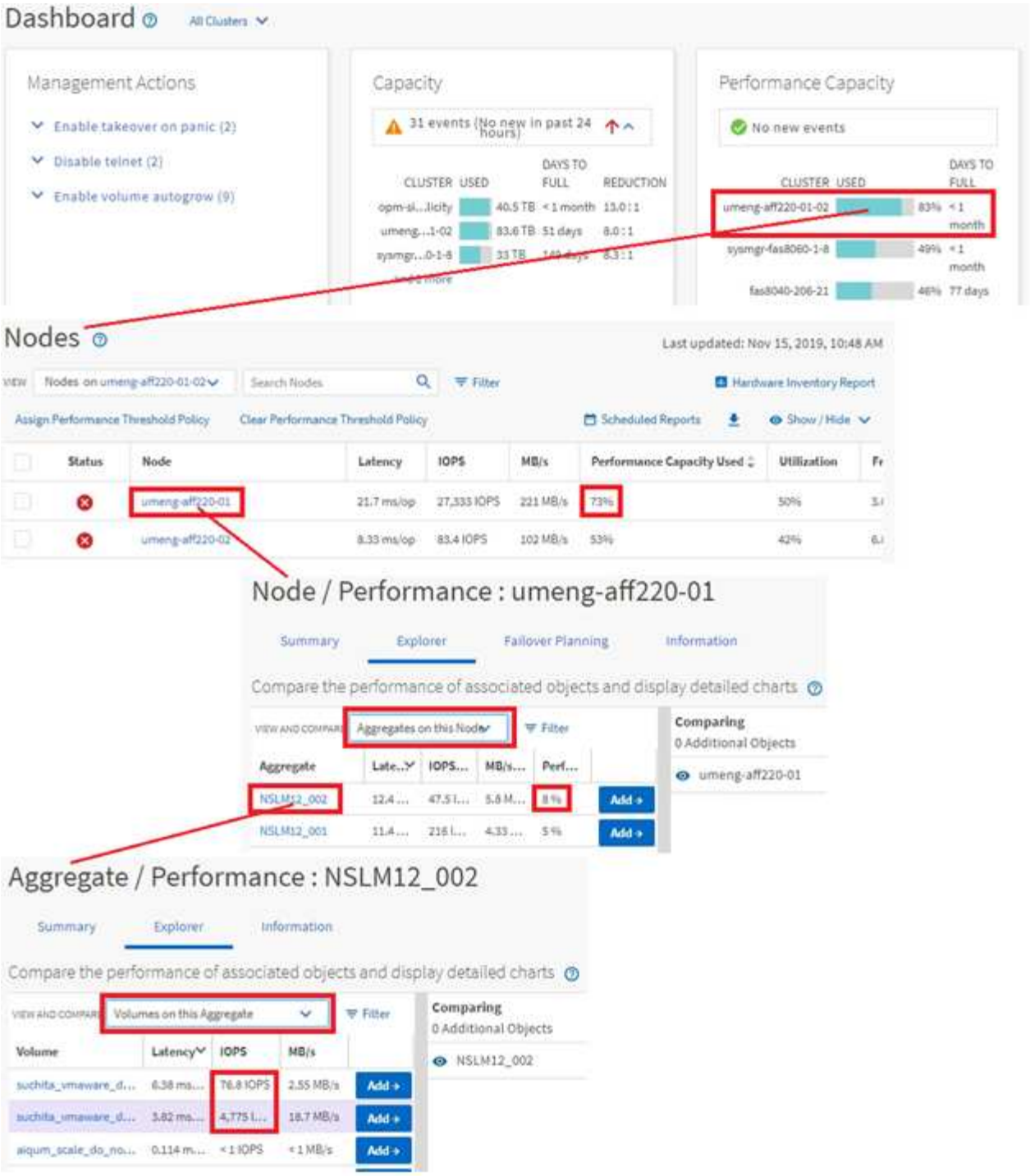
Überwachen Sie die Navigation von Cluster-Objekten

Sie können die Performance aller Objekte in jedem Cluster überwachen, das 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. Überprüfen Sie auf der Seite Dashboard die Details im Bereich Performance Capacity, um das Cluster zu identifizieren, das die höchste Performance-Kapazität verwendet, und klicken Sie auf das Balkendiagramm, um zur Liste der Nodes für dieses Cluster zu navigieren.
2. Identifizieren Sie den Node mit dem höchsten Kapazitätswert und klicken Sie auf diesen Node.
3. Klicken Sie auf der Seite Knoten / Performance Explorer im Menü Ansicht und Vergleich auf **Aggregate auf diesem Knoten**.
4. Identifizieren Sie das Aggregat, das die höchste Performance-Kapazität nutzt, und klicken Sie auf das Aggregat.
5. Klicken Sie auf der Seite Aggregat / Performance Explorer im Menü Ansicht und Vergleich auf **Volumes auf diesem Aggregat**.
6. Sie können die Volumes ermitteln, die die meisten IOPS verwenden.

Sie sollten sich diese Volumes untersuchen, um zu sehen, ob Sie eine QoS-Richtlinie oder eine Performance-Service Level-Richtlinie anwenden oder die Richtlinieneinstellungen ändern sollten, damit diese Volumes nicht so einen großen Prozentsatz von IOPS auf dem Cluster verwenden.



Monitoring der Navigation zur Cluster-Performance

Sie können die Performance aller von Unified Manager gemanagten Cluster überwachen. 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. Klicken Sie im linken Navigationsbereich auf **Storage** > **Aggregate**.
2. Um Informationen zur Performance in diesen Aggregaten anzuzeigen, wählen Sie die Ansicht Performance: Alle Aggregate aus.
3. Identifizieren Sie das Aggregat, das Sie untersuchen möchten, und klicken Sie auf diesen Aggregatnamen, um zur Seite Aggregat-/Performance 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.

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 **Ereignisverwaltung**.
2. Klicken Sie im Menü Ansicht auf **Aktive Leistungsereignisse**.
3. Klicken Sie auf den Namen des Ereignisses, das Sie untersuchen möchten, und die Seite Ereignisdetails wird angezeigt.
4. Sehen Sie sich die Beschreibung des Ereignisses an und prüfen Sie die vorgeschlagenen Aktionen (sofern verfügbar), um weitere Details zu dem Ereignis anzuzeigen, das Ihnen bei der Behebung des Problems helfen kann. Klicken Sie auf die Schaltfläche **Workload analysieren**, um detaillierte Performance-Diagramme anzuzeigen, um das Problem weiter zu analysieren.

Suche nach Speicherobjekten

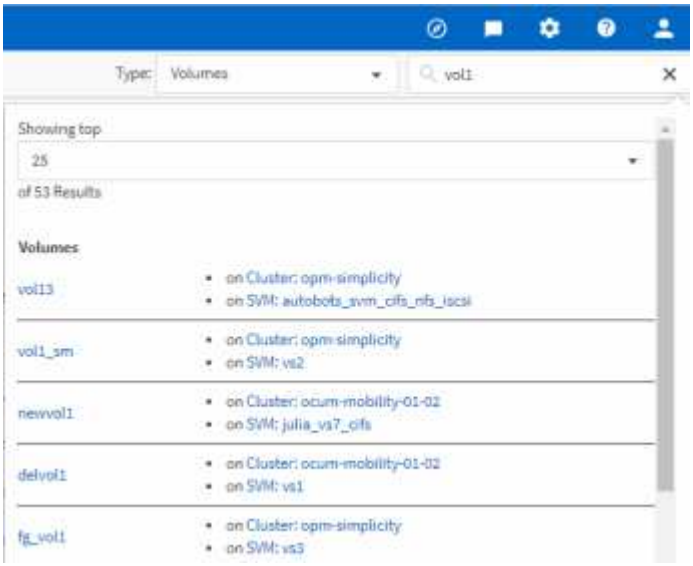
Um schnell auf ein bestimmtes Objekt zuzugreifen, können Sie das Feld **Alle Speicherobjekte durchsuchen** oben in der Menüleiste verwenden. Mit dieser Methode der globalen Suche über alle Objekte können Sie schnell bestimmte Objekte nach Typ finden. Die Suchergebnisse sind nach Storage-Objekttyp sortiert und können über das Dropdown-Menü gefiltert werden. Eine gültige Suche muss mindestens drei Zeichen enthalten.

Die globale Suche zeigt die Gesamtzahl der Ergebnisse an, aber nur die 25 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 klicken und **Alle** auswählen, um gleichzeitig alle Objekte und Ereignisse zu durchsuchen. Alternativ können Sie auf das Dropdown-Feld klicken, um den Objekttyp anzugeben. Geben Sie mindestens drei Zeichen des Objekt- oder Ereignisnamens in das Feld **Alle Speicherobjekte durchsuchen** ein, und drücken Sie dann **Enter**, um die Suchergebnisse anzuzeigen, wie z. B.:

- 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 ist im Dropdown-Feld 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.

Inhalt der Bestandsseite wird gefiltert

Sie können die Daten auf den Inventarseiten in Unified Manager filtern, um Daten anhand spezifischer 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, um nur die Daten anzuzeigen, in denen Sie interessiert sind.

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 rechts neben der Schaltfläche Filter die Anzahl der angewendeten Filter angezeigt.

Es werden drei Filterparameter unterstützt.

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

Die Felder Spalte, Operator und Wert sind für jeden Filter erforderlich. Die verfügbaren Filter spiegeln die filterbaren Spalten auf der aktuellen Seite wider. 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 die Schaltfläche **Filter**. Das Filterfenster wird angezeigt.
2. Klicken Sie auf die linke Dropdown-Liste und wählen Sie ein Objekt aus, z. B. *Cluster* oder einen Performance-Zähler.
3. Klicken Sie auf die mittlere Dropdown-Liste, und wählen Sie den gewünschten Operator aus.
4. Wählen Sie in der letzten Liste einen Wert aus oder geben Sie einen Wert ein, um den Filter für dieses Objekt abzuschließen.
5. Um einen anderen 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.
6. Klicken Sie Auf **Filter Anwenden**. Die Filteroptionen werden auf das Raster angewendet und die Anzahl der Filter wird rechts neben der Schaltfläche Filter angezeigt.
7. Verwenden Sie den Filterbereich, um einzelne Filter zu entfernen, indem Sie auf das Papierkorb-Symbol rechts neben dem zu entfernenden Filter klicken.
8. 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, schließt sich das Filterfenster, wendet Ihre Filter an und zeigt die Anzahl der angewendeten Filter an (3).

Monitoring der Cluster-Performance über das Dashboard

Das Unified Manager Dashboard bietet einige Felder, die den Performance-Status aller Cluster anzeigen, 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 zu den Performance-Fenstern auf dem Dashboard

Das Unified Manager Dashboard bietet einige Bereiche mit hohem Performance-Status für alle Cluster, die in Ihrer Umgebung überwacht werden. Sie können den Status aller Cluster oder für einzelne Cluster anzeigen.

Neben Leistungsinformationen werden in den meisten Feldern auch die Anzahl der aktiven Ereignisse in dieser Kategorie sowie die Anzahl der neuen Ereignisse angezeigt, die in den letzten 24 Stunden hinzugefügt wurden. Anhand dieser Informationen können Sie festlegen, welche Cluster Sie möglicherweise weiter analysieren müssen, um gemeldete Ereignisse zu lösen. Wenn Sie auf die Ereignisse klicken, werden die wichtigsten Ereignisse angezeigt und es wird ein Link zur Seite „Ereignismanagement“ angezeigt, die gefiltert wurde, um die Ereignisse in dieser Kategorie anzuzeigen.

Die folgenden Bereiche stellen den Leistungsstatus bereit.

- **Performance Capacity Panel**

  Bei der Anzeige aller Cluster zeigt dieses Feld den Performance-Kapazitätswert für jedes Cluster (durchschnittlich über die vorherige 1 Stunde) und die Anzahl der Tage an, bis die Performance-Kapazität die Obergrenze erreicht (basierend auf der täglichen Wachstumsrate). Durch Klicken auf das Balkendiagramm gelangen Sie zur Seite „Nodes-Inventar“ für dieses Cluster. Beachten Sie, dass auf der Seite Nodes-Inventar die durchschnittliche Performance-Kapazität der letzten 72 Stunden angezeigt wird. Dieser Wert stimmt daher möglicherweise nicht mit dem Dashboard-Wert überein.

  Wenn Sie ein einzelnes Cluster anzeigen, wird in diesem Bereich die Cluster-Performance-Kapazität, die IOPS-Gesamtkapazität und der Gesamtdurchsatz angezeigt.

- **Workload IOPS Panel**

  Wenn das aktive Workload-Management aktiviert ist und wenn ein einzelnes Cluster angezeigt wird, werden in diesem Bereich die Gesamtzahl der Workloads angezeigt, die derzeit in einem bestimmten IOPS-Bereich ausgeführt werden.

- **Workload Performance Panel**

  Wenn das aktive Workload-Management aktiviert ist, wird in diesem Bereich die Gesamtzahl der Workloads angezeigt, die jedem definierten Performance-Service-Level zugeordnet sind und denen nicht entsprechen. Durch Klicken auf ein Balkendiagramm gelangen Sie zu den Workloads, die dieser Richtlinie auf der Seite Workloads zugewiesen sind.

- **Anwendungsübersicht**

  Bei der Anzeige aller Cluster können Sie Cluster nach den höchsten IOPS oder dem höchsten Durchsatz (MB/s) anzeigen.

  Bei der Anzeige eines einzelnen Clusters können Sie Workloads auf diesem Cluster nach den höchsten

IOPS oder dem höchsten Durchsatz (MB/s) anzeigen.

Performance-Banner-Meldungen und -Beschreibungen

Unified Manager zeigt möglicherweise auf der Seite Benachrichtigungen (über die Bell wird über Benachrichtigung) Bannermeldungen 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.

Was Sie brauchen

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

Das Problem der Performancestatistiken Sammlungen nicht rechtzeitig beendet wird durch die Banner-Meldungen oder `Data collection is taking too long on cluster <cluster_name>` angezeigt `Unable to consistently collect from 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-Einrichtung 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 Manager-Wartungskonsole 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.

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.

Fehlersuche bei Workloads mithilfe der Workload Analyzer

Die Workload-Analyse bietet eine Möglichkeit, wichtige Gesundheits- und Performancekriterien für einen einzelnen Workload auf einer einzelnen Seite anzuzeigen, um die Fehlerbehebung zu unterstützen. Durch die Anzeige aller aktuellen und bisherigen Ereignisse für einen Workload erhalten Sie eine bessere Vorstellung davon, warum der Workload jetzt ein Performance- oder Kapazitätsproblem haben könnte.

Mit diesem Tool können Sie auch feststellen, ob Speicher die Ursache von Performance-Problemen für eine Anwendung ist oder ob das Problem durch ein Netzwerk oder ein anderes zusammenhänges Problem verursacht wird.

Sie können diese Funktion von einer Vielzahl von Orten in der Benutzeroberfläche aus starten:

- Wählen Sie die Option Workload Analysis im linken Navigationsmenü aus
- Klicken Sie auf der Seite Ereignisdetails auf die Schaltfläche **Workload analysieren**
- Klicken Sie auf einer beliebigen Seite zur Workload-Inventarisierung (Volume, LUN, Workload, NFS-Freigabe oder SMB/CIFS-Freigabe) auf das Symbol Mehr ⋮ und dann auf **Workload analysieren**
- Klicken Sie auf der Seite Virtuelle Maschinen auf die Schaltfläche **Workload analysieren** von einem beliebigen Datastore-Objekt aus

Wenn Sie das Tool im linken Navigationsmenü starten, können Sie den Namen eines beliebigen Workloads

eingeben, den Sie analysieren möchten, und den Zeitbereich auswählen, für den Sie eine Fehlerbehebung durchführen möchten. Wenn Sie das Tool von einer beliebigen Arbeitslast oder einer Inventarseite für virtuelle Maschinen starten, wird der Name des Workloads automatisch ausgefüllt, und die Daten des Workloads werden mit dem Standardzeitbereich von 2 Stunden angezeigt. Wenn Sie das Tool auf der Seite „Ereignisdetails“ starten, wird automatisch der Name des Workloads eingegeben, und die Daten von 10 Tagen werden angezeigt.

Welche Daten werden vom Workload Analyzer angezeigt

Die Seite Workload Analyzer enthält Informationen zu aktuellen Ereignissen, die Auswirkungen auf den Workload haben könnten, Empfehlungen zur potenziellen Behebung des Ereignisses und Diagramme zur Analyse des Performance- und Kapazitätsverlaufs.

Oben auf der Seite geben Sie den Namen des Workloads (Volume oder LUN) an, den Sie analysieren möchten, und den Zeitrahmen, über den Sie Statistiken anzeigen möchten. Sie können den Zeitrahmen jederzeit ändern, wenn Sie einen kürzeren oder längeren Zeitraum anzeigen möchten.

In den anderen Bereichen der Seite werden die Analyseergebnisse sowie die Performance- und Kapazitätsdiagramme angezeigt.

> Workload-Diagramme für LUNs bieten nicht dasselbe Maß an Statistiken wie die Diagramme für Volumes. Daher werden bei der Analyse dieser beiden Workload-Typen Unterschiede feststellen.

- **Veranstaltungsübersicht**

  Zeigt eine kurze Übersicht über Anzahl und Art der Ereignisse an, die im Laufe des Zeitraums aufgetreten sind. Wenn es Ereignisse aus verschiedenen Wirkungsbereichen gibt (z. B. Leistung und Kapazität), werden diese Informationen angezeigt, sodass Sie Details für den gewünschten Ereignistyp auswählen können. Klicken Sie auf den Ereignistyp, um eine Liste der Ereignisnamen anzuzeigen.

  Wenn während des Zeitraums nur ein Ereignis auftritt, wird für einige Ereignisse eine Liste mit Empfehlungen zur Behebung des Problems aufgeführt.

- **Veranstaltungstermine**

  Zeigt alle Vorkommen von Ereignissen während des angegebenen Zeitraums an. Bewegen Sie den Cursor über jedes Ereignis, um den Ereignisnamen anzuzeigen.

  Wenn Sie auf dieser Seite angekommen sind, indem Sie auf der Seite Ereignisdetails auf die Schaltfläche **Workload analysieren** klicken, erscheint das Symbol für das ausgewählte Ereignis größer, sodass Sie das Ereignis identifizieren können.

- **Bereich der Performance-Diagramme**

  Zeigt Diagramme für Latenz, Durchsatz (sowohl IOPS als auch MB/s) und Auslastung (sowohl für den Node als auch für das Aggregat) basierend auf dem ausgewählten Zeitraum an. Sie können auf den Link Performance-Details anzeigen klicken, um die Seite im Performance Explorer für den Workload anzuzeigen, falls Sie eine weitere Analyse durchführen möchten.

  - **Latenz** zeigt die Latenz für den Workload über den ausgewählten Zeitraum an. Das Diagramm enthält drei Ansichten, mit denen Sie Folgendes anzeigen können:

- * Total * Latenz
- **Aufschlüsselung** Latenz (aufgeschlüsselt nach Lese-, Schreib- und anderen Prozessen)
- **Cluster-Komponenten** Latenz (aufgeschlüsselt nach Cluster-Komponente)

Eine Beschreibung der hier angezeigten Clusterkomponenten finden Sie unter"Cluster-Komponenten und warum sie über Konflikte verfügen können". *** Throughput* zeigt IOPS und MB/s Durchsatz für den Workload über den ausgewählten Zeitraum an. Das Diagramm hat vier Ansichten, die es Ihnen ermöglichen zu sehen:** * **Gesamtdurchsatz * Aufschlüsselung Durchsatz (gebrochen durch Lese-, Schreib- und andere Prozesse)** * **Cloud Throughput** (die MB/s, die zum Schreiben von Daten in die Cloud und zum Lesen von Daten verwendet werden; Für Workloads, die Tiering-Kapazität in die Cloud darstellen) *** IOPS mit Prognose (eine Vorhersage darüber, welche Werte für den oberen und unteren IOPS-Durchsatz über den Zeitraum hinweg erwartet wurden) Dieses Diagramm zeigt auch Quality of Service (QoS) maximale und minimale Durchsatzschwellenwerte, falls konfiguriert, Sie sehen also, wo das System den Durchsatz absichtlich mit QoS-Richtlinien begrenzt. Auslastung** zeigt die Auslastung sowohl für das Aggregat als auch für den Node an, auf dem der Workload über den ausgewählten Zeitraum ausgeführt wird. Von hier aus sehen Sie, ob Ihr Aggregat oder die Knoten überausgelastet sind, was möglicherweise zu hoher Latenz führt. Bei der Analyse von FlexGroup Volumes werden in den Nutzungsdiagrammen mehrere Nodes und mehrere Aggregate aufgeführt.

- **Kapazität Diagrammbereich**

  Zeigt Diagramme für die Datenkapazität und Snapshot-Kapazität der letzten einen Monat für den Workload an.

  Bei Volumes können Sie über den Link Kapazitätsdetails anzeigen auf die Seite Integritätsdetails für den Workload anzeigen klicken, falls Sie weitere Analysen durchführen möchten. LUNs stellen diesen Link nicht bereit, da für LUNs keine Seite „Integritätsdetails“ vorhanden ist.

  - **Kapazitätsansicht** zeigt den gesamten verfügbaren Speicherplatz an, der für den Workload und den logischen genutzten Speicherplatz zugewiesen ist (nach allen NetApp Optimierungen).
  - **Snapshot View** zeigt den gesamten reservierten Speicherplatz für Snapshot Kopien und die Menge des derzeit genutzten Speicherplatzes an. Beachten Sie, dass LUNs keine Snapshot-Ansicht bereitstellen.
  - **Cloud Tier View** zeigt an, wie viel Kapazität in der lokalen Performance-Tier verwendet wird und wie viel in der Cloud Tier verwendet wird. Diese Diagramme beinhalten eine Schätzung der verbleibenden Zeit, bevor die Kapazität für diesen Workload voll ist. Diese Informationen basieren auf historischer Nutzung und erfordern mindestens 10 Tage Daten. Wenn die Kapazität weniger als 30 Tage verbleibt, identifiziert Unified Manager den Storage als „`nahezu voll`“.

Wann würde ich den Workload Analyzer verwenden

In der Regel dient die Workload-Analyse zur Behebung eines von einem Benutzer gemeldeten Latenzproblems, zur gründeren Analyse eines gemeldeten Ereignisses oder einer Warnung oder zur Untersuchung der Workloads, die angezeigt werden, wird nicht ordnungsgemäß ausgeführt.

Wenn Benutzer Sie kontaktiert haben, um zu sagen, dass die Applikation, die sie verwenden, sehr langsam läuft, können Sie die Latenz, den Durchsatz und die Auslastungsdiagramme für den Workload überprüfen, auf dem die Applikation ausgeführt wird, um festzustellen, ob Storage die Ursache des Performance-Problems ist. Sie können das Kapazitätsdiagramm auch verwenden, um zu prüfen, ob die Kapazität niedrig ist, da ein ONTAP System, in dem die genutzte Kapazität über 85 % liegt, Performance-Probleme verursachen kann. Anhand dieser Diagramme können Sie feststellen, ob das Problem durch den Speicher oder durch ein

Netzwerk oder ein anderes zusammenhängenes Problem verursacht wurde.

Wenn Unified Manager ein Performance-Ereignis generiert hat und Sie die Ursache des Problems genauer überprüfen möchten, können Sie die Workload-Analyse von der Seite Ereignisdetails starten, indem Sie auf die Schaltfläche * Workload analysieren* klicken, um einige der Latenz, den Durchsatz, Und Kapazitätstrends für den Workload.

Wenn Sie einen Workload bemerken, der bei der Anzeige einer Workload-Bestandsseite (Volume, LUN, Workload, NFS-Freigabe oder SMB/CIFS-Freigabe) ungewöhnlich funktioniert, können Sie auf das Symbol Mehr und dann auf **Workload analysieren** klicken, um die Seite Workload-Analyse zu öffnen und den Workload weiter zu untersuchen.

Workload Analyzer verwenden

Es gibt viele Möglichkeiten, die Workload-Analyse von der Benutzeroberfläche aus zu starten. Hier beschreiben wir das Starten des Tools aus dem linken Navigationsbereich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Workload Analysis**.

   Die Seite Workload Analysis wird angezeigt.

2. Wenn Sie den Workload-Namen kennen, geben Sie den Namen ein. Wenn Sie den vollständigen Namen nicht sicher sind, geben Sie mindestens 3 Zeichen ein, und das System zeigt eine Liste von Workloads an, die mit dem String übereinstimmen.
3. Wählen Sie den Zeitbereich aus, wenn Sie Statistiken länger als die Standardstunden anzeigen möchten, und klicken Sie auf **Anwenden**.
4. Zeigen Sie den Übersichtsbereich an, um die Ereignisse anzuzeigen, die während des Zeitraums aufgetreten sind.
5. In den Performance- und Kapazitätsdiagrammen finden Sie Informationen dazu, wann irgendwelche Metriken anormal sind, und überprüfen Sie, ob Ereignisse auf den anormalen Eintrag ausgerichtet sind.

Monitoring der Cluster-Performance über die Startseite des Performance Cluster

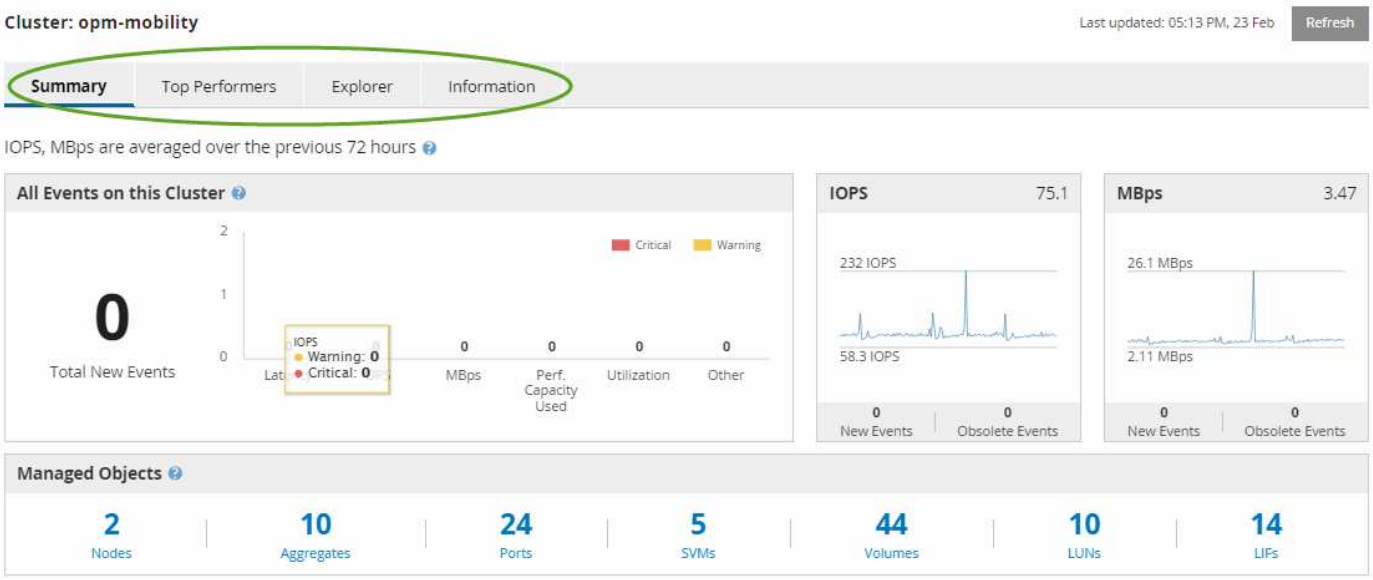
Auf der Seite „Performance Cluster Landing“ wird der Performance-Status eines ausgewählten Clusters angezeigt, der von einer Instanz von Unified Manager überwacht wird. Auf dieser Seite können Sie die allgemeine Performance eines bestimmten Clusters bewerten und schnell alle erkannten Cluster-spezifischen 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.

Die Landing Page für Performance Cluster enthält vier Registerkarten, die die Cluster-Details in vier Informationsbereiche trennen:

- Übersichtsseite
  - Bereich Cluster-Ereignisse
  - Diagramme der MB/s- und IOPS-Performance
  - Bereich „Managed Objects“
- Seite „Top Performers“
- Explorer-Seite
- Informationsseite

Performance Cluster Summary

Die Seite „Performance Cluster Summary“ enthält eine Zusammenfassung der aktiven Ereignisse, der IOPS Performance und der MB/s Performance eines Clusters. 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.

Die Diagrammdaten (vertikale Zählerbalken) werden bei kritischen Ereignissen rot () und bei Warnungsereignissen gelb ( ) angezeigt. 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 von MB/s des Clusters für den vorherigen 72-Stunden-Zeitraum. Sie können den Cursor über die Trendlinie des Diagramms positionieren, um den MB/s-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.

- **Storage VMs**

  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. FlexGroup Komponenten sind darin nicht enthalten.

- **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.

- **Netzwerkschnittstellen**

  Eine logische Netzwerkschnittstelle, die einen Netzwerkzugriffspunkt für einen Node darstellt. Die Zählung umfasst alle Schnittstellentypen.

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 Storage VMs die SVMs mit den höchsten IOPS, die höchste Latenz oder die niedrigste MB/s anzeigen Diese Seite zeigt auch, ob eine der Top-Performer aktive Performanceereignisse hat (Neu oder bestätigt).

Auf der Seite Top Performers werden maximal 10 Objekte angezeigt. Das Objekt des Volumes umfasst sowohl FlexVol Volumes als auch FlexGroup Volumes.

- **Zeitbereich**

  Sie können einen Zeitbereich für die Anzeige der Top-Performer auswählen. Der ausgewählte Zeitbereich gilt für alle Speicherobjekte. Verfügbare Zeitbereiche:

  - Letzte Stunde
  - Die Letzten 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 **MB/s**. Durch Ändern des Zählers werden die Plattendaten basierend auf dem ausgewählten Zähler mit den Top-Performern neu geladen.

Verfügbare Zähler:

- Latenz
- IOPS
- MB/s
- 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 ein Schwellwertbruch aktiv ist (ein neues oder bestätigtes Ereignis), wird der Balken in der Farbe für das Ereignis angezeigt: Warnungsereignisse werden gelb ( ) und kritische Ereignisse rot ( ) angezeigt. 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 aktive kritische () oder Warning ( ) Ereignisse in den Diagrammen der besten Performer angezeigt. 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 eine `.csv` Datei, die die Daten enthält, die in der Zählerleiste angezeigt werden. 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 „Bestandsaufnahme der Performance/Alle Nodes“ in der Spalte **Nodes** auf ein Node-Objekt. Die Seite Objektdetails enthält detaillierte Informationen und Details zum ausgewählten Objekt, einschließlich eines Gegenübers aktiver Ereignisse.

Anzeigen der Seiten zum Performance-Inventar für alle Storage-Objekte

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.

Standardmäßig werden Objekte auf den Ansichtsseiten nach Wichtigkeit des Ereignisses sortiert. 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.

Sie können Daten aus diesen Seiten in eine kommagetrennte (`.csv`Datei mit Werten), eine Microsoft Excel-Datei (.xlsx`) oder (`.pdf`ein)-Dokument exportieren, indem Sie die Schaltfläche **Reports** verwenden und dann die exportierten Daten zum Erstellen von Berichten verwenden. Darüber hinaus können Sie die Seite anpassen und einen Bericht über die Schaltfläche **geplante Berichte** regelmäßig erstellen und per E-Mail senden.

Alle Felder auf diesen Seiten können in benutzerdefinierten Ansichten und in Berichten verwendet werden. Einige Felder sind mit verwandten Seiten verknüpft, wodurch eine detailliertere Ansicht möglich ist.

Performance: Ansicht aller Cluster

Die Ansicht „Performance: Alle Cluster“ zeigt für jeden Cluster einen Überblick über die Performance-Ereignisse, Daten und Konfigurationsinformationen, die durch eine Instanz von Unified Manager überwacht werden. Auf dieser Seite können Sie die Performance des Clusters überwachen sowie Performance-Probleme und Schwellenwertereignisse beheben.

Über die Schaltflächen **Performance Threshold Policy** und **Clear Performance Threshold Policy** können Sie Schwellenwertrichtlinien auf den Objektbestandsseiten zuweisen oder löschen.

In der Ansicht „Performance: All Clusters“ sind einige wichtige Felder aufgeführt.

- Cluster-FQDN: Der vollständig qualifizierte Domain-Name (FQDN) des Clusters.
- IOPS: Die ein-/Ausgabevorgänge pro Sekunde auf dem Cluster.
- MB/s: Der Durchsatz auf dem Cluster, gemessen in MiB pro Sekunde.
- Kapazitätsfelder: Freie und Gesamtkapazität in gib.
- Host-Name oder IP-Adresse: Der Host-Name oder die IP-Adresse (IPv4 oder IPv6) der Cluster-Management-LIF.
- 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. Sie können die auf jedem Node installierte ONTAP-Version in der Ansicht Leistung: Alle Nodes anzeigen.

- Schwellenwertrichtlinie: Benutzerdefinierte Performance-Schwellenwertrichtlinie oder aktive Richtlinien für dieses Storage-Objekt. Sie können den Cursor über Richtliniennamen mit Ellipsen (…) positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen „Richtlinie für Leistungsschwellenwert zuweisen“ und „Richtlinie für Leistungsschwellenwert löschen“ bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Performance: Ansicht aller Volumes

Die Ansicht „Performance: Alle Volumes“ 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.

Wenn Sie die Latenz und den Durchsatz eines bestimmten Objekts analysieren möchten, klicken Sie auf die Schaltfläche Mehr Optionen und dann auf **Workload analysieren**. Auf der Seite Workload-Analyse können Sie Performance- und Kapazitätsdiagramme anzeigen. Sie können die Details im System Manager anzeigen, vorausgesetzt, Sie haben gültige Anmeldedaten für System Manager.

> Für Datensicherungs-Volumes (DP) werden nur Zählerwerte für den benutzergenerierten Datenverkehr angezeigt. Root-Volumes werden auf dieser Seite nicht angezeigt.

Im Folgenden sind einige wichtige Felder in der Ansicht „Performance: Alle Volumes“ aufgeführt.

- Stil: Entweder FlexVol oder FlexGroup.
- Latenz: Bei FlexVol Volumes ist dies die durchschnittliche Antwortzeit des Volume für alle I/O-Anfragen, die in Millisekunden pro Vorgang ausgedrückt wird. Bei FlexGroup Volumes ist dies die durchschnittliche

Latenz aller zusammengehörigen Volumes.

- IOPS/TB: Die Anzahl der pro Sekunde verarbeiteten Input/Output-Vorgänge, basierend auf dem gesamten Speicherplatz, der vom Workload in Terabyte verbraucht wird. Dieser Zähler ermittelt, wie viel Performance über eine bestimmte Storage-Kapazität bereitgestellt werden kann.
- IOPS: Für FlexVol Volumes ist dies die Anzahl der ein-/Ausgabe-Vorgänge pro Sekunde für das Volume. Bei FlexGroup Volumes ist dies die Summe der IOPS für alle zusammengehörigen Volumes.
- MB/s: Für FlexVol-Volumes ist dies der Durchsatz auf dem Volume, der in Megabyte pro Sekunde gemessen wird. Bei FlexGroup Volumes entspricht dies der Summe von MB/s für alle zusammengehörigen Volumes.
- Kapazitätsfelder: Freie und Gesamtkapazität in gib.

Weitere Informationen finden Sie unter den folgenden Links:

- "Zuweisen von Richtlinien zu Performance-Schwellenwerten zu Storage-Objekten"
- "Entfernen von Richtlinien für Performance-Schwellenwerte aus Storage-Objekten"
- "Arten von Workloads, die von Unified Manager überwacht werden"
- "Anzeigen der QoS-Richtliniengruppeneinstellungen, die auf bestimmte Volumes oder LUNs angewendet wurden"
- "Analyse der Empfehlungen von Unified Manager für das Tiering von Daten in die Cloud"
- "Anzeigen von Performance-Diagrammen zum Vergleich von Volumes oder LUNs in derselben QoS-Richtliniengruppe"

Performance: Ansicht aller Aggregate

Die Ansicht „Performance: Alle Aggregate“ zeigt für jedes Aggregat eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen, die durch eine Instanz von Unified Manager überwacht werden. Auf dieser Seite können Sie die Performance Ihrer Aggregate überwachen und Fehler bei Performance-Problemen und Schwellenwerten beheben.

Die folgenden wichtigen Bereiche der Performance: Ansicht aller Aggregate.

- Typ: Der Typ des Aggregats:
  - 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
  - Festplatte (FabricPool): Kombiniert HDDs und ein Cloud-Tier
  - VMDisk (SDS): Virtuelle Laufwerke innerhalb einer virtuellen Maschine
  - VMDisk (FabricPool): Kombiniert virtuelle Festplatten mit einer Cloud-Tier
  - LUN (FlexArray)
- Inaktive Datenberichterstellung: Gibt an, ob die Funktion zur Berichterstellung inaktiver Daten auf diesem Aggregat aktiviert oder deaktiviert ist. Wenn die Funktion aktiviert ist, zeigen Volumes auf diesem Aggregat im Bild „Performance: Alle Volumes“ den Umfang der „kalten“ Daten an. Der Wert in diesem Feld lautet „N/A“, wenn die Version von ONTAP keine inaktive Datenberichterstattung unterstützt.

- Schwellenwertrichtlinie: Benutzerdefinierte Performance-Schwellenwertrichtlinie oder aktive Richtlinien für dieses Storage-Objekt. Sie können den Cursor über Richtliniennamen mit Ellipsen (…) positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen „Richtlinie für Leistungsschwellenwert zuweisen“ und „Richtlinie für Leistungsschwellenwert löschen“ bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken. Weitere Informationen finden Sie unter den folgenden Links:
- "Zuweisen von Richtlinien zu Performance-Schwellenwerten zu Storage-Objekten"
- "Entfernen von Richtlinien für Performance-Schwellenwerte aus Storage-Objekten"

Performance: Alle Nodes anzeigen

Die Ansicht Performance: Alle Nodes zeigt für jeden Node, der von einer Instanz von Unified Manager überwacht wird, eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen an. So können Sie die Performance Ihrer Nodes schnell überwachen und Performance-Probleme und Schwellwerte beheben.

Flash Cache Lesevorgänge liefert den Prozentsatz von 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.

Im Menü **Berichte** wird die Option **Hardware Inventory Report** zur Verfügung gestellt, wenn Unified Manager und die Cluster, die es verwaltet, an einem Standort ohne externe Netzwerkverbindung installiert sind. Über diese Schaltfläche wird eine .csv-Datei generiert, die eine vollständige Liste von Cluster- und Node-Informationen enthält, z. B. Angaben zu Hardwaremodellen, Seriennummern, Festplattentypen und Anzahl sowie installierte Lizenzen. Diese Berichtsfunktion ist hilfreich zur Vertragsverlängerung innerhalb sicherer Standorte, die nicht mit der NetApp Active IQ Plattform verbunden sind. Über die Schaltflächen **Performance Threshold Policy** und **Clear Performance Threshold Policy** können Sie Schwellenwertrichtlinien auf den Objektbestandsseiten zuweisen oder löschen.

Weitere Informationen finden Sie unter den folgenden Links:

- "Zuweisen von Richtlinien zu Performance-Schwellenwerten zu Storage-Objekten"
- "Entfernen von Richtlinien für Performance-Schwellenwerte aus Storage-Objekten"
- "Erstellen eines Hardware-Bestandsberichts zur Vertragsverlängerung"

Performance: Ansicht aller Storage VMs

Die Ansicht „Performance: Alle Storage VMs“ gibt einen Überblick über die 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. Das Latenzfeld auf dieser Seite meldet die durchschnittliche Antwortzeit für alle I/O-Anfragen, die in Millisekunden pro Vorgang ausgedrückt wird.

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.

Weitere Informationen finden Sie unter den folgenden Links:

- "Zuweisen von Richtlinien zu Performance-Schwellenwerten zu Storage-Objekten"
- "Entfernen von Richtlinien für Performance-Schwellenwerte aus Storage-Objekten"

Performance: Ansicht aller LUNs

Die Ansicht „Performance: Alle LUNs“ 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.

Wenn Sie die Latenz und den Durchsatz eines bestimmten Objekts analysieren möchten, klicken Sie auf das Symbol Mehr ⋮, dann auf **Workload analysieren** und Sie können Performance- und Kapazitätsdiagramme auf der Seite **Workload-Analyse** anzeigen.

Weitere Informationen finden Sie unter den folgenden Links:

- "Überwachung von LUNs in einer Konsistenzgruppe"
- "Bereitstellung von LUNs"
- "Zuweisen von Richtlinien zu Performance-Schwellenwerten zu Storage-Objekten"
- "Entfernen von Richtlinien für Performance-Schwellenwerte aus Storage-Objekten"
- "Anzeigen von Volumes oder LUNs in derselben QoS-Richtliniengruppe".
- "Anzeigen der QoS-Richtliniengruppeneinstellungen, die auf bestimmte Volumes oder LUNs angewendet wurden"
- "Bereitstellung von LUNs mithilfe von APIs"

Performance: Alle NVMe Namesaces Ansicht

Die Ansicht „Performance: Alle NVMe Namesaces“ gibt einen Überblick über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jeden NVMe Namespace, 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.

Folgende Informationen werden unter anderem berichtet: 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 - der Namespace hat nicht mehr genügend Speicherplatz.

Weitere Informationen finden Sie unter den folgenden Links:

- "Zuweisen von Richtlinien zu Performance-Schwellenwerten zu Storage-Objekten"
- "Entfernen von Richtlinien für Performance-Schwellenwerte aus Storage-Objekten"

Performance: Ansicht aller Netzwerkschnittstellen

Die Ansicht Performance: Alle Netzwerkschnittstellen zeigt eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jede Netzwerkschnittstelle (LIF) an, die von dieser Instanz von Unified Manager überwacht wird. Auf dieser Seite können Sie die Leistung Ihrer Schnittstellen schnell überwachen und Leistungsprobleme und Schwellenwertereignisse beheben. Im Folgenden sind einige wichtige Felder in der Ansicht Leistung: Alle Netzwerkschnittstellen aufgeführt.

- IOPS: Die ein-/Ausgabevorgänge pro Sekunde. IOPS gelten nicht für NFS LIFs und CIFS LIFs und wird für diese Typen als „k. A.“ angezeigt.
- Latenz: Die durchschnittliche Reaktionszeit aller I/O-Anfragen in Millisekunden pro Vorgang. Die Latenz gilt nicht für NFS LIFs und CIFS LIFs und wird für diese Typen als K. A. angezeigt.

- Home Standort: Der Home-Standort für die Schnittstelle, angezeigt als Knotenname und Portname, durch einen Doppelpunkt getrennt (:). Wenn die Position mit Ellipsen (…) angezeigt wird, können Sie den Cursor über den Ortsnamen positionieren, um die vollständige Position anzuzeigen.
- Aktueller Speicherort: Der aktuelle Speicherort der Schnittstelle, angezeigt als Knotenname und Portname, durch einen Doppelpunkt getrennt (:). Wenn die Position mit Ellipsen (…) angezeigt wird, können Sie den Cursor über den Ortsnamen positionieren, um die vollständige Position anzuzeigen.
- Rolle: Die Schnittstellenrolle: Daten, Cluster, Knoten-Management oder Intercluster.

Die auf dieser Seite aufgeführten Schnittstellen umfassen Daten-LIFs, Cluster-LIFs, Node-Management-LIFs und Intercluster-LIFs. Unified Manager verwendet keine System-LIFs oder zeigt diese an.

Performance: Alle Ports anzeigen

Die Ansicht „Performance: Alle Ports“ zeigt für jeden Port, der von einer Instanz von Unified Manager überwacht wird, eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen an. So können Sie die Performance Ihrer Ports schnell überwachen und Performance-Probleme sowie Schwellenwertereignisse beheben. Für eine Port-Rolle wird die Netzwerk-Port-Funktion angezeigt, entweder Daten oder Cluster. FCP-Ports können keine Rolle enthalten, und die Rolle wird als „N/A“ angezeigt

Die Werte des Performance-Zähler werden nur für physische Ports angezeigt. Zählerwerte werden nicht für VLANs oder Interface Groups angezeigt.

Weitere Informationen finden Sie unter den folgenden Links:

- "Zuweisen von Richtlinien zu Performance-Schwellenwerten zu Storage-Objekten"
- "Entfernen von Richtlinien für Performance-Schwellenwerte aus Storage-Objekten"

Performance: Ansicht QoS-Richtliniengruppen

In der Ansicht QoS Policy Groups werden die QoS-Richtliniengruppen angezeigt, die auf den Clustern verfügbar sind, die von Unified Manager überwacht werden. Dazu gehören herkömmliche QoS-Richtlinien, anpassungsfähige QoS-Richtlinien und QoS-Richtlinien, die durch Performance-Service-Level zugewiesen werden.

In der Ansicht „Performance: QoS Policy Groups“ sind einige wichtige Felder aufgeführt.

- QoS Policy Group: Der Name der QoS Policy Group. Bei NSLM (NetApp Service Level Manager) 1.3-Richtlinien, die in Unified Manager 9.7 oder höher importiert wurden, enthält der hier angezeigte Name den SVM-Namen sowie andere Informationen, die nicht dem Namen enthalten, als der Performance-Service-Levelin NSLM definiert wurde. Der Name „NSLM_vs6_Performance_2_0“ bedeutet beispielsweise, dass dies die vom NSLM-System definierte „Performance“ PSL-Richtlinie ist, die auf SVM „vs6“ erstellt wurde und eine erwartete Latenz von „2 ms/op“ hat.
- SVM: Die Storage-VM (SVM), der die QoS-Richtliniengruppe angehört. Sie können auf den Namen der Storage-VM klicken, um zur Detailseite der Storage-VM zu gelangen. Beachten Sie, dass dieses Feld leer ist, wenn die QoS-Richtlinie auf der Admin Storage-VM erstellt wurde, da dieser Storage-VM-Typ für das Cluster steht.
- Min. Durchsatz: Der Mindestdurchsatz in IOPS, den die Richtliniengruppe garantiert. Für anpassungsfähige Richtlinien stellt dies die erwartete Mindestzahl an IOPS pro TB dar, die dem Volume oder der LUN zugewiesen ist. Grundlage dafür ist die zugewiesene Storage-Objektgröße.

- Max. Durchsatz: Der Durchsatz in IOPS und/oder MB/s, den die Richtliniengruppe nicht überschreiten darf. Wenn dieses Feld leer ist, bedeutet dies, dass die in ONTAP definierte maximale Anzahl unbegrenzt ist. Bei anpassungsfähigen Richtlinien stellt dies die maximal (maximal) IOPS pro TB dar, die dem Volume oder der LUN zugewiesen werden können. Die Grundlage dafür ist die zugewiesene Storage-Objektgröße oder die verwendete Storage-Objektgröße.
- Absolutes IOPS-Minimum: Bei anpassungsfähigen Richtlinien ist dies der absolute IOPS-Mindestwert, der als Überschreiben verwendet wird, wenn die erwarteten IOPS kleiner als dieser Wert ist.
- Blockgröße: Die Blockgröße, die für die adaptive QoS-Richtlinie angegeben ist.
- Min Zuweisung: Wird der maximale Durchsatz (Spitzenwert) der IOPS verwendet, unabhängig davon, ob der „zugewiesene Speicherplatz“ oder der „genutzte Speicherplatz“ verwendet werden.
- Erwartete Latenz: Die erwartete durchschnittliche Latenz für Storage-Input/Output-Vorgänge
- Shared: Bei herkömmlichen QoS-Richtlinien wird festgelegt, ob die in der Richtliniengruppe definierten Durchsatzwerte von mehreren Objekten gemeinsam genutzt werden.
- Zugeordnete Objekte: Die Anzahl der Workloads, die der QoS-Richtliniengruppe zugewiesen sind. Sie können auf die Schaltfläche erweitern () neben dem Gruppennamen der QoS-Richtlinie klicken , um weitere Details zur Richtliniengruppe anzuzeigen.
- Zugewiesene Kapazität: Die Menge an Speicherplatz, die die Objekte in der QoS-Richtliniengruppe derzeit verwenden.
- Zugehörige Objekte: Anzahl der Workloads, die der QoS-Richtliniengruppe zugewiesen werden, getrennt in Volumes und LUNs. Sie können auf die Nummer klicken, um zu einer Seite zu navigieren, die weitere Details zu den ausgewählten Volumes oder LUNs enthält.

Weitere Informationen finden Sie in den Themen unter "Management der Performance mithilfe von QoS-Richtliniengruppeninformationen".

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.

Schritt

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.

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.

Schritt

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 das Filterfeld können Sie die Rasteransicht entsprechend Ihren Einstellungen anpassen. Die verfügbaren Filteroptionen basieren auf dem Objekttyp, der im Raster angezeigt wird. Wenn aktuell Filter angewendet werden, wird rechts neben der Schaltfläche Filter die Anzahl der angewendeten Filter angezeigt.

Es werden drei Filterparameter unterstützt.

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

Die Felder Spalte, Operator und Wert sind für jeden Filter erforderlich. Die verfügbaren Filter spiegeln die filterbaren Spalten auf der aktuellen Seite wider. 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 die Schaltfläche **Filter**. Das Filterfenster wird angezeigt.
2. Klicken Sie auf die linke Dropdown-Liste und wählen Sie ein Objekt aus, z. B. *Cluster* oder einen Performance-Zähler.
3. Klicken Sie auf die mittlere Dropdown-Liste, und wählen Sie den gewünschten Operator aus.
4. Wählen Sie in der letzten Liste einen Wert aus oder geben Sie einen Wert ein, um den Filter für dieses Objekt abzuschließen.
5. Um einen anderen 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.
6. Klicken Sie Auf **Filter Anwenden**. Die Filteroptionen werden auf das Raster angewendet und die Anzahl der Filter wird rechts neben der Schaltfläche Filter angezeigt.
7. Verwenden Sie den Filterbereich, um einzelne Filter zu entfernen, indem Sie auf das Papierkorb-Symbol rechts neben dem zu entfernenden Filter klicken.
8. 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, schließt sich das Filterfenster, wendet Ihre Filter an und zeigt die Anzahl der angewendeten Filter an ().

Analyse der Empfehlungen von Unified Manager für das Tiering von Daten in die Cloud

Die Ansicht Leistung: Alle Volumes zeigt Informationen zur Größe der auf dem inaktiven (kalten) Volume gespeicherten Benutzerdaten an. 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 wurde die **`auto`** Tiering Policy in ONTAP 9.4 eingeführt und die **`all`** Tiering Policy wurde in ONTAP 9.6 eingeführt. Wenn die Empfehlung ist, die Auto Tiering Policy zu verwenden, müssen Sie ein Upgrade auf ONTAP 9.4 oder höher durchführen.

Die folgenden drei Performance-Felder sind in der Ansicht „Alle Volumes“ enthalten Informationen darüber, ob Sie die Festplattenauslastung Ihres Storage-Systems verbessern und Speicherplatz auf der 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 Software verwendet wird, weil es erfordert, dass das Aggregat, auf dem das Volume bereitgestellt wird **`inactive data reporting parameter`**, auf, gesetzt **`enabled`** ist und dass die minimale Anzahl der Kühltage Schwelle erreicht wurde (für Volumes, die die OR **`auto`** Tiering Policy verwenden **`snapshot-only`**). 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 ONTAP System Manager, ONTAP CLI-Befehle oder eine Kombination dieser Tools.

Wenn Sie mit der Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ bei Unified Manager angemeldet sind, steht in der Cloud-Empfehlung der Link **Volume konfigurieren** zur Verfügung, 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.

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.

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.

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 Performance-Statistiken für diesen Zeitraum werden in den Diagrammen und in der Chronik von Ereignissen 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.

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 ( ) entspricht der Farbe der Trend-Datenlinie des Objekts in den Diagrammen.

2. **Optional:** Daten für ausgewählte Objekte ausblenden oder anzeigen:

Hier…	Führen Sie diese Aktion durch…
Ausgewähltes Objekt ausblenden	Klicken Sie im Vergleichsfenster auf das Augensymbol des ausgewählten Objekts ( ). 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. **Optional:** 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 bei den durchschnittlichen Latenzwerten die I/O-Gewichtung berücksichtigt wird.
Latenz - Aufschlüsselung	Die gleichen Informationen werden unter Latenz insgesamt angezeigt, allerdings mit getrennten Performance-Daten in Lese-, Schreib- und sonstige Latenz. Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume, eine LUN, Oder Namespace.
Latenz – Cluster-Komponenten	Die gleichen Informationen werden unter Latenz insgesamt angezeigt, jedoch mit den Performance-Daten getrennt in Latenz nach Clusterkomponente. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volume ist.
IOPS – gesamt	Anzahl der pro Sekunde verarbeiteten ein-/Ausgabevorgänge. Wenn für einen Node angezeigt wird, zeigt die Auswahl „`Total`“ die IOPS für Daten an, die durch diesen Node verschoben werden, der sich auf dem lokalen oder dem Remote-Node befindet, und durch Auswahl von „`Total (Local)`“ werden die IOPS für Daten angezeigt, die sich nur auf dem aktuellen Node befinden.

Verfügbare Diagramme	Diagrammbeschreibung
IOPS – Aufschlüsselung	Die gleichen Informationen, die auf dem IOPS-Wert insgesamt angezeigt werden, jedoch mit getrennten Performance-Daten in Lese-, Schreib- und sonstige IOPS. Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt eine SVM, einen Node, ein Aggregat, ein Volume, eine LUN, Oder Namespace. Wenn in der Zoom-Ansicht angezeigt wird, zeigt das Volume-Diagramm die minimalen und maximalen Durchsatzwerte der QoS an, sofern diese in ONTAP konfiguriert sind. Wenn für einen Knoten angezeigt wird, zeigt die Auswahl „`Breakdown`“ den IOPS-Aufschlüsselung für Daten an, die sich durch diesen Knoten bewegen, der sich möglicherweise auf dem lokalen oder dem Remote-Knoten befindet, und bei Auswahl von „`Breakdown (Local)`“ wird der IOPS-Aufschlüsselung für Daten angezeigt, die sich nur auf dem aktuellen Knoten befinden.
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 wird auch als I/O-Dichte bezeichnet und misst, wie viel Performance mit einer bestimmten Menge an Storage-Kapazität bereitgestellt werden kann. Bei Anzeige in der Zoom-Ansicht zeigt das Diagramm Volumes die Werte für die erwartete QoS und den Spitzendurchsatz an, sofern diese in ONTAP konfiguriert sind. 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.

Verfügbare Diagramme	Diagrammbeschreibung
MB/s - Aufschlüsselung	Die gleichen Informationen, die im MB/s-Diagramm angezeigt werden, jedoch mit getrennten Durchsatzdaten in Festplattenlesevorgänge, Flash Cache Lese-, Schreib und andere. Wenn in der Zoom-Ansicht angezeigt wird, zeigt das Volume-Diagramm die 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. 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
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.
Auslastung – Gesamt	Verfügbarer Prozentsatz der verfügbaren Ressource des Objekts, das verwendet wird. Die Auslastung zeigt die Node-Auslastung für Nodes, die Festplattenauslastung von Aggregaten und die Bandbreitenauslastung für Ports an. Diese Diagrammoption wird nur angewendet, wenn das ausgewählte Objekt ein Node, ein Aggregat oder ein Port ist.
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.

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.

Schritt

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.

Was Sie brauchen

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.

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.

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.

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 Performance-Statistiken für diesen Zeitraum werden in den Diagrammen und in der Chronik von Ereignissen 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.

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.

Schritt

1. Wählen Sie das, das einer Richtlinie zugeordnet ist, aus, oder heben Sie die Auswahl auf.

   Der ausgewählte Schwellenwert wird auf die Zoom-Ansicht der Zählerdiagramme angewendet. Kritische Schwellenwerte werden als rote Linie angezeigt. Warnschwellenwerte werden als gelbe Linie angezeigt.

Anzeigen der Volume-Latenz nach Clusterkomponente

Sie können detaillierte Latenzinformationen zu einem Volume mithilfe der Seite „Volume Performance 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.

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-Limit Max
- QoS-Limit Min
- Netzwerkverarbeitung
- Cluster Interconnect
- Datenverarbeitung
- Aggregatvorgänge
- Volume-Aktivierung
- MetroCluster-Ressourcen
- Cloud-Latenz

- Sync SnapMirror

Schritte

1. Wählen Sie auf der Seite **Volume Performance 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 der Cluster-Komponente aufheben oder auswählen .

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.

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-FC

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 des mit einem Protokoll verknüpften s aufheben oder auswählen .

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.

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 in der **Performance: Alle Volumes** Ansicht oder **Performance: Alle LUNs** Ansicht den gewünschten Volume 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.

Anzeigen der Performance für All-SAN-Array-Cluster

Sie können die Ansicht Performance: All Clusters verwenden, um den Leistungsstatus Ihrer All-SAN-Array-Cluster anzuzeigen.

Was Sie brauchen

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

Sie können die Überblicksinformationen für alle SAN-Array-Cluster in der Ansicht Leistung: Alle Cluster und Details auf der Seite Cluster / Performance Explorer anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Cluster**.
2. Stellen Sie sicher, dass die Spalte „`personality`“ in der Ansicht **Health: All Clusters** angezeigt wird, oder fügen Sie sie mit dem Steuerelement **Anzeigen / Ausblenden** hinzu.

   In dieser Spalte wird „`All-SAN-Array`“ für Ihre All-SAN-Array-Cluster angezeigt.

3. Um Informationen zur Leistung in diesen Clustern anzuzeigen, wählen Sie die Ansicht **Performance: Alle Cluster** aus.

   Zeigen Sie die Performance-Informationen für das All-SAN-Array-Cluster an.

4. Um detaillierte Informationen zur Performance in diesen Clustern anzuzeigen, klicken Sie auf den Namen eines All-SAN-Array-Clusters.
5. Klicken Sie auf die Registerkarte **Explorer**.
6. Wählen Sie auf der Seite **Cluster / Performance Explorer** im Menü **Ansicht und Vergleich Knoten in diesem Cluster** aus.

   Sie können die Performance-Statistiken beider Nodes auf diesem Cluster vergleichen, um sicherzustellen, dass die Last auf beiden Nodes nahezu identisch ist. Wenn zwischen den beiden Knoten große Unterschiede bestehen, können Sie den zweiten Knoten zu den Diagrammen hinzufügen und die Werte

über einen längeren Zeitraum vergleichen, um mögliche Konfigurationsprobleme zu erkennen.

Anzeigen von Node-IOPS auf Basis von Workloads, die sich nur auf dem lokalen Node befinden

Das Node-IOPS-Zählerdiagramm kann hervorheben, wo die Vorgänge nur den lokalen Node durchlaufen, indem eine Netzwerk-LIF zum Ausführen von Lese-/Schreibvorgängen auf Volumes auf einem Remote-Node verwendet wird. Die Diagramme IOPS - „`Total (Local)`“ und „`Breakdown (Local)`“ zeigen die IOPS für Daten an, die sich nur auf dem aktuellen Node in lokalen Volumes befinden.

Die Versionen der „`Local`“ dieser Zählerdiagramme sind denen der Node-Diagramme für die Performance-Kapazität und -Auslastung ähnlich, da sie außerdem nur die Statistiken für Daten anzeigen, die sich auf lokalen Volumes befinden.

Durch den Vergleich der Versionen „`Local`“ dieser Zählerdiagramme mit den regulären Total-Versionen dieser Zählerdiagramme sehen Sie, ob sich viel Datenverkehr durch den lokalen Knoten bewegt, um auf Volumes auf dem entfernten Knoten zuzugreifen. Diese Situation kann zu Performance-Problemen führen, die möglicherweise durch hohe Auslastung auf dem Node angezeigt werden, wenn zu viele Vorgänge den lokalen Node durchlaufen, um ein Volume auf einem Remote-Node zu erreichen. In diesen Fällen möchten Sie möglicherweise ein Volume zum lokalen Node verschieben oder eine LIF auf dem Remote-Node erstellen, wo der Datenverkehr von Hosts, die auf dieses Volume zugreifen, verbunden werden kann.

Schritte

1. Wählen Sie auf der Seite **Performance/Node Explorer** für den ausgewählten Knoten im IOPS-Diagramm im Dropdown-Menü die Option **Gesamt** aus.

   Das Diagramm IOPS – Total wird angezeigt.

2. Klicken Sie auf **Zoom View**, um eine größere Version des Diagramms in einem neuen Browser-Tab anzuzeigen.
3. Zurück auf der Seite **Performance/Node Explorer** wählen Sie im IOPS-Diagramm im Dropdown-Menü die Option **Gesamt (lokal)** aus.

   Das Diagramm IOPS – Total (Local) wird angezeigt.

4. Klicken Sie auf **Zoom View**, um eine größere Version des Diagramms in einem neuen Browser-Tab anzuzeigen.
5. Sie können die beiden Diagramme nebeneinander anzeigen und Bereiche identifizieren, in denen die IOPS-Werte recht unterschiedlich zu sein scheinen.
6. Bewegen Sie den Mauszeiger über diese Bereiche, um den lokalen und den gesamten IOPS für einen bestimmten Zeitpunkt zu vergleichen.

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.

- **MB/s**

  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

- **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 gelb ( ) angezeigt.

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 MB/s-Performance des Objekts an und gibt an, wie viele Daten in Megabyte pro Sekunde an das Objekt übertragen wurden. Das MB/s-Zählerdiagramm bietet einen allgemeinen Überblick über den Zustand der MB/s des Objekts für den Zeitraum von 72 Stunden.

  Oben (Zählerwert): die Zahl in der Kopfzeile zeigt die durchschnittliche Anzahl von MB/s für den vorangegangenen 72-Stunden-Zeitraum an.

  Mitte (Leistungsdiagramm): der Wert unten im Diagramm zeigt die niedrigste Anzahl von MB/s an, und der Wert oben im Diagramm zeigt die höchste Anzahl von MB/s für den vorangegangenen 72-Stunden-Zeitraum an. Positionieren Sie den Cursor über die Trendlinie des Diagramms, um den MB/s-Wert 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 **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. Diese Funktionalität ermöglicht die Anzeige des Latenzdiagramms zur Unterstützung des NetApp „Performance-Garantie“-Programms.

- **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.

Management der Performance mithilfe von QoS-Richtliniengruppeninformationen

Mit Unified Manager können Sie die QoS-Richtliniengruppen (Quality of Service) anzeigen, die auf allen von Ihnen überwachten Clustern verfügbar sind. Die Richtlinien können mithilfe der ONTAP Software (System Manager oder die ONTAP CLI) oder durch Richtlinien auf Unified Manager Performance Service Level definiert wurden. Unified Manager zeigt außerdem an, welchen Volumes und LUNs eine QoS-Richtliniengruppe zugewiesen ist.

Weitere Informationen zum Anpassen von QoS-Einstellungen finden Sie unter "Performance Management – Überblick"

Kontrolle des Workload-Durchsatzes durch Storage-QoS

Sie können eine Richtliniengruppe für Quality of Service (QoS) erstellen, um das I/O-Limit (IOPS) oder das Durchsatzlimit (MB/s) für die in ihm 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.

„herkömmliche“ QoS-Richtliniengruppen können einzelnen Workloads zugewiesen werden, zum Beispiel einzelnen Volumes oder LUNs. In diesem Fall kann der Workload das volle Durchsatzlimit verwenden. QoS-Richtliniengruppen können auch mehreren Workloads zugewiesen werden. In diesem Fall ist das Durchsatzlimit zwischen den Workloads „srot“. 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 der Spitzenwert beispielsweise auf 5,000 IOPS/TB in einer anpassungsfähigen QoS-Richtlinie festgelegt wurde, hat ein 10-TB-Volume einen Durchsatz von maximal 50,000 IOPS. Wenn die Größe des Volumes später auf 20 TB geändert wird, passt die anpassungsfähige QoS das Maximum auf 100,000 IOPS an.

Ab ONTAP 9.5 können Sie die Blockgröße einschließen, wenn Sie eine anpassungsfähige QoS-Richtlinie definieren. Dadurch wird die Richtlinie in Fällen, in denen Workloads sehr große Blockgrößen verwenden und letztendlich einen hohen Prozentsatz des Durchsatzes nutzen, effektiv von einem IOPS/TB-Schwellenwert 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 Performanceereignis durch die Richtliniengruppendrosselung generiert wird, wird in der Ereignisbeschreibung der Name der beteiligten Richtliniengruppe angezeigt.

In der Ansicht „Performance: Alle Volumes“ können die betroffenen Volumes nach IOPS und MB/s sortiert

werden, um zu ermitteln, welche Workloads die höchste Auslastung aufweisen und welche dazu möglicherweise beigetragen haben. Auf der Seite „Performance/Volumes Explorer“ können Sie andere Volumes oder LUNs auf dem Volume auswählen, um sie mit den betroffenen Workload-IOPS oder der Durchsatzrate pro Sekunde 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, die ONTAP-Befehle oder Unified Manager Performance Service Level verwenden, um Richtliniengruppen zu managen, 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

Anzeigen aller QoS-Richtliniengruppen, die auf allen Clustern verfügbar sind

Sie können eine Liste aller QoS-Richtliniengruppen anzeigen, die in den von Unified Manager überwachten Clustern verfügbar sind. Dies umfasst herkömmliche QoS-Richtlinien, anpassungsfähige QoS-Richtlinien und QoS-Richtlinien, die durch Unified Manager Performance Service Level-Richtlinien gemanagt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **QoS Policy Groups**.

   Die Ansicht „Performance: Traditionelle QoS-Richtliniengruppen“ wird standardmäßig angezeigt.

2. Zeigen Sie die detaillierten Konfigurationseinstellungen für jede verfügbare herkömmliche QoS-Richtliniengruppe an.
3. Klicken Sie auf die Schaltfläche erweitern ( ) neben dem Namen der QoS-Richtliniengruppe, um weitere Details zur Richtliniengruppe anzuzeigen.
4. Wählen Sie im Menü Ansicht eine der zusätzlichen Optionen aus, um alle adaptiven QoS-Richtliniengruppen anzuzeigen oder alle QoS-Richtliniengruppen anzuzeigen, die mit Unified Manager Performance Service-Leveln erstellt wurden.

Anzeigen von Volumes oder LUNs in derselben QoS-Richtliniengruppe

Sie können eine Liste der Volumes und LUNs anzeigen, die derselben QoS-Richtliniengruppe zugewiesen wurden.

Bei herkömmlichen QoS-Richtliniengruppen, die zwischen mehreren Volumes „`shared`“ sind, kann dies hilfreich sein, um zu prüfen, ob bestimmte Volumes den für die Richtliniengruppe definierten Durchsatz überbeanspruchen. Es kann auch bei der Entscheidung helfen, anderen Volumes ohne einen negativen Einfluss auf die anderen Volumes weitere Volumes hinzuzufügen.

Bei anpassungsfähigen QoS-Richtlinien und Unified Manager-Performance-Service-Leveln Dies ist unter

Umständen hilfreich, alle Volumes oder LUNs anzuzeigen, die eine Richtliniengruppe verwenden. So sehen Sie, welche Objekte sich auswirken würden, wenn Sie die Konfigurationseinstellungen für die QoS-Richtlinie ändern.

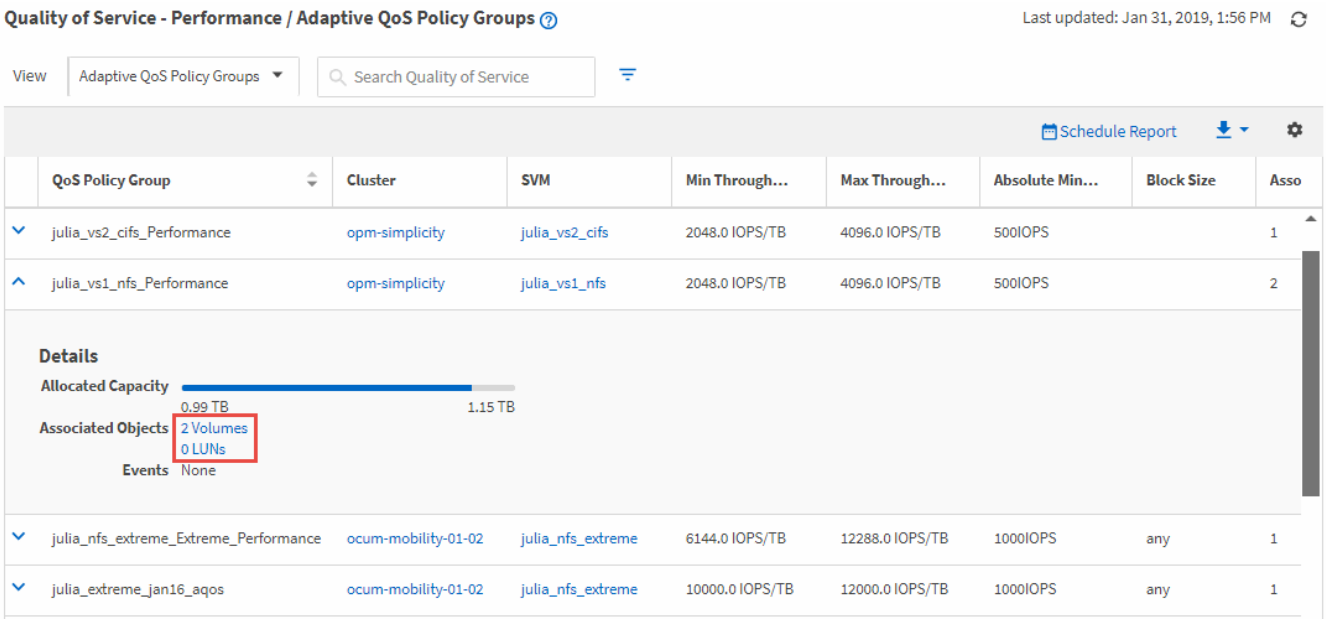
Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **QoS Policy Groups**.

   Die Ansicht „Performance: Traditionelle QoS-Richtliniengruppen“ wird standardmäßig angezeigt.

2. Wenn Sie sich für eine traditionelle Gruppe interessieren, bleiben Sie auf dieser Seite. Wählen Sie andernfalls eine der zusätzlichen View-Optionen aus, um alle adaptiven QoS-Richtliniengruppen oder alle QoS-Richtliniengruppen anzuzeigen, die durch Unified Manager Performance-Service-Level erstellt wurden.

3. Klicken Sie in der QoS-Richtlinie, die Sie interessieren, auf die Schaltfläche erweitern ( ) neben dem Namen der QoS-Richtliniengruppe, um weitere Details anzuzeigen.



4. Klicken Sie auf den Link Volumes oder LUNs, um die Objekte anzuzeigen, die diese QoS-Richtlinie verwenden.

   Die Seite „Performance Inventory“ für Volumes oder LUNs wird mit der Liste der Objekte angezeigt, die die QoS-Richtlinie verwenden.

Anzeigen der QoS-Richtliniengruppeneinstellungen, die auf bestimmte Volumes oder LUNs angewendet wurden

Sie können die QoS-Richtliniengruppen anzeigen, die auf Ihre Volumes und LUNs angewendet wurden, und Sie können einen Link zur Ansicht „Performance/QoS-Richtliniengruppen“ erstellen, um die detaillierten Konfigurationseinstellungen für jede QoS-Richtlinie anzuzeigen.

Nachfolgend sind die Schritte zur Anzeige der QoS-Richtlinie, die auf ein Volume angewendet wird, aufgeführt. Die Schritte zum Anzeigen dieser Informationen für eine LUN sind ähnlich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.

   Die Ansicht „Systemzustand: Alle Volumes“ wird standardmäßig angezeigt.

2. Wählen Sie im Menü Ansicht die Option **Leistung: Volumes in QoS Policy Group** aus.
3. Suchen Sie nach dem zu übersehenden Volumen, und scrollen Sie nach rechts, bis die Spalte **QoS Policy Group** angezeigt wird.
4. Klicken Sie auf den Namen der QoS-Richtliniengruppe.

   Die entsprechende Seite mit der Quality of Service wird angezeigt, je nachdem, ob es sich um eine herkömmliche QoS-Richtlinie, eine anpassungsfähige QoS-Richtlinie oder eine QoS-Richtlinie handelt, die mit Unified Manager Performance Service-Leveln erstellt wurde.

5. Detaillierte Konfigurationseinstellungen für die QoS-Richtliniengruppe anzeigen
6. Klicken Sie auf die Schaltfläche erweitern ( ) neben dem Namen der QoS-Richtliniengruppe, um weitere Details zur Richtliniengruppe anzuzeigen.

Anzeigen von Performance-Diagrammen zum Vergleich von Volumes oder LUNs in derselben QoS-Richtliniengruppe

Sie können die Volumes und LUNs in denselben QoS-Richtliniengruppen anzeigen und anschließend die Performance in einem einzelnen Diagramm mit IOPS, MB/s oder IOPS/TB vergleichen, um Probleme zu identifizieren.

Die Schritte zum Vergleich der Performance von Volumes in derselben QoS-Richtliniengruppe sind unten dargestellt. Die Schritte zum Anzeigen dieser Informationen für eine LUN sind ähnlich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.

   Die Ansicht „Systemzustand: Alle Volumes“ wird standardmäßig angezeigt.

2. Wählen Sie im Menü Ansicht die Option **Leistung: Volumes in QoS Policy Group** aus.
3. Klicken Sie auf den Namen des Volumes, das Sie überprüfen möchten.

   Die Seite Performance Explorer wird für das Volume angezeigt.

4. Wählen Sie im Menü Ansicht und Vergleich die Option **Volumes in derselben QoS Policy Group** aus.

   Die anderen Volumes, die dieselbe QoS-Richtlinie aufweisen, sind in der nachfolgenden Tabelle aufgelistet.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**, um die Volumes zu den Diagrammen hinzuzufügen, sodass Sie die IOPS, MB/s, IOPS/TB und andere Leistungsindikatoren für alle ausgewählten Volumes in den Diagrammen vergleichen können.

   Sie können den Zeitbereich ändern, um die Leistung über verschiedene Zeitintervalle zu sehen, außer dem Standard von 72 Stunden.

Die Darstellung der verschiedenen QoS-Richtlinien in den Durchsatzdiagrammen

Sie können die von ONTAP definierten Quality of Service-Richtlinieneinstellungen (QoS) anzeigen, die auf ein Volume oder eine LUN angewendet wurden. Sie finden sie im Performance-Explorer und in den Diagrammen für Workload-Analysen, IOPS/TB und MB/s. Die in den Diagrammen angezeigten Informationen unterscheiden sich je nach QoS-Richtlinie, die auf den Workload angewendet wurde.

Eine Einstellung für maximalen Durchsatz (oder „Peak“) definiert den maximalen Durchsatz, den der Workload nutzen kann, und begrenzt damit die Auswirkungen auf konkurrierende Workloads für Systemressourcen. Ein Mindestdurchsatz (bzw. „erwarteten“) definiert den Mindestdurchsatz, der für den Workload verfügbar sein muss, damit ein kritischer Workload die Mindestdurchsatz-Ziele erfüllt, unabhängig von der Nachfrage durch konkurrierende Workloads.

Gemeinsam genutzte und nicht gemeinsam genutzte QoS-Richtlinien für IOPS und MB/s definieren Boden und Decke mit den Begriffen „minimum“ und „mahximum“. 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 - verwendet" an. Definiert

in IOPS/TB“ oder „QoS Adaptive – zugewiesen, definiert in IOPS/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 128 GB ist. In der Tabelle werden Lücken angezeigt, wenn die genutzte Kapazität während des ausgewählten Zeitrahmens unter 128 GB fällt.

Anzeige der minimalen und maximalen Einstellungen für Workload-QoS im Performance Explorer

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.

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**.

Ihr Ziel ist	Tun Sie das…
MB/s-Obergrenze anzeigen (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 IOPS- und MB/s-Werte im Vergleich zur QoS-Einstellung anzuzeigen, bewegen Sie den Cursor in den Diagrammbereich, um das Popup-Fenster anzuzeigen.

Wenn bestimmte Volumes oder LUNs eine sehr hohe IOPS oder MB/s haben und Systemressourcen betonen, können Sie mit System Manager oder der ONTAP CLI die QoS-Einstellungen so anpassen, dass diese Workloads die Performance anderer Workloads nicht beeinträchtigen.

Weitere Informationen zum Anpassen von QoS-Einstellungen finden Sie unter "Performance Management – Überblick"

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

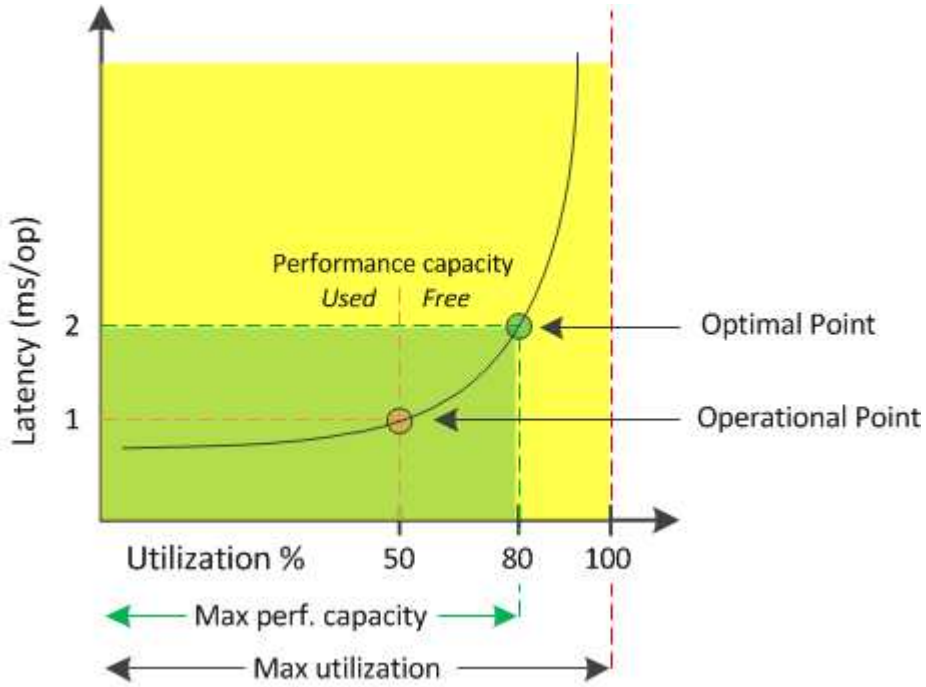
Punkt hinaus zu schieben, wodurch die Fehlerbehebung verringert wird.

- 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.

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.

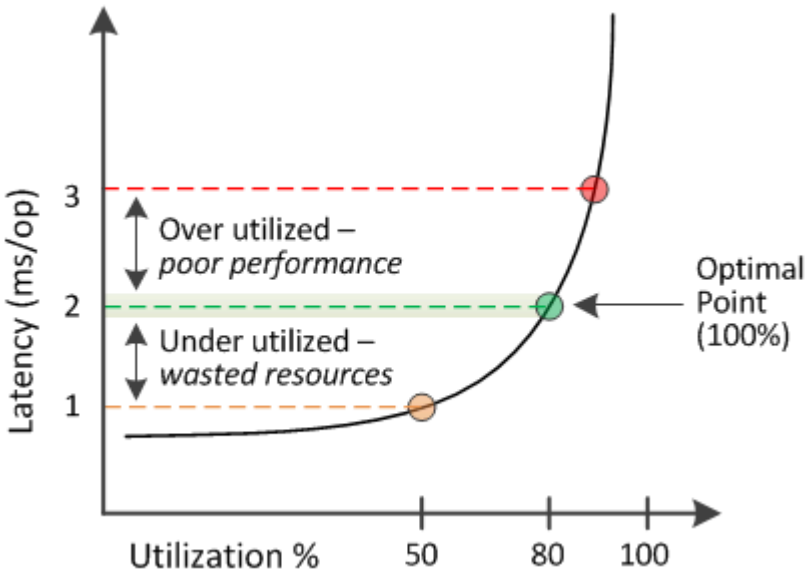
In einigen Fällen kann der Auslastungszähler jedoch höher auf der Dashboard-Seite sein. Dies ist normal, da das Dashboard die aktuellen Zählerwerte zu jedem Erfassungszeitraum aktualisiert. Es werden die Durchschnittswerte über einen Zeitraum nicht angezeigt, wie die anderen Seiten in der Benutzeroberfläche 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.

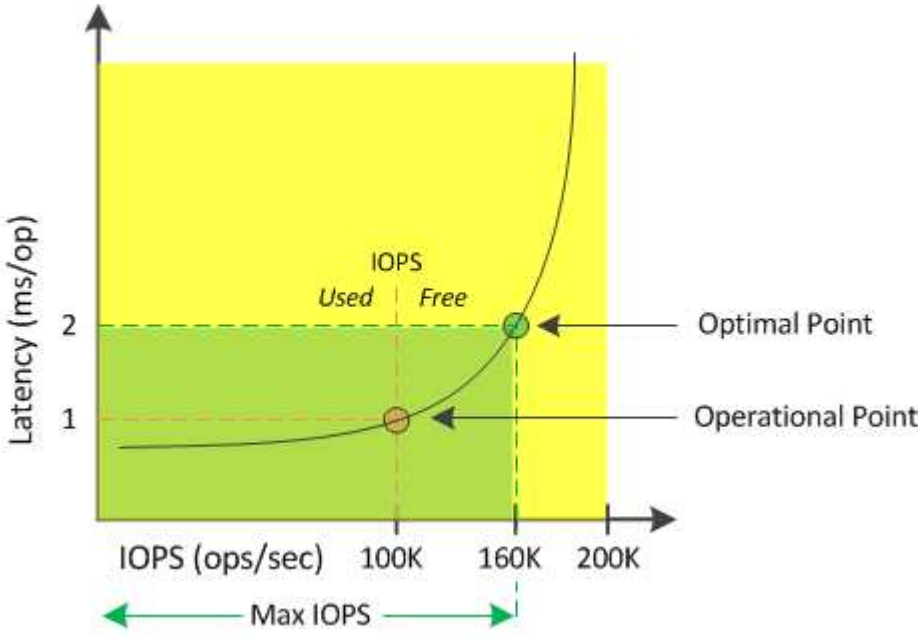
Die gesamten IOPS, die ein Node bereitstellen kann, basieren auf den physischen Eigenschaften des Node, beispielsweise auf der Anzahl der CPUs, der CPU-Geschwindigkeit und dem RAM-Umfang. Die gesamten IOPS, die ein Aggregat bereitstellen kann, basieren auf den physischen Eigenschaften der Festplatten, zum Beispiel auf einer SATA-, SAS- oder SSD-Festplatte.

Die Gesamtzahl der IOPS aller Volumes in einem Aggregat entspricht möglicherweise nicht den IOPS-Werten des Aggregats. Dies wird im folgenden Knowledge Base Artikel diskutiert: KB "Warum entspricht die Summe aller Volume IOPS in einem Aggregat nicht den aggregierten IOPS?"

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.

Die folgende Abbildung zeigt eine Beispiellatenz im Vergleich zur IOPS-Kurve für einen Node.



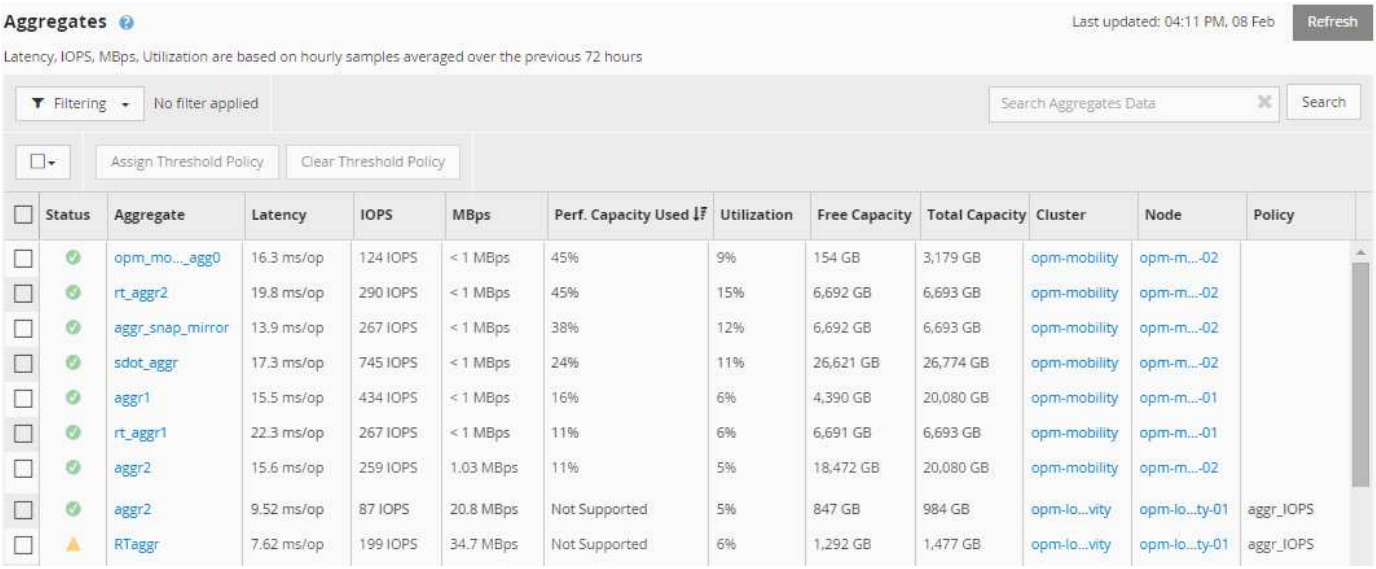
Die maximale Anzahl an IOPS, die eine Ressource liefern kann, ist die Anzahl der IOPS, wenn der Zähler für die Performance-Kapazität bei 100 % liegt (der optimale Punkt). Der Betriebspunkt identifiziert, dass der Node derzeit bei 100.000 IOPS mit einer Latenz von 1.0 ms/op arbeitet Auf der Grundlage 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 Dashboard, auf den Seiten Performance Inventory, auf der Seite Top Performers, Create Threshold Policy, auf den Seiten Performance Explorer und in Detaildiagrammen angezeigt. Beispielsweise bietet die Seite Performance: Alle Aggregate eine Spalte. Die Performance-Kapazität wird verwendet, um den verwendeten Wert für die Performance-Kapazität aller Aggregate anzuzeigen.



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

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 auf den Seiten „Performance Inventory“ und in den Seitendiagrammen des Performance Explorers für Nodes und Aggregate angezeigt. Wenn Sie beispielsweise einen Node auf der Seite „Node/Performance Explorer“ anzeigen, können Sie das Zählerdiagramm „`verfügbare IOPS`“ in der Liste auswählen, damit Sie die verfügbaren IOPS-Werte für den Node und 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.

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
Aggregat	Verwendete Performance-Kapazität	80 % erreicht	95 % erreicht	

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.

> Latenz- und IOPS-Werte, die auf dieser Seite und auf der Seite „Performance/Node Performance Explorer“ angezeigt werden, stimmen möglicherweise nicht überein, da verschiedene Performance-Zähler zum Berechnen der Werte für das Prognose des Node Failover verwendet werden.

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 am 8. Februar um 11 Uhr für den Knoten „Geschätzte Übernahme“ 73 %. 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.

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 Latenzbereich für alle überwachten Workloads prognostiziert.

Unified Manager muss mindestens 3 Tage Workload-Aktivität erfassen, bevor diese mit der Analyse beginnen kann und bevor die Latenzprognose für die I/O-Reaktionszeit auf der Seite Workload Analysis und auf der Seite Event Details angezeigt werden kann. Während diese Aktivität erfasst wird, werden in der Latenzprognose nicht alle Änderungen der Workload-Aktivität angezeigt. Nach Erfassung der Aktivität von 3 Tagen passt Unified Manager die Latenzprognose alle 24 Stunden um 12:00 Uhr an, um die Änderungen der Workload-Aktivität widerzuspiegeln und einen präziseren dynamischen Performance-Schwellenwert festzulegen.

Wenn in den ersten 4 Tagen, an denen Unified Manager einen Workload überwacht, mehr als 24 Stunden seit der letzten Datenerfassung vergangen sind, werden in den Latenzdiagrammen nicht die Latenzprognose für diesen Workload angezeigt. Ereignisse, die vor der letzten Sammlung erkannt wurden, sind weiterhin verfügbar.

> Bei der Sommerzeit (Sommerzeit) wird die Systemzeit geändert, wodurch die Latenzprognose für Performance-Statistiken für überwachte Workloads verändert wird. Unified Manager beginnt sofort mit der Korrektur des Latenzvorhersage, das etwa 15 Tage dauert. Während dieser Zeit können Sie Unified Manager weiterhin verwenden. Da Unified Manager jedoch die Latenzprognose verwendet, um dynamische Ereignisse zu erkennen, sind einige Ereignisse möglicherweise nicht korrekt. Ereignisse, die vor der Zeitänderung erkannt wurden, werden nicht beeinträchtigt.

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 Volume, LUN, NFS-Freigabe, SMB/CIFS-Freigabe und ein Workload 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. (DP Volumes werden für vom Benutzer erzeugten Datenverkehr überwacht.)
- 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:

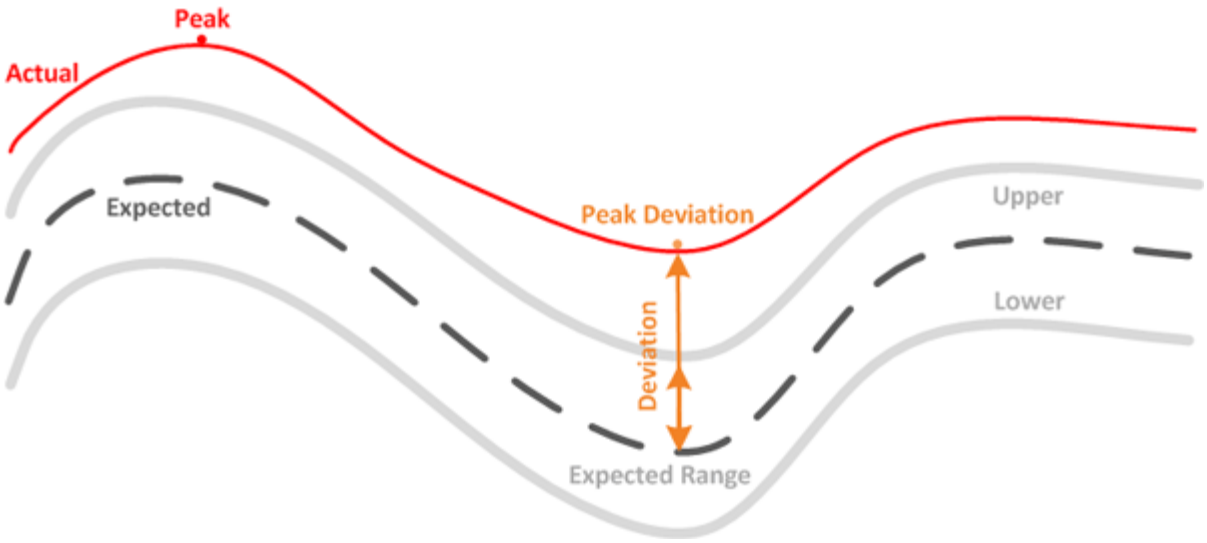
  - Storage-Effizienz, z. B. Deduplizierung
  - Der Zustand der Festplatte, einschließlich RAID-Rekonstruktion, Disk-Schrubben usw.
  - Datenreplizierung, z. B. SnapMirror Kopien
  - Management-Aktivitäten
  - Systemzustand des File-Systems, der verschiedene WAFL-Aktivitäten umfasst
  - Filesystem-Scanner, 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.

Messwerte für die Workload-Performance

Unified Manager misst die Performance von Workloads auf einem Cluster basierend auf historischen und erwarteten statistischen Werten, die die Latenzprognose für Werte für die Workloads bilden. Es vergleicht die tatsächlichen statistischen Workload-Werte mit der Latenzprognose, um zu ermitteln, ob die Workload-Performance zu hoch oder zu niedrig ist. Ein Workload, der nicht wie erwartet ausgeführt wird, löst ein dynamisches Performance-Ereignis aus, um Sie zu benachrichtigen.

In der folgenden Abbildung stellt der tatsächliche Wert in Rot die tatsächlichen Performance-Statistiken im Zeitrahmen dar. Der tatsächliche Wert hat den Performance-Schwellenwert überschritten, was den oberen Grenzwert der Latenzprognose darstellt. Der Peak ist der höchste ist-Wert im Zeitrahmen. Die Abweichung misst die Änderung zwischen den erwarteten Werten (der Prognose) und den Istwerten, während die Peak-Abweichung die größte Änderung zwischen den erwarteten Werten und den Istwerten 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.
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.

Messung	Beschreibung
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 (Latenzprognose) zu ermitteln.
Latenzprognose (Erwarteter Bereich)	Die Latenzprognose stellt eine Vorhersage des Wert für die obere und untere Performance dar, die 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 ein dynamisches Performance-Ereignis 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.
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	Die Menge an Schreibdurchsatz in Megabyte pro Sekunde (MB/s), von Workloads in einem lokalen Cluster zum Partner-Cluster in einer MetroCluster-Konfiguration.

Der erwartete Leistungsbereich

Die Latenzprognose stellt eine Vorhersage des Wert für die obere und untere Performance dar, die 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 ein dynamisches Performance-Ereignis aus.

Während der normalen Geschäftszeiten von 9:00 Uhr bis 5:00 Uhr können die meisten Mitarbeiter ihre E-Mails

beispielsweise zwischen 9:00 Uhr und 10:30 Uhr abrufen. Der gestiegene Bedarf an E-Mail-Servern führt zu einer Zunahme der Workload-Aktivitäten auf dem Back-End-Speicher während dieser Zeit. Mitarbeiter können von ihren E-Mail-Clients langsame Reaktionszeiten feststellen.

Während der Mittagspause zwischen 12:00 und 1:00 Uhr und am Ende des Arbeitstages nach 5:00 Uhr sind die meisten Mitarbeiter wahrscheinlich nicht am Computer. 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 Virenprüfungen stattfinden, die nach 5:00 Uhr beginnen und die Aktivität im Back-End-Speicher steigern.

Über mehrere Tage bestimmt der Anstieg und die Abnahme der Workload-Aktivität den erwarteten Bereich (Latenzprognose) der Aktivität, wobei obere und untere Grenzen für einen Workload festgelegt 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.

Bildung der Latenzprognose

Unified Manager muss die Workload-Aktivität mindestens 3 Tage lang sammeln, bevor sie mit der Analyse beginnen kann und bevor die Latenzprognose für die I/O-Reaktionszeit auf der GUI angezeigt werden kann. Die erforderliche Mindesterfassung berücksichtigt nicht alle Änderungen, die von der Workload-Aktivität durchgeführt werden. Nachdem die ersten 3 Tage der Aktivität erfasst wurden, passt Unified Manager die Latenzprognose alle 24 Stunden um 12:00 Uhr an, um Änderungen der Workload-Aktivität widerzuspiegeln und einen genaueren dynamischen Leistungsschwellenwert festzulegen.

Bei der Sommerzeit (Sommerzeit) wird die Systemzeit geändert, wodurch die Latenzprognose für Performance-Statistiken für überwachte Workloads verändert wird. Unified Manager beginnt sofort mit der Korrektur des Latenzvorhersage, das etwa 15 Tage dauert. Während dieser Zeit können Sie Unified Manager weiterhin verwenden. Da Unified Manager jedoch die Latenzprognose verwendet, um dynamische Ereignisse zu erkennen, sind einige Ereignisse möglicherweise nicht korrekt. Ereignisse, die vor der Zeitänderung erkannt wurden, werden nicht beeinträchtigt.

Verwendung der Latenzprognose für die Performance-Analyse

Unified Manager verwendet die Latenzprognose, um die typischen Aktivitäten der I/O-Latenz (Reaktionszeit) für überwachte Workloads darzustellen. Er benachrichtigt Sie, wenn die tatsächliche Latenz für einen Workload über den oberen Grenzen der Latenzprognose liegt. Dadurch wird ein dynamisches Performance-Ereignis ausgelöst, sodass Sie das Performance-Problem analysieren und Korrekturmaßnahmen ergreifen können.

Durch die Latenzprognose wird die Performance-Baseline für den Workload festgelegt. 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 dynamischen Leistungsschwellenwert. Unified Manager verwendet die Basiskapazität, um zu ermitteln, ob die tatsächliche Latenz einen Schwellenwert oder einen anderen Schwellenwert überschreitet 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 dynamischen 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 Aktivität mit hohen Workloads über einen langen Zeitraum konsistent bleibt, z. B. über mehrere Stunden, berücksichtigt Unified Manager die Aktivität als „Normal“ und passt die Latenzprognose dynamisch an, um den neuen dynamischen Performance-Schwellenwert zu bilden.

Einige Workloads weisen möglicherweise durchgängig niedrige Aktivitäten auf, bei denen die Latenzprognose für Latenz im Laufe der Zeit keine hohen Änderungsraten aufweisen. Um die Anzahl von Ereignissen während der Analyse von Performance-Ereignissen zu minimieren, löst Unified Manager 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 graue Latenzprognosen von 3.5 Millisekunden pro Betrieb (ms/op) mit dem niedrigsten Wert und 5.5 ms/op bei dem höchsten Wert auf. Wird die tatsächliche Latenz blau auf plötzlich 10 ms/op erhöht, weil der Netzwerk-Traffic oder die Konflikte einer Cluster-Komponente zeitweise zu hoch sind, liegt sie über der Latenzprognose und hat den dynamischen Performance-Schwellenwert überschritten.

Wenn der Netzwerk-Traffic gesunken ist oder die Cluster-Komponente keine Konflikte mehr hat, gibt die Latenz innerhalb der Latenzprognose zurück. 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

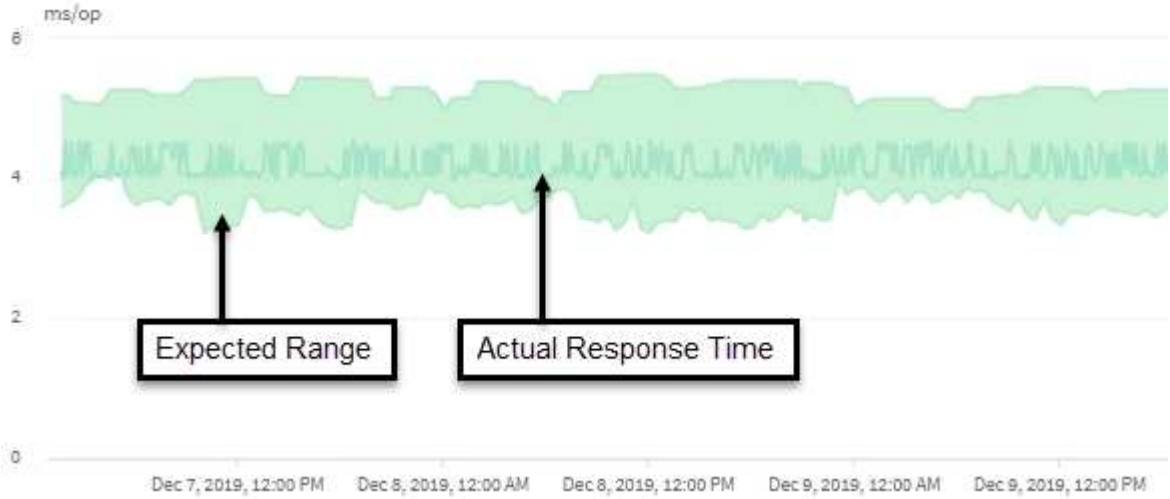
Die Workload-Latenz (Reaktionszeit) ist die Zeit, die ein Volume auf einem Cluster benötigt, um auf I/O-Anforderungen von Client-Applikationen zu reagieren. Unified Manager verwendet die Latenz, um Performance-Ereignisse zu erkennen und zu benachrichtigen.

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 dynamischen Performance-Schwellenwert des erwarteten Bereichs (Latenzprognose) überschreitet, analysiert Unified Manager das Ereignis, um zu ermitteln, ob es sich um ein Performance-Ereignis handelt, das möglicherweise behoben werden muss. Die Latenz wird in Millisekunden pro Vorgang (ms/op) gemessen.

Auf dem Diagramm „Latenz insgesamt“ auf der Seite „Workload-Analyse“ können Sie eine Analyse der Latenzstatistiken anzeigen, um zu ermitteln, wie die Aktivitäten einzelner Prozesse, wie z. B. Lese- und Schreibanfragen, mit den allgemeinen Latenzstatistiken vergleichen. 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 . Die Aktivität der tatsächlichen Reaktionszeit (Latenz) ist blau und die Latenzprognose (erwarteter Bereich) ist grün.

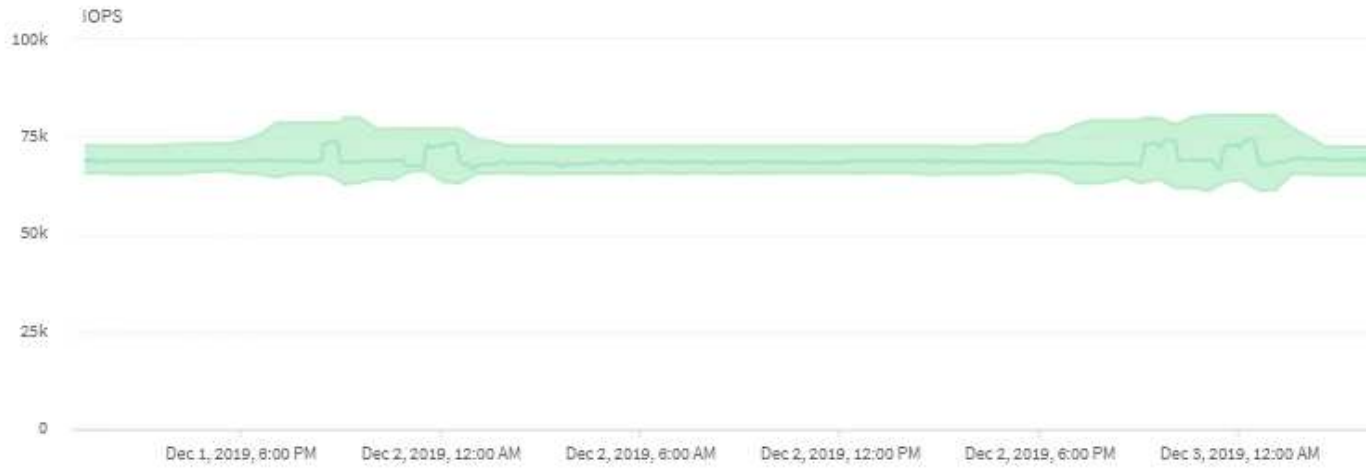
In der blauen Zeile kann es zu Lücken kommen, wenn Unified Manager keine Daten erfassen konnte. Dies kann eintreten, da das Cluster oder Volume nicht erreichbar war, Unified Manager während dieser Zeit ausgeschaltet wurde oder die Sammlung länger als den 5-Minuten-Erfassungszeitraum nahm.

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. Die tatsächliche Betriebsstatistik ist eine blaue Linie, und die IOPS-Prognose für die Betriebsstatistiken ist grün.

In einigen Fällen, in denen ein Cluster überlastet ist, zeigt Unified Manager möglicherweise die Meldung `Data collection is taking too long on Cluster *cluster_name*`an. 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.

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.

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.

Sie können den Durchsatz eines beliebigen Clusters in einer MetroCluster Konfiguration anzeigen, indem Sie die Workloads der entsprechenden LUNs und Volumes auf den folgenden Bildschirmen analysieren. Sie können die Ergebnisse nach dem Cluster filtern. Im linken Navigationsbereich:

- **Storage > Cluster > Performance: Alle Cluster** Ansicht. Siehe
- **Speicher > Volumes > Performance: Alle Volumes** Ansicht.
- **Speicher > LUNs > Performance: Alle LUNs** Ansicht.
- **Workload-Analyse > Alle Workloads**

Verwandte Informationen

"Performance-Ereignisanalyse und -Benachrichtigung"

"Performance-Ereignisanalyse für eine MetroCluster-Konfiguration"

"Rollen von Workloads, die an einem Performance-Ereignis beteiligt sind"

"Identifizierung der Opfer-Workloads, die an einem Performance-Ereignis beteiligt sind"

"Identifizierung problematischer Workloads, die an einem Performance-Ereignis beteiligt sind"

"Ermittlung von Shark Workloads, die an einem Performance-Ereignis beteiligt sind"

Allgemeines zu Performance-Ereignissen und Meldungen

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.

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 zeigt, dass die Workloads eines ONTAP Systems aufgrund anderer Workloads mit hoher Nutzung von gemeinsam genutzten Cluster-Komponenten 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.

Weitere Informationen finden Sie unter den folgenden Links:

- "Was passiert, wenn ein Ereignis empfangen wird"
- "Welche Informationen sind in einer Alarm-E-Mail enthalten"
- "Hinzufügen von Meldungen"
- "Hinzufügen von Meldungen für Performance-Ereignisse"

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 Explorers wird ein Änderungssymbol () angezeigt , um das Datum und die Uhrzeit anzuzeigen, zu der die Änderung erkannt wurde.

Sie können die Performance-Diagramme auf den Seiten des Performance Explorers und auf der Seite Workload Analysis 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 Normalzustand zurück und alle Ereignisse, die durch diese Spitzen verursacht werden, 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.

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 aus systemdefinierten Performance-Schwellenwertrichtlinien unnötige Ereignisse erhalten, können Sie die Ereignisse für einzelne Richtlinien auf der Seite Event Setup deaktivieren.

Cluster-Schwellenwertrichtlinien

Die systemdefinierten Schwellwerte für die Cluster-Performance werden standardmäßig jedem von Unified Manager überwachten Cluster zugewiesen:

- **Unwucht Clusterlast**

  Identifiziert Situationen, in denen ein Node mit einer viel höheren Last betrieben wird als andere Nodes im Cluster und somit die Workload-Latenzen potenziell beeinträchtigen.

  Dazu wird der verwendete Wert der Performance-Kapazität für alle Nodes in einem Cluster verglichen, um festzustellen, ob ein Node den Schwellenwert von 30 % für mehr als 24 Stunden überschritten hat. Dies ist ein Warnereignis.

- **Unwucht Clusterkapazität**

  Ermittelt Situationen, in denen ein Aggregat eine viel höhere genutzte Kapazität als andere Aggregate im Cluster hat und so potenziell den für Vorgänge erforderlichen Speicherplatz beeinträchtigt.

  Dazu vergleichen Sie den verwendeten Kapazitätswert für alle Aggregate im Cluster, um zu ermitteln, ob es zwischen allen Aggregaten einen Unterschied von 70 % gibt. Dies ist ein Warnereignis.

Richtlinien für Node-Schwellwerte

Die systemdefinierten Richtlinien für Node-Performance-Schwellenwerte werden standardmäßig jedem Node in den von Unified Manager überwachten Clustern zugewiesen:

- **Überschreitung Der Leistungskapazität Des Schwellenwerts**

  Identifiziert Situationen, in denen ein einzelner Node über dem Grenzen seiner betrieblichen Effizienz arbeitet und so Workload-Latenzen potenziell beeinträchtigen kann.

  Dies ergibt sich aus Nodes, die mehr als 12 Stunden lang mehr als 100 % ihrer Performance-Kapazität nutzen. Dies ist ein Warnereignis.

- **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 erfolgt durch einen Blick auf den verwendeten Wert für die Performance-Kapazität der beiden Nodes im HA-Paar. Wenn die kombinierte Performance-Kapazität der beiden Nodes über 200 % für mehr als 12 Stunden beträgt, wirkt sich ein Controller-Failover auf die Workload-Latenzen aus. Dies ist ein Informationsereignis.

- **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 systemdefinierte Aggregat-Performance-Schwellenwertrichtlinie wird standardmäßig jedem Aggregat in den von Unified Manager überwachten Clustern zugewiesen:

- **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.

Workload-Latenzschwellenrichtlinien

Die vom System definierten Schwellwerte für die Workload-Latenz werden jedem Workload mit einer konfigurierten Performance-Service-Level-Richtlinie zugewiesen, die über einen definierten Wert für „`erwartete Latenz`“ verfügt:

- **Workload Volume/LUN Latenzschwellenwert verletzt gemäß Performance Service Level**

  Identifiziert Volumes (Dateifreigaben) und LUNs, die ihr Limit für „`erwartete Latenz`“ überschritten haben und die die Workload-Performance beeinträchtigen. Dies ist ein Warnereignis.

  Dies entspricht Workloads, die für 30 % der Zeit während der vorherigen Stunde den erwarteten Latenzwert überschritten haben.

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 Durchsatzbegrenzungen von MB/s überschritten haben und die 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 teilen, wird dies durch Hinzufügen der IOPS oder MB/s aller Workloads in der Richtlinie möglich und es wird überprüft, ob die Gesamtsumme im Vergleich zum Schwellenwert enthalten ist.

- **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 gilt nur dann auf Volumes, wenn das Cluster mit ONTAP 9.3 und neuer Software installiert wird.

  Wurde in der anpassungsfähigen QoS-Richtlinie das Element „`Blockgröße`“ definiert, wird dieser Schwellenwert basierend auf der Größe jedes Volumes in einen QoS-Maximalwert für MB/s umgewandelt. Dann sucht es nach Volumes, die die QoS-max. MB/s während jedes Performance-Erfassungszeitraums für die vorherige Stunde überschritten haben.

  Diese Richtlinie gilt nur dann auf Volumes, wenn das Cluster mit ONTAP 9.5 und neuer Software installiert wird.

Performance-Ereignisanalyse und -Benachrichtigung

Bei Performance-Ereignissen werden Sie über Probleme mit der I/O-Performance bei einem Workload informiert, der durch Konflikte bei einer Cluster-Komponente verursacht wurde. 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 dynamischen Performance-Schwellenwert überschreitet, löst Unified Manager ein Performance-Ereignis aus, 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 dynamischen Performance-Schwellenwert überschritten hat, der Obergrenze der Latenzprognose ist:
  - Bei Volumes auf Festplatten- oder Flash Pool-Hybrid-Aggregaten (lokales Tier) werden Ereignisse nur ausgelöst, wenn die Latenz mehr als 5 Millisekunden (ms) beträgt und die IOPS mehr als 10 Operationen pro Sekunde sind (OPs/Sek.).
  - Bei Volumes auf reinen SSD-Aggregaten oder FabricPool-Aggregaten (Cloud-Tier) werden Ereignisse nur ausgelöst, wenn die Latenz mehr als 1 ms beträgt und die IOPS mehr als 100 OPs/s.
- 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.

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 Ereignisse werden auf der Dashboard-Seite und auf vielen anderen Seiten der Benutzeroberfläche angezeigt und Warnmeldungen für diese Ereignisse werden an die angegebenen E-Mail-Adressen gesendet. Sie können detaillierte Analyseinformationen zu einem Ereignis anzeigen und Vorschläge zu seiner Behebung auf der Seite Ereignisdetails und auf der Seite Workload Analysis erhalten.

Interaktion mit Ereignissen

Auf der Seite Ereignisdetails und auf der Seite Workload Analysis können Sie auf folgende Weise mit Ereignissen interagieren:

- Wenn Sie die Maus über ein Ereignis bewegen, wird eine Meldung angezeigt, die das Datum und die Uhrzeit anzeigt, zu der das Ereignis erkannt wurde.

  Wenn mehrere Ereignisse für den gleichen Zeitraum vorhanden sind, wird in der Meldung die Anzahl der Ereignisse angezeigt.

- Durch Klicken auf ein einzelnes Ereignis wird ein Dialogfeld angezeigt, in dem ausführlichere Informationen zu dem Ereignis angezeigt werden, einschließlich der involvierten Cluster-Komponenten.

  Die Komponente in Konflikt ist eingekreist und rot hervorgehoben. Klicken Sie auf **vollständige Analyse anzeigen**, um die vollständige Analyse auf der Seite Veranstaltungsdetails anzuzeigen. Wenn mehrere Ereignisse für den gleichen Zeitraum vorhanden sind, werden im Dialogfeld Details zu den drei letzten Ereignissen angezeigt. Sie können auf eine Veranstaltung klicken, um die Ereignisanalyse auf der Seite Ereignisdetails anzuzeigen.

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 (Latenzprognose) von Werten. Die Differenz zwischen den zuletzt analysierten Werten und dem erwarteten Wertebereich identifiziert die Workloads, deren Performance am stärksten von dem Ereignis beeinflusst wurde.

Nehmen wir beispielsweise an, ein Cluster enthält zwei Workloads: Workload A und Workload B. die für Workload A prognostizierte Latenz beträgt 5-10 Millisekunden pro Vorgang (ms/op) und die tatsächliche Latenz beträgt in der Regel etwa 7 ms/op Die Latenzprognose für Workload B liegt bei 10-20 ms/op, wobei die tatsächliche Latenz in der Regel rund 15 ms/op. Liegt Beide Workloads liegen deutlich innerhalb der Latenzprognose. Aufgrund von Konflikten im Cluster erhöht sich die Latenz beider Workloads auf 40 ms/op, sodass der dynamische Performance-Schwellenwert überschritten wird. Dies ist die obere Grenze der

Latenzprognose 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 zeigen die roten Punkte (🔴) einen Performance-Schwellenwert an, der durch eine betroffene Workload und die nachfolgenden Auswirkungen auf die Latenz überschritten wird. 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 der Workloads, die die Komponente nutzen, verlangsamen sich und ihre Reaktionszeit (Latenz) für Client-Anforderungen steigt. Dadurch wird ein Ereignis in Unified Manager ausgelöst.

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

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

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

- **Netzwerk**

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

- * Netzwerkverarbeitung*

  Repräsentiert die Softwarekomponente in dem Cluster, die mit I/O-Verarbeitung zwischen Protokollebene und Cluster beteiligt ist Der Knoten, der die Netzwerkverarbeitung verarbeitet, hat sich seit dem Erkennen des Ereignisses möglicherweise geändert. Wenn die Netzwerkverarbeitungskomponente einen Konflikt

verursacht, bedeutet dies, dass eine hohe Auslastung des Node zur Netzwerkverarbeitung die Latenz eines oder mehrerer Workloads beeinträchtigt.

Wenn Sie in einer aktiv/aktiv-Konfiguration ein All-SAN-Array-Cluster verwenden, wird der Wert für die Netzwerklatenz für beide Nodes angezeigt, sodass Sie überprüfen können, ob die Nodes die Last gleichmäßig teilen.

- **QoS-Limit max.**

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

- * QoS Limit Min.*

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

- * Cluster Interconnect*

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

- **Datenverarbeitung**

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

- **Volume-Aktivierung**

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

- **MetroCluster Ressourcen**

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

- **Aggregate oder SSD Aggregate Ops**

  Repräsentiert das Storage-Aggregat, auf dem die Workloads ausgeführt werden Wenn die Aggregat-Komponente Konflikte verursacht, bedeutet dies, dass eine hohe Auslastung des Aggregats sich auf die

Latenz eines oder mehrerer Workloads auswirkt. Ein Aggregat besteht aus allen HDDs oder einer Kombination aus HDDs und SSDs (einem Flash Pool Aggregat) oder einer Kombination aus HDDs und einem Cloud Tier (einem FabricPool Aggregat). Ein „`SSD Aggregat`“ besteht aus allen SSDs (ein All-Flash-Aggregat) oder einer Kombination aus SSDs und einer Cloud Tier (ein FabricPool Aggregat).

- **Cloud-Latenz**

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

- **Sync SnapMirror**

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

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 seit der Latenzprognose (erwarteter Bereich) deutlich zugenommen hat.
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.

Rolle	Beschreibung
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. 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.

Management von 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 aus systemdefinierten Performance-Schwellenwertrichtlinien unnötige Ereignisse erhalten, können Sie einzelne Richtlinien auf der Seite Event Setup 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
Aggregat	Auslastung	65 % erreicht	85 % erreicht	

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 % erreicht	Es wird kein Ereignis gemeldet.
15 Millisekunden	75 % erreicht	Ein Warnereignis wird gemeldet.
25 Millisekunden	75 % erreicht	Ein Warnereignis wird gemeldet.
25 Millisekunden	90 % erreicht	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 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 „Alarmkonfiguration“ 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/s	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/s
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/s	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.

Storage Objekt	Performance-Zähler	Beschreibung
Verwendete Performance-Kapazität	Durchschnittlicher Prozentsatz der Performance-Kapazität, die vom Aggregat verbraucht wird.	Storage-VM
IOPS	Durchschnittliche Anzahl der ein-/Ausgabevorgänge, die das SVM pro Sekunde verarbeitet.	MB/s
Durchschnittliche Anzahl der Megabyte an Daten, die pro Sekunde an diese SVM und von dieser SVM übertragen werden.	Latenz	Durchschnittliche Anzahl von Millisekunden, die die SVM benötigt, um auf Applikationsanforderungen zu reagieren.
Datenmenge	IOPS	Durchschnittliche Anzahl der ein-/Ausgabevorgänge die Volume-Prozesse pro Sekunde.
MB/s	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/s	Durchschnittliche Anzahl der Megabyte an Daten, die pro Sekunde an und von dieser LUN übertragen werden.	Latenz
Durchschnittliche Anzahl von Millisekunden, die die LUN benötigt, um auf Applikationsanforderungen zu reagieren.	Namespace	IOPS

Storage Objekt	Performance-Zähler	Beschreibung
Durchschnittliche Anzahl der ein-/Ausgabevorgänge, die der Namespace pro Sekunde verarbeitet.	MB/s	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
Bandbreitenauslastung	Durchschnittlicher Prozentsatz der verfügbaren Bandbreite des Ports, die verwendet wird.	MB/s
Durchschnittliche Anzahl der Megabyte an Daten, die in diesen Port pro Sekunde übertragen werden.	Netzwerkschnittstelle (LIF)	MB/s

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
Volume-MB/s	Aggregatauslastung
Verwendete Aggregat-Performance-Kapazität	Node-Auslastung
Verwendete Node-Performance-Kapazität	Verwendete Node-Performance-Kapazität – Übernahme
LUN-Latenz	LUN IOPS
LUN-MB/s	Aggregatauslastung
Verwendete Aggregat-Performance-Kapazität	Node-Auslastung

Primäres Speicherobjekt und Zähler	Sekundäres Storage Objekt und Zähler
Verwendete Node-Performance-Kapazität	Verwendete Node-Performance-Kapazität – Übernahme

Wenn eine Volume-Combination Policy auf ein FlexGroup Volume anstatt auf ein FlexVol Volume angewendet wird, können nur die Attribute „`Volume IOPS`“ und „`Volume MB/s`“ 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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Sie erstellen Richtlinien für Leistungsschwellenwerte, indem Sie die Schwellenwerte auf der Seite Richtlinie für Leistungsschwellenwert 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 **Ereignisschwellenwerte** > **Leistung** aus.

   Die Seite 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 „Richtlinie für Leistungsschwellenwert erstellen“ oder „Richtlinie für Leistungsschwellenwert 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 zur Seite „Performance Schwellenwerte“ zurück. 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.

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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Die Richtlinie für Performance-Schwellenwerte oder -Richtlinien, die Sie auf das Objekt anwenden möchten, müssen vorhanden sein.

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

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	Das Drop-down-Feld, und wählen Sie **Alle Objekte auf dieser Seite auswählen**.
Alle Objekte desselben Typs	Das Drop-down-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 „Richtlinie für Leistungsschwellenwert zuweisen“ wird angezeigt. Hier wird eine Liste mit Schwellenwertrichtlinien angezeigt, die für den spezifischen Typ des Speicherobjekts 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.

Wenn Benachrichtigungen über E-Mail oder als SNMP-Trap gesendet werden sollen, um Sie darüber zu informieren, dass ein bestimmtes Leistungsereignis generiert wurde, müssen Sie die Einstellungen für die Warnmeldung auf der Seite „Alarmkonfiguration“ konfigurieren.

Anzeigen von Richtlinien für Performance-Schwellenwerte

Sie können alle derzeit definierten Performance-Schwellenwertrichtlinien auf der Seite Performance-Schwellenwerte anzeigen.

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.

Schritt

1. Wählen Sie im linken Navigationsbereich **Ereignisschwellenwerte** > **Leistung** aus.

   Die Seite 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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

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 **Ereignisschwellenwerte** > **Leistung** aus.

   Die Seite Leistungsschwellenwerte wird angezeigt.

2. Wählen Sie die Schwellenwertrichtlinie aus, die Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

   Die Seite Richtlinie für Leistungsschwellenwert bearbeiten wird angezeigt.

3. Nehmen Sie Ihre Änderungen an der Schwellenwertrichtlinie vor und klicken Sie auf **Speichern**.

   Sie gelangen zur Seite „Performance Schwellenwerte“ zurück.

Nachdem sie gespeichert wurden, werden Änderungen sofort für alle Speicherobjekte aktualisiert, die die Richtlinie verwenden.

Abhängig von der Art der Änderungen, die Sie an der Richtlinie vorgenommen haben, sollten Sie möglicherweise die für die Objekte, die die Richtlinie verwenden, auf der Seite „Alarmkonfiguration“ konfigurierten Warnungseinstellungen überprüfen.

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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

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 ☐▾ in die Spaltenüberschrift.

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 „Workload Analysis“ wird in der Zeitleiste „Ereignisse“ ein Symbol für Änderungsereignisse angezeigt, um den Zeitpunkt anzugeben, zu dem 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 mit dem Befehl ein Aggregat von einem Node auf einen anderen Node verschieben `aggregate relocation start`, werden sowohl Richtlinien für einen einfachen als auch für eine Kombination für alle Objekte beibehalten. 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.

Weitere Informationen finden Sie unter "Volume-Verhalten während des Umschalens und Zurück".

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

Sie können auf der Seite „Inventar des Event Managements“ eine Liste aller Performance-Ereignisse 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.

Was Sie brauchen

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

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

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

3. 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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue oder veraltete Performanceereignisse vorliegen.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis 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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue oder veraltete Performanceereignisse vorliegen.

Schritte

1. Rufen Sie die Seite **Ereignisdetails** auf, um Informationen über das Ereignis 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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Ereignisse für die Leistung vorliegen.

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 **Ereignisdetails** auf, um Informationen über das Ereignis 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 die Blockgröße in der QoS-Richtlinie 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:

```
MB/s = (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 diese Workload 96. Wenn dieselbe Workload durchschnittlich 3,000 IOPS ist 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 effektiv auf 80 MB/s ((2500 IOPS * 32 KB) / 1000) für ein Volumen mit 1 TB genutzter Kapazität festgelegt. 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/s
1TB	2,250 IOPS	72 MB/s
2TB	4,500 IOPS	144 MB/s
5TB	11,250 IOPS	360 MB/s

Wenn das Volume 2 TB des verfügbaren Speicherplatzes verwendet und der IOPS 4,000 ist und die QoS-Blockgröße auf 32 KB auf dem Client eingestellt ist, dann beträgt der Durchsatz von MB/s 128 MB/s ((4,000 IOPS * 32 KB) / 1000). Kein Ereignis wird in diesem Szenario generiert, da sowohl 4,000 IOPS als auch 128 MB/s unter dem Schwellenwert für ein Volume liegen, das 2 TB Speicherplatz verbraucht.

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, aber der MB/s-Wert von 256 MB/s liegt über dem Schwellenwert von 144 MB/s und ein Ereignis wird generiert.

Wenn aus diesem Grund ein Ereignis aufgrund einer MB/s-Sicherheitsverletzung für eine adaptive QoS-Richtlinie ausgelöst wird, die die Blockgröße enthält, wird auf der Seite Ereignisdetails ein MB/s-Diagramm im Abschnitt Systemdiagnose 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 eine Sicherheitsverletzung sowohl für IOPS als auch für MB/s auftritt, erhalten Sie zwei Ereignisse.

Weitere Informationen zum Anpassen der QoS-Einstellungen finden Sie unter "Performance Management – Überblick".

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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue oder veraltete Performanceereignisse vorliegen.

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 **Ereignisdetails** auf, um Informationen über das Ereignis 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.

Reaktion auf Unausgeglichenheit der Performance im Cluster

Unified Manager generiert Warnereignisse bei einem Cluster-Ungleichgewicht, wenn ein Node in einem Cluster mit einer deutlich höheren Auslastung arbeitet als andere Nodes, und dies beeinträchtigt möglicherweise die Workload-Latenzen. Diese systemdefinierten Ereignisse bieten die Möglichkeit, potenzielle Performance-Probleme zu beheben, bevor viele Workloads von der Latenz beeinträchtigt werden.

Was Sie brauchen

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

Unified Manager generiert Warnereignisse für Richtlinienverstöße im Cluster-Ungleichgewicht, indem der für alle Nodes im Cluster verwendete Performance-Wert verglichen wird, um zu sehen, ob zwischen allen Nodes ein Lastunterschied von 30 % erzielt wird.

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. 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 zeigt die Meldung „`der verwendete Zähler für die Performance-Kapazität einen Lastunterschied von 62 % zwischen den Nodes auf Cluster Dallas-1-8 an und hat ein WARNEREIGNIS basierend auf dem Systemschwellenwert von 30 %` ausgelöst. Dies gibt an, dass die Performance-Kapazität auf einem der Nodes überlastet ist und die Node-Performance beeinträchtigt wird.

3. Prüfen Sie den Text in den **vorgeschlagenen Aktionen**, um ein leistungsstarkes Volume von dem Node mit der verwendeten hohen Performance-Kapazität auf einen Node mit dem niedrigsten Wert für die Performance zu verschieben.
4. Die Nodes mit der höchsten und niedrigsten Performance-Kapazität identifizieren, die verwendet wird:
   a. Klicken Sie im Abschnitt **Ereignisinformationen** auf den Namen des Quellclusters.
   b. Klicken Sie auf der Seite **Cluster / Leistungsübersicht** im Bereich **verwaltete Objekte** auf **Knoten**.
   c. Sortieren Sie auf der Seite **Nodes** Inventar die Knoten anhand der Spalte **verwendete Performance-Kapazität**.
   d. Die Nodes mit dem verwendeten Wert für die höchste und niedrigste Performance-Kapazität identifizieren und diese Namen notieren.
5. Ermitteln Sie das Volume mithilfe der meisten IOPS auf dem Node mit dem höchsten Wert für die verwendete Performance-Kapazität:
   a. Klicken Sie auf den Node mit dem Wert für die höchste genutzte Performance-Kapazität.
   b. Wählen Sie auf der Seite **Node / Performance Explorer** im Menü **Ansicht und Vergleich Aggregate auf diesem Knoten** aus.
   c. Klicken Sie auf das Aggregat mit dem gewohnt höchsten Performance-Wert.
   d. Wählen Sie auf der Seite **Aggregat / Performance Explorer** aus dem Menü **Ansicht und Vergleich Volumes auf diesem Aggregat** aus.
   e. Sortieren Sie die Volumes nach der Spalte **IOPS**, und notieren Sie den Namen des Volumes mit den meisten IOPS, und den Namen des Aggregats, in dem sich das Volume befindet.
6. Ermittlung des Aggregats mit der niedrigsten Auslastung auf dem Node, der die geringste Performance-Kapazität verwendet hat:
   a. Klicken Sie auf **Storage** > **Aggregate**, um die Seite **Aggregates** Inventar anzuzeigen.
   b. Wählen Sie die Ansicht **Performance: Alle Aggregate** aus.
   c. Klicken Sie auf die Schaltfläche **Filter** und fügen Sie einen Filter hinzu, wobei „`Node`“ dem Namen des Knotens entspricht, dessen Kapazität die niedrigste Leistung hat, die Sie in Schritt 4 geschrieben haben.
   d. Notieren Sie sich den Namen des Aggregats, das den Wert der am wenigsten genutzten Performance-

Kapazität hat.

7. Verschieben Sie das Volume vom überlasteten Node zum Aggregat, das Sie bei dem neuen Node als niedrige Auslastung identifiziert haben.

   Sie können den Vorgang der Verschiebung mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools ausführen.

Prüfen Sie nach einigen Tagen, ob im Cluster dasselbe Ungleichgewicht auftritt.

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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete dynamische Leistungsereignisse vorliegen.

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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete dynamische Leistungsereignisse vorliegen.

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. Zeigen Sie die Seite Ereignisdetails an, um Informationen zum 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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Es gibt ein neues, anerkanntes oder überholes dynamisches Ereignis für die Leistung.

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.

Performanceereignisse von beiden Clustern in der MetroCluster-Konfiguration werden zudem auf der Seite „Unified Manager Dashboard“ angezeigt. Sie können auch die Systemzustandsseiten 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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application 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.

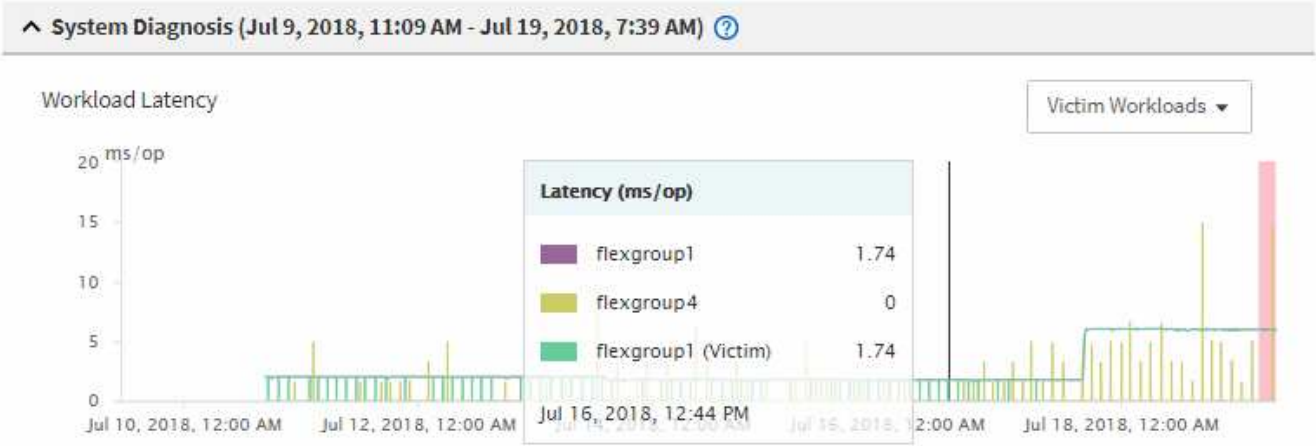
Schritte

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.

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 problematische Workloads weisen eine hohe Abweichung beim Schreibdurchsatz (MB/s) auf.

   Dieses Diagramm zeigt auf hoher Ebene das Muster für den Schreibdurchsatz (MB/s) für die Workloads an. Sie können das MB/s-Muster für Schreibvorgänge überprüfen, um einen anormalen Durchsatz zu identifizieren, der darauf hindeutet, dass ein Workload die MetroCluster-Ressourcen überausgelastet ist.

   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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application 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

Sie können mit Unified Manager ein Performance-Ereignis untersuchen, das durch eine QoS-Richtliniengruppe (Quality of Service) 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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application 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-Auslastung **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. Klicken Sie im Bereich **Suggested Actions** auf die Schaltfläche **Analyze Workload** für den oberen Workload.
7. Legen Sie auf der Seite Workload-Analyse das Latenzdiagramm fest, um alle Cluster-Komponenten und das Durchsatzdiagramm zur Anzeige der Aufschlüsselung anzuzeigen.

   Die Aufschlüsselung werden unter dem Latenzdiagramm und dem IOPS-Diagramm angezeigt.

8. Vergleichen Sie die QoS-Limits im Diagramm * Latenz*, um zu sehen, welche Drosselung sich zum Zeitpunkt des Ereignisses auf die Latenz ausgewirkt hat.

   Die QoS-Richtliniengruppe weist einen maximalen Durchsatz von 1,000 Operationen pro Sekunde (in op/s) auf, die die Workloads in ihrer Gruppe nicht gemeinsam übersteigen 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

9. Vergleichen Sie die **Lese/Schreib Latenz** Werte mit den **Lese-/Schreibvorgängen/anderen** Werten.

   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.

10. Verwenden Sie ONTAP System Manager, um die aktuelle Obergrenze für die Richtliniengruppe auf 1,300 Op/Sek. zu erhöhen
11. Kehren Sie nach einem Tag zu Unified Manager zurück und geben Sie den Workload ein, den Sie in Schritt 3 auf der Seite * Workload Analysis* aufgezeichnet haben.
12. Wählen Sie das Diagramm zum Durchsatz aus.

    Das Diagramm Lese-/Schreibvorgänge/Sonstiges wird angezeigt.

13. Zeigen Sie oben auf der Seite mit dem Cursor auf das Symbol Ereignis ändern () für die Richtliniengruppe Limit change.
14. 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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application 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. Aktualisieren Sie die **Veranstaltungsdetails**.

   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. Klicken Sie im Bereich **Suggested Actions** auf die Schaltfläche **Analyze Workload** für den oberen Workload.
9. Legen Sie auf der Seite **Workload Analysis** den Zeitbereich fest, um die letzten 24 Stunden (1 Tag) der Daten für das ausgewählte Volumen anzuzeigen.

   In der Ereigniszeitleiste zeigt ein roter Punkt (🛑) an, wann das Festplattenfehler-Ereignis aufgetreten ist.

10. Verbergen Sie im Diagramm für die Knotenauslastung und Aggregat die Zeile für die Knoten-Statistiken, so dass nur die Aggregat-Zeile bleibt.
11. Vergleichen Sie die Daten in diesem Diagramm mit den Daten zum Zeitpunkt des Ereignisses im Diagramm **Latenz**.

    Zum Zeitpunkt des Ereignisses zeigt die aggregierte Auslastung einen hohen Anteil an Lese- und

Schreibvorgängen durch die RAID-Rekonstruktionsprozesse an, wodurch die Latenz des ausgewählten Volumes erhöht wurde. 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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application 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 Volumes.

   Die Seite Volume Performance Explorer wird angezeigt. Oben auf der Seite, in der Ereigniszeitzeile, zeigt ein Änderungssymbol ( ) die Zeit an, zu der Unified Manager den Start der HA-Übernahme erkannt hat.

4. Zeigen Sie den Mauszeiger auf das Änderungsereignis-Symbol für die HA-Übernahme und Details zur HA-Übernahme werden in Hover-Text 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. Klicken Sie auf **Zoom View**, um das Latenzdiagramm auf einer neuen Seite anzuzeigen.
6. Wählen Sie im Menü Ansicht die Option **Cluster Components** aus, um die Gesamtlatenz nach Clusterkomponente anzuzeigen.
7. Zeigen Sie mit der Maus auf das Änderungssymbol für den Start des HA-Takeover und vergleichen Sie die Latenz für die Datenverarbeitung mit der gesamten 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.

8. Nach der Behebung des fehlerhaften Knotens führt ONTAP System Manager ein HA-Giveback durch, wodurch die Workloads vom Partner-Node zum festgelegten Node verschoben werden.

9. Nach Abschluss des HA-Giveback. Ermitteln Sie nach der nächsten Konfigurationsermittlung im Unified Manager (ca. 15 Minuten) das Ereignis und den Workload, das durch den HA-Takeover auf der Seite **Event Management** Inventory ausgelöst wurde.

   Das durch die HA Übernahme ausgelöste Ereignis weist jetzt einen Status als veraltet auf, sodass das Ereignis gelöst werden kann. 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, ONTAP 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, hat 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 Workload-Analyse überprüfen, um festzustellen, wann eine kürzlich erfolgte Konfigurationsänderung aufgetreten ist, und sie mit den Vorgängen und Latenz (Reaktionszeit) vergleichen, um zu prüfen, ob eine Änderung der Aktivität für den ausgewählten Volume-Workload stattgefunden hat.

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 Workload-Analyse für jeden Volume-Workload 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 ONTAP 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	Überlegungen
• Verbesserung des Lastausgleichs: • Verringern Sie den indirekten Zugriff.	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 ONTAP System Manager und die CLI-Befehle von ONTAP, um LIFs manuell zu verschieben.

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 ONTAP 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 enthält alle SSD-Aggregate oder HDD-Aggregate (beginnend mit ONTAP 9.8) als lokale Performance-Tier und einen Objektspeicher, den Sie als Cloud-Tier angeben. Beim Konfigurieren von FabricPool können Sie festlegen, welche Storage-Tiers (das lokale Tier oder das Cloud-Tier) Daten basierend darauf gespeichert werden sollen, ob häufig auf die 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 ONTAP 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 ONTAP 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 für einen 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 ONTAP 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 den folgenden Befehl auf dem Aggregat ausführen, um zu ermitteln, 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. ein Aggregat, das sich in Konflikt befindet.

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 Systemzustand der Cluster in einer MetroCluster-Konfiguration über IP oder FC 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 **Ereignisverwaltung** auswählen, um eine Liste aktueller Ereignisse anzuzeigen. Anschließend können Sie die Filter verwenden, um nur MetroCluster-Konfigurationsereignisse anzuzeigen.

Weitere Informationen finden Sie unter "Überprüfen des Systemzustands von Clustern in einer MetroCluster-Konfiguration"

Überprüfung der MetroCluster-Konfiguration

Sie können Performance-Probleme bei gespiegelten Workloads in einer MetroCluster over FC- und IP-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.

Anweisungen zum Einrichten der Cluster in der MetroCluster-Konfiguration, einschließlich der Fibre Channel-Switches (FC), Kabel und Inter-Switch-Links (ISLs), finden Sie unter "MetroCluster-Dokumentation". Darüber hinaus unterstützt Sie die Konfiguration der MetroCluster Software, sodass die lokalen und Remote Cluster mit gespiegelten Volume-Daten kommunizieren können. Informationen zu Ihrem MetroCluster-over-IP-Setup finden Sie unter "Installieren Sie eine MetroCluster IP-Konfiguration".

Sie können Ihre MetroCluster-Konfiguration mit den Anforderungen in vergleichen "MetroCluster-Dokumentation", um zu ermitteln, ob ein Ändern oder Aktualisieren von Komponenten 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?

Verwandte Informationen

- Informationen zum Austauschen oder Aktualisieren von MetroCluster-Komponenten finden Sie im "MetroCluster-Dokumentation".
- Informationen zum Upgrade von Controllern finden Sie unter "Upgrades von Controllern in einer MetroCluster FC-Konfiguration mithilfe von Switchover und Switchback" und "Upgrades von Controllern in einer MetroCluster IP-Konfiguration mithilfe von Switchover und Switchback"

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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application 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.
- Unified Manager muss einen Monat oder mehrere Performance-Daten erfasst und analysiert haben.

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 den Vorgang der Verschiebung mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools ausführen.

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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application 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.
- Unified Manager muss Performance-Daten für einen Monat oder länger erfassen und analysieren haben.

Durch dieses Verfahren werden die folgenden Ressourcen ermittelt, damit hochperformante Workloads auf einen weniger ausgelasteten Node verschoben werden können:

- 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 **Storage** > **Aggregate** und wählen Sie im Menü Ansicht die Option **Performance** > **Alle Aggregate** aus.

      Die Performance: Die Ansicht aller 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: Alle Aggregate Ansicht 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 Ansicht Leistung: Alle 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 den Vorgang der Verschiebung mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools ausführen.

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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application 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.
- Unified Manager muss einen Monat oder mehrere Performance-Daten erfasst und analysiert haben.

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 **Storage** > **Aggregate** und wählen Sie im Menü Ansicht die Option **Performance** > **Alle Aggregate** aus.

      Die Performance: Die Ansicht aller 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: Alle Aggregate Ansicht 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.

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 Ansicht Leistung: Alle 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 den Vorgang der Verschiebung mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools ausführen.

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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application 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.
- Unified Manager muss Performance-Daten für einen Monat oder länger erfassen und analysieren haben.

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. Durch dieses Verfahren werden die folgenden Ressourcen ermittelt, damit Sie hochperformante Workloads auf einen Node mit mehr freier Performance-Kapazität auf einem anderen HA-Paar verschieben können:

- 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 auf diesem Cluster wird in der Ansicht Performance: Alle 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 in der Ansicht **Leistung: Alle Knoten** auf die Spalte **verwendete Leistungskapazität**, 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 in der Ansicht **Leistung: Alle 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 Ansicht Leistung: Alle 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 den Vorgang der Verschiebung mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools ausführen.

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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application 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.
- Unified Manager muss einen Monat oder mehrere Performance-Daten erfasst und analysiert haben.

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 **Storage** > **Cluster** und wählen Sie im Menü Ansicht die Option **Leistung** > **Alle Cluster** aus.

      Die Ansicht Performance: Alle Cluster wird angezeigt.

   b. Klicken Sie im Feld **Knotenanzahl** für den aktuellen Cluster auf die Zahl.

      Die Ansicht Leistung: Alle 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 **Storage** > **Aggregate** und wählen Sie im Menü Ansicht die Option **Performance** > **Alle Aggregate** aus.

      Die Performance: Die Ansicht aller 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: Alle Aggregate Ansicht 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 Ansicht Leistung: Alle 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 den Vorgang der Verschiebung mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools ausführen.

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 ONTAP 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 in der Ansicht Leistung: Alle 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 **Speicher** > **LUNs** und wählen Sie im Menü Ansicht die Option **Leistung** > **Alle LUNs** aus.
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 ONTAP 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 ONTAP System Manager oder den ONTAP-Befehlen können Sie einem Aggregat Festplatten hinzufügen.

"Technischer Bericht 3838: Konfigurationsleitfaden Für Storage-Subsysteme"

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.

Statistikgruppe	Enthaltene Daten	Details
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.

In Knowledge Base-Artikel 30096 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.

NetApp testet und verifiziert keine bestimmten Versionen von Graphite oder anderen Tools von Drittanbietern.

Der Graphite-Server empfängt keine Performance-Daten für Volumes von Unified Manager.

Nachdem Sie Graphite gemäß den Installationsanweisungen installiert haben, müssen Sie zur Unterstützung der statistischen Datenübertragung von Unified Manager folgende Änderungen vornehmen:

- In der `/opt/graphite/conf/carbon.conf` Datei muss die maximale Anzahl von Dateien, die pro Minute auf dem Graphite-Server erstellt werden können(**`MAX_CREATES_PER_MINUTE = 200`**, auf *200* gesetzt werden.

  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, muss der Wert für LINE_RECEIVER_INTERFACE in der `/opt/graphite/conf/carbon.conf` Datei von „`0.0.0.0`“ in „`::`“ geändert werden(**`LINE_RECEIVER_INTERFACE = ::`**.
- In der `/opt/graphite/conf/storage-schemas.conf` Datei muss der `retentions` Parameter verwendet werden, um die Frequenz auf 5 Minuten und die Aufbewahrungsfrist auf die Anzahl der Tage einzustellen, die für Ihre Umgebung relevant sind.

  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 für Unified Manager mithilfe des Parameters ein Abschnitt definiert `pattern`, und durch die Werte wird die initiale Frequenz auf 5 Minuten und die Aufbewahrungsfrist auf 100 Tage festgelegt: **`[OPM]`**

  ```
  pattern = ^netapp-performance\..

  retentions = 5m:100d
  ```

  Wenn das Standard-Hersteller-Tag von „`NetApp-Performance`“ zu einem anderen geändert wird, muss diese Änderung auch im Parameter widergespiegelt werden `pattern`.

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.

Was Sie brauchen

- 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.

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 Manager-Wartungskonsole 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. Wenn Sie dazu aufgefordert werden, geben Sie 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. Wenn Sie dazu aufgefordert werden, geben Sie ein, um zu `y` überprüfen, ob die eingegebenen Informationen korrekt 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. Wenn Sie dazu aufgefordert werden, geben Sie 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` - PERFORMANCE_INDICATOR (Standard) `1` - RESOURCE_UTILIZATION `2` - DRILL_DOWN

Für.	Eingeben…
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. Wenn Sie beispielsweise die Statistiken eingeben **`stats.performance.netapp`**, werden Sie unter **stats** > **Performance** > **NetApp** angezeigt.
Übertragungsintervall	**`5`** (Standard), **`10`**, oder **`15`** Minuten
Aktivieren/deaktivieren	**`0`** - Deaktivieren **`1`** - Enable (Standard)

11. Wenn Sie dazu aufgefordert werden, geben Sie ein, um zu **`y`** überprüfen, ob die eingegebenen Informationen korrekt sind.
12. Drücken Sie eine beliebige Taste, um zum Menü External Server Connection zurückzukehren.
13. Geben Sie ein **`x`**, um die Wartungskonsole zu verlassen.

Nachdem Sie die Verbindung konfiguriert haben, werden die ausgewählten Performancedaten zum angegebenen Zeitintervall an den Zielserver gesendet. Es dauert einige Minuten, bis die Metriken im externen Tool 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 Active IQ Unified Manager Monitoring des Systemzustands

Active IQ Unified Manager (ehemals OnCommand Unified Manager) hilft Ihnen, eine große Anzahl von Systemen mit ONTAP Software über eine zentrale Benutzeroberfläche zu überwachen. Die Unified Manager Serverinfrastruktur bietet Skalierbarkeit, Unterstützbarkeit sowie verbesserte Monitoring- und Benachrichtigungsfunktionen.

Zu den wichtigsten Funktionen von Unified Manager gehören Monitoring-, Warnfunktionen-, Management der Verfügbarkeit und Kapazität von Clustern, Management der Sicherungsfunktionen und Bündelung von Diagnosedaten sowie der Versand 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.

Physische und logische Kapazität

Unified Manager nutzt die Konzepte von physischem und logischem Speicherplatz für ONTAP Storage-Objekte.

- Physische Kapazität: Physischer Speicherplatz bezieht sich auf die physischen Blöcke des Storage, der im Volume verwendet wird. „Genutzte physische Kapazität“ ist in der Regel kleiner als die logische genutzte Kapazität, da Storage-Effizienzfunktionen wie Deduplizierung und Komprimierung reduziert werden.
- Logische Kapazität: Logischer Speicherplatz bezeichnet den nutzbaren Speicherplatz (die logischen Blöcke) in einem Volume. Logischer Speicherplatz bezeichnet die Art und Weise, wie theoretischer Speicherplatz verwendet werden kann, ohne dabei die Folgen der Deduplizierung oder Komprimierung berücksichtigen zu müssen. Der „logische Platz“ ist der verwendete physische Speicherplatz plus die Einsparungen durch Storage-Effizienzfunktionen (wie Deduplizierung und Komprimierung), die konfiguriert wurden. Diese Messung erscheint oft größer als die physisch genutzte Kapazität, da diese nicht auf die Datenkomprimierung und andere Reduzierungen des physischen Speicherplatzes zurückführt. Somit kann die logische Gesamtkapazität über dem bereitgestellten Speicherplatz liegen.

Kapazitätsmesseinheiten

Unified Manager berechnet die Storage-Kapazität auf der Grundlage von binären Einheiten von 1024 (2^{10}) Byte. In ONTAP 9.10.0 und früher wurden diese Einheiten als KB, MB, GB, TB und PB angezeigt. Ab ONTAP 9.10.1 werden sie im Unified Manager als KiB, MiB, gib, tib und PiB angezeigt.

Die für den Durchsatz verwendeten Einheiten betragen für alle ONTAP-Versionen weiterhin Kilobyte pro Sekunde (Kbit/s), Megabyte pro Sekunde (MB/s), Gigabyte pro Sekunde (GB/s) oder Terabyte pro Sekunde (Tbit/s) usw.

In Unified Manager für ONTAP 9.10.0 und früher angezeigte Kapazitätseinheit	Im Unified Manager für ONTAP 9.10.1 wird die Kapazitätseinheit angezeigt	Berechnung	Wert in Byte
KB	KiB	1024	1024 Byte
MB	MIB	1024 * 1024	1.048.576 Byte
GB	Gib	1024 * 1024 * 1024	1.073.741.824 Byte
TB	TIB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 Byte

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-Freigaben SMB-Freigaben, Benutzer- und Gruppenkontingente, QoS-Richtliniengruppen 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-over-FC- und IP-Konfigurationen: Anzeigen und Überwachen der Konfiguration, Probleme und des Konnektivitätsstatus der Cluster-Komponenten MetroCluster-Switches und Bridges für MetroCluster-over-FC-Konfigurationen
- 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 von SVMs mit FlexVol oder FlexGroup 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, Performance 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. Hier sind die automatisierten Workflows verfügbar:

  "Storage Automation Store"

Unified Manager-Schnittstellen, die zum Management des Zustands des Storage-Systems verwendet werden

Diese Abschnitte enthalten Informationen zu den beiden Benutzeroberflächen, die Active IQ 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 diesen Abschnitten 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-UI von Unified Manager angezeigt werden.

Wartungskonsole

Die Unified Manager-Wartungskonsole ermöglicht Administratoren das Überwachen, Diagnostizieren und behandeln von Betriebssystemproblemen, Problemen mit dem Versionsaktualisierung, Problemen mit dem Benutzerzugriff und Netzwerkproblemen im Zusammenhang mit dem Unified Manager-Server selbst. Wenn die Web-UI von Unified Manager nicht verfügbar ist, stellt die Wartungskonsole die einzige Zugriffsmöglichkeit auf Unified Manager dar.

Sie können diese Informationen für den Zugriff auf die Wartungskonsole verwenden, um Probleme im Zusammenhang mit der Funktionsweise des Unified Manager-Servers zu beheben.

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.

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 ONTAP System Manager oder der ONTAP CLI ausfällt.

> Die Funktion zur Überwachung von Node-Root-Volumes ist nicht verfügbar, wenn auf Clustern ONTAP 9.14.1 oder höher ausgeführt wird.

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 ONTAP System Manager oder der ONTAP CLI angehalten wird.

Die Funktion zum Monitoring von Node-Root-Aggregaten ist nicht verfügbar, wenn auf Clustern ONTAP 9.14.1 oder höher ausgeführt wird.

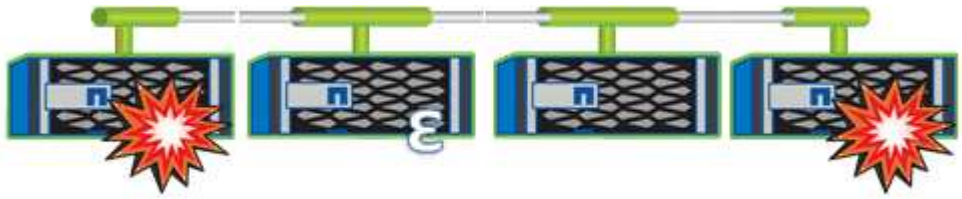
Verständnis von Quorum und Epsilon

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 Node im Cluster ist an einem Abstimmungsprotokoll beteiligt, das einen Node-Master wählt. Jeder verbleibende Node ist ein sekundärer. 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 in einem Cluster mit einer geraden Anzahl von Nodes eine Krawatte möglich ist, verfügt ein Node über 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 über den Befehl „Cluster Quorum-Service options modify“ auf der erweiterten Berechtigungsebene deaktivieren.

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 nutzen Cluster HA, in dem keine der Nodes Epsilon enthält; stattdessen werden beide Nodes ununterbrochen 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 Ansicht Health: All Clusters verwenden, um Ihr Inventar der Cluster anzuzeigen. Die Kapazität: Alle Cluster-Ansichten ermöglichen die Anzeige zusammengefasste Informationen zur Storage-Kapazität und Auslastung in allen Clustern.

Was Sie brauchen

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

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 mithilfe der Seite „Cluster/Health Details“.

Die Details in der Ansicht Health: All Clusters, Capacity: All Clusters und die Seite Cluster / Health Details helfen Ihnen bei der Planung Ihres Speichers. Vor dem Bereitstellen eines neuen Aggregats können Sie beispielsweise aus der Ansicht Systemzustand: Alle Cluster einen bestimmten Cluster auswählen und Kapazitätsdetails abrufen, um zu ermitteln, ob der Cluster über den erforderlichen Speicherplatz verfügt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Cluster**.
2. Wählen Sie im Menü Ansicht die Ansicht **Systemzustand: Alle Cluster** aus, um die Gesundheitsinformationen anzuzeigen, oder die Ansicht **Kapazität: Alle Cluster**, um Details zur Speicherkapazität und Auslastung in allen Clustern anzuzeigen.
3. Klicken Sie auf den Namen eines Clusters, um die vollständigen Details des Clusters auf der Seite **Cluster / Health** Details anzuzeigen.

Verwandte Informationen

- "„Cluster/Systemzustand“-Details"
- "Performance: Ansicht aller Cluster"
- "Monitoring der MetroCluster Konfigurationen"
- "Anzeigen des Sicherheitsstatus für Cluster und Storage VMs"
- "Welche Sicherheitskriterien werden bewertet"

Überprüfen des Systemzustands von Clustern in einer MetroCluster-Konfiguration

Mit Active IQ Unified Manager (Unified Manager) können Sie den Betriebszustand der Cluster und ihrer Komponenten in MetroCluster over FC- und MetroCluster over IP-Konfigurationen 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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application 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 über FC und IP müssen von derselben Instanz von Unified Manager überwacht werden.

Ermitteln des Clusterzustands in der MetroCluster-over-FC-Konfiguration

Befolgen Sie diese Schritte, um den Cluster-Zustand in einer MetroCluster über FC-Konfiguration zu bestimmen.

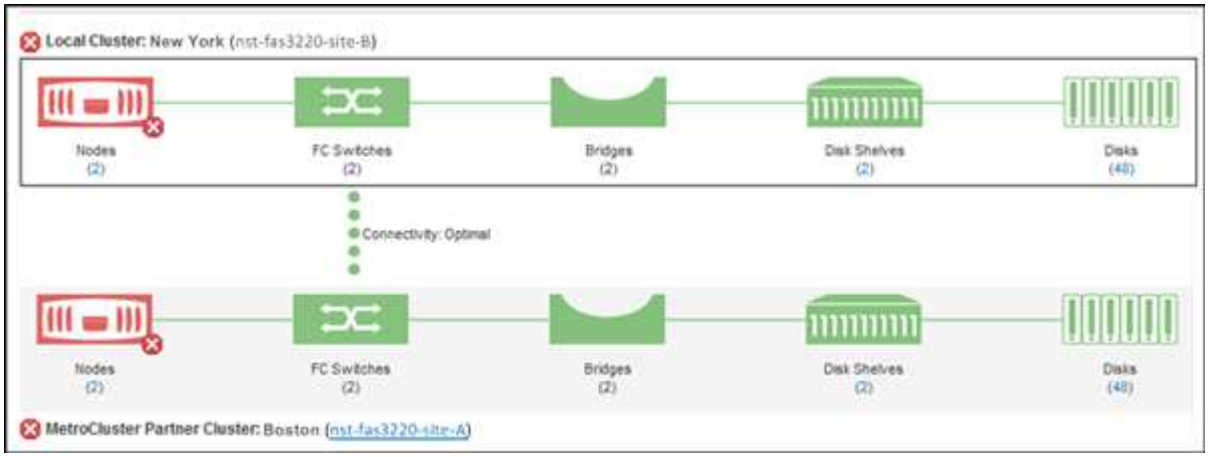
Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**, um die Ereignisliste anzuzeigen.
2. Wählen Sie im Filter-Panel alle MetroCluster-Filter unter der Kategorie **Quelltyp** aus. Sie sehen alle in Ihrer Umgebung aufgeworfenen Ereignisse für alle MetroCluster Konfigurationen.
3. Klicken Sie neben einem MetroCluster-Ereignis auf den Namen des Clusters.

   Wenn keine MetroCluster-Ereignisse angezeigt werden, können Sie mithilfe der Suchleiste nach dem Namen des am Ereignis beteiligten Clusters suchen, das mit Ihnen MetroCluster über FC-Konfiguration in Verbindung steht.

   Die Ansicht Systemzustand: Alle Cluster wird mit detaillierten Informationen über das Ereignis angezeigt.

4. Wählen Sie die Registerkarte **MetroCluster Connectivity** aus, um den Zustand der Verbindung zwischen dem ausgewählten Cluster und seinem Partner-Cluster anzuzeigen.

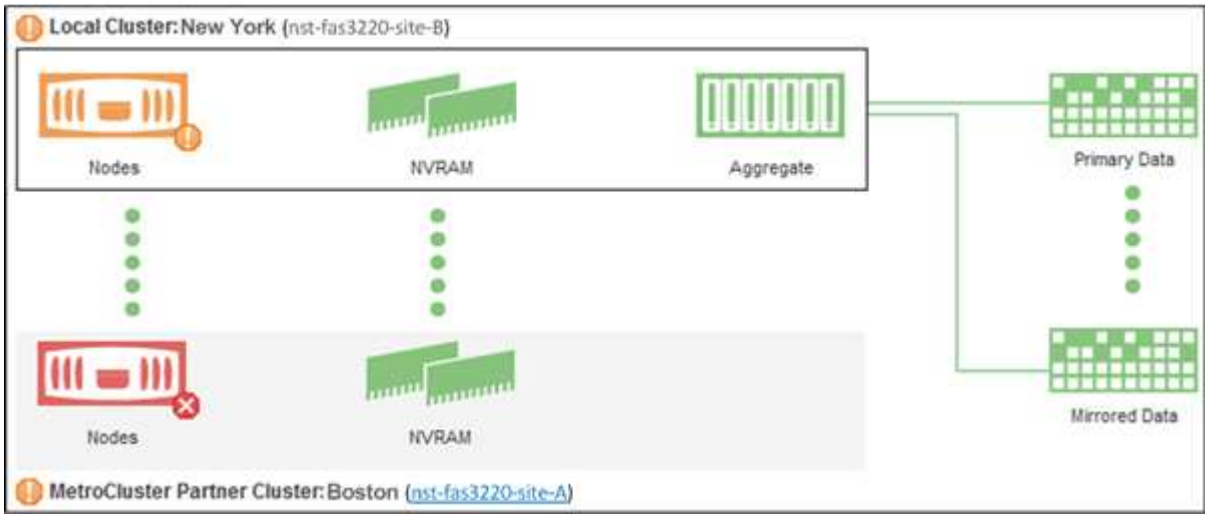


In diesem Beispiel werden die Namen und die Komponenten des lokalen Clusters und dessen Partner-

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.

Ermitteln des Clusterzustands in der MetroCluster-over-IP-Konfiguration

Befolgen Sie diese Schritte, um den Cluster-Zustand in einer MetroCluster über IP-Konfiguration zu bestimmen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**, um die Ereignisliste anzuzeigen.
2. Wählen Sie im Filterbereich unter der Kategorie **Quellentyp** den Filter aus `MetroCluster Relationship`. Sie sehen alle in Ihrer Umgebung aufgeworfenen Ereignisse für alle MetroCluster Konfigurationen.

> Wenn Sie die gemeldeten MetroCluster-Ereignisse nicht sehen können, können Sie mithilfe der Suchleiste den Namen des Clusters, das an dem Ereignis in Bezug auf Sie MetroCluster über IP-Konfiguration beteiligt ist, durchsuchen.

3. Klicken Sie neben dem entsprechenden MetroCluster-Ereignis auf den Namen des Clusters. Die Seite Cluster wird mit den Details dieses Clusters angezeigt. Informationen zum Bestimmen von Gesundheitsproblemen finden Sie unter "Überwachen von Konnektivitätsproblemen in der MetroCluster-over-IP-Konfiguration".

Anzeigen des Funktionszustands und Kapazitätsstatus aller SAN-Array-Cluster

Mithilfe der Cluster-Bestandsseiten können Sie den Zustand und den Kapazitätsstatus Ihrer All-SAN-Array-Cluster anzeigen.

Was Sie brauchen

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

Sie können die Übersichtsinformationen für alle SAN-Array-Cluster in der Ansicht Systemzustand: Alle Cluster und Kapazität: Alle Cluster anzeigen. Außerdem können Sie Details auf der Seite „Cluster/Health Details“ anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Cluster**.
2. Stellen Sie sicher, dass die Spalte „`personality`“ in der Ansicht **Health: All Clusters** angezeigt wird, oder fügen Sie sie mit dem Steuerelement **Anzeigen / Ausblenden** hinzu.

   In dieser Spalte wird „`All-SAN-Array`“ für Ihre All-SAN-Array-Cluster angezeigt.
3. Überprüfen Sie die Informationen.
4. Um Informationen zur Speicherkapazität in diesen Clustern anzuzeigen, wählen Sie die Ansicht Kapazität: Alle Cluster aus.
5. Um detaillierte Informationen zum Systemzustand und zur Storage-Kapazität in diesen Clustern anzuzeigen, klicken Sie auf den Namen eines All-SAN-Array-Clusters.

   Zeigen Sie auf der Seite Cluster/Integritätsdetails die Details auf den Registerkarten Systemzustand, Kapazität und Nodes an

Anzeigen der Node-Liste und der Details

Sie können die Ansicht Systemzustand: Alle Knoten verwenden, um die Liste der Knoten in Ihren Clustern anzuzeigen. Mit der Seite „Cluster/Systemzustand“ werden ausführliche Informationen zu Nodes angezeigt, die Teil des überwachten Clusters sind.

Was Sie brauchen

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

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 **Speicherung** > **Knoten**.
2. Klicken Sie in der Ansicht **Health: Alle Nodes** auf den Knoten, dessen Details Sie anzeigen möchten.

   Die detaillierten Informationen für den ausgewählten Node werden auf der Seite „Cluster/Health 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**.

Weitere Informationen finden Sie unter:

- "Performance: Alle Nodes anzeigen"
- "Anzeigen der verfügbaren IOPS-Werte für Node und Aggregat"
- "Anzeigen der verwendeten Werte für die Node- und Aggregat-Performance"

Erstellen eines Hardware-Bestandsberichts zur Vertragsverlängerung

Sie können einen Bericht generieren, der eine vollständige Liste von Cluster- und Node-Informationen enthält, wie z. B. Hardware-Modellnummern, Seriennummern, Festplattentypen und -Anzahl, installierte Lizenzen usw. Dieser Bericht unterstützt Sie bei der Vertragsverlängerung innerhalb sicherer Standorte („`dARK`“-Websites), die keine Verbindung zur NetAppActive IQ Plattform aufweisen.

Was Sie brauchen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherung** > **Knoten**.
2. Gehen Sie zur **Gesundheit: Alle Knoten** Ansicht oder **Leistung: Alle Knoten** Ansicht.
3. Wählen Sie **Berichte** > ***** > Hardware Inventory Report* Aus.

   Der Hardware-Bestandsbericht wird als .csv-Datei mit vollständigen Informationen ab dem aktuellen Datum heruntergeladen.

4. Stellen Sie diese Informationen Ihrem NetApp Support-Ansprechpartner für eine Vertragsverlängerung bereit.

Anzeigen der Liste und Details der Speicher-VM

Aus der Ansicht „Systemzustand“: Alle Storage VMs können Sie Ihr Inventar an Storage Virtual Machines (SVMs) überwachen. Mithilfe der Seite Storage VM/Health Details können Sie detaillierte Informationen zu überwachten SVMs anzeigen.

Was Sie brauchen

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

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 **Storage** > **Storage VMs**.
2. Wählen Sie eine der folgenden Möglichkeiten, um die SVM-Details anzuzeigen:
   - Um Informationen über den Zustand aller SVMs in allen Clustern anzuzeigen, wählen Sie im Menü Ansicht den Status: Alle Storage-VMs aus.
   - Um die vollständigen Details anzuzeigen, klicken Sie auf den Namen der Speicher-VM.

     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.

Verwandte Informationen

- "Storage VM: Health Details Seite"
- "Performance: Ansicht aller Storage VMs"
- "Sicherheit: Ansicht gegen Ransomware"
- "Anzeigen des Sicherheitsstatus für Cluster und Storage VMs"
- "Beziehung: Ansicht aller Beziehungen"

Anzeigen der Aggregatliste und der Details

Aus der Ansicht „Systemzustand“: Alle Aggregate können Sie Ihr Inventar an Aggregaten überwachen. Die Kapazität: Alle Aggregatansicht ermöglicht es Ihnen, Informationen über Kapazität und Auslastung von Aggregaten in allen Clustern anzuzeigen.

Was Sie brauchen

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

Sie können Details wie Aggregatskapazität und -Konfiguration sowie Festplatteninformationen über die Seite „Aggregate/Health Details“ anzeigen. Sie können diese Details verwenden, bevor Sie die Schwellenwerteinstellungen konfigurieren, falls erforderlich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Aggregate**.
2. Wählen Sie eine der folgenden Möglichkeiten, um die Aggregatdetails anzuzeigen:
   - Um Informationen über den Zustand aller Aggregate in allen Clustern anzuzeigen, wählen Sie im Menü Ansicht den Eintrag Systemzustand: Alle Aggregate aus.
   - Um Informationen zur Kapazität und Auslastung aller Aggregate in allen Clustern anzuzeigen, wählen Sie im Menü Ansicht die Option Kapazität: Alle Aggregate anzeigen.
   - 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.

Verwandte Informationen

- "Registerkarte „Aggregate/Health Details“"
- "Performance: Ansicht aller Aggregate"
- "Anpassung der Berichte zur Aggregatskapazität"

Anzeigen von Informationen zur FabricPool-Kapazität

Sie können FabricPool Kapazitätsinformationen für Cluster, Aggregate und Volumes auf den Seiten zu Kapazität und Performance-Inventar anzeigen sowie Details zu diesen Objekten. Auf diesen Seiten werden auch Informationen zur FabricPool-Spiegelung angezeigt, wenn eine Spiegelebene konfiguriert wurde.

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

Wenn ein Cloud-Tier zu einem anderen Cloud-Provider (die “mMirror Tier”) gespiegelt wird, werden beide Cloud-Ebenen auf der Seite Aggregate / Health Details angezeigt.

Schritte

1. Führen Sie einen der folgenden Schritte aus:

So zeigen Sie Kapazitätsinformationen für…	Tun Sie das…
Cluster	a. Klicken Sie in der Ansicht Capacity: All Clusters auf ein Cluster. b. Klicken Sie auf der Seite Cluster / Health 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. Auf der Ansicht Kapazität: Alle Aggregate klicken Sie auf ein Aggregat, in dem das Feld Typ „`SSD (FabricPool)`“ oder „`HDD (FabricPool)`“ anzeigt. b. Klicken Sie auf der Seite Aggregate / Health Details auf die Registerkarte **Capacity**. Auf dem Display wird die Gesamtkapazität angezeigt, die im Cloud-Tier verwendet wird. c. Klicken Sie auf die Registerkarte **Disk Information**. Das Display zeigt den Namen der Cloud-Tier und die verwendete Kapazität an. d. Klicken Sie auf die Registerkarte **Konfiguration**. Das Display zeigt den Namen der Cloud-Tier sowie weitere detaillierte Informationen zum Cloud-Tier an.
Volumes	a. Auf der Ansicht Kapazität: Alle Volumes klicken Sie im Feld „`Tiering Policy`“ auf ein Volume mit einem Richtliniennamen. b. Klicken Sie auf der Seite Volume/Health Details auf die Registerkarte **Konfiguration**. Auf der Anzeige wird der Name der FabricPool-Tiering-Richtlinie angezeigt, die dem Volume zugewiesen ist.

2. Auf der Seite **Workload Analysis** können Sie im Bereich **Capacity Trend** „`Cloud Tier View`“ auswählen, um die im lokalen Performance Tier und in der Cloud Tier im Vormonat verwendete Kapazität anzuzeigen.

Weitere Informationen zu FabricPool-Aggregaten finden Sie unter "Überblick über Festplatten und Aggregate".

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.

Was Sie brauchen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **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

In der Ansicht „Systemzustand: Alle Volumes“ können Sie Ihr Inventar von Volumes überwachen. Die Kapazität: Die Ansicht aller Volumes ermöglicht die Anzeige von Informationen zur Kapazität und Auslastung von Volumes in einem Cluster.

Was Sie brauchen

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

Auf der Seite Volume/Health Details können Sie auch detaillierte Informationen zu überwachten Volumes anzeigen, einschließlich 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 **Storage** > **Volumes**.
2. Es gibt folgende Möglichkeiten, die Volume-Details anzuzeigen:
   - Um detaillierte Informationen zum Systemzustand von Volumes in einem Cluster anzuzeigen, wählen Sie im Menü Ansicht den Eintrag Systemzustand: Alle Volumes aus.
   - Um ausführliche Informationen zur Kapazität und Auslastung von Volumes in einem Cluster anzuzeigen, wählen Sie im Menü Ansicht die Option Kapazität: Alle Volumes aus.
   - 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. **Optional:** Anzeigen Sie die Objekte, die mit dem Volumen in Verbindung stehen, indem Sie im Dialogfeld mit den minimalen Details auf **Related** klicken.

Verwandte Informationen

- "Volumen: Health Details Seite"

- "Performance: Ansicht aller Volumes"
- "Sicherheit: Ansicht gegen Ransomware"
- "Anzeigen von Volume-Sicherungsbeziehungen"
- "Erstellen eines Berichts, um verfügbare Volume-Kapazitätsdiagramme anzuzeigen"

Anzeigen von Details zu NFS-Freigaben

Sie können Details zu allen NFS-Freigaben anzeigen, z. B. ihren Status, den dem Volume zugeordneten Pfad (FlexGroup Volumes oder FlexVol Volumes), die Zugriffsebenen von Clients auf die NFS-Shares und die für die exportierten Volumes definierte Exportrichtlinie. Nutzung der Ansicht „Systemzustand“: Alle NFS-Freigaben anzeigen, um alle NFS-Freigaben auf allen überwachten Clustern anzuzeigen. Auf der Seite Storage VM/Health Details können Sie alle NFS-Freigaben auf einer bestimmten Storage Virtual Machine (SVM) anzeigen.

Was Sie brauchen

- Die NFS-Lizenz muss auf dem Cluster aktiviert sein.
- Netzwerkschnittstellen, die die NFS-Freigaben erfüllen, müssen konfiguriert sein.
- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Schritt

1. Befolgen Sie im linken Navigationsbereich die nachstehenden Schritte, je nachdem, ob Sie alle NFS-Freigaben oder nur die NFS-Freigaben für eine bestimmte SVM anzeigen möchten.

An…	Führen Sie die folgenden Schritte aus…
Alle NFS-Freigaben anzeigen	Klicken Sie auf **Storage** > **NFS-Freigaben**
Anzeigen von NFS-Freigaben für eine einzelne SVM	a. Klicken Sie auf **Storage** > **Storage VMs** b. Klicken Sie auf die SVM, deren Details zu NFS-Freigaben angezeigt werden sollen. c. Klicken Sie auf der Seite mit den Details zu Speicher-VM/Systemzustand auf die Registerkarte **NFS-Freigaben**.

Weitere Informationen finden Sie unter "Bereitstellen von Dateifreigabe-Volumes" und "Bereitstellen von CIFS- und NFS-Dateifreigaben mithilfe von APIs".

Anzeigen von Details zu SMB/CIFS-Freigaben

Sie können Details zu allen SMB-/CIFS-Freigaben anzeigen, z. B. Freigabename, Verbindungspfad, mit Objekten, Sicherheitseinstellungen und für die Freigabe definierten Exportrichtlinien. Nutzung der Ansicht „Systemzustand“: Alle SMB-Freigaben anzeigen, um alle SMB-Freigaben auf allen überwachten Clustern anzuzeigen. Auf der Seite Storage VM/Health Details können Sie alle SMB-Freigaben auf einer bestimmten Storage

Virtual Machine (SVM) anzeigen.

Was Sie brauchen

- Die CIFS-Lizenz muss auf dem Cluster aktiviert sein.
- Netzwerkschnittstellen, die die SMB/CIFS-Freigaben unterstützen, müssen konfiguriert werden.
- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Freigaben in Ordnern werden nicht angezeigt.

Schritt

1. Führen Sie im linken Navigationsbereich die folgenden Schritte aus, je nachdem, ob Sie alle SMB/CIFS-Freigaben oder nur die Freigaben für eine bestimmte SVM anzeigen möchten.

An…	Führen Sie die folgenden Schritte aus…
Alle SMB-/CIFS-Freigaben anzeigen	Klicken Sie auf **Storage** > **SMB-Freigaben**
Anzeigen von SMB-/CIFS-Freigaben für eine einzelne SVM	a. Klicken Sie auf **Storage** > **Storage VMs** b. Klicken Sie auf die SVM, deren Details zur SMB/CIFS-Freigabe angezeigt werden sollen. c. Klicken Sie auf der Seite mit den Details zu Speicher-VM/Systemzustand auf die Registerkarte **SMB-Freigaben**.

Weitere Informationen finden Sie unter "Bereitstellen von CIFS- und NFS-Dateifreigaben mithilfe von APIs".

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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Das Volume, das die Snapshot Kopien enthält, muss online sein.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie in der Ansicht **Systemzustand: Alle Volumes** das Volume aus, das die Snapshot Kopien enthält, die Sie anzeigen möchten.
3. Klicken Sie auf der Seite **Volumen / Gesundheit** Details auf die Registerkarte **Kapazität**.
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.

Verwandte Informationen

"Systemzustand/Volumes-Seite"

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.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ 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.

- Die Basis-Snapshot Kopie in einem übergeordneten Volume kann nicht gelöscht werden, wenn ein FlexClone Volume diese Snapshot Kopie nutzt.

  Die Basis-Snapshot-Kopie ist die Snapshot Kopie, mit der das FlexClone Volume erstellt wird. Hier werden der Status und die Applikationsabhängigkeit `Busy, Vclone` im übergeordneten Volume angezeigt `Busy`.

- 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 **Storage** > **Volumes**.
2. Wählen Sie in der Ansicht **Systemzustand: Alle Volumes** 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 **Volumen / Gesundheit** Details auf die Registerkarte **Kapazität**.
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.

Was Sie brauchen

- Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.
- Das Volume muss sich online sein.
- Das Volume muss ein FlexVol Volume sein. Diese Funktion wird nicht mit FlexGroup Volumes unterstützt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie in der Ansicht **Systemzustand: Alle Volumes** 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 **Volumen / Gesundheit** Details auf die Registerkarte **Kapazität**.
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. Sie können die Benutzeroberfläche des System Manager jetzt aus den folgenden ABSCHNITTEN FÜR SPEICHER und SCHUTZ des BESTANDS starten.

- Cluster Inventory, Cluster Health und Cluster Performance Seiten
- Aggregierte Seiten „Inventar“, „Aggregatzustand“ und „aggregierte Performance“
- Volume-Bestand, Volume-Zustand und Volume Performance
- Seiten „Node Inventory“ und „Node Performance“
- StorageVM Inventory, StorageVM Health und StorageVM Performance Seiten
- Schutzbeziehungen Seiten

Gemeinsame Workflows und Aufgaben im Zusammenhang mit Unified Manager

Zu den geläufigsten administrativen Workflows und Aufgaben für Unified Manager gehört

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

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

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

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

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

- Diagnose und Management von Verfügbarkeitsproblemen

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

- Konfiguration und Monitoring von Performance-Vorfällen

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

- Diagnose und Management von Kapazitätsproblemen bei Volumes

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

- Konfiguration, Monitoring und Diagnose von Problemen bei der Sicherungsbeziehung

  Nach dem Erstellen und Konfigurieren von Sicherungsbeziehungen können Storage-Administratoren mögliche Probleme im Zusammenhang mit Sicherungsbeziehungen, den aktuellen Zustand der Sicherungsbeziehungen, die aktuellen und historischen Sicherungsinformationen zu den betroffenen Beziehungen sowie Hinweise zur Fehlerbehebung anzeigen. "Erstellen, Überwachen und Beheben von Sicherungsbeziehungen"Weitere Informationen finden Sie im.

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

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

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

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

Monitoring und Fehlerbehebung der Datenverfügbarkeit

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

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

Scannen und Beheben von Verbindungsproblemen für Storage Failover Interconnect

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

Was Sie brauchen

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**.
2. Wählen Sie auf der Seite * Event Management* Inventory die Option **Active Availability Events** aus.
3. Klicken Sie oben in der Spalte **Event Management** Inventory Page **Name** auf  und geben Sie in das Textfeld ein `*failover`, um das Ereignis auf Speicher-Failover-Ereignisse zu beschränken.

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

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

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

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

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

   Die Seite Ereignisdetails für dieses Ereignis wird angezeigt.

   a. Auf der Seite Ereignisdetails können Sie eine oder mehrere der folgenden Aufgaben ausführen:
      - Überprüfen Sie die Fehlermeldung im Feld Ursache, und bewerten Sie das Problem.
      - Weisen Sie das Ereignis einem Administrator zu.
      - Bestätigen Sie das Ereignis.

Verwandte Informationen

"Seite mit den Veranstaltungsdetails"

"Unified Manager Benutzer-Rollen und -Funktionen"

Durchführen von Korrekturmaßnahmen für Storage Failover Interconnect-Verbindungen als inaktiv

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

Was Sie brauchen

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

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

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

Summary

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

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

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

Schritte

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

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

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

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

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.

Verwandte Informationen

"Seite mit den Veranstaltungsdetails"

"Unified Manager Benutzer-Rollen und -Funktionen"

Lösung von Offline-Problemen des Volumes

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

Was Sie brauchen

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

Volumes können aus verschiedenen Gründen offline gemeldet werden:

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

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

Schritte

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

   Die Seite Ereignisdetails für den Verfügbarkeitsereignis wird angezeigt.

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

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

   - Im Bereich „Notizen“ und „Updates“ werden alle Angaben darüber gemacht, dass der SVM-Administrator das fragliche Volume absichtlich offline geschaltet hat.
   - Klicken Sie auf die Quelle des Ereignisses, in diesem Fall auf das offline gemeldete Volume, um weitere Informationen zu diesem Volume zu erhalten.
   - Weisen Sie das Ereignis einem Administrator zu.
   - Bestätigen Sie das Ereignis oder markieren Sie es gegebenenfalls als erledigt.

Durchführung von Diagnoseaktionen für Offline-Bedingungen des Volumes

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

Was Sie brauchen

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

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

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

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

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

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

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

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

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

Verwandte Informationen

"Unified Manager Benutzer-Rollen und -Funktionen"

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

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

Was Sie brauchen

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

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

Schritte

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

   Auf der Seite Storage VM / Health Details werden Informationen zur SVM (Hosting Storage Virtual

Machine) des Offline-Volumes angezeigt.

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

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

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

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

4. Klicken Sie in der Ansicht Systemzustand: Alle Volumes auf das Rastersymbol und wählen Sie dann die Option **Cluster Nodes** aus.

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

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

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

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

Nachdem Sie 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.

Was Sie brauchen

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

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

Schritte

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

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

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

   Die Informationen für diese SVM sind in einer Tabelle dargestellt.

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

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

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

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

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

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

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

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

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

Was Sie brauchen

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

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

Schritte

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

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

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

   Die Seite „Cluster/Health Details“ wird angezeigt.

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

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

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

Behebung von Kapazitätsproblemen

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

Was Sie brauchen

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

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

Schritte

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

   Die Seite Ereignisdetails für den Fehler wird angezeigt.

2. Auf der Seite **Event** Details können Sie eine oder mehrere der folgenden Aufgaben ausführen:
   - Überprüfen Sie die Fehlermeldung im Feld Ursache, und klicken Sie auf die Vorschläge unter vorgeschlagene Korrekturmaßnahmen, um Beschreibungen möglicher Korrekturmaßnahmen zu prüfen.
   - Klicken Sie im Feld Quelle auf den Objektnamen, in diesem Fall ein Volume, um Details zum Objekt anzuzeigen.
   - Suchen Sie nach Notizen, die zu diesem Event hinzugefügt wurden.
   - Fügen Sie dem Ereignis eine Notiz hinzu.
   - Das Ereignis einem anderen Benutzer zuweisen.
   - Bestätigen Sie das Ereignis.

◦ Markieren Sie das Ereignis als erledigt.

Verwandte Informationen

"Seite mit den Veranstaltungsdetails"

Durchführung von vorgeschlagenen Abhilfemaßnahmen für ein vollständiges Volumen

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

Was Sie brauchen

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

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

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

Mögliche Abhilfemaßnahmen für ein komplettes Volume sind:

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

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

Schritte

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

   Sie entscheiden, die Größe des Volumes zu ändern.

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

Verwandte Informationen

"Seite mit den Veranstaltungsdetails"

Verwalten von Systemzustandsschwellenwerten

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

Welche Schwellenwerte für den Zustand von Storage-Kapazität sind

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

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

Konfigurieren von globalen Schwellenwerteinstellungen für den Systemzustand

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

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

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

- Weitere Informationen finden Sie unter "Konfigurieren von globalen Integritätsschwellenwerten für das Aggregat".

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

- Weitere Informationen finden Sie unter "Konfigurieren von globalen Schwellenwerten für den Zustand des Volumes".

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

- Weitere Informationen finden Sie unter "Konfigurieren von globalen qtree-Zustandsschwellenwerten".

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

- Weitere Informationen finden Sie unter "Bearbeiten von Verzögerungszustands-Schwellenwerten für nicht verwaltete Schutzbeziehungen".

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

Konfigurieren von globalen Integritätsschwellenwerten für das Aggregat

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

Was Sie brauchen

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

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

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

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

Systemzustandsschwellenwerte gelten nicht für das Root-Aggregat des Nodes.

Schritte

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

Verwandte Informationen

"Benutzer hinzufügen"

Konfigurieren von globalen Schwellenwerten für den Zustand des Volumes

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

Was Sie brauchen

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

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

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

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

Schritte

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

Verwandte Informationen

"Benutzer hinzufügen"

Konfigurieren von globalen qtree-Zustandsschwellenwerten

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

Was Sie brauchen

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

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisschwellenwerte** > **qtree**.

2. Konfigurieren Sie die entsprechenden Kapazitätsschwellenwerte.
3. Klicken Sie Auf **Speichern**.

Konfigurieren von Verzögerungsschwellenwerten für nicht verwaltete Schutzbeziehungen

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

Was Sie brauchen

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

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

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

Schritte

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

Verwandte Informationen

"Benutzer hinzufügen"

Bearbeiten einzelner Zustandsschwellenwerte für das Aggregat

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

Was Sie brauchen

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

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

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

Volume-Größe.

Schritte

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

Verwandte Informationen

"Benutzer hinzufügen"

Bearbeiten von Schwellenwerten für den Zustand einzelner Volumes

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

Was Sie brauchen

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

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

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

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

Schritte

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

4. Klicken Sie Auf **Speichern**.

Verwandte Informationen

"Benutzer hinzufügen"

Bearbeiten einzelner qtree-Statusschwellenwerte

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

Was Sie brauchen

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

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

Schritte

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

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

Verwalten von Zielen für die Cluster-Sicherheit

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

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

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

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

Weitere Informationen finden Sie unter "Welche Sicherheitskriterien werden bewertet".

Welche Sicherheitskriterien werden bewertet

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

Einige der Sicherheitsprüfungen umfassen:

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

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

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

Weitere Informationen finden Sie unter "Verwalten von Zielen für die Cluster-Sicherheit".

Cluster-Compliance-Kategorien

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

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

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

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
Globaler FIPS	Gibt an, ob der Compliance-Modus Global FIPS (Federal Information Processing Standard) 140-2 aktiviert oder deaktiviert ist. Wenn FIPS aktiviert ist, sind TLSv1 und SSLv3 deaktiviert und nur TLSv1.1 und TLSv1.2 zulässig.	Aktiviert	Ja.
Telnet	Gibt an, ob Telnet-Zugriff auf das System aktiviert oder deaktiviert ist. NetApp empfiehlt Secure Shell (SSH) für den sicheren Remote-Zugriff.	Deaktiviert	Ja.
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, z. B. Chiffren, die mit *cbc beginnen.	Nein	Ja.
Anmelde-Banner	Zeigt an, ob das Anmeldebanner für Benutzer, die auf das System zugreifen, aktiviert oder deaktiviert ist.	Aktiviert	Ja.
Cluster-Peering	Gibt an, ob die Kommunikation zwischen Peering-Clustern verschlüsselt oder unverschlüsselt ist. Für diesen Parameter muss sowohl auf den Quell- als auch auf den Ziel-Clustern konfiguriert werden, damit er als konform betrachtet werden kann.	Verschlüsselt	Ja.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
Network Time Protocol	Gibt an, ob das Cluster über einen oder mehrere konfigurierte NTP-Server verfügt. Aus Gründen der Redundanz und des besten Service empfiehlt NetApp, mindestens drei NTP-Server mit dem Cluster zu verknüpfen.	Konfiguriert	Ja.
OCSP	Ab 9.14.1 bietet Active IQ Unified Manager Statusinformationen zum Online Certificate Status Protocol (OCSP) auf Ebene der Storage Virtual Machine (SVM, früher als Vserver bezeichnet). Das bedeutet, dass die OCSP-Validierung auf alle SSL/TLS-Verbindungen angewendet wird, die an der SVM vorgenommen werden, und die Integrität und Gültigkeit der in diesen Verbindungen verwendeten Zertifikate sicherstellt.	Aktiviert	Nein
Remote Audit-Protokollierung	Gibt an, ob die Protokollweiterleitung (Syslog) verschlüsselt ist oder nicht verschlüsselt ist.	Verschlüsselt	Ja.
AutoSupport HTTPS-Übertragung	Zeigt an, ob HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport Meldungen an den NetApp Support verwendet wird.	Aktiviert	Ja.

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

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
Remote Shell	Zeigt an, ob RSH aktiviert ist. Aus Sicherheitsgründen sollte RSH deaktiviert werden. Vorzugsweise ist Secure Shell (SSH) für sicheren Remote-Zugriff.	Deaktiviert	Ja.
MD5 wird verwendet	Zeigt an, ob ONTAP-Benutzerkonten die weniger sichere MD5-Hash-Funktion verwenden. Die MD5-Hashed-Benutzerkonten-Migration auf die sicherere kryptografische Hash-Funktion wie SHA-512 wird bevorzugt.	Nein	Ja.
Zertifikataussteller Typ	Gibt den Typ des verwendeten digitalen Zertifikats an.	CA-signiert	Nein

Compliance-Kategorien für Storage-VMs

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

Parameter	Beschreibung	Empfehlung	Beeinträchtigt SVM-Compliance
Überwachungsprotokoll	Gibt an, ob die Überwachungsprotokollierung aktiviert oder deaktiviert ist.	Aktiviert	Ja.
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, z. B. Chiffren, die mit beginnen `cbc*`.	Nein	Ja.

Parameter	Beschreibung	Empfehlung	Beeinträchtigt SVM-Compliance
Anmelde-Banner	Zeigt an, ob das Anmeldebanner für Benutzer, die auf SVMs im System zugreifen, aktiviert oder deaktiviert ist.	Aktiviert	Ja.
LDAP-Verschlüsselung	Gibt an, ob LDAP-Verschlüsselung aktiviert oder deaktiviert ist.	Aktiviert	Nein
NTLM-Authentifizierung	Gibt an, ob die NTLM-Authentifizierung aktiviert oder deaktiviert ist.	Aktiviert	Nein
LDAP Payload-Signatur	Gibt an, ob LDAP-Payload-Signatur aktiviert oder deaktiviert ist.	Aktiviert	Nein
CHAP-Einstellungen	Gibt an, ob CHAP aktiviert oder deaktiviert ist.	Aktiviert	Nein
Kerberos V5	Gibt an, ob die Kerberos-V5-Authentifizierung aktiviert oder deaktiviert ist.	Aktiviert	Nein
NIS-Authentifizierung	Gibt an, ob die Verwendung der NIS-Authentifizierung konfiguriert ist.	Deaktiviert	Nein
FPolicy Status aktiv	Zeigt an, ob FPolicy erstellt wird oder nicht.	Ja.	Nein
SMB-Verschlüsselung aktiviert	Gibt an, ob SMB -Signing & Sealing nicht aktiviert ist.	Ja.	Nein
SMB-Signatur aktiviert	Gibt an, ob SMB -Signing nicht aktiviert ist.	Ja.	Nein

Volume Compliance-Kategorien

Diese Tabelle beschreibt die Verschlüsselungsparameter des Volumes, die von Unified Manager geprüft werden, um zu ermitteln, ob die Daten auf Ihren Volumes vor dem

Zugriff durch unbefugte Benutzer angemessen geschützt sind.

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

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

Was bedeutet nicht, dass Compliance-Anforderungen erfüllt werden

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

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

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

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

Anzeigen des Sicherheitsstatus für Cluster und Storage VMs

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

Die Sicherheitsempfehlungen finden Sie im "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9"

Anzeigen des Sicherheitsstatus auf Objektebene auf der Sicherheitsseite

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

Schritte

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

Durch Klicken auf die Balkendiagramme, Zählungen und `View Reports` Links gelangen Sie zur Seite Volumes, Cluster oder Speicher-VMs, auf der Sie die entsprechenden Details anzeigen oder Berichte nach Bedarf generieren können.

Auf der Seite Sicherheit werden die folgenden Felder angezeigt:

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

Zeigen Sie auf der Seite Cluster die Sicherheitsdetails aller Cluster an

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

Schritte

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

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

Sie können auf die Schaltfläche Weitere Optionen klicken ⋮ und die Sicherheitsdetails auf der Seite **Sicherheit** von Unified Manager oder auf System Manager anzeigen. Sie sollten gültige Anmeldeinformationen zum Anzeigen der Details in System Manager haben.

> ⓘ Wenn ein Cluster über ein abgelaufenes Zertifikat verfügt, können Sie unter **Clusterzertifikat Gültigkeit** klicken `expired` und es von System Manager (9.10.1 und höher) erneuern. Sie können nicht klicken `expired`, wenn die System Manager-Instanz eine Version vor 9.10.1 ist.

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

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

Schritte

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

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

Sie können auf die Schaltfläche Weitere Optionen klicken ⋮ und die Sicherheitsdetails auf der Seite **Sicherheit** von Unified Manager oder auf System Manager anzeigen. Sie sollten gültige Anmeldeinformationen zum Anzeigen der Details in System Manager haben.

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

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

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

Was Sie brauchen

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

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

Schritte

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

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

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

   Auf der Seite werden alle aktiven Sicherheitsereignisse für Upgrades angezeigt.

Anzeige des Managements der Benutzerauthentifizierung auf allen Clustern

Auf der Seite Sicherheit werden die Authentifizierungstypen angezeigt, die zur Authentifizierung von Benutzern in jedem Cluster verwendet werden, sowie die Anzahl

der Benutzer, die mit jedem Typ auf das Cluster zugreifen. So können Sie überprüfen, ob die Benutzerauthentifizierung gemäß den Anforderungen Ihres Unternehmens sicher durchgeführt wird.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Wählen Sie oben im Dashboard im Dropdown-Menü * Alle Cluster* aus.
3. Klicken Sie im Fenster **Sicherheit** auf den rechten Pfeil, und die Seite **Sicherheit** wird angezeigt.
4. Zeigen Sie die **Cluster Authentication**-Karte an, um die Anzahl der Benutzer anzuzeigen, die mit jedem Authentifizierungstyp auf das System zugreifen.
5. Zeigen Sie die **Cluster Security**-Karte an, um die Authentifizierungsmechanismen anzuzeigen, die zur Authentifizierung von Benutzern in jedem Cluster verwendet werden.

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

Anzeigen des Verschlüsselungsstatus aller Volumes

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

Was Sie brauchen

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

Auf ein Volume können folgende Verschlüsselungsarten angewendet werden:

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Gesundheit** > **Volumen-Verschlüsselung**
3. Sortieren Sie in der Ansicht **Health: Volumes Encryption** das Feld **Verschlüsselungstyp**, oder verwenden Sie den Filter, um Volumes mit einem bestimmten Verschlüsselungstyp anzuzeigen oder die nicht verschlüsselt sind (Verschlüsselungstyp von „`Keine`“).

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

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

Was Sie brauchen

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

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

Anzeigen der Sicherheitsinformationen aller Volumes mit Ransomware-Erkennung

Schritte

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

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

Anzeigen der Sicherheitsinformationen aller Storage-VMs mit Ransomware-Erkennung

Schritte

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

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

Anzeigen aller aktiven Sicherheitsereignisse

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

Was Sie brauchen

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

Schritte

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

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

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

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

Hinzufügen von Warnmeldungen für Sicherheitsereignisse

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

Was Sie brauchen

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Alarm-Setup**.
2. Klicken Sie auf der Seite **Alarm-Setup** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
4. Klicken Sie auf **Ressourcen** und wählen Sie den Cluster oder den Cluster aus, auf dem Sie diese Warnung aktivieren möchten.
5. Klicken Sie auf **Events** und führen Sie die folgenden Aktionen aus:
   a. Wählen Sie in der Liste Ereignis Severity die Option **Warnung** aus.
   b. Wählen Sie in der Liste passende Ereignisse die Option **Telnet-Protokoll aktiviert**.
6. Klicken Sie auf **Aktionen** und wählen Sie dann den Namen des Benutzers aus, der die Benachrichtigung per E-Mail im Feld * Diese Benutzer benachrichtigen* erhält.
7. Konfigurieren Sie alle anderen Optionen auf dieser Seite, um die Benachrichtigungshäufigkeit zu erhöhen, SNMP-Taps auszugeben und ein Skript auszuführen.
8. Klicken Sie Auf **Speichern**.

Bestimmte Sicherheitsereignisse deaktivieren

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

Was Sie brauchen

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

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

Schritte

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

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

Sicherheitsereignisse

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

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

Managen von Backup- und Restore-Vorgängen

Sie können Backups von Active IQ Unified Manager erstellen und das Backup mit der Wiederherstellungsfunktion auf dasselbe (lokale) System oder ein neues (Remote-)System im Falle eines Systemausfalls oder Datenverlust wiederherstellen.

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

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

Diese verschiedenen Methoden werden in den folgenden Abschnitten beschrieben.

Backup und Restore für Unified Manager auf der virtuellen Appliance

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

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

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

   Wenn der Datastore nicht auf einem System mit ONTAP-Software gehostet wird, befolgen Sie die Richtlinien des Storage-Anbieters, um ein Backup des VMware-Snapshots zu erstellen.
3. Replizierung der NetApp Snapshot Kopie (oder vergleichbarer Snapshot) in einem alternativen Storage
4. Löschen Sie den VMware Snapshot.

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

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

Sichern und Wiederherstellen mithilfe eines MySQL Datenbank-Dump

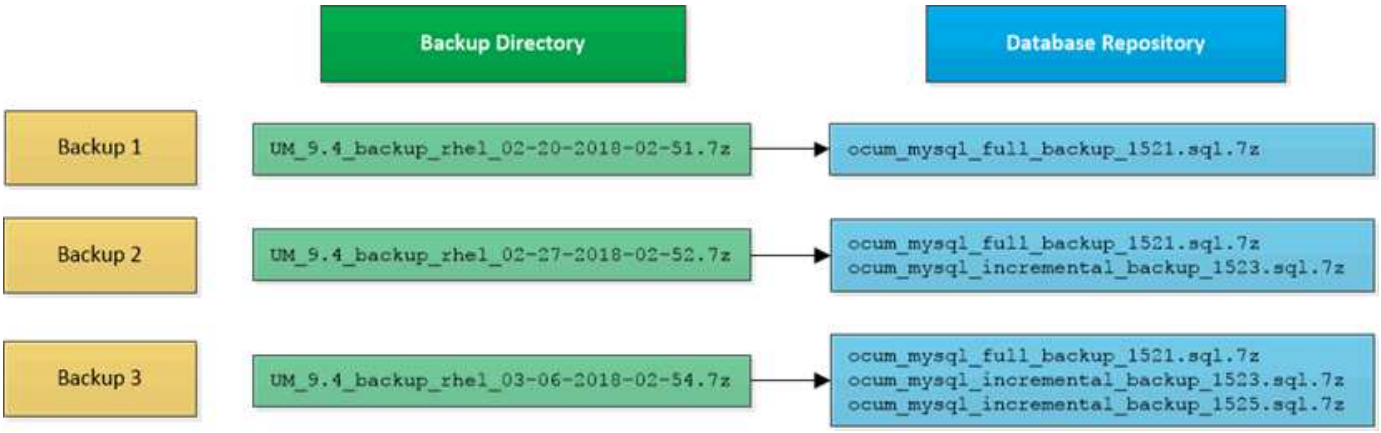
Ein MySQL Datenbank Dump Backup ist eine Kopie der Active IQ Unified Manager-Datenbank und Konfigurationsdateien, die Sie im Falle eines Systemausfalls oder Datenverlust verwenden können. Sie können ein Backup so planen, dass es auf ein lokales Ziel oder auf ein Remote-Ziel geschrieben wird. Es wird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

einen Remote-Standort außerhalb des Active IQ Unified Manager Host-Systems zu definieren.

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

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

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



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

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

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

Konfigurieren des Ziels und Planen für Datenbank-Dump-Backups

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

jedoch einen Backup-Zeitplan festlegen.

Was Sie brauchen

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

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

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

  Berechtigungen: 0750, Eigentum: jboss:Maintenance

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

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

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

Schritte

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

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

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

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

Was ist ein Datenbank-Restore

Bei einer Wiederherstellung einer MySQL Datenbank wird eine vorhandene Unified Manager Backup-Datei auf demselben oder einem anderen Unified Manager Server

wiederhergestellt. Sie führen die Wiederherstellung über die Unified Manager-Wartungskonsole aus.

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

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

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

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

Verwandte Informationen

"Erstellen eines HTTPS-Sicherheitszertifikats"

"Aktivieren der SAML-Authentifizierung"

"Authentifizierung mit Active Directory oder OpenLDAP"

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

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

Was Sie brauchen

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

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

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

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

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

Schritte

1. Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager die UI nicht oder konfigurieren Sie nach Abschluss der Installation keine Cluster, Benutzer oder Authentifizierungseinstellungen. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.
2. Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domänennamen des Unified Manager-Systems her.
3. Melden Sie sich beim System mit dem Wartungs-Benutzer (umadmin) und dem Passwort an.
4. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
5. Geben Sie in der Wartungskonsole **Hauptmenü** die Nummer für die Option **Backup Restore** ein.
6. Geben Sie die Nummer für die * MySQL-Sicherung wiederherstellen* ein.
7. Geben Sie bei entsprechender Aufforderung den absoluten Pfad der Sicherungsdatei ein.

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

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

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

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

Wiederherstellen einer MySQL-Datenbank-Sicherung unter Windows

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

Was Sie brauchen

- Sie müssen über Administratorrechte für Windows verfügen.

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

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

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

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

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

Schritte

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

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

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

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

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

Backup und Restore mit NetApp Snapshots

Eine NetApp Snapshot Kopie erstellt ein zeitpunktgenaues Image der Unified Manager

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

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

Backup wird unter Linux konfiguriert

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

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

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

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

  Wenn Sie beispielsweise ein Backup mit Unified Manager 9.14 erstellt haben, kann das Backup nur auf Unified Manager 9.14-Systemen wiederhergestellt werden.

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

Speicherort für Snapshot-Kopien wird konfiguriert

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

Was Sie brauchen

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

- Cluster-Anforderungen:
  - ONTAP 9.3 oder höher muss installiert sein
  - Sie sollten sich in geographischer Nähe zum Unified Manager-Server befinden
  - Die Software kann zwar von Unified Manager überwacht werden, ist aber nicht erforderlich
- Storage-VM-Anforderungen:
  - Der Namensschalter und die Namenszuweisung müssen auf „`files`“ gesetzt werden.
  - Lokale Benutzer wurden erstellt, um den Client-seitigen Benutzern zu entsprechen

- Stellen Sie sicher, dass alle Lese-/Schreibzugriff ausgewählt ist
- Stellen Sie sicher, dass Superuser Access in der Exportrichtlinie auf „`any`“ eingestellt ist
- NFS für NetApp Snapshot für Linux
- NFSv4 muss auf dem NFS-Server und der NFSv4-ID-Domäne aktiviert sein, die auf dem Client und der Storage-VM angegeben ist
- Das Volume sollte mindestens die doppelte Größe von Unified Manager/opt/netapp/Data Directory haben

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

- Volume-Anforderungen:
  - Das Volume sollte mindestens die doppelte Größe des Unified Manager/opt/netapp/Datenververzeichnisses haben
  - Der Sicherheitsstil muss auf UNIX festgelegt sein
  - Die lokale Snapshot-Richtlinie muss deaktiviert werden
  - Die automatische Volume-Größe sollte aktiviert sein
  - Das Performance-Service-Level sollte auf eine Richtlinie mit hohen IOPS-Werten und niedriger Latenz, wie z. B. „`Extreme`“, festgelegt werden.

Detaillierte Schritte zum Erstellen des NFS-Volumes finden Sie unter "So konfigurieren Sie NFSv4 in ONTAP 9" und "ONTAP 9 NFS Configuration Express-Handbuch" .

Angeben des Zielorts für Snapshot Kopien

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

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

Schritte

1. Verwenden Sie Secure Shell, um eine Verbindung mit der IP-Adresse oder dem FQDN des Active IQ Unified Manager-Systems herzustellen.
2. Melden Sie sich beim System mit dem Wartungs-Benutzer (umadmin) und dem Passwort an.
3. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
4. Geben Sie in der Wartungskonsole **Hauptmenü** die Nummer für die Option **Backup Restore** ein.
5. Geben Sie die Nummer für * NetApp Snapshot Backup konfigurieren* ein.
6. Geben Sie die Nummer ein, die NFS konfiguriert werden soll.

7. Überprüfen Sie die Informationen, die Sie angeben müssen, und geben Sie dann die Nummer für **Backup Configuration Details** ein.
8. Um das Volume zum Schreiben des Snapshot zu identifizieren, geben Sie die IP-Adresse der Cluster Management Schnittstelle, den Namen der Storage VM, den Namen des Volumes, LUN-Namen, den Benutzernamen und das Passwort des Storage-Systems sowie den Mount-Pfad ein.
9. Überprüfen Sie diese Informationen und geben Sie `y`.

   Das System führt die folgenden Aufgaben aus:

   - Stellt die Verbindung zum Cluster her
   - Stoppt alle Dienste
   - Erstellt ein neues Verzeichnis im Volume und kopiert die Konfigurationsdateien der Active IQ Unified Manager Datenbank
   - Löscht die Dateien aus Active IQ Unified Manager und erstellt ein Symlink zum neuen Datenbankverzeichnis
   - Startet alle Dienste neu
10. Beenden Sie die Wartungskonsole und starten Sie die Schnittstelle Active IQ Unified Manager, um einen Zeitplan für die Snapshot Kopie zu erstellen, falls Sie dies noch nicht getan haben.

Backup wird unter Windows konfiguriert

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

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

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

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

Konfigurieren des Backup-Standorts für Windows

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

Was Sie brauchen

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

- Cluster-Anforderungen:
  - ONTAP 9.3 oder höher muss installiert sein
  - Sie sollten sich in geographischer Nähe zum Unified Manager-Server befinden

- Die Überwachung erfolgt durch Unified Manager

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

    Dadurch wird auch auf dem Volume die gleiche Größenanforderung festgelegt.

  - Stellen Sie sicher, dass alle Lese-/Schreibzugriff ausgewählt ist
  - Stellen Sie sicher, dass Superuser Access in der Exportrichtlinie auf „`any`“ eingestellt ist
- Volume- und LUN-Anforderungen:
  - Das Volume sollte mindestens die doppelte Größe im Unified Manager MySQL-Datenverzeichnis haben.
  - Der Sicherheitsstil muss auf Windows festgelegt sein
  - Die lokale Snapshot-Richtlinie muss deaktiviert werden
  - Die automatische Volume-Größe sollte aktiviert sein
  - Das Performance-Service-Level sollte auf eine Richtlinie mit hohen IOPS-Werten und niedriger Latenz, wie z. B. „`Extreme`“, festgelegt werden.

ONTAP-Cluster wird konfiguriert

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

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

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

Sie müssen folgende Konfiguration durchführen:

Schritte

1. Konfigurieren Sie eine iSCSI-fähige Storage-VM oder verwenden Sie eine vorhandene Storage-VM mit derselben Konfiguration.
2. Konfigurieren Sie eine Netzwerkroute für die konfigurierte Storage-VM.

3. Konfigurieren Sie ein Volume mit entsprechender Kapazität und eine einzelne LUN darin, damit das Volume nur für diese LUN reserviert ist.

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

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

Windows-Hostcomputer wird konfiguriert

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

Was Sie brauchen

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

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

Schritte

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

Festlegen des Zielorts für Snapshot Kopien unter Windows

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

- Sie müssen über die Administratorberechtigung für Windows Host verfügen, auf dem Active IQ Unified Manager installiert ist.

- Sie müssen über eine Benutzer-ID und ein Passwort verfügen, um sich bei der Wartungskonsole des Unified Manager-Servers anzumelden.
- Sie müssen über die IP-Adresse für das Cluster-Management, den Namen der Storage-VM, den Namen des Volumes, den LUN-Namen und den Benutzernamen und das Kennwort des Speichersystems verfügen.
- Sie müssen das Volume als Netzwerklaufwerk auf den Active IQ Unified Manager-Host gemountet haben, und Sie müssen das Mount-Laufwerk haben.

Schritte

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

   Das System führt die folgenden Aufgaben aus:

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

Konfigurieren eines Backups mit Snapshot-Kopie von der Wartungskonsole

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

Was Sie brauchen

Sie sollten für Ihr System die folgenden Informationen haben:

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

Schritte

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

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

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

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

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

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

Definieren eines Backup-Zeitplans für Linux und Windows

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

Was Sie brauchen

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

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

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

Schritte

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

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

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

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

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

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

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

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

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

Auf der Seite „Alarmkonfiguration“ konfigurieren Sie Warnmeldungen.

Wiederherstellung von Unified Manager mithilfe von Snapshot Kopien

Im Falle eines Datenverlustes oder einer Beschädigung von Daten können Sie Unified Manager in den vorherigen stabilen Zustand bei minimalem Datenverlust wiederherstellen. Sie können die Snapshot-Datenbank von Unified Manager mithilfe der

Wartungskonsole auf einem lokalen oder Remote-Betriebssystem wiederherstellen.

Was Sie brauchen

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

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

Schritte

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

   Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager die UI nicht oder konfigurieren Sie nach Abschluss der Installation keine Cluster, Benutzer oder Authentifizierungseinstellungen. Geben Sie 1 ein, um **NetApp Snapshot Backup konfigurieren** auszuwählen und die Einstellungen für Snapshot Kopien so zu konfigurieren, wie sie sich auf dem Originalsystem befinden.
6. Geben Sie 3 ein, um **Restore mit NetApp Snapshot** auszuwählen.
7. Wählen Sie die Snapshot Kopie aus, aus der Sie Unified Manager wiederherstellen möchten. Drücken Sie **Enter**.
8. Melden Sie sich nach Abschluss des Wiederherstellungsprozesses in der Benutzeroberfläche von Unified Manager an.

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

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

Ändern des Backup-Typs

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

Was Sie brauchen

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

Schritte

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

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

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

On-Demand Backup für Unified Manager

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

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

Migration einer virtuellen Unified Manager Appliance zu einem Linux System

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

Was Sie brauchen

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

Authentifizierungseinstellungen auf dem Linux-System. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsprozesses aus.

- Sie müssen über die Stammbenutzeranmeldeinformationen für den Linux-Host verfügen.

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

Schritte

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

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

7. Melden Sie sich als Root-Benutzer beim Linux-Host an, auf dem Unified Manager installiert ist, und kopieren Sie die Backup-Dateien unter Verwendung von SCP aus /Support auf der virtuellen Appliance.`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .`

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

   Stellen Sie sicher, dass Sie die Sicherungsdatei .7z und alle Dateien des .7z-Repository im Unterverzeichnis /Database-Dumps-repo kopiert haben.

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

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

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

Sie sollten die folgenden Aufgaben durchführen:

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

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

Verwalten von Skripten

Mithilfe von Skripten können mehrere Storage-Objekte in Unified Manager automatisch

geändert oder aktualisiert werden. Das Skript ist einer Warnung zugeordnet. Wenn ein Ereignis eine Warnung auslöst, wird das Skript ausgeführt. Sie können benutzerdefinierte Skripts hochladen und deren Ausführung testen, wenn eine Warnung erzeugt wird.

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

Funktionsweise von Skripten mit Warnmeldungen

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

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

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

Das Skript verwendet die folgenden Argumente zur Ausführung:

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

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

Beispiel zum Abrufen von Argumenten aus Skripts

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

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

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

Skripte werden hinzugefügt

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

Was Sie brauchen

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

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

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

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

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

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Scripts**.
2. Klicken Sie auf der Seite **Skripts** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Skript hinzufügen** auf **Durchsuchen**, um die Skriptdatei auszuwählen.

4. Geben Sie eine Beschreibung für das ausgewählte Skript ein.
5. Klicken Sie Auf **Hinzufügen**.

Skripte werden gelöscht

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

Was Sie brauchen

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

Schritte

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

Skriptausführung wird getestet

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

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

Schritte

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

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

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

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

Verwalten und Überwachen von Gruppen

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

Allgemeines zu Gruppen

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

Was eine Gruppe ist

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

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

Funktionsweise von Gruppenregeln für Gruppen

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

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

angehören.

Bestimmten Bedingungen

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

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

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

Storage-Objekttyp	Anwendbare Operanden
Datenmenge	• 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 Volume

Die `Change_capacity_threshold` Gruppenaktion hat immer Vorrang vor der `Change_snapshot_copies` Gruppenaktion und wird auf Volume A angewendet. Wenn Unified Manager einen Überwachungszyklus abgeschlossen hat, werden die Integritätsschwellenwertereignisse von Volume A gemäß der Gruppenaktion neu bewertet `Change_capacity_threshold`. Sie können keinen anderen Volume-Schwellenwerttyp für Gruppenaktion für G1- oder G2-Gruppe konfigurieren.

Hinzufügen von Gruppen

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

Was Sie brauchen

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

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

Schritte

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

Gruppen werden bearbeitet

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

Was Sie brauchen

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppen** die Gruppe aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Gruppe bearbeiten** den Namen, die Beschreibung oder beides für die Gruppe.
4. Klicken Sie Auf **Speichern**.

Gruppen werden gelöscht

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

Was Sie brauchen

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

Schritte

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

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

Gruppenregeln werden hinzugefügt

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

Was Sie brauchen

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.

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

Zu erstellen	Tun Sie das…
Ein Zustand	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:

Schritte

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

Gruppenregeln werden bearbeitet

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

Was Sie brauchen

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

Schritte

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

   Sie können den Zielobjekttyp für eine Gruppenregel nicht ändern.

4. Klicken Sie Auf **Speichern**.

Gruppenregeln werden gelöscht

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

Was Sie brauchen

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

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

Schritte

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

Gruppenaktionen werden hinzugefügt

Sie können Gruppenaktionen konfigurieren, die Sie auf Speicherobjekte in einer Gruppe

anwenden möchten. Durch das Konfigurieren von Aktionen für eine Gruppe sparen Sie Zeit, da Sie diese Aktionen nicht einzeln zu jedem Objekt hinzufügen müssen.

Was Sie brauchen

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

Schritte

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

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

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

Gruppenaktionen werden bearbeitet

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

Was Sie brauchen

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

Schritte

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

Konfigurieren von Schwellenwerten für den Zustand von Volumes für Gruppen

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

Was Sie brauchen

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

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

angewendet.

Schritte

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

Gruppenaktionen werden gelöscht

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

Was Sie brauchen

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

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

Schritte

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

Gruppenaktionen neu anordnen

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

Was Sie brauchen

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

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

Schritte

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

Priorisieren von Storage-Objektereignissen mithilfe von Anmerkungen

Sie können 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.

Was Sie brauchen

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

Schritte

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

Hinzufügen von Werten zu Beschriftungen

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

Was Sie brauchen

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

Sie können vordefinierten Anmerkungen keine Werte hinzufügen.

Schritte

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

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

4. Klicken Sie Auf **Hinzufügen**.

Anmerkungen werden gelöscht

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

Was Sie brauchen

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

Schritte

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

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

Anzeigen der Anmerkungsliste und der Details

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

Schritte

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

Löschen von Werten aus Anmerkungen

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

Was Sie brauchen

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

Werte können nicht aus vordefinierten Anmerkungen gelöscht werden.

Schritte

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

4. Klicken Sie im Dialogfeld **Warnung** auf **Ja**.

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

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.

Was Sie brauchen

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

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

Schritte

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

Zu erstellen…	Tun Sie das…
Ein Zustand	a. Wählen Sie einen Operand aus der Liste der Operanden aus. b. Wählen Sie als Operator entweder **enthält** oder **IS** aus. c. Geben Sie einen Wert ein, oder wählen Sie einen Wert aus der Liste verfügbar aus.

Zu erstellen…	Tun Sie das…
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:

Schritte

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 `svm_data`ein.
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 `vol`ein.
11. Klicken Sie auf **Bedingung hinzufügen**.
12. Wiederholen Sie die Schritte 8 bis 10, indem Sie **Datenpriorität** als Operand in Schritt 8, **ist** als Operator in Schritt 9 und **unternehmenskritisch** als Wert in Schritt 10 auswählen.
13. Klicken Sie Auf **Hinzufügen**.

Anmerkungen manuell zu einzelnen Speicherobjekten hinzufügen

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

Was Sie brauchen

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

Schritte

1. Navigieren Sie zu den Storage-Objekten, die Anmerkungen machen sollen:

So fügen Sie Kommentare hinzu:	Tun Sie das…
Cluster	a. Klicken Sie Auf **Storage** > **Cluster**. b. Wählen Sie ein oder mehrere Cluster aus.
Volumes	a. Klicken Sie Auf **Storage** > **Volumes**. b. Wählen Sie ein oder mehrere Volumes aus.
SVMs	a. Klicken Sie auf **Storage** > **SVMs**. b. Wählen Sie eine oder mehrere SVMs aus.

2. Klicken Sie auf **Annotate** und wählen Sie ein Name-Wert-Paar aus.
3. Klicken Sie Auf **Anwenden**.

Anmerkungsregeln werden bearbeitet

Sie können Anmerkungsregeln bearbeiten, um die Bedingungsgruppen und -Bedingungen innerhalb der Bedingungsgruppe zu ändern, um Anmerkungen zu Speicherobjekten hinzuzufügen oder sie aus ihnen zu entfernen.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Anmerkungen werden vom Speicherobjekt distanziert, wenn Sie die zugehörigen Anmerkungsregeln bearbeiten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungsregeln** die Anmerkungsregel aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Aktionen** > **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Anmerkungsregel bearbeiten** den Regelnamen, den Anmerkungsnamen und den Wert, die Bedingungsgruppen und die Bedingungen nach Bedarf.

   Sie können den Zielobjekttyp für eine Anmerkungsregel nicht ändern.

4. Klicken Sie Auf **Speichern**.

Konfigurieren von Bedingungen für Anmerkungsregeln

Sie können eine oder mehrere Bedingungen konfigurieren, um Anmerkungsregeln zu erstellen, die Unified Manager für die Speicherobjekte anwendet. Die Speicherobjekte,

die die Anmerkungsregel erfüllen, werden mit dem in der Regel angegebenen Wert versehen.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **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:

Schritte

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 `svm_data`ein.
7. Klicken Sie Auf **Hinzufügen**.

Anmerkungsregeln werden gelöscht

Anmerkungsregeln können Sie aus Active IQ Unified Manager löschen, wenn die Regeln nicht mehr benötigt werden.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn Sie eine Anmerkungsregel löschen, wird die Anmerkung getrennt und aus den Speicherobjekten entfernt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.

2. Wählen Sie auf der Registerkarte **Anmerkungsregeln** die Anmerkungsregel aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie im Dialogfeld **Warnung** auf **Ja**, um den Löschvorgang zu bestätigen.

Anmerkungsregeln neu anordnen

Sie können die Reihenfolge ändern, in der Unified Manager Anmerkungsregeln auf Storage-Objekte 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.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können entweder eine einzelne oder mehrere Zeilen auswählen und viele Drag-and-Drop-Vorgänge durchführen, um den Rang der Anmerkungsregeln zu ändern. Sie müssen jedoch die Änderungen speichern, damit die Neupriorisierung auf der Registerkarte Anmerkungsregeln angezeigt werden kann.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungsregeln** auf **Neuordnung**.
3. Ziehen Sie im Dialogfeld **Anmerkungsregel neu anordnen** einzelne oder mehrere Zeilen per Drag-and-Drop, um die Reihenfolge der Anmerkungsregeln neu anzuordnen.
4. Klicken Sie Auf **Speichern**.

   Sie müssen die Änderungen speichern, damit die Neuordnung angezeigt werden kann.

Senden eines Support-Bundles über eine Web-UI und eine Wartungskonsole

Sie sollten ein Support-Bundle senden, wenn das Problem, das Sie haben, detailliertere Diagnose und Fehlerbehebung erfordert als eine AutoSupport-Meldung. Sie können ein Support-Paket über die Unified Manager Web-UI und die Wartungskonsole an den technischen Support senden.

Unified Manager speichert maximal zwei komplette Support Bundles und drei schlanke Support-Bundles gleichzeitig.

Verwandte Informationen

"Unified Manager Benutzer-Rollen und -Funktionen"

Senden von AutoSupport Meldungen und Support Bundles an den technischen Support

Auf der Seite AutoSupport können Sie vordefinierte und On-Demand AutoSupport Meldungen an Ihr technisches Support-Team senden, um einen ordnungsgemäßen Betrieb Ihrer Umgebung zu gewährleisten und die Integrität Ihrer Umgebung zu wahren. AutoSupport ist standardmäßig aktiviert und sollte nicht deaktiviert werden, damit Sie die

Vorteile von NetAppActive IQ nutzen können.

Sie können Diagnosesystem-Informationen und detaillierte Daten zum Unified Manager Server in einer Meldung senden, die bei Bedarf gesendet werden soll, eine Meldung in regelmäßigen Abständen planen oder sogar Support-Bundles an das technische Support-Team generieren und versenden.

> Ein Benutzer mit einer Storage-Administratorrolle kann AutoSupport Meldungen und Support Bundles nach Bedarf an den technischen Support generieren und senden. Jedoch kann nur ein Administrator oder ein Wartungbenutzer periodische AutoSupport aktivieren oder deaktivieren und die HTTP-Einstellungen wie im Abschnitt Einrichten des HTTP-Proxyservers beschrieben konfigurieren. In einer Umgebung, in der ein HTTP Proxy-Server verwendet werden muss, sollte die Konfiguration abgeschlossen sein, bevor ein Storage-Administrator AutoSupport Meldungen und Support Bundles nach Bedarf an den technischen Support senden kann.

Senden von On-Demand AutoSupport Nachrichten

Sie können eine On-Demand-Nachricht an den technischen Support, an einen bestimmten E-Mail-Empfänger oder an beide senden.

Schritte

1. Navigieren Sie zu **Allgemein** > **AutoSupport**, und führen Sie eine oder beide der folgenden Aktionen aus:
2. Wenn Sie die AutoSupport-Nachricht an den technischen Support senden möchten, aktivieren Sie das Kontrollkästchen **an den technischen Support senden**.
3. Wenn Sie die AutoSupport-Nachricht an einen bestimmten E-Mail-Empfänger senden möchten, aktivieren Sie das Kontrollkästchen **an E-Mail-Empfänger** und geben Sie die E-Mail-Adresse des Empfängers ein.
4. Klicken Sie Auf **Speichern**.
5. Klicken Sie auf **AutoSupport generieren und senden**.

Aktivieren von regelmäßigen AutoSupport

Sie können dem technischen Support spezifische, vordefinierte Meldungen zur Fehlerbehebung in regelmäßigen Abständen senden. Diese Funktion ist standardmäßig aktiviert. Wenn diese Option deaktiviert ist, kann ein Administrator oder Wartungsbenutzer die Einstellungen aktivieren.

Schritte

1. Navigieren Sie zu **Allgemein** > **AutoSupport**.
2. Aktivieren Sie im Abschnitt Periodensystem AutoSupport das Kontrollkästchen **AutoSupport-Daten regelmäßig an Active IQ** senden aktivieren.
3. Legen Sie bei Bedarf den Namen, den Port und die Authentifizierungsinformationen für den HTTP-Proxy-Server fest, wie im Abschnitt Einrichten des HTTP-Proxyservers beschrieben.
4. Klicken Sie Auf **Speichern**.

Supportpaket nach Bedarf hochladen

Je nach Anforderung zur Fehlerbehebung können Sie ein Support Bundle an den technischen Support generieren und senden. Unified Manager speichert nur die zwei zuletzt erstellten Support Bundles. Ältere Supportpakete werden aus dem System gelöscht.

Da einige Arten von Support-Daten große Mengen von Cluster-Ressourcen nutzen oder sehr lange in Anspruch nehmen können, wenn Sie das vollständige Support Bundle auswählen, können Sie bestimmte Datentypen ein- oder ausschließen, um die Größe des Support-Pakets zu verringern. Sie haben auch die

Möglichkeit, ein einfaches Support-Bundle zu erstellen, das nur 30 Tage Protokolle und Konfigurationsdatenbanken enthält - es schließt Performancedaten, Erfassungsdateien und Server Heap Dump aus.

Schritte

1. Navigieren Sie zu **Allgemein** > **AutoSupport**.
2. Klicken Sie im Bereich „On-Demand Support Bundle“ auf **Support Bundle generieren und senden**.
3. Um ein leichtes Supportpaket an den technischen Support zu senden, aktivieren Sie im Pop-up-Pop-up-Paket Erzeugen und Senden das Kontrollkästchen**Lichtstützpaket erzeugen**.
4. Wenn Sie ein komplettes Supportpaket senden möchten, aktivieren Sie alternativ das Kontrollkästchen **komplettes Supportpaket erzeugen**. Wählen Sie die spezifischen Datentypen aus, die im Supportpaket enthalten oder ausgeschlossen werden sollen.

   Auch wenn Sie keine Datentypen auswählen, wird das Support-Paket immer noch mit anderen Unified Manager-Daten generiert.

5. Aktivieren Sie das Kontrollkästchen **Paket an technischen Support senden**, um das Paket zu generieren und an den technischen Support zu senden. Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird das Bundle lokal auf dem Unified Manager-Server generiert und gespeichert. Das generierte Supportpaket steht für die spätere Verwendung im Verzeichnis /Support auf VMware-Systemen, in Linux-Systemen und in auf Windows-Systemen `ProgramData\NetApp\OnCommandAppData\ocum\support` zur Verfügung `/opt/netapp/data/support/`.
6. Klicken Sie Auf **Senden**.

Einrichten des HTTP-Proxyservers

Sie können einen Proxy für den Internetzugriff festlegen, um AutoSupport-Inhalte zu unterstützen, falls Ihre Umgebung keinen direkten Zugriff vom Unified Manager-Server bietet. Dieser Abschnitt ist nur für Administrator- und Wartungsbenutzer verfügbar.

- **HTTP Proxy verwenden**

  Aktivieren Sie dieses Kontrollkästchen, um den Server zu identifizieren, der als HTTP-Proxy verwendet wird.

  Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers und die Portnummer ein, die für die Verbindung mit dem Server verwendet wird.

- **Authentifizierung verwenden**

  Aktivieren Sie dieses Kontrollkästchen, wenn Sie Authentifizierungsinformationen für den Zugriff auf den Server angeben müssen, der als HTTP-Proxy verwendet wird.

  Geben Sie den Benutzernamen und das Kennwort ein, das für die Authentifizierung mit dem HTTP-Proxy erforderlich ist.

HTTP-Proxys, die nur grundlegende Authentifizierung bereitstellen, werden nicht unterstützt.

Zugriff auf die Wartungskonsole

Wenn die Benutzeroberfläche von Unified Manager nicht ausgeführt wird oder Sie

Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Wartungskonsole zugreifen, um Ihr Unified Manager System zu verwalten.

Was Sie brauchen

Sie müssen Unified Manager installiert und konfiguriert haben.

Nach 15 Minuten Inaktivität meldet die Wartungskonsole sie aus.

Wenn Sie auf VMware installiert sind und sich bereits über die VMware-Konsole als Wartungsbenutzer angemeldet haben, können Sie sich nicht gleichzeitig mit Secure Shell anmelden.

Schritt

1. Führen Sie die folgenden Schritte aus, um auf die Wartungskonsole zuzugreifen:

Auf diesem Betriebssystem…	Führen Sie die folgenden Schritte aus…
VMware	a. Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domänennamen der virtuellen Unified Manager-Appliance her. b. Melden Sie sich mit Ihrem Wartungs-Benutzernamen und -Passwort an der Wartungskonsole an.
Linux	a. Stellen Sie mithilfe von Secure Shell eine Verbindung mit der IP-Adresse oder dem vollständig qualifizierten Domänennamen des Unified Manager-Systems her. b. Melden Sie sich beim System mit dem Wartungs-Benutzer (umadmin) und dem Passwort an. c. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
Windows	a. Melden Sie sich mit den Administratoranmeldeinformationen beim Unified Manager-System an. b. Starten Sie PowerShell als Windows-Administrator. c. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.

Das Menü der Unified Manager-Wartungskonsole wird angezeigt.

Erstellen und Hochladen eines Supportpakets

Sie können ein Support-Paket mit Diagnoseinformationen erstellen, damit Sie es an den technischen Support senden können, um Hilfe zur Fehlerbehebung zu erhalten.

Wenn Ihr Unified Manager Server ab Unified Manager 9.8 mit dem Internet verbunden ist, können Sie das Support Bundle über die Wartungskonsole auch auf NetApp hochladen.

Was Sie brauchen

Sie müssen als Wartungbenutzer Zugriff auf die Wartungskonsole haben.

Da einige Arten von Support-Daten große Mengen von Cluster-Ressourcen verwenden oder sehr viel Zeit in Anspruch nehmen können, können Sie bei Auswahl des vollständigen Support-Pakets Datentypen angeben, die ein- oder ausschließen sollen, um die Größe des Support-Pakets zu verringern. Sie haben auch die Möglichkeit, ein einfaches Support-Bundle zu erstellen, das nur 30 Tage Protokolle und Konfigurationsdatenbanken enthält - es schließt Performancedaten, Erfassungsdateien und Server Heap Dump aus.

Unified Manager speichert nur die zwei zuletzt erstellten Support Bundles. Ältere Supportpakete werden aus dem System gelöscht.

Schritte

1. Wählen Sie in der Wartungskonsole **Hauptmenü** die Option **Support/Diagnose**.
2. Wählen Sie * Light Support Bundle erzeugen* oder **Support Bundle generieren** abhängig von der Detailebene aus, die Sie im Support Bundle haben möchten.
3. Wenn Sie das vollständige Support-Paket auswählen, wählen Sie die folgenden Datentypen aus, die im Support-Bundle enthalten oder ausschließen sollen:

   - **Datenbankauszug**

     Ein Dump der MySQL Server Datenbank.

   - **Haufendump**

     Ein Snapshot des Status der wichtigsten Unified Manager Serverprozesse. Diese Option ist standardmäßig deaktiviert und sollte nur ausgewählt werden, wenn sie vom Kundendienst angefordert wird.

   - **Aufnahmeaufzeichnungen**

     Eine Aufzeichnung der gesamten Kommunikation zwischen Unified Manager und den überwachten Clustern.

   Wenn Sie die Auswahl aller Datentypen aufheben, wird das Support-Paket immer noch mit anderen Unified Manager-Daten generiert.

4. Geben Sie, ein `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. Geben Sie, ein `y`, und drücken Sie dann die Eingabetaste, um das Supportpaket zu generieren.

Wenn Sie das Supportpaket zu diesem Zeitpunkt nicht generieren möchten, geben Sie, ein `n` und drücken Sie dann die Eingabetaste.

6. Wenn Sie Datenbank-Dump-Dateien in das vollständige Support-Bundle aufgenommen haben, werden Sie aufgefordert, den Zeitraum anzugeben, für den Performance-Statistiken enthalten sein sollen. Das Einführen von Performance-Statistiken kann viel Zeit und Speicherplatz beanspruchen, sodass Sie auch eine Dump-Datenbank ohne inklusive der Performance-Statistiken erstellen können:

   a. Geben Sie das Startdatum im Format YYYYMMDD ein.

      Geben Sie beispielsweise für den 1. Januar 2021 ein `20210101`. Geben Sie ein `n`, wenn keine Performance-Statistiken enthalten sein sollen.

   b. Geben Sie die Anzahl der einzuschließen Tage der Statistik ein, beginnend ab 12 Uhr am angegebenen Startdatum.

      Sie können eine Zahl zwischen 1 und 10 eingeben.

   Wenn Sie Performance-Statistiken vorhalten, zeigt das System den Zeitraum an, für den Performance-Statistiken erfasst werden sollen.

7. Nach Erstellung des Support Bundles werden Sie gefragt, ob Sie es nach NetApp hochladen möchten. Geben Sie, ein `y`, und drücken Sie dann die Eingabetaste.

   Sie werden aufgefordert, Ihre Support-Case-Nummer einzugeben.

8. Wenn Sie bereits eine Case-Nummer haben, geben Sie die Nummer ein, und drücken Sie die Eingabetaste. Anderenfalls drücken Sie einfach die Eingabetaste.

   Das Support Bundle wird auf NetApp hochgeladen.

Wenn Ihr Unified Manager-Server nicht mit dem Internet verbunden ist oder Sie das Support-Paket aus einem anderen Grund nicht hochladen können, können Sie es abrufen und manuell senden. Sie können den Client mit einem SFTP-Client oder unter Verwendung von UNIX- oder Linux-CLI-Befehlen abrufen. Unter Windows-Installationen können Sie Remote Desktop (RDP) verwenden, um das Supportpaket abzurufen.

Das generierte Supportpaket befindet sich im Verzeichnis /Support auf VMware Systemen, in /opt/netapp/Data/Support/ auf Linux Systemen und in ProgramData\NetApp\OnCommandAppData\ocum\Unterstützung auf Windows Systemen.

Verwandte Informationen

"Unified Manager Benutzer-Rollen und -Funktionen"

Abrufen des Support-Pakets über einen Windows-Client

Als Windows-Benutzer können Sie ein Tool herunterladen und installieren, um das Support-Paket von Ihrem Unified Manager-Server abzurufen. Sie können das Support Bundle an den technischen Support senden, um eine detailliertere Diagnose eines Problems zu erhalten. FileZilla oder WinSCP sind Beispiele für Werkzeuge, die Sie verwenden können.

Was Sie brauchen

Sie müssen der Wartungbenutzer sein, um diese Aufgabe ausführen zu können.

Sie müssen ein Werkzeug verwenden, das SCP oder SFTP unterstützt.

Schritte

1. Laden Sie ein Tool herunter und installieren Sie es, um das Support Bundle abzurufen.
2. Öffnen Sie das Werkzeug.
3. Stellen Sie über SFTP eine Verbindung mit dem Unified Manager-Managementserver her.

   Das Tool zeigt den Inhalt des /Support-Verzeichnisses an und Sie können alle bestehenden Support-Bundles anzeigen.
4. Wählen Sie das Zielverzeichnis für das Supportpaket aus, das Sie kopieren möchten.
5. Wählen Sie das Supportpaket aus, das Sie kopieren möchten, und kopieren Sie die Datei vom Unified Manager-Server auf Ihr lokales System.

Abrufen des Support-Pakets über einen UNIX oder Linux Client

Wenn Sie UNIX- oder Linux-Benutzer sind, können Sie das Support Bundle über Ihre vApp abrufen, indem Sie die Befehlszeilenschnittstelle (CLI) auf Ihrem Linux-Client-Server verwenden. Sie können das Supportpaket entweder mit SCP oder SFTP abrufen.

Was Sie brauchen

Sie müssen der Wartungbenutzer sein, um diese Aufgabe ausführen zu können.

Sie müssen ein Support-Bundle mit der Wartungskonsole generiert haben und den Support-Bundle-Namen haben.

Schritte

1. Greifen Sie über Telnet oder die Konsole auf die CLI über Ihren Linux-Client-Server zu.
2. Greifen Sie auf das `/support` Verzeichnis zu.
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 zum Abrufen des Supportpakets verwendet:

```
        `$ scp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
support_bundle_20160216_145359.7z   100%  119MB  11.9MB/s   00:10
```

Im folgenden Beispiel wird SFTP zum Abrufen des Supportpakets verwendet:

```
        `$ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

Senden eines Support Bundle an den technischen Support

Wenn ein Problem detailliertere Diagnose- und Fehlerbehebungsinformationen erfordert als eine AutoSupport Meldung, können Sie ein Support Bundle an den technischen Support senden.

Was Sie brauchen

Sie müssen Zugriff auf das Support-Bundle haben, um es an den technischen Support zu senden.

Sie müssen über die technische Support-Website eine Case-Nummer generiert haben.

Schritte

1. Loggen Sie sich auf der NetApp Support Site ein.
2. Laden Sie die Datei hoch.

   "Wie zum Hochladen einer Datei auf NetApp"

Aufgaben und Informationen im Zusammenhang mit mehreren Workflows

Einige Aufgaben und Referenztexte, die Ihnen helfen, einen Workflow zu verstehen und abzuschließen, sind für viele Workflows in Unified Manager üblich. Dazu gehören das Hinzufügen und Prüfen von Notizen zu einem Ereignis, das Zuweisen eines Ereignisses, das Erkennen und Beheben von Ereignissen sowie Details zu Volumes, Storage Virtual Machines (SVMs), Aggregaten, Und so weiter.

Cluster-Komponenten und warum sie über Konflikte verfügen können

Sie können Probleme mit der Cluster-Performance identifizieren, wenn ein Konflikt zwischen einer Cluster-Komponente besteht. Die Performance der Workloads, die die Komponente nutzen, verlangsamen sich und ihre Reaktionszeit (Latenz) für Client-Anforderungen steigt. Dadurch wird ein Ereignis in Unified Manager ausgelöst.

Eine Komponente, die einen Konflikt verursacht, kann nicht auf einer optimalen Ebene ausgeführt werden. Die Performance ist gesunken, und die Performance anderer Cluster-Komponenten und Workloads, sogenannten *Opfern*, hat möglicherweise eine höhere Latenz zur Verfügung. Um die Konflikte einer Komponente zu beseitigen, müssen Sie ihre Workloads verringern oder die Fähigkeit erhöhen, mehr Arbeit zu erledigen, damit die Performance wieder auf das normale Niveau kommt. Da Unified Manager die Workload-Performance in fünf-Minuten-Intervallen erfasst und analysiert, wird nur erkannt, wenn eine Cluster-Komponente konsistent überlastet ist. Vorübergehende Überlastungsspitzen, die nur für eine kurze Dauer innerhalb des fünfminütigen Intervalls dauern, werden nicht erkannt.

Beispielsweise könnte ein Storage-Aggregat unter Konflikt stehen, da ein oder mehrere Workloads darauf konkurrierende, dass ihre I/O-Anfragen erfüllt werden. Andere Workloads auf dem Aggregat können beeinträchtigt werden, was zu einer Abnahme der Performance führt. Um die Aktivitätsmenge auf dem Aggregat zu verringern, können verschiedene Schritte durchgeführt werden, beispielsweise zum Verschieben von einem oder mehreren Workloads auf ein weniger ausgelastete Aggregat oder Node, um die allgemeinen Workload-Anforderungen des aktuellen Aggregats zu verringern. Bei einer QoS-Richtliniengruppe können Sie das Durchsatzlimit anpassen oder Workloads in eine andere Richtliniengruppe verschieben, sodass die Workloads nicht mehr gedrosselt werden.

Unified Manager überwacht die folgenden Cluster-Komponenten, um bei Engpässen eine Warnung zu erhalten:

- **Netzwerk**

  Zeigt die Wartezeit von I/O-Anfragen durch die externen Netzwerkprotokolle auf dem Cluster an. Die Wartezeit beträgt bis zum Abschluss von „`Transfer ready`“-Transaktionen, bevor das Cluster auf eine I/O-Anforderung reagieren kann. Wenn die Netzwerkkomponente stark betroffen ist, bedeutet dies, dass hohe Wartezeiten auf der Protokollebene die Latenz eines oder mehrerer Workloads beeinflussen.

- * Netzwerkverarbeitung*

  Repräsentiert die Softwarekomponente in dem Cluster, die mit I/O-Verarbeitung zwischen Protokollebene und Cluster beteiligt ist Der Knoten, der die Netzwerkverarbeitung verarbeitet, hat sich seit dem Erkennen des Ereignisses möglicherweise geändert. Wenn die Netzwerkverarbeitungskomponente einen Konflikt verursacht, bedeutet dies, dass eine hohe Auslastung des Node zur Netzwerkverarbeitung die Latenz eines oder mehrerer Workloads beeinträchtigt.

  Wenn Sie in einer aktiv/aktiv-Konfiguration ein All-SAN-Array-Cluster verwenden, wird der Wert für die Netzwerklatenz für beide Nodes angezeigt, sodass Sie überprüfen können, ob die Nodes die Last gleichmäßig teilen.

- **QoS-Limit max.**

  Steht für den maximalen Durchsatz (Spitzenwert) der dem Workload zugewiesenen Richtliniengruppe für Storage Quality of Service (QoS). Wenn die Richtliniengruppe Konflikte hat, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch das festgelegte Durchsatzlimit gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- * QoS Limit Min.*

  Zeigt die Latenz einem Workload an, der durch die dem anderen Workload zugewiesene Mindestmenge für den QoS-Durchsatz (erwartet) verursacht wird. Wenn das QoS-Minimum für bestimmte Workloads den Großteil der Bandbreite verwendet, um den versprochenen Durchsatz zu gewährleisten, werden andere Workloads gedrosselt und es wird mehr Latenz erreicht.

- * Cluster Interconnect*

  Stellt die Kabel und Adapter dar, mit denen die physischen Nodes des Clustern verbunden sind. Wenn die Cluster-Interconnect-Komponente einen Konflikt verursacht, bedeutet dies hohe Wartezeiten bei I/O-Anfragen am Cluster Interconnect, die sich auf die Latenz eines oder mehrerer Workloads auswirken.

- **Datenverarbeitung**

  Zeigt die Softwarekomponente in dem Cluster an, die mit I/O-Verarbeitung zwischen dem Cluster und dem Storage-Aggregat, das den Workload enthält. Der Node, der die Datenverarbeitung verarbeitet, hat sich seit dem Erkennen des Ereignisses geändert. Wenn die Datenverarbeitungkomponente einen Konflikt verursacht, bedeutet dies, dass eine hohe Auslastung am Datenverarbeitungs-Node die Latenz eines oder mehrerer Workloads beeinträchtigt.

- **Volume-Aktivierung**

  Stellt den Prozess dar, der die Nutzung aller aktiven Volumes verfolgt. In großen Umgebungen, in denen mehr als 1000 Volumes aktiv sind, verfolgt dieser Prozess, wie viele kritische Volumes gleichzeitig auf Ressourcen über den Node zugreifen müssen. Wenn die Anzahl gleichzeitiger aktiver Volumes den empfohlenen maximalen Schwellenwert überschreitet, kommt es bei einigen der nicht kritischen Volumes zu einer Latenz, die hier angegeben wurde.

- **MetroCluster Ressourcen**

  Repräsentiert die MetroCluster-Ressourcen, einschließlich NVRAM und Interswitch Links (ISLs), die zur Spiegelung von Daten zwischen Clustern in einer MetroCluster Konfiguration verwendet werden. Wenn die MetroCluster Komponente Konflikte verursacht, bedeutet dies einen hohen Schreibdurchsatz von Workloads auf dem lokalen Cluster oder ein Link-Systemzustandsproblem Auswirkungen auf die Latenz einer oder mehrerer Workloads auf dem lokalen Cluster. Wenn das Cluster nicht in einer MetroCluster-Konfiguration befindet, wird dieses Symbol nicht angezeigt.

- **Aggregate oder SSD Aggregate Ops**

  Repräsentiert das Storage-Aggregat, auf dem die Workloads ausgeführt werden Wenn die Aggregat-Komponente Konflikte verursacht, bedeutet dies, dass eine hohe Auslastung des Aggregats sich auf die Latenz eines oder mehrerer Workloads auswirkt. Ein Aggregat besteht aus allen HDDs oder einer Kombination aus HDDs und SSDs (einem Flash Pool Aggregat) oder einer Kombination aus HDDs und einem Cloud Tier (einem FabricPool Aggregat). Ein „`SSD Aggregat`“ besteht aus allen SSDs (ein All-Flash-Aggregat) oder einer Kombination aus SSDs und einer Cloud Tier (ein FabricPool Aggregat).

- **Cloud-Latenz**

  Stellt die Softwarekomponente in dem Cluster dar, die mit I/O-Verarbeitung zwischen dem Cluster und dem Cloud-Tier beschäftigt ist, auf dem Benutzerdaten gespeichert werden Wenn die Komponente für die Cloud-Latenz aufgrund von Konflikten vorliegen, bedeutet dies, dass sich ein großer Anteil der in der Cloud-Ebene gehosteten Lesevorgänge auf die Latenz eines oder mehrerer Workloads auswirkt.

- **Sync SnapMirror**

Repräsentiert die Software-Komponente in dem Cluster, die mit der Replizierung von Benutzerdaten vom primären Volume auf das sekundäre Volume in einer SnapMirror Synchronous-Beziehung beteiligt ist Wenn die synchrone SnapMirror Komponente Konflikte verursacht, bedeutet dies, dass die Aktivitäten des synchronen Betriebs von SnapMirror sich auf die Latenz eines oder mehrerer Workloads auswirken.

Seite „Volume/Health Details“

Auf der Seite Volume/Health Details können Sie ausführliche Informationen zu einem ausgewählten Volume anzeigen, z. B. Kapazität, Storage-Effizienz, Konfiguration, Sicherung, Kommentare und erzeugte Ereignisse. Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für dieses Volume anzeigen.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für das ausgewählte Volume ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Ermöglicht die Navigation zur Seite Volume-/Performance-Details.

- **Aktionen**
  - Alarm Hinzufügen

    Ermöglicht das Hinzufügen einer Warnmeldung zum ausgewählten Volume.

  - Schwellenwerte Bearbeiten

    Ermöglicht das Ändern der Schwellenwerteinstellungen für das ausgewählte Volume.

  - Anmerkungen Hinzufügen

    Ermöglicht Ihnen, das ausgewählte Volume mit Anmerkungen zu versehen.

  - Sichern

    Ermöglicht die Erstellung von SnapMirror oder SnapVault Beziehungen für das ausgewählte Volume.

  - Beziehung

    Ermöglicht Ihnen die Ausführung folgender Sicherungsbeziehungsvorgänge:

    - Bearbeiten

      Öffnet das Dialogfeld „Beziehung bearbeiten“, in dem Sie vorhandene SnapMirror Richtlinien, Zeitpläne und maximale Übertragungsraten für eine vorhandene Sicherungsbeziehung ändern können.

    - Abbrechen

      Bricht Transfers ab, die für eine ausgewählte Beziehung in Bearbeitung sind. Optional können Sie den Checkpoint beim Neustart für andere Transfers als den Basistransfer entfernen. Sie können

den Kontrollpunkt für einen Basistransfer nicht entfernen.

- Stilllegen

  Zeitweilige Aktualisierungen für eine ausgewählte Beziehung werden vorübergehend deaktiviert. Transfers, die bereits in Bearbeitung sind, müssen vor der Stilllegung abgeschlossen werden.

- Pause

  Bricht die Beziehung zwischen Quell- und Zielvolumen ab und ändert das Ziel in ein Lese-Schreib-Volume.

- Entfernen

  Löscht dauerhaft die Beziehung zwischen der ausgewählten Quelle und dem ausgewählten Ziel. Die Volumes werden nicht zerstört und die Snapshot-Kopien auf den Volumes werden nicht entfernt. Dieser Vorgang kann nicht rückgängig gemacht werden.

- Fortsetzen

  Ermöglicht geplante Transfers für eine stillgelegte Beziehung. Beim nächsten geplanten Transferintervall wird ein Neustart-Checkpoint verwendet, falls vorhanden.

- Neu Synchronisieren

  Ermöglicht Ihnen die Neusynchronisierung einer zuvor unterbrochenen Beziehung.

- Initialisierung/Aktualisierung

  Ermöglicht Ihnen, eine erste Basistransfer für eine neue Schutzbeziehung durchzuführen oder eine manuelle Aktualisierung durchzuführen, wenn die Beziehung bereits initialisiert ist.

- Reverse Resync

  Ermöglicht Ihnen die Wiederherstellung einer zuvor unterbrochenen Schutzbeziehung, indem Sie die Funktion von Quelle und Ziel umkehren, indem Sie der Quelle eine Kopie des ursprünglichen Ziels machen. Der Inhalt der Quelle wird durch den Inhalt des Ziels überschrieben, und alle Daten, die neuer als die Daten der gemeinsamen Snapshot Kopie sind, werden gelöscht.

◦ Wiederherstellen

Ermöglicht Ihnen die Wiederherstellung von Daten von einem Volume auf einem anderen Volume. Weitere Informationen finden Sie unter "Wiederherstellen von Daten mithilfe der Seite Volume / Health Details".

Die Schaltfläche „Wiederherstellen“ und die Schaltflächen zum Beziehungsvorgang stehen für Volumes, die sich in synchronen Schutzbeziehungen befinden, nicht zur Verfügung.

- **View Volumes**

Ermöglicht Ihnen die Navigation zur Ansicht „Systemzustand: Alle Volumes“.

Registerkarte „Kapazität“

Auf der Registerkarte Kapazität werden Details zum ausgewählten Volume angezeigt, z. B. seine physische Kapazität, logische Kapazität, Schwellwerte, Kontingentkapazität und Informationen über jede beliebige Volume-Verschiebung:

- **Kapazität Physisch**

  Detaillierte Informationen zur physischen Kapazität des Volumes:

  - Snapshot-Überlauf

    Zeigt den Speicherplatz an, der von den Snapshot Kopien verbraucht wird.

  - Verwendet

    Zeigt den Speicherplatz an, der von Daten im Volume verwendet wird.

  - Warnung

    Zeigt an, dass der Speicherplatz im Volume fast voll ist. Wird diese Schwelle nicht erreicht, wird das Ereignis „Space Fast Full“ generiert.

  - Fehler

    Zeigt an, dass der Speicherplatz im Volume voll ist. Wird dieser Schwellenwert nicht erreicht, wird das Ereignis „Space Full“ generiert.

  - Nicht Nutzbar

    Zeigt an, dass der risikobehaftete Speicherplatz des Thin Provisioning Volume generiert wird und dass der Speicherplatz im Thin Provisioning Volume aufgrund von Kapazitätsproblemen im Aggregat gefährdet ist. Die nicht nutzbare Kapazität wird nur für Volumes angezeigt, die über Thin Provisioning bereitgestellt wurden.

  - Datendiagramm

    Zeigt die Gesamtkapazität und die genutzte Datenkapazität des Volume an.

    Wenn Autogrow aktiviert ist, wird im Datendiagramm der verfügbare Speicherplatz im Aggregat angezeigt. Das Datendiagramm zeigt den effektiven Speicherplatz, der von Daten auf dem Volume genutzt werden kann. Dies kann einer der folgenden Werte sein:

    - Tatsächliche Datenkapazität des Volumes für die folgenden Bedingungen:
      - Autogrow ist deaktiviert.
      - Das autogrow-fähige Volume hat die maximale Größe erreicht.
      - Autogrow-aktivierte Volumes mit Thick Provisioning können nicht weiter wachsen.
    - Datenkapazität des Volumes unter Berücksichtigung der maximalen Volume-Größe (für Volumes mit Thin Provisioning und für Thick Provisioning Volumes, wenn das Aggregat über genügend Platz für das Volume verfügt, um die maximale Größe zu erreichen)
    - Datenkapazität des Volumes nach Berücksichtigung der nächsten möglichen Autogrow Größe (für Thick Provisioning Volumes, die einen Autogrow-Prozentwert haben)

  - Diagramm Snapshot Kopien

Dieses Diagramm wird nur angezeigt, wenn die verwendete Snapshot-Kapazität oder die Snapshot-Reserve nicht null ist.

Beide Diagramme zeigen die Kapazität an, um die die Snapshot-Kapazität die Snapshot-Reserve überschreitet, wenn die verwendete Snapshot-Kapazität die Snapshot-Reserve überschreitet.

- **Kapazität Logisch**

  Zeigt die logischen Platzeigenschaften des Volumes an. Der logische Speicherplatz gibt die tatsächliche Größe der auf Festplatte gespeicherten Daten an, ohne dabei die Einsparungen durch die ONTAP Storage-Effizienztechnologien zu verwenden.

  - Bericht Zu Logischem Speicherplatz

    Zeigt an, ob für das Volume ein Bericht über den logischen Speicherplatz konfiguriert ist. Der Wert kann aktiviert, deaktiviert oder nicht zutreffend sein. „`not anwendbare`“ wird für Volumes auf älteren ONTAP-Versionen oder auf Volumes angezeigt, die kein logisches Speicherplatz-Reporting unterstützen.

  - Verwendet

    Zeigt die Menge des logischen Speicherplatzes an, der von Daten im Volume verwendet wird, und den Prozentsatz des logischen Speicherplatzes, der basierend auf der Gesamtkapazität genutzt wird.

  - Durchsetzung Des Logischen Speicherplatzes

    Zeigt an, ob die Durchsetzung des logischen Speicherplatzes für über Thin Provisioning bereitgestellte Volumes konfiguriert ist. Bei Einstellung auf aktiviert kann die verwendete logische Größe des Volumes nicht größer sein als die aktuell eingestellte physische Volume-Größe.

- **Autogrow**

  Zeigt an, ob das Volumen automatisch wächst, wenn es nicht mehr genügend Speicherplatz hat.

- * Raumgarantie*

  Zeigt die FlexVol-Lautstärkeregelung an, wenn ein Volume freie Blöcke aus einem Aggregat entfernt. Diese Blöcke sind dann garantiert für Schreibvorgänge auf Dateien im Volume verfügbar. Die Speicherplatzgarantie kann auf eine der folgenden gesetzt werden:

  - Keine

    Es wurde keine Speicherplatzzusage für das Volume konfiguriert.

  - Datei

    Die vollständige Größe von dünn geschriebenen Dateien (zum Beispiel LUNs) ist garantiert.

  - Datenmenge

    Die volle Größe des Volumens wird garantiert.

  - Teilweise

    Das FlexCache-Volume reserviert basierend auf seiner Größe Speicherplatz. Wenn die Größe des FlexCache-Volumes 100 MB oder mehr ist, ist die Mindestplatzgarantie standardmäßig auf 100 MB

gesetzt. Wenn die Größe des FlexCache-Volumes weniger als 100 MB ist, wird die Mindestplatzgarantie auf die Größe des FlexCache-Volumes gesetzt. Wenn die Größe des FlexCache-Volumes später erhöht wird, wird die Mindestplatzgarantie nicht erhöht.

Die Speicherplatzzusage ist ein Teil, wenn es sich um ein Volume vom Typ Data-Cache handelt.

- **Details (Physisch)**

  Zeigt die physischen Merkmale des Volumes an.

- **Gesamtkapazität**

  Zeigt die gesamte physische Kapazität im Volume an.

- **Datenkapazität**

  Zeigt den vom Volume genutzten physischen Speicherplatz (genutzte Kapazität) und die Menge an verfügbarem (freier Kapazität) physischen Speicherplatz im Volume an. Diese Werte werden auch als Prozentsatz der gesamten physischen Kapazität angezeigt.

  Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, wird die vom Volume verwendete Menge an Speicherplatz (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht verwendet werden kann (nicht nutzbare Kapazität), da die Kapazität des Aggregats angezeigt wird.

- **Snapshot Reserve**

  Zeigt die Menge an Speicherplatz an, der von den Snapshot Kopien verwendet (genutzte Kapazität) und die Menge an Speicherplatz, die für Snapshot Kopien verfügbar ist (freie Kapazität) im Volume an. Diese Werte werden auch als Prozentsatz der gesamten Snapshot-Reserve angezeigt.

  Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, dann wird die Menge an Speicherplatz, der von den Snapshot Kopien verwendet wird (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht für die Erstellung von Snapshot Kopien verwendet werden kann (nicht nutzbare Kapazität). Aufgrund von Aggregat-Kapazitätsproblemen wird angezeigt.

- **Volumenschwellwerte**

  Zeigt die folgenden Schwellenwerte für die Volume-Kapazität an:

  - Nahezu Vollständig. Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Volumen fast voll ist.

  - Vollständiger Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Volume voll ist.

- **Weitere Details**

  - Autogrow Maximalgröße

    Zeigt die maximale Größe an, bis die Lautstärke automatisch erweitert werden kann. Der Standardwert

ist 120 % der Volume-Größe bei der Erstellung. Dieses Feld wird nur angezeigt, wenn Autogrow für das Volume aktiviert ist.

- Der Qtree Kontingent Verplante Kapazität

  Zeigt den Speicherplatz an, der in den Quoten reserviert wurde.

- Qtree-Kontingent Überbeansprucht Kapazität

  Zeigt die Menge an Speicherplatz an, die verwendet werden kann, bevor das System das überverplante Ereignis des Volume Qtree-Kontingents generiert.

- Fraktionale Reserve

  Steuert die Größe der Überschreibungsreserve. Standardmäßig ist die fraktionale Reserve auf 100 festgelegt und gibt an, dass 100 Prozent des erforderlichen reservierten Speicherplatzes reserviert werden, damit die Objekte für Überschreibungen vollständig gesichert sind. Wenn die fraktionale Reserve weniger als 100 Prozent beträgt, wird der reservierte Speicherplatz für alle platzreservierten Dateien in diesem Volume auf den Prozentsatz der fraktionalen Reserve reduziert.

- Tägliche Snapshot Wachstumsrate

  Zeigt die Änderung an (in Prozent oder in KB, MB, GB usw.), die alle 24 Stunden in den Snapshot Kopien des ausgewählten Volumes stattfindet.

- Snapshot Tage voll belegt

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor der für die Snapshot Kopien im Volume reservierte Speicherplatz den angegebenen Schwellenwert erreicht.

  Das Feld „Snapshot Days to Full“ zeigt einen nicht anwendbaren Wert an, wenn das Wachstum der Snapshot-Kopien im Volume null oder negativ ist oder wenn es keine Daten zur Berechnung der Wachstumsrate gibt.

- Snapshot Automatisch Löschen

  Gibt an, ob Snapshot Kopien automatisch in freien Speicherplatz gelöscht werden, wenn ein Schreibvorgang auf ein Volume aufgrund von fehlendem Speicherplatz im Aggregat ausfällt.

- Snapshots

  Zeigt Informationen über die Snapshot-Kopien im Volume an.

  Die Anzahl der Snapshot Kopien auf dem Volume wird als Link angezeigt. Wenn Sie auf den Link klicken, werden die Snapshot Kopien in dem Dialogfeld Volume geöffnet, in dem Details zu den Snapshot Kopien angezeigt werden.

Die Anzahl der Snapshot Kopien wird etwa jede Stunde aktualisiert. Die Liste der Snapshot-Kopien wird jedoch zu dem Zeitpunkt aktualisiert, zu dem Sie auf das Symbol klicken. Dies kann zu einem Unterschied zwischen der in der Topologie angezeigten Anzahl der Snapshot Kopien und der Anzahl der aufgelisteten Snapshot Kopien führen, wenn Sie auf das Symbol klicken.

- **Volume Move**

  Zeigt den Status der aktuellen oder der letzten Volume-Verschiebung an, die am Volume durchgeführt wurde, und weitere Details an, z. B. die aktuelle Phase der Verschiebung eines Volumes – im Gange ist,

das Quellaggregat, das Zielaggregat, die Startzeit, die Endzeit, Und die geschätzte Endzeit.

Zeigt außerdem die Anzahl der Vorgänge zum Verschieben von Volumes an, die auf dem ausgewählten Volume ausgeführt werden. Weitere Informationen über die Vorgänge zum Verschieben von Volumes erhalten Sie, indem Sie auf den Link **Protokoll zum Verschieben von Volumes** klicken.

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration werden Details zum ausgewählten Volume angezeigt, z. B. Richtlinie für den Export, RAID-Typ, Kapazität und Storage-Effizienz-Funktionen des Volumes:

- **Übersicht**
  - Vollständiger Name

    Zeigt den vollständigen Namen des Volumes an.

  - Aggregate

    Zeigt den Namen des Aggregats, auf dem sich das Volume befindet, oder die Anzahl der Aggregate an, auf denen sich das FlexGroup Volume befindet.

  - Tiering-Richtlinie

    Zeigt die Tiering-Richtlinie für das Volume an; wenn das Volume auf einem FabricPool-fähigen Aggregat implementiert wird. Die Richtlinie kann „Keine“, „nur Snapshot“, „Backup“, „automatisch“ oder „Alle“ lauten.

  - Storage-VM

    Zeigt den Namen der SVM an, die das Volume enthält.

  - Verbindungspfad

    Zeigt den Status des Pfads an, der aktiv oder inaktiv sein kann. Der Pfad in der SVM, auf den das Volume angehängt ist, wird ebenfalls angezeigt. Sie können auf den Link **Verlauf** klicken, um die letzten fünf Änderungen am Verbindungspfad anzuzeigen.

  - Exportrichtlinie

    Zeigt den Namen der Exportrichtlinie an, die für das Volume erstellt wurde. Über den Link können Sie Details zu den Exportrichtlinien, den Authentifizierungsprotokollen und den aktivierten Zugriff auf die Volumes anzeigen, die zu der SVM gehören.

  - Stil

    Zeigt den Volumenstil an. Der Volume-Stil kann FlexVol oder FlexGroup sein.

  - Typ

    Zeigt den Typ des ausgewählten Volumens an. Der Volume-Typ kann Lese-/Schreibvorgänge, Lastverteilung, Datensicherung, Daten-Cache oder temporär sein.

  - RAID-Typ

    Zeigt den RAID-Typ des ausgewählten Volumes an. Der RAID-Typ kann RAID0, RAID4, RAID-DP oder

RAID-TEC sein.

> Es können mehrere RAID-Typen für FlexGroup Volumes angezeigt werden, da sich die zusammengehörigen Volumes für FlexGroups auf Aggregaten unterschiedlicher Typen sein können.

  - SnapLock-Typ

    Zeigt den SnapLock-Typ des Aggregats an, der das Volume enthält.

  - SnapLock Expiry

    Zeigt das Ablaufdatum des SnapLock-Volume an.

- * Kapazität*
  - Thin Provisioning

    Zeigt an, ob Thin Provisioning für das Volume konfiguriert ist.

  - Autogrow

    Zeigt an, ob das flexible Volume automatisch innerhalb eines Aggregats wächst.

  - Snapshot Automatisch Löschen

    Gibt an, ob Snapshot Kopien automatisch in freien Speicherplatz gelöscht werden, wenn ein Schreibvorgang auf ein Volume aufgrund von fehlendem Speicherplatz im Aggregat ausfällt.

  - Kontingente

    Gibt an, ob die Quoten für das Volume aktiviert sind.

- * Effizienz*
  - Komprimierung

    Gibt an, ob die Komprimierung aktiviert oder deaktiviert ist.

  - Deduplizierung

    Gibt an, ob die Deduplizierung aktiviert oder deaktiviert ist.

  - Deduplizierungsmodus

    Gibt an, ob der auf einem Volume aktivierte Deduplizierungsvorgang ein manueller, geplanter oder richtlinienbasierter Vorgang ist. Wenn der Modus auf „geplant“ eingestellt ist, wird der Betriebsplan angezeigt, und wenn der Modus auf eine Richtlinie festgelegt ist, wird der Richtlinienname angezeigt.

  - Deduplizierungsart

    Gibt den Typ des Deduplizierungsvorgangs an, der auf dem Volume ausgeführt wird. Wenn das Volume eine SnapVault-Beziehung hat, wird als SnapVault angezeigt. Für jedes andere Volumen wird der Typ als normal angezeigt.

  - Storage-Effizienzrichtlinie

Gibt den Namen der Storage-Effizienzrichtlinie an, die diesem Volume durch Unified Manager zugewiesen wurde. Diese Richtlinie steuert die Komprimierungs- und Deduplizierungseinstellungen.

- **Schutz**
  - Snapshots

    Gibt an, ob die automatischen Snapshot Kopien aktiviert oder deaktiviert sind.

Registerkarte „Schutz“

Auf der Registerkarte Schutz werden Sicherungsdetails zum ausgewählten Volume angezeigt, z. B. Verzögerungsinformationen, Beziehungstyp und Topologie der Beziehung.

- **Zusammenfassung**

  Zeigt die Eigenschaften der Sicherungsbeziehungen (SnapMirror, SnapVault oder Storage VM DR) für ein ausgewähltes Volume an. Für einen anderen Beziehungstyp wird nur die Eigenschaft Beziehungstyp angezeigt. Wenn ein primäres Volume ausgewählt wird, werden nur die Richtlinie für verwaltete und lokale Snapshot-Kopien angezeigt. Für SnapMirror und SnapVault Beziehungen werden folgende Eigenschaften angezeigt:

  - Quell-Volume

    Zeigt den Namen der Quelle des ausgewählten Volumes an, wenn das ausgewählte Volume ein Ziel ist.

  - Verzögerungsstatus

    Zeigt den Status der Update- oder Transferverzögerungen für eine Schutzbeziehung an. Der Status kann „Fehler“, „Warnung“ oder „kritisch“ sein.

    Der lag-Status gilt nicht für synchrone Beziehungen.

  - Verzögerungsdauer

    Zeigt die Zeit an, mit der die Daten auf dem Spiegel hinter der Quelle liegen.

  - Letzte Erfolgreiche Aktualisierung

    Zeigt Datum und Uhrzeit der letzten erfolgreichen Schutzaktualisierung an.

    Die letzte erfolgreiche Aktualisierung gilt nicht für synchrone Beziehungen.

  - Storage Service-Mitglied

    Zeigt entweder Ja oder Nein an, um anzugeben, ob das Volume zu einem Storage-Service gehört und von diesem gemanagt wird.

  - Versionsflexible Replizierung

    Zeigt entweder Ja, Ja mit Sicherungsoption oder Keine an. Ja zeigt an, dass die SnapMirror Replizierung möglich ist, auch wenn auf Quell- und Ziel-Volumes unterschiedliche Versionen der ONTAP Software ausgeführt werden. Ja, mit der Backup-Option bezeichnet die Implementierung von SnapMirror Sicherung mit der Möglichkeit, mehrere Versionen von Backup-Kopien auf dem Zielsystem aufzubewahren. Keine gibt an, dass die Version Flexible Replikation nicht aktiviert ist.

- Beziehungsfähigkeit

  Zeigt die ONTAP-Funktionen an, die für die Sicherungsbeziehung verfügbar sind.

- Protection Service

  Zeigt den Namen des Schutzdienstes an, wenn die Beziehung von einer Schutzpartneranwendung verwaltet wird.

- Beziehungstyp

  Zeigt alle Beziehungstypen an, einschließlich Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync, Und Synchronisierung.

- Beziehungsstatus

  Zeigt den Status der SnapMirror oder SnapVault Beziehung an. Der Staat kann ohne Initialisierung, SnapMirrored oder Abbruch erfolgen. Wenn ein Quell-Volume ausgewählt ist, ist der Beziehungsstatus nicht zutreffend und wird nicht angezeigt.

- Übertragungsstatus

  Zeigt den Übertragungsstatus der Schutzbeziehung an. Der Übertragungsstatus kann einer der folgenden Werte sein:

  - Wird Abgebrochen

    SnapMirror-Transfers sind aktiviert; ein Vorgang, bei dem der Transfer abgebrochen wird, während das Checkpoint entfernt wird.

  - Prüfen

    Das Zielvolumen wird einer Diagnose-Prüfung unterzogen und es wird keine Übertragung durchgeführt.

  - Abschließen

    SnapMirror Transfers sind aktiviert. Das Volume befindet sich derzeit in der Phase nach dem Transfer für inkrementelle SnapVault Transfers.

  - Leerlauf

    Transfers sind aktiviert, und es wird keine Übertragung durchgeführt.

  - Synchronisiert

    Die Daten in den beiden Volumes in der synchronen Beziehung werden synchronisiert.

  - Out-of-Sync

    Die Daten im Ziel-Volume werden nicht mit dem Quell-Volume synchronisiert.

  - Vorbereitung

    SnapMirror Transfers sind aktiviert. Das Volume befindet sich derzeit in der Phase vor der Übertragung für inkrementelle SnapVault Transfers.

- Warteschlange

  SnapMirror Transfers sind aktiviert. Es werden keine Transfers durchgeführt.

- Stillgelegt

  SnapMirror Transfers sind deaktiviert. Es wird keine Übertragung durchgeführt.

- Wird Stillgelegt

  Ein SnapMirror Transfer läuft. Zusätzliche Transfers sind deaktiviert.

- Übertragung

  SnapMirror Transfers sind aktiviert, und ein Transfer läuft.

- Übergang

  Der asynchrone Datentransfer aus dem Quell- zum Ziel-Volume ist abgeschlossen, und der Übergang zum synchronen Betrieb wurde gestartet.

- Warten

  Ein SnapMirror Transfer wurde initiiert, aber einige zugehörige Aufgaben warten darauf, in die Warteschlange verschoben zu werden.

◦ Max. Übertragungsrate

Zeigt die maximale Übertragungsrate für die Beziehung an. Die maximale Übertragungsrate kann ein numerischer Wert in Kilobyte pro Sekunde (Kbit/s), Megabyte pro Sekunde (Mbit/s), Gigabyte pro Sekunde (Gbit/s) oder Terabyte pro Sekunde (Tbit/s) sein. Wenn kein Limit angezeigt wird, ist die Basistransfer zwischen Beziehungen unbegrenzt.

◦ SnapMirror Richtlinie

Zeigt die Schutzrichtlinie für das Volume an. DPDefault gibt die standardmäßige Richtlinie für den Schutz der asynchronen Spiegelung an, XDPDefault gibt die standardmäßige asynchrone Vault-Richtlinie an, und DPSyncStandard gibt die standardmäßige asynchrone MirrorVault-Richtlinie an. StrictSync gibt die standardmäßige Richtlinie für den synchronen strengen Schutz an, und Sync gibt die standardmäßige synchrone Richtlinie an. Sie können auf den Richtliniennamen klicken, um die mit dieser Richtlinie verknüpften Details anzuzeigen, einschließlich der folgenden Informationen:

- Übertragungspriorität
- Einstellung der Zugriffszeit ignorieren
- Limit für Versuche
- Kommentare
- SnapMirror-Labels
- Aufbewahrungseinstellungen
- Tatsächliche Snapshot Kopien
- Bewahren Sie Snapshot Kopien auf
- Schwellenwert für Warnung bei Aufbewahrung

        - Snapshot-Kopien ohne Aufbewahrungseinstellungen in einer kaskadierenden SnapVault-Beziehung, wobei die Quelle ein Datensicherungs-Volume (DP) ist, gilt nur die Regel „`sm_created`“.
    - Zeitplan Aktualisieren

      Zeigt den SnapMirror Zeitplan an, der der Beziehung zugewiesen ist. Wenn Sie den Cursor über das Informationssymbol positionieren, werden die Terminplandetails angezeigt.

    - Lokale Snapshot-Richtlinie

      Zeigt die Snapshot Kopie-Richtlinie für das Volume an. Die Richtlinie ist Standard, Keine oder ein beliebiger Name, der einer benutzerdefinierten Richtlinie zugewiesen wurde.

    - Geschützt Durch

      Zeigt den Schutztyp an, der für das ausgewählte Volume verwendet wird. Wenn ein Volume z. B. durch Konsistenzgruppe und SnapMirror Volume-Beziehungen geschützt ist, wird in diesem Feld sowohl SnapMirror als auch die Konsistenzgruppe angezeigt. Dieses Feld enthält auch einen Link, über den Sie zur Seite „Beziehungen“ weitergeleitet werden, um den Status einer einheitlichen Beziehung anzuzeigen. Der Link gilt nur für zusammengebende Beziehungen.

    - Konsistenzgruppe

      Für Volumes, die durch aktive SnapMirror-Synchronisierungsbeziehungen geschützt sind, zeigt diese Spalte die Konsistenzgruppe des Volumes an.

- **Ausblick**

  Zeigt die Schutztopologie des ausgewählten Volumes an. Die Topologie enthält grafische Darstellungen aller Volumes, die sich auf das ausgewählte Volume beziehen. Das ausgewählte Volumen wird durch einen dunkelgrauen Rahmen angezeigt, und Linien zwischen Volumes in der Topologie geben den Schutzbeziehungstyp an. Die Richtung der Beziehungen in der Topologie wird von links nach rechts angezeigt, wobei die Quelle jeder Beziehung auf der linken Seite und das Ziel auf der rechten Seite.

  Zweifett gedruckte Zeilen geben eine asynchrone Spiegelbeziehung an. Eine einzelne, fett gedruckte Zeile gibt eine asynchrone Vault-Beziehung an, doppelte Einzelzeilen geben eine asynchrone MirrorVault-Beziehung an, und eine fettgedruckte Zeile und eine nicht fettgedruckte Zeile gibt eine synchrone Beziehung an. Die folgende Tabelle gibt an, ob die synchrone Beziehung StrictSync oder Sync ist.

  Durch Klicken mit der rechten Maustaste auf ein Volume wird ein Menü angezeigt, aus dem Sie entweder das Volume schützen oder Daten darauf wiederherstellen können. Mit der rechten Maustaste auf eine Beziehung klicken wird ein Menü angezeigt, aus dem Sie entweder bearbeiten, abbrechen, stilllegen, brechen, entfernen, Oder nehmen Sie eine Beziehung wieder auf.

  Die Menüs werden in den folgenden Fällen nicht angezeigt:

    - Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operatorrechte verfügen
    - Wenn sich das Volume in einer synchronen Schutzbeziehung befindet
    - Wenn die Volume-ID unbekannt ist, z. B. wenn eine Intercluster-Beziehung vorliegt und das Ziel-Cluster noch nicht erkannt wurde, wird durch Klicken auf ein anderes Volume in der Topologie Informationen für das entsprechende Volume ausgewählt und angezeigt. Ein Fragezeichen ( ) in der oberen linken Ecke eines Volumens zeigt an, dass entweder das Volume fehlt oder noch nicht erkannt 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. Durch Klicken auf ein Snapshot-Kopie-Symbol () wird die Liste der Snapshot Kopien für ein Volume angezeigt. 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 Beziehungsübertragung und die Größe der eingehenden Beziehungsübertragung. Die Verlaufsdaten werden nur angezeigt, wenn Sie ein Zielvolume auswählen. Wenn Sie ein primäres Volume auswählen, sind die Diagramme leer und die Meldung Keine Daten gefunden wird angezeigt. Wenn die Volumes durch eine

Konsistenzgruppe und synchrone SnapMirror Beziehungen geschützt sind, werden die Informationen für die Dauer der Beziehungsübertragung und die Größe der Beziehungsübertragung nicht angezeigt.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Historische Grafiken können Ihnen bei der Identifizierung von Trends helfen: Wenn zum Beispiel große Datenmengen zur gleichen Zeit des Tages oder der Woche übertragen werden oder wenn der lag-Warn- oder lag-Fehlerschwellenwert konsistent verletzt wird, können Sie geeignete Maßnahmen ergreifen. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

Sicherungsverlauf-Diagramme zeigen die folgenden Informationen an:

- **Beziehungsdauer**

  Anzeige von Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Anzeige von Tagen, Monaten oder Jahren auf der horizontalen Achse (x), abhängig vom ausgewählten Zeitraum. Der obere Wert auf der Y-Achse gibt die maximale Verzögerungsdauer an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. In der orangefarbenen Linie im Diagramm wird der lag-Fehlerschwellenwert angezeigt, während die horizontale gelbe Linie den lag-Warnungsschwellenwert darstellt. Wenn Sie den Mauszeiger über diese Zeilen positionieren, wird die Schwellenwerteinstellung angezeigt. Die waagerechte blaue Linie zeigt die Verzögerungsdauer an. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen interessanten Bereich positionieren.

- **Dauer Der Beziehungsübertragung**

  Anzeige von Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Anzeige von Tagen, Monaten oder Jahren auf der horizontalen Achse (x), abhängig vom ausgewählten Zeitraum. Der obere Wert auf der Y-Achse gibt die maximale Übertragungsdauer an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den Bereich von Interesse positionieren.

  Dieses Diagramm ist nicht für Volumes verfügbar, die sich in synchronen Sicherungsbeziehungen befinden.

- **Beziehung Übertragen Größe**

  Zeigt Bytes, Kilobyte, Megabyte usw. auf der vertikalen Achse (y) je nach Übertragungsgröße an und zeigt Tage, Monate oder Jahre auf der horizontalen Achse (x) je nach ausgewähltem Zeitraum an. Der obere Wert auf der Y-Achse gibt die maximale Übertragungsgröße an, die im auf der x-Achse angezeigten Zeitraum erreicht wurde. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen interessanten Bereich positionieren.

  Dieses Diagramm ist nicht für Volumes verfügbar, die sich in synchronen Sicherungsbeziehungen befinden.

Historienbereich

Im Bereich Verlauf werden Diagramme angezeigt, die Informationen über die Kapazität und die Platzreservierungen des ausgewählten Volumes enthalten. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

Diagramme sind möglicherweise leer und die Meldung Keine Daten gefunden, die angezeigt werden, wenn die

Daten oder der Status des Volumes für einen bestimmten Zeitraum unverändert bleiben.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Verlaufsdiagramme können Ihnen dabei helfen, Trends zu erkennen - wenn beispielsweise die Volumennutzung den Schwellenwert „nahezu voll“ konsistent überschreitet, können Sie entsprechende Maßnahmen ergreifen.

Verlaufsdiagramme zeigen folgende Informationen an:

- **Verwendete Volume-Kapazität**

  Zeigt die verwendete Kapazität im Volume und den Trend in der Art und Weise an, wie die Volume-Kapazität basierend auf dem Nutzungsverlauf verwendet wird, als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende zu „Volume Used Capacity“ klicken, wird die Zeile des Diagramms „Volume Used Capacity“ ausgeblendet.

- **Verwendete Volume-Kapazität vs Gesamt**

  Zeigt den Trend der Volume-Kapazität basierend auf dem Nutzungsverlauf sowie der verwendeten Kapazität, der Gesamtkapazität und den Details der Speicherersparnis durch Deduplizierung und Komprimierung an. Dies sind Liniendiagramme in Byte, Kilobyte, Megabyte, Und so weiter, auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „verwendete Trend-Kapazität“ klicken, wird das Diagramm „verwendete Trendkapazität“ ausgeblendet.

- **Verwendete Volume-Kapazität (%)**

  Zeigt die verwendete Kapazität im Volumen und den Trend in der Art und Weise an, wie die Volume-Kapazität basierend auf dem Nutzungsverlauf, als Liniendiagramme, in Prozent, auf der vertikalen (y) Achse verwendet wird. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende zu „Volume Used Capacity“ klicken, wird die Zeile des Diagramms „Volume Used Capacity“ ausgeblendet.

- **Verwendete Snapshot-Kapazität (%)**

  Zeigt den Schwellenwert für die Snapshot-Reserve und die Snapshot-Warnung als Liniendiagramme und die von den Snapshot Kopien verwendete Kapazität als Diagramm in Prozent auf der vertikalen Achse (y) an. Der Snapshot-Überlauf ist mit verschiedenen Farben dargestellt. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende der Snapshot Reserve klicken, wird die Grafik der Snapshot Reserve ausgeblendet.

Ereignisliste

In der Ereignisliste werden Details zu neuen und bestätigten Ereignissen angezeigt:

- **Severity**

  Zeigt den Schweregrad des Ereignisses an.

- **Veranstaltung**

  Zeigt den Ereignisnamen an.

- **Auslösezeit**

  Zeigt die Zeit an, die seit der Erzeugung des Ereignisses verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, zu dem das Ereignis generiert wurde.

Bereich „Verwandte Anmerkungen“

Im Bereich Verwandte Anmerkungen können Sie Anmerkungsdetails anzeigen, die mit dem ausgewählten Volume verknüpft sind. Die Details umfassen den Anmerkungsnamen und die Anmerkungswerte, die auf das Volumen angewendet werden. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie SVMs, Aggregate, qtrees, LUNs und Snapshot Kopien anzeigen und navigieren, die mit dem Volume zusammenhängen:

- **Storage Virtual Machine**

  Zeigt die Kapazität und den Integritätsstatus der SVM an, die das ausgewählte Volume enthält.

- * Aggregat*

  Zeigt die Kapazität und den Integritätsstatus des Aggregats an, das das ausgewählte Volume enthält. Für FlexGroup Volumes wird die Anzahl der Aggregate aufgelistet, die die FlexGroup umfassen.

- **Volumen im Aggregat**

  Zeigt die Anzahl und Kapazität aller Volumes an, die zum übergeordneten Aggregat des ausgewählten Volumes gehören. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt. Wenn beispielsweise ein Aggregat zehn Volumes enthält, von denen fünf den Warnstatus und die übrigen fünf den kritischen Status anzeigen, ist der angezeigte Status kritisch. Diese Komponente wird für FlexGroup-Volumes nicht angezeigt.

- **Qtrees**

  Zeigt die Anzahl der vom ausgewählten Volume enthaltenen qtrees sowie die Kapazität von qtrees mit Kontingent an, die das ausgewählte Volume enthält. Die Kapazität der qtrees mit Kontingent wird in Bezug auf die Volume-Datenkapazität angezeigt. Auf der Grundlage des höchsten Schweregrades wird auch der Integritätsstatus der qtrees angezeigt. Wenn ein Volume beispielsweise zehn qtrees, fünf mit Warnstatus und die verbleibenden fünf mit kritischem Status aufweist, ist der angezeigte Status kritisch.

- **NFS-Shares**

Zeigt die Anzahl und den Status der NFS-Freigaben an, die mit dem Volume verknüpft sind.

- **SMB-Shares**

  Zeigt die Anzahl und den Status der SMB/CIFS-Freigaben an.

- **LUNs**

  Zeigt die Anzahl und Gesamtgröße aller LUNs im ausgewählten Volume an. Auf der Grundlage des höchsten Schweregrades wird außerdem der Systemzustand der LUNs angezeigt.

- **Benutzer- und Gruppenquoten**

  Zeigt die Anzahl und den Status der Quoten für Benutzer und Benutzergruppen im Zusammenhang mit dem Volume und seinen qtrees an.

- **FlexClone Volumes**

  Zeigt die Anzahl und Kapazität aller geklonten Volumes des ausgewählten Volumes an. Anzahl und Kapazität werden nur angezeigt, wenn das ausgewählte Volume geklonte Volumes enthält.

- **Parent Volume**

  Zeigt den Namen und die Kapazität des übergeordneten Volume eines ausgewählten FlexClone Volume an. Das übergeordnete Volume wird nur angezeigt, wenn das ausgewählte Volume ein FlexClone Volume ist.

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ können Sie die Liste der Gruppen anzeigen, die dem ausgewählten Volume zugeordnet sind.

Bereich „Verwandte Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnmeldungen anzeigen, die für das ausgewählte Volume erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Storage VM / Health Details Seite

Sie können auf der Seite Storage VM / Health Details ausführliche Informationen über die ausgewählte Storage-VM anzeigen, z. B. Systemzustand, Kapazität, Konfiguration, Datenrichtlinien, logische Schnittstellen (LIFs), LUNs, qtrees, Benutzer, User Group Quotas und Sicherungsdetails . Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für die Storage-VM anzeigen.

Sie können nur Storage VM überwachen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für die ausgewählte Storage-VM ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Ermöglicht Ihnen die Navigation zur Seite Storage VM / Performance Details.

- **Aktionen**
  - Alarm Hinzufügen

    Ermöglicht Ihnen das Hinzufügen einer Warnung zur ausgewählten Speicher-VM.

  - Anmerkungen Hinzufügen

    Ermöglicht Ihnen, die ausgewählte Storage-VM Anmerkungen zu machen.

- **View Storage VMs**

  Ermöglicht Ihnen die Navigation zur Ansicht „Systemzustand: Alle Storage VMs“.

Registerkarte Systemzustand

Auf der Registerkarte Systemzustand werden detaillierte Informationen zur Datenverfügbarkeit, Datenkapazität und Sicherung verschiedener Objekte wie Volumes, Aggregate, NAS LIFs, SAN LIFs, LUNs, angezeigt. Protokolle, Services, NFS-Freigaben und CIFS-Freigaben.

Sie können auf das Diagramm eines Objekts klicken, um die gefilterte Liste der Objekte anzuzeigen. Beispielsweise können Sie auf das Diagramm für die Volume-Kapazität klicken, das Warnungen anzeigt, um die Liste der Volumes mit Kapazitätsproblemen mit dem Schweregrad „Warnung“ anzuzeigen.

- **Verfügbarkeitsprobleme**

  Zeigt als Diagramm die Gesamtzahl der Objekte an, einschließlich Objekten mit Verfügbarkeitsproblemen und Objekten, die keine Probleme mit der Verfügbarkeit haben. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Verfügbarkeitsproblemen, die sich auf die Verfügbarkeit von Daten in der Storage-VM auswirken oder bereits davon betroffen sein können. Beispielsweise werden Informationen zu den NAS-LIFs und den SAN-LIFs angezeigt, die ausgefallen sind und die Volumes offline sind.

  Zudem können Sie Informationen zu den aktuell ausgeführten Protokollen und Services sowie zur Anzahl und dem Status von NFS- und CIFS-Freigaben anzeigen.

- **Kapazitätsprobleme**

  Zeigt als Diagramm die Gesamtzahl der Objekte an, einschließlich Objekten mit Kapazitätsproblemen und Objekten, die keine Kapazitätsprobleme haben. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Kapazitätsproblemen, die sich auf die Kapazität von Daten in der Storage-VM auswirken oder bereits beeinträchtigen können. Beispielsweise werden Informationen zu Aggregaten angezeigt, die mit hoher Wahrscheinlichkeit die festgelegten Schwellenwerte überschreiten.

- **Schutzprobleme**

  Bietet eine schnelle Übersicht über den Schutz von Storage-VMs, indem die Gesamtzahl der Beziehungen, einschließlich Beziehungen mit Schutzproblemen und Beziehungen, die keine Probleme mit der Sicherung haben, als Feld angezeigt wird. Sie können auch den Status der Storage-VM-DR-Beziehung für die ausgewählte Storage-VM anzeigen. Die Ereignisse für Storage-VM-DR-Beziehungen werden hier angezeigt und durch Klicken auf die Ereignisse gelangen Sie zur Seite mit den Ereignisdetails. Wenn nicht

geschützte Volumes vorhanden sind, führt ein Klick auf den Link zur Ansicht „Systemzustand: Alle Volumes“, in der eine gefilterte Liste der ungeschützten Volumes auf der Storage-VM angezeigt werden kann. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Durch Klicken auf ein Diagramm gelangen Sie zur Beziehungsansicht „Alle Beziehungen“, in der Sie eine gefilterte Liste mit Details zu den Schutzbeziehungen anzeigen können. Die Informationen unten im Diagramm enthalten Details zu Sicherungsproblemen, die sich auf den Schutz von Daten in der Storage-VM auswirken oder bereits davon betroffen sein können. Beispielsweise werden Informationen über Volumes angezeigt, die eine Snapshot Kopie-Reserve haben, die fast voll ist, oder über Probleme mit der SnapMirror Beziehungs-Verzögerung.

Registerkarte „Kapazität“

Auf der Registerkarte Kapazität werden ausführliche Informationen zur Datenkapazität der ausgewählten SVM angezeigt.

Die folgenden Informationen werden für eine Storage-VM mit FlexVol-Volume oder FlexGroup-Volume angezeigt:

- * Kapazität*

  Im Kapazitätsbereich werden Details zur verwendeten und verfügbaren Kapazität angezeigt, die aus allen Volumes zugewiesen sind:

  - Gesamtkapazität

    Zeigt die Gesamtkapazität der Storage-VM an.

  - Verwendet

    Zeigt den Speicherplatz an, der von Daten in den Volumes verwendet wird, die zur Storage-VM gehören.

  - Garantiert Verfügbar

    Zeigt den garantierten verfügbaren Speicherplatz für Daten an, die für Volumes in der Storage-VM verfügbar sind.

  - Nicht Garantiert

    Zeigt den verfügbaren Speicherplatz für Daten an, die in der Storage-VM für Thin Provisioning Volumes zugewiesen sind.

- **Volumen mit Kapazitätsproblemen**

  Die Liste der Volumes mit Kapazitätsproblemen zeigt in tabellarischer Form Details zu den Volumes mit Kapazitätsproblemen an:

  - Status

    Zeigt an, dass das Volumen ein kapazitätsbezogenes Problem mit einem angezeigten Schweregrad hat.

    Sie können den Mauszeiger über den Status bewegen, um weitere Informationen zu dem kapazitätsbezogenen Ereignis oder den für das Volume generierten Ereignissen anzuzeigen.

Wenn der Status des Volumes durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen wurde, und die Ursache des Ereignisses anzeigen. Sie können die Schaltfläche **Details anzeigen** verwenden, um weitere Informationen über die Veranstaltung anzuzeigen.

Wenn der Status des Volumes durch mehrere Ereignisse desselben Schweregrades bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

> Ein Volume kann mehrere Ereignisse desselben Schweregrades oder unterschiedlicher Schweregrade aufweisen. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Volume zwei Ereignisse mit Schweregraden für Fehler und Warnung enthält, wird nur der Schweregrad Fehler angezeigt.

- Datenmenge

  Zeigt den Namen des Volumes an.

- Genutzte Datenkapazität

  Zeigt als Diagramm Informationen zur Auslastung der Volume-Kapazität (in Prozent) an.

- Tage voll

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor das Volume die volle Kapazität erreicht.

- Thin Provisioning

  Zeigt an, ob die Platzgarantie für das ausgewählte Volume festgelegt ist. Gültige Werte sind Ja und Nein

- Aggregate

  Zeigt für FlexVol Volumes den Namen des Aggregats an, das das Volume enthält. Für FlexGroup-Volumes zeigt die Anzahl der Aggregate an, die in der FlexGroup verwendet werden.

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration werden Konfigurationsdetails zur ausgewählten Storage-VM angezeigt, z. B. Cluster, Root-Volume, der zugehörige Volume-Typ (FlexVol-Volumes), Richtlinien und Sicherung, die auf der Storage-VM erstellt wurden:

- **Übersicht**
  - Cluster

    Zeigt den Namen des Clusters an, zu dem die Storage-VM gehört.

  - Zulässiger Volume-Typ

    Zeigt den Typ der Volumes an, die in der Storage-VM erstellt werden können. Der Typ kann FlexVol

oder FlexVol/FlexGroup sein.

- Root-Volume

  Zeigt den Namen des Root-Volumes der Speicher-VM an.

- Zulässige Protokolle

  Zeigt den Typ der Protokolle an, die auf der Storage-VM konfiguriert werden können. Zeigt auch an, ob ein Protokoll up (), down ( ) oder nicht konfiguriert ist ().

- **Datennetzwerkschnittstellen**
  - NAS

    Zeigt die Anzahl der NAS-Schnittstellen an, die der Speicher-VM zugeordnet sind. Zeigt auch an, ob die Schnittstellen up () oder down ( ) sind.

  - San

    Zeigt die Anzahl der SAN-Schnittstellen an, die der Speicher-VM zugeordnet sind. Zeigt auch an, ob die Schnittstellen up () oder down ( ) sind.

  - FC-NVMe

    Zeigt die Anzahl der FC-NVMe-Schnittstellen an, die der Storage-VM zugeordnet sind. Zeigt auch an, ob die Schnittstellen up () oder down ( ) sind.

- **Management-Netzwerk-Schnittstellen**
  - Gesteigerte

    Zeigt die Anzahl der Managementschnittstellen an, die der Storage-VM zugeordnet sind. Zeigt auch an, ob die Management-Schnittstellen auf () oder ab ( ) stehen.

- **Richtlinien**
  - Snapshots

    Zeigt den Namen der Snapshot-Richtlinie an, die auf der Storage-VM erstellt wird.

  - Exportrichtlinien

    Zeigt entweder den Namen der Exportrichtlinie an, wenn eine einzelne Richtlinie erstellt wird, oder zeigt die Anzahl der Exportrichtlinien an, wenn mehrere Richtlinien erstellt werden.

- **Schutz**
  - DR von Storage-VMs

    Zeigt an, ob die ausgewählte Storage-VM geschützt, Ziel oder ungeschützt ist, und den Namen des Ziels, auf dem die Storage-VM geschützt ist. Wenn die ausgewählte Speicher-VM Ziel ist, werden die Details der Quell-Speicher-VM angezeigt. Im Falle eines Fan-out zeigt dieses Feld die Anzahl der gesamten Ziel-Storage-VMs an, auf denen die Speicher-VM geschützt ist. Der Link „count“ führt Sie zum Storage-VM-Beziehungsraster, das auf der Quell-Storage-VM gefiltert ist.

  - Geschützte Volumes

Zeigt die Anzahl der geschützten Volumes auf der ausgewählten Speicher-VM aus den gesamten Volumes an. Wenn Sie eine Ziel-Storage-VM anzeigen, ist der Zahlenlink für die Ziel-Volumes der ausgewählten Speicher-VM.

- Ungesicherte Volumes

  Zeigt die Anzahl der ungeschützten Volumes in der ausgewählten Storage-VM an.

- **Services**
  - Typ

    Zeigt den Servicetyp an, der auf der Storage-VM konfiguriert ist. Der Typ kann Domain Name System (DNS) oder Network Information Service (NIS) sein.

  - Status

    Zeigt den Status des Dienstes an, der auf (), ab ( ) oder nicht konfiguriert ( ) sein kann.

  - Domain-Name

    Zeigt die vollständig qualifizierten Domänennamen (FQDNs) des DNS-Servers für die DNS-Dienste oder NIS-Server für die NIS-Dienste an. Wenn der NIS-Server aktiviert ist, wird der aktive FQDN des NIS-Servers angezeigt. Wenn der NIS-Server deaktiviert ist, wird die Liste aller FQDNs angezeigt.

  - IP-Adresse

    Zeigt die IP-Adressen des DNS- oder NIS-Servers an. Wenn der NIS-Server aktiviert ist, wird die aktive IP-Adresse des NIS-Servers angezeigt. Wenn der NIS-Server deaktiviert ist, wird die Liste aller IP-Adressen angezeigt.

Registerkarte Netzwerkschnittstellen

Auf der Registerkarte Netzwerkschnittstellen werden Details zu den Datennetzwerkschnittstellen (LIFs) angezeigt, die auf der ausgewählten Storage-VM erstellt wurden:

- **Netzwerkschnittstelle**

  Zeigt den Namen der Schnittstelle an, die auf der ausgewählten Speicher-VM erstellt wird.

- **Betriebsstatus**

  Zeigt den Betriebsstatus der Schnittstelle an, der up (), Down () oder Unknown ( ) sein kann. Der Betriebsstatus einer Schnittstelle wird durch den Status ihrer physischen Ports bestimmt.

- **Verwaltungsstatus**

  Zeigt den administrativen Status der Schnittstelle an, der up (), Down () oder Unknown ( ) sein kann. Der Administrationsstatus einer Schnittstelle wird vom Storage-Administrator gesteuert, um Änderungen an der Konfiguration oder zu Wartungszwecken vorzunehmen. Der Administrationsstatus kann sich vom Betriebsstatus unterscheiden. Wenn jedoch der Administrationsstatus einer Schnittstelle „Inaktiv“ lautet, ist der Betriebsstatus standardmäßig „Inaktiv“.

- **IP-Adresse / WWPN**

  Zeigt die IP-Adresse für Ethernet-Schnittstellen und den World Wide Port Name (WWPN) für FC LIFs an.

- **Protokolle**

  Zeigt die Liste der für die Schnittstelle angegebenen Datenprotokolle an, z. B. CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe und FlexCache.

- * Rolle*

  Zeigt die Schnittstellenrolle an. Die Rollen können Daten oder Management sein.

- * Home Port*

  Zeigt den physischen Port an, dem die Schnittstelle ursprünglich zugeordnet war.

- **Aktueller Port**

  Zeigt den physischen Port an, dem die Schnittstelle derzeit zugeordnet ist. Wenn die Schnittstelle migriert wird, unterscheidet sich der aktuelle Port möglicherweise vom Home Port.

- **Portsatz**

  Zeigt den Port-Satz an, dem die Schnittstelle zugeordnet ist.

- **Failover-Richtlinie**

  Zeigt die Failover-Richtlinie an, die für die Schnittstelle konfiguriert ist. Für NFS-, CIFS- und FlexCache-Schnittstellen ist die standardmäßige Failover-Richtlinie Next verfügbar. Failover-Richtlinie gilt nicht für FC- und iSCSI-Schnittstellen.

- **Routing-Gruppen**

  Zeigt den Namen der Routinggruppe an. Sie können weitere Informationen zu den Routen und dem Ziel-Gateway anzeigen, indem Sie auf den Namen der Routinggruppe klicken.

  Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt. Daher wird für diese Cluster eine leere Spalte angezeigt.

- **Failover-Gruppe**

  Zeigt den Namen der Failover-Gruppe an.

Registerkarte „qtrees“

Auf der Registerkarte qtrees werden Details zu qtrees und ihren Kontingenten angezeigt. Sie können auf die Schaltfläche **Schwellenwerte bearbeiten** klicken, wenn Sie die gesundheitlichen Schwellenwerte für qtree-Kapazität für eine oder mehrere qtrees bearbeiten möchten.

Verwenden Sie die Schaltfläche **Export**, um eine kommagetrennte Datei (.csv) zu erstellen, die die Details aller überwachten qtrees enthält. Beim Export in eine CSV-Datei können Sie wahlweise einen qtrees-Bericht für die aktuelle Storage VM, alle Storage VMs im aktuellen Cluster oder alle Storage VMs für alle Cluster im Datacenter erstellen. In der exportierten CSV-Datei werden einige zusätzliche Felder „qtrees“ angezeigt.

- **Status**

  Zeigt den aktuellen Status des qtree an. Der Status kann kritisch (), Fehler ( ), Warnung ( ) oder Normal ( ) sein.

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 Storage-VM an. Sie können Informationen wie den Status des Kontingents, den Namen des Benutzers oder der Benutzergruppe, die auf den Festplatten und Dateien festgelegten Soft- und Hard-Limits, den Speicherplatz und die Anzahl der verwendeten Dateien sowie den Schwellenwert für die Festplatte anzeigen. Sie können auch die E-Mail-Adresse ändern, die einem Benutzer oder einer Benutzergruppe zugeordnet ist.

- **Schaltfläche 'Email-Adresse bearbeiten'**

  Öffnet das Dialogfeld E-Mail-Adresse bearbeiten, in dem die aktuelle E-Mail-Adresse des ausgewählten Benutzers oder der ausgewählten Benutzergruppe angezeigt wird. Sie können die E-Mail-Adresse ändern. Wenn das Feld **E-Mail-Adresse bearbeiten** leer ist, wird die Standardregel verwendet, um eine E-Mail-Adresse für den ausgewählten Benutzer oder die ausgewählte Benutzergruppe zu generieren.

  Wenn mehrere Benutzer das gleiche Kontingent haben, werden die Namen der Benutzer als kommagetrennte Werte angezeigt. Außerdem wird die Standardregel nicht verwendet, um die E-Mail-Adresse zu generieren; Sie müssen daher die erforderliche E-Mail-Adresse angeben, damit Benachrichtigungen gesendet werden können.

- **Schaltfläche E-Mail-Regeln konfigurieren**

  Mit diesem Service können Sie Regeln erstellen oder ändern, um eine E-Mail-Adresse für die Kontingente von Benutzern oder Benutzergruppen zu erstellen, die für die Storage-VM konfiguriert sind. Bei einer Quota-Verletzung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

- **Status**

  Zeigt den aktuellen Status des Kontingents an. Der Status kann kritisch (), Warnung ( ) oder Normal ( ) sein.

  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-Freigaben“

Auf der Registerkarte NFS-Shares werden Informationen über NFS Shares angezeigt, z. B. sein Status, der dem Volume zugeordnete Pfad (FlexGroup Volumes oder FlexVol Volumes), die Zugriffsebenen von Clients auf die NFS-Shares und die für die exportierten Volumes definierte Exportrichtlinie. NFS-Freigaben werden unter folgenden Bedingungen nicht angezeigt: Wenn das Volume nicht gemountet wurde oder wenn die mit der Exportrichtlinie für das Volume verknüpften Protokolle keine NFS-Freigaben enthalten.

- **Status**

  Zeigt den aktuellen Status der NFS-Freigaben an. Der Status kann Error () oder Normal ( ) sein.

- **Verbindungspfad**

  Zeigt den Pfad an, auf den das Volume angehängt ist. Wird auf einen qtree eine explizite NFS Exportrichtlinie angewendet, zeigt die Spalte den Pfad des Volume an, über das auf den qtree zugegriffen werden kann.

- **Verbindungspfad Aktiv**

  Zeigt an, ob der Pfad für den Zugriff auf das bereitgestellte Volume aktiv oder inaktiv ist.

- **Volumen oder Qtree**

  Zeigt den Namen des Volumes oder qtree an, auf das die NFS-Exportrichtlinie angewendet wird. Wenn eine NFS-Exportrichtlinie auf einen qtree im Volume angewendet wird, werden in der Spalte sowohl die Namen des Volume als auch der qtree angezeigt.

  Sie können auf den Link klicken, um Details zum Objekt auf der entsprechenden Detailseite anzuzeigen. Wenn es sich bei dem Objekt um einen qtree handelt, werden sowohl für den qtree als auch für das Volume Links angezeigt.

- **Volume-Status**

  Zeigt den Status des Volumes an, das exportiert wird. Der Status kann Offline, Online, eingeschränkt oder gemischt sein.

  - Offline

    Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

  - Online

    Lese- und Schreibzugriff auf das Volume ist zulässig.

  - Eingeschränkt

    Begrenzte Vorgänge, wie etwa die Paritätsrekonstruktion, sind zulässig, der Datenzugriff jedoch nicht.

  - Gemischt

Die Komponenten eines FlexGroup-Volumes sind nicht alle im selben Zustand.

- **Sicherheitsstil**

  Zeigt die Zugriffsberechtigung für die exportierten Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder gemischt sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume haben UNIX Berechtigungen.

  - Virtualisierung

    Dateien und Verzeichnisse im Volume weisen einen einheitlichen Sicherheitsstil auf.

  - NTFS (CIFS-Clients)

    Dateien und Verzeichnisse im Volume haben Windows NTFS-Berechtigungen.

  - Gemischt

    Dateien und Verzeichnisse auf dem Volume können entweder UNIX Berechtigungen oder Windows NTFS Berechtigungen haben.

- **UNIX-Erlaubnis**

  Zeigt die UNIX-Berechtigungsbits in einem Oktal-String-Format an, das für die exportierten Volumes festgelegt ist. Es ähnelt den Berechtigungsbits im UNIX-Stil.

- **Exportrichtlinie**

  Zeigt die Regeln an, die die Zugriffsberechtigung für exportierte Volumes definieren. Sie können auf den Link klicken, um Details zu den Regeln anzuzeigen, die mit der Exportrichtlinie verknüpft sind, z. B. die Authentifizierungsprotokolle und die Zugriffsberechtigung.

Registerkarte „SMB-Freigaben“

Zeigt Informationen zu den SMB-Freigaben auf der ausgewählten Storage-VM an. Sie können Informationen anzeigen, wie z. B. den Status der SMB-Freigabe, den Freigabennamen, den mit der Storage-VM verknüpften Pfad, den Status des Verbindungspfads der Freigabe, das Objekt, den Status des enthaltenden Volumes, die Sicherheitsdaten der Freigabe und die für die Freigabe definierten Exportrichtlinien. Sie können auch feststellen, ob ein äquivalenter NFS-Pfad für die SMB-Freigabe vorhanden ist.

Freigaben in Ordnern werden auf der Registerkarte SMB-Freigaben nicht angezeigt.

- **Befehlsschaltfläche Benutzerzuordnung anzeigen**

  Öffnet das Dialogfeld Benutzerzuordnung.

  Sie können die Details der Benutzerzuordnung für die Storage-VM anzeigen.

- **ACL-Befehlstaste anzeigen**

  Öffnet das Dialogfeld „Zugriffskontrolle“ für die Freigabe.

Sie können Benutzer- und Berechtigungsdetails für die ausgewählte Freigabe anzeigen.

- **Status**

  Zeigt den aktuellen Status der Freigabe an. Der Status kann Normal () oder Error ( ) sein.

- **Name Der Weitergabe**

  Zeigt den Namen der SMB-Freigabe an.

- **Pfad**

  Zeigt den Verbindungspfad an, auf dem die Freigabe erstellt wird.

- **Verbindungspfad Aktiv**

  Zeigt an, ob der Pfad für den Zugriff auf die Freigabe aktiv oder inaktiv ist.

- **Objekt**

  Zeigt den Namen des enthaltenden Objekts an, zu dem die Freigabe gehört. Das zugehörige Objekt kann ein Volume oder ein qtree sein.

  Durch Klicken auf den Link können Sie auf der entsprechenden Detailseite Details über das zugehörige Objekt anzeigen. Wenn es sich bei dem enthaltenen Objekt um einen qtree handelt, werden sowohl für qtree als auch für das Volume Links angezeigt.

- **Volume-Status**

  Zeigt den Status des Volumes an, das exportiert wird. Der Status kann Offline, Online, eingeschränkt oder gemischt sein.

  - Offline

    Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

  - Online

    Lese- und Schreibzugriff auf das Volume ist zulässig.

  - Eingeschränkt

    Begrenzte Vorgänge, wie etwa die Paritätsrekonstruktion, sind zulässig, der Datenzugriff jedoch nicht.

  - Gemischt

    Die Komponenten eines FlexGroup-Volumes sind nicht alle im selben Zustand.

- **Sicherheit**

  Zeigt die Zugriffsberechtigung für die exportierten Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder gemischt sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume haben UNIX Berechtigungen.

- Virtualisierung

  Dateien und Verzeichnisse im Volume weisen einen einheitlichen Sicherheitsstil auf.

- NTFS (CIFS-Clients)

  Dateien und Verzeichnisse im Volume haben Windows NTFS-Berechtigungen.

- Gemischt

  Dateien und Verzeichnisse auf dem Volume können entweder UNIX Berechtigungen oder Windows NTFS Berechtigungen haben.

- **Exportrichtlinie**

  Zeigt den Namen der Exportrichtlinie an, die für die Freigabe gilt. Wenn keine Exportrichtlinie für die Storage-VM angegeben ist, wird der Wert als nicht aktiviert angezeigt.

  Sie können auf den Link klicken, um Details zu den Regeln anzuzeigen, die der Exportrichtlinie zugeordnet sind, z. B. Zugriffsprotokolle und Berechtigungen. Der Link ist deaktiviert, wenn die Exportrichtlinie für die ausgewählte Speicher-VM deaktiviert ist.

- **NFS-Äquivalent**

  Gibt an, ob ein Äquivalent zu NFS für die Freigabe vorhanden ist.

REGISTERKARTE „SAN“

Zeigt Details zu LUNs, Initiatorgruppen und Initiatoren für die ausgewählte Storage-VM an. Standardmäßig wird die Ansicht LUNs angezeigt. Sie können Details zu den Initiatorgruppen auf der Registerkarte Initiatorgruppen und Details zu Initiatoren auf der Registerkarte Initiatoren anzeigen.

- **LUNs-Registerkarte**

  Zeigt Details zu den LUNs an, die zur ausgewählten Speicher-VM gehören. Sie können Informationen anzeigen, wie z. B. den LUN-Namen, den LUN-Zustand (online oder offline), den Namen des Filesystems (Volume oder qtree), das die LUN enthält, den Typ des Host-Betriebssystems, die Gesamtkapazität und die Seriennummer der LUN. Die Spalte LUN Performance enthält einen Link zur Seite LUN/Performance Details.

  Sie können auch anzeigen, ob Thin Provisioning auf der LUN aktiviert ist und ob die LUN einer Initiatorgruppe zugeordnet ist. Wenn er einem Initiator zugeordnet ist, können Sie die Initiatorgruppen und Initiatoren anzeigen, die der ausgewählten LUN zugeordnet sind.

- **Registerkarte Initiatorgruppen**

  Zeigt Details zu Initiatorgruppen an. Sie können Details anzeigen, z. B. den Namen der Initiatorgruppe, den Zugriffsstatus, den Typ des Host-Betriebssystems, das von allen Initiatoren in der Gruppe verwendet wird, und das unterstützte Protokoll. Wenn Sie in der Spalte Zugriffsstatus auf den Link klicken, können Sie den aktuellen Zugriffsstatus der Initiatorgruppe anzeigen.

  - **Normal**

    Die Initiatorgruppe ist mit mehreren Zugriffspfaden verbunden.

◦ * Einzelner Pfad*

Die Initiatorgruppe ist mit einem einzelnen Zugriffspfad verbunden.

◦ **Keine Pfade**

Es ist kein Zugriffspfad mit der Initiatorgruppe verbunden.

Sie können anzeigen, ob Initiatorgruppen über einen Port-Satz allen Schnittstellen oder spezifischen Schnittstellen zugeordnet sind. Wenn Sie in der Spalte zugeordnete Schnittstellen auf den Link Zählen klicken, werden entweder alle Schnittstellen angezeigt oder bestimmte Schnittstellen für einen Port-Satz werden angezeigt. Schnittstellen, die über das Zielportal zugeordnet sind, werden nicht angezeigt. Es wird die Gesamtzahl der Initiatoren und LUNs angezeigt, die einer Initiatorgruppe zugeordnet sind.

Sie können auch die LUNs und Initiatoren anzeigen, die der ausgewählten Initiatorgruppe zugeordnet sind.

- **Registerkarte Initiatoren**

Zeigt den Namen und Typ des Initiators und die Gesamtzahl der Initiatorgruppen an, die diesem Initiator für die ausgewählte Storage-VM zugeordnet sind.

```
initiator groups that are mapped to the selected initiator group.
```

Bereich „Verwandte Anmerkungen“

Im Fensterbereich Verwandte Anmerkungen können Sie die mit der ausgewählten Speicher-VM verknüpften Anmerkungsdetails anzeigen. Details umfassen den Anmerkungsnamen und die Anmerkungswerte, die auf die Storage-VM angewendet werden. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie Cluster, Aggregate und Volumes anzeigen, die mit der Storage-VM in Verbindung stehen:

- * Cluster*

Zeigt den Integritätsstatus des Clusters an, zu dem die Storage-VM gehört.

- **Aggregate**

Zeigt die Anzahl der Aggregate an, die zur ausgewählten Storage-VM gehören. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt. Wenn z. B. eine Speicher-VM zehn Aggregate enthält, von denen fünf den Warnstatus und die übrigen fünf den kritischen Status anzeigen, ist der angezeigte Status kritisch.

- * Zugewiesene Aggregate*

Zeigt die Anzahl der Aggregate an, die einer Storage-VM zugewiesen sind. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt.

- **Bände**

Zeigt die Anzahl und Kapazität der Volumes an, die zur ausgewählten Speicher-VM gehören. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt. In der Storage-VM sind FlexGroup Volumes enthalten, die Anzahl auch FlexGroups. FlexGroup Komponenten sind darin nicht enthalten.

Bereich „Verwandte Gruppen“

Im Fensterbereich Verwandte Gruppen können Sie die Liste der Gruppen anzeigen, die der ausgewählten Speicher-VM zugeordnet sind.

Bereich „Verwandte Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnmeldungen anzeigen, die für die ausgewählte Storage-VM erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link **Alarm hinzufügen** klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Namen der Warnmeldung klicken.

„Cluster/Systemzustand“-Details

Auf der Seite „Cluster/Systemzustand“ finden Sie ausführliche Informationen über ein ausgewähltes Cluster, z. B. Angaben zu Systemzustand, Kapazität und Konfiguration. Sie können auch Informationen zu Netzwerkschnittstellen (LIFs), Nodes, Festplatten, zugehörigen Geräten und zugehörigen Warnmeldungen für das Cluster anzeigen.

Der Status neben dem Cluster-Namen, z. B. (gut), stellt den Kommunikationsstatus dar, ob Unified Manager mit dem Cluster kommunizieren kann. Er stellt nicht den Failover-Status oder den Gesamtstatus des Clusters dar.

Befehlsschaltflächen

Mit den Schaltflächen des Befehls können Sie die folgenden Aufgaben für das ausgewählte Cluster ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Ermöglicht Ihnen die Navigation zur Seite „Cluster/Performance Details“.

- **Aktionen**

  - Alarm hinzufügen: Öffnet das Dialogfeld Alarm hinzufügen, in dem Sie dem ausgewählten Cluster eine Warnung hinzufügen können.
  - Erneut entdecken: Initiiert eine manuelle Aktualisierung des Clusters, sodass Unified Manager die neuesten Änderungen am Cluster erkennen kann.

    Bei Kombination von Unified Manager mit OnCommand Workflow Automation erfasst der Wiederauffindungvorgang ggf. auch zwischengespeicherte Daten von WFA.

  Nachdem der Vorgang zur erneuten Erkennung initiiert wurde, wird ein Link zu den zugehörigen Jobdetails angezeigt, um die Nachverfolgung des Jobstatus zu ermöglichen.

  - Anmerkungen: Ermöglicht es Ihnen, das ausgewählte Cluster zu kommentieren.

- **Cluster Anzeigen**

  Ermöglicht die Navigation in der Ansicht „Health: All Clusters“.

Registerkarte Systemzustand

Zeigt detaillierte Informationen zur Datenverfügbarkeit und zu Kapazitätsproblemen der verschiedenen Cluster-Objekte wie Nodes, SVMs und Aggregate an. Verfügbarkeitsprobleme hängen von der Datenserverfunktion der Cluster-Objekte ab. Kapazitätsprobleme stehen im Zusammenhang mit der Datenspeicherfunktion der Cluster-Objekte.

Sie können auf das Diagramm eines Objekts klicken, um eine gefilterte Liste der Objekte anzuzeigen. Beispielsweise können Sie auf das SVM-Kapazitätsdiagramm klicken, in dem Warnungen angezeigt werden, um eine gefilterte Liste der SVMs anzuzeigen. Diese Liste enthält SVMs mit Volumes oder qtrees, deren Kapazitätsprobleme mit einem Schweregrad von Warnung auftreten. Sie können auch auf das Diagramm „SVMs Verfügbarkeit“ klicken, in dem Warnungen angezeigt werden, um die Liste der SVMs mit Verfügbarkeitsproblemen und einem Schweregrad „Warnung“ anzuzeigen.

Verfügbarkeitsprobleme

Grafische Darstellung der Gesamtzahl an Objekten, einschließlich Objekten mit Verfügbarkeitsproblemen und Objekten, bei denen keine Probleme mit der Verfügbarkeit auftreten Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Verfügbarkeitsproblemen, die sich auf die Verfügbarkeit von Daten im Cluster auswirken oder bereits davon betroffen sein können. Beispielsweise werden Informationen über Festplatten-Shelfs angezeigt, die ausgefallen sind und Aggregate, die offline sind.

Die für das SFO-Balkendiagramm angezeigten Daten basieren auf dem HA-Status der Nodes. Die für alle anderen Balkendiagramme angezeigten Daten werden auf Grundlage der generierten Ereignisse berechnet.

Kapazitätsprobleme

Grafische Darstellung der Gesamtzahl an Objekten, einschließlich Objekten mit Kapazitätsproblemen und Objekten, die keine Kapazitätsprobleme haben. Die Farben im Diagramm stellen die verschiedenen Schweregrade für die Probleme dar. Die Informationen unten im Diagramm enthalten Details zu Kapazitätsproblemen, die sich auf die Kapazität von Daten im Cluster auswirken oder bereits sie beeinträchtigen können. Beispielsweise werden Informationen zu Aggregaten angezeigt, die mit hoher Wahrscheinlichkeit die festgelegten Schwellenwerte überschreiten.

Registerkarte „Kapazität“

Zeigt detaillierte Informationen zur Kapazität des ausgewählten Clusters an.

Kapazität

Zeigt das Datenkapazitätsdiagramm zu der genutzten Kapazität und der verfügbaren Kapazität aus allen zugewiesenen Aggregaten an:

- Genutzter Logischer Speicherplatz

  Die tatsächliche Größe der Daten, die auf allen Aggregaten auf diesem Cluster gespeichert werden, ohne dabei die Einsparungen durch die ONTAP Storage-Effizienztechnologien zu verwenden. Dies umfasst keine Snapshot-Kopien.

- Datenreduzierung

  Zeigt das Verhältnis ohne Snapshot-Kopien und mit zwei signifikanten Ziffern, z. B. 1.8 zu 1, an. Dieses Verhältnis basiert auf den konfigurierten ONTAP Storage-Effizienzeinstellungen.

- Verwendet

  Die physische Kapazität, die von Daten auf allen Aggregaten verwendet wird. Dies schließt nicht die Kapazität ein, die für Parität, richtige Dimensionierung und Reservierung verwendet wird.

- Verfügbar

  Zeigt die für Daten verfügbare Kapazität an.

- Ersatzteile

  Zeigt die verfügbare Speicherkapazität für die Speicherung aller freien Festplatten an.

- Provisioniert

  Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

Details

Zeigt detaillierte Informationen zur verwendeten und verfügbaren Kapazität an. Die Berechnung schließt die Daten des Root-Aggregats aus.

- Gesamtkapazität

  Zeigt die Gesamtkapazität des Clusters an. Dies schließt nicht die Kapazität ein, die Parität zugewiesen ist.

- Verwendet

  Zeigt die Kapazität an, die von Daten verwendet wird. Dies schließt nicht die Kapazität ein, die für Parität, richtige Dimensionierung und Reservierung verwendet wird.

- Verfügbar

  Zeigt die für Daten verfügbare Kapazität an.

- Provisioniert

  Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

- Ersatzteile

  Zeigt die verfügbare Speicherkapazität für die Speicherung aller freien Festplatten an.

Cloud-Tier

Zeigt die insgesamt genutzte Cloud-Tier-Kapazität und die Kapazität der einzelnen verbundenen Cloud-Tiers für FabricPool-fähige Aggregate im Cluster an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

Physische Kapazität Breakout nach Festplattentyp

Im Bereich physische Kapazität Breakout nach Festplattentyp werden ausführliche Informationen zur Festplattenkapazität der verschiedenen Festplattentypen im Cluster angezeigt. Durch Klicken auf den Festplattentyp werden weitere Informationen zum Festplattentyp auf der Registerkarte Laufwerke angezeigt.

- Nutzbare Gesamtkapazität –

  Zeigt die verfügbare Kapazität und freie Kapazität der Datenfestplatten an.

- HDD

  Grafische Darstellung der verwendeten Kapazität und der verfügbaren Kapazität aller Festplatten im Cluster. Die gestrichelte Linie stellt die freie Kapazität der Datenfestplatten dar.

- Flash
  - SSD-Daten

    Grafische Darstellung der verwendeten Kapazität und der verfügbaren Kapazität der SSD-Datenfestplatten im Cluster

  - SSD Cache

    Zeigt grafisch die speicherbare Kapazität der SSD-Cache-Laufwerke im Cluster an.

  - SSD Spare

    Grafische Darstellung der freien Kapazität der SSD-, Daten- und Cache-Festplatten im Cluster

- Nicht Zugewiesene Festplatten

  Zeigt die Anzahl der nicht zugewiesenen Festplatten im Cluster an.

Aggregate mit Kapazitätsproblemen

Zeigt Details zur verwendeten Kapazität und zur verfügbaren Kapazität der Aggregate mit Kapazitätsproblemen in Tabellenform an.

- Status

  Zeigt an, dass das Aggregat ein kapazitätsbezogenes Problem mit einem bestimmten Schweregrad hat.

  Sie können den Zeiger auf den Status verschieben, um weitere Informationen zu dem für das Aggregat generierten Ereignis oder Ereignissen anzuzeigen.

  Wenn der Status des Aggregats durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugewiesen wurde, und die Ursache des Ereignisses anzeigen. Sie können auf die Schaltfläche **Details anzeigen** klicken, um weitere Informationen über die Veranstaltung anzuzeigen.

  Wenn der Status des Aggregats durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen angezeigt, z. B. Ereignisname, Uhrzeit und Datum, an dem die Ereignisse ausgelöst werden, und der Name des Administrators, dem das Ereignis zugewiesen ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

Ein Aggregat kann mehrere kapazitätsbezogene Ereignisse vom gleichen Schweregrad oder verschiedene Schweregrade aufweisen. Jedoch wird nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Aggregat zwei Ereignisse mit dem Schweregrad „Fehler“ und „kritisch“ hat, wird nur der Schweregrad „kritisch“ angezeigt.

- Aggregat

  Zeigt den Namen des Aggregats an.

- Genutzte Datenkapazität

  Grafische Anzeige von Informationen zur Kapazitätsauslastung des Aggregats (in Prozent)

- Tage voll

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor die volle Kapazität des Aggregats erreicht ist.

Registerkarte Konfiguration

Zeigt Details zum ausgewählten Cluster an, z. B. IP-Adresse, Kontakt und Standort:

Cluster – Überblick

- Managementoberfläche

  Zeigt die Cluster-Management-LIF an, die Unified Manager zum Herstellen einer Verbindung mit dem Cluster verwendet. Der Betriebsstatus der Schnittstelle wird ebenfalls angezeigt.

- Host-Name oder IP-Adresse

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse der Clusterverwaltungs-LIF an, die Unified Manager zur Verbindung mit dem Cluster verwendet.

- FQDN

  Zeigt den vollständig qualifizierten 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.

- Kontakt

  Zeigt Details zum Administrator an, an den Sie bei Cluster-Problemen wenden sollten.

- Standort

  Zeigt den Speicherort des Clusters an.

- Persönlichkeit

  Gibt an, ob es sich um ein für All-SAN-Arrays konfiguriertes Cluster handelt.

Überblick Über Das Remote-Cluster

Enthält Details zum Remote-Cluster in einer MetroCluster-Konfiguration. Diese Informationen werden nur für MetroCluster-Konfigurationen angezeigt.

- Cluster

  Zeigt den Namen des Remote-Clusters an. Sie können auf den Cluster-Namen klicken, um zur Detailseite des Clusters zu navigieren.

- Host-Name oder IP-Adresse

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Remote-Clusters an.

- Standort

  Zeigt den Speicherort des Remote-Clusters an.

Übersicht über MetroCluster

Details zum lokalen Cluster in MetroCluster over FC oder MetroCluster over IP Konfigurationen Diese Informationen werden nur für MetroCluster über FC- oder IP-Konfigurationen angezeigt.

- Typ

  Zeigt an, ob es sich bei dem MetroCluster-Typ um zwei oder vier Nodes handelt. Bei MetroCluster over IP werden nur vier Nodes unterstützt.

- Konfiguration

  Zeigt die MetroCluster-Konfiguration über FC und IP an, die folgende Werte aufweisen kann:

Für FC

- Stretch-Konfiguration mit SAS-Kabeln
- Stretch-Konfiguration mit FC-SAS Bridge
- Fabric-Konfiguration mit FC Switches

> Bei einem MetroCluster mit vier Nodes wird nur eine Fabric-Konfiguration mit FC-Switches unterstützt.

Für IP

- IP-Konfiguration mit Ethernet-Switches (L2 oder L3, je nach Konfiguration des Clusters)
  - Automatisiertes ungeplantes Switchover (AUSO)

    Zeigt an, ob das automatisierte ungeplante Switchover für das lokale Cluster aktiviert ist. Standardmäßig ist AUSO für alle Cluster in einer MetroCluster-Konfiguration mit zwei Knoten in Unified Manager aktiviert. Sie können die AUSO-Einstellung über die Befehlszeilenschnittstelle ändern. Dies wird nur für MetroCluster über FC unterstützt.

  - Umschaltmodus

Zeigt den Umschaltmodus für die MetroCluster-over-IP-Konfiguration an. Die verfügbaren Werte sind: `Active`, `Negotiated Switchover` Und `Automatic Unplanned Switchover`.

Knoten

- Gesteigerte

  Zeigt die Anzahl der Knoten an, die im Cluster nach oben ( ) oder nach unten ( ) sind .

- Betriebssystemversionen

  Zeigt die ONTAP-Versionen, die die Nodes ausführen, sowie die Anzahl der Nodes, auf denen eine bestimmte Version von ONTAP ausgeführt wird. Beispielsweise gibt 9.6 (2), 9.3 (1) an, dass zwei Nodes ONTAP 9.6 ausführen und auf einem Node ONTAP 9.3 ausgeführt wird.

Storage Virtual Machines

- Gesteigerte

  Zeigt die Anzahl der SVMs an, die im Cluster nach oben ( ) oder unten ( ) sind .

Netzwerkschnittstellen

- Gesteigerte

  Zeigt die Anzahl der nicht-Daten-LIFs an, die im Cluster up ( ) oder down ( ) sind .

- Cluster-Management-Schnittstellen

  Zeigt die Anzahl der Cluster-Management-LIFs an.

- Node-Management-Schnittstellen

  Zeigt die Anzahl der LIFs für das Node-Management an.

- Cluster-Schnittstellen

  Zeigt die Anzahl der Cluster-LIFs an.

- Intercluster-Schnittstellen

  Zeigt die Anzahl der Intercluster-LIFs an.

Protokolle

- Datenprotokolle

  Zeigt die Liste der lizenzierten Datenprotokolle an, die für den Cluster aktiviert sind. Datenprotokolle sind iSCSI, CIFS, NFS, NVMe und FC/FCoE.

Darstellt

- Mediatoren

  Zeigt an, ob das Cluster Mediatoren unterstützt und der Verbindungsstatus des Mediators. Er gibt an, ob der Mediator konfiguriert ist, und wenn er konfiguriert ist, zeigt er den Status der Mediatoren an.

  - Keine Angabe

    Wird angezeigt, wenn das Cluster keine Mediatoren unterstützt.

  - Nicht Konfiguriert

    Zeigt an, wenn das Cluster Mediatoren unterstützt, aber der Mediator nicht konfiguriert ist.

  - IP-Adresse

    Zeigt an, wenn das Cluster Mediatoren unterstützt und der Mediator konfiguriert ist. Der Mediatorstatus wird durch Farbe angezeigt. Die Farbe grün zeigt an, dass der Mediatorstatus erreichbar ist. Die Farbe Rot zeigt an, dass der Mediator-Status nicht erreichbar ist.

Cloud-Tiers

In sind die Namen der Cloud-Tiers aufgeführt, mit denen dieses Cluster verbunden ist. Außerdem werden die Typen (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage oder StorageGRID) und die Status der Cloud-Tiers (verfügbar oder nicht verfügbar) aufgelistet.

Registerkarte MetroCluster-Konnektivität

Zeigt die Probleme und den Konnektivitätsstatus der Cluster-Komponenten in der MetroCluster over FC-Konfiguration an. Ein Cluster wird in einem roten Feld angezeigt, wenn der Disaster-Recovery-Partner des Clusters Probleme hat.

Die Registerkarte MetroCluster-Konnektivität wird nur für Cluster angezeigt, die sich in einer MetroCluster über die FC-Konfiguration befinden.

Sie können zur Detailseite eines Remote-Clusters navigieren, indem Sie auf den Namen des Remote-Clusters klicken. Sie können die Details der Komponenten auch anzeigen, indem Sie auf den Zähllink einer Komponente klicken. Wenn Sie beispielsweise auf den Zähllink des Node im Cluster klicken, wird auf der Detailseite des Clusters die Registerkarte Node angezeigt. Wenn Sie auf den Link Zählen der Festplatten im Remote-Cluster klicken, wird die Registerkarte Festplatte auf der Detailseite des Remote-Clusters angezeigt.

Beim Verwalten einer MetroCluster Konfiguration mit acht Nodes wird durch Klicken auf den Zähllink der Komponente Platten-Shelfs nur die lokalen Shelfs des Standard-HA-Paars angezeigt. Es gibt auch keine Möglichkeit, die lokalen Shelfs auf dem anderen HA-Paar anzuzeigen.

Sie können den Mauszeiger über die Komponenten bewegen, um bei jedem Problem die Details und den Konnektivitätsstatus der Cluster anzuzeigen. Außerdem werden weitere Informationen zu dem für das Problem erzeugten Ereignis oder Ereignissen angezeigt.

Wenn der Status des Verbindungsproblem zwischen den Komponenten durch ein einziges Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum anzeigen, an dem das Ereignis ausgelöst wurde, den Namen des Administrators, dem das Ereignis zugeordnet ist, und die Ursache

des Ereignisses anzeigen. Die Schaltfläche Details anzeigen enthält weitere Informationen zum Ereignis.

Wenn der Status des Verbindungsproblem zwischen den Komponenten durch mehrere Ereignisse des gleichen Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie Ereignisname, Uhrzeit und Datum bei Auslösung der Ereignisse und dem Namen des Administrators angezeigt, dem das Ereignis zugeordnet ist. Sie können weitere Details zu den einzelnen Ereignissen anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

Registerkarte „MetroCluster-Replikation“

Zeigt den Status der Daten an, die in einer MetroCluster over FC-Konfiguration repliziert werden. Sie können die Registerkarte MetroCluster-Replikation verwenden, um die Datensicherung durch synchrones Spiegeln der Daten mit den bereits Peering-Clustern zu gewährleisten. Ein Cluster wird in einem roten Feld angezeigt, wenn der Disaster-Recovery-Partner des Clusters Probleme hat.

> Die Registerkarte MetroCluster-Replikation wird nur für Cluster angezeigt, die sich in einer MetroCluster über die FC-Konfiguration befinden.

In einer MetroCluster-Umgebung können Sie diese Registerkarte verwenden, um die logischen Verbindungen und Peering des lokalen Clusters mit dem Remote-Cluster zu überprüfen. Sie können die objektive Darstellung der Cluster-Komponenten mit ihren logischen Verbindungen anzeigen. Dadurch werden Probleme identifiziert, die bei der Spiegelung von Metadaten und Daten auftreten können.

Auf der Registerkarte MetroCluster-Replikation bietet das lokale Cluster eine detaillierte grafische Darstellung des ausgewählten Clusters. MetroCluster-Partner bezieht sich auf das Remote-Cluster.

Registerkarte Netzwerkschnittstellen

Zeigt Details zu allen nicht-Daten-LIFs an, die auf dem ausgewählten Cluster erstellt wurden.

Netzwerkschnittstelle

Zeigt den Namen der logischen Schnittstelle an, die im ausgewählten Cluster erstellt wird.

Betriebsstatus

Zeigt den Betriebsstatus der Schnittstelle an, der up (), Down ()  oder Unknown ( )  sein kann  . Der Betriebsstatus einer Netzwerkschnittstelle wird durch den Status ihrer physischen Ports bestimmt.

Administrationsstatus

Zeigt den administrativen Status der Schnittstelle an, der up (), Down ()  oder Unknown ( )  sein kann  . Sie können den Administrationsstatus einer Schnittstelle steuern, wenn Sie Änderungen an der Konfiguration oder während der Wartung vornehmen. Der Administrationsstatus kann sich vom Betriebsstatus unterscheiden. Wenn jedoch der Administrationsstatus eines LIF „Inaktiv“ lautet, ist der Betriebsstatus standardmäßig „Inaktiv“.

IP-Adresse

Zeigt die IP-Adresse der Schnittstelle an.

Rolle

Zeigt die Rolle der Schnittstelle an. Mögliche Rollen sind Cluster-Management-LIFs, Node-Management-LIFs, Cluster-LIFs und Intercluster-LIFs.

Home Port

Zeigt den physischen Port an, dem die Schnittstelle ursprünglich zugeordnet war.

Aktueller Port

Zeigt den physischen Port an, dem die Schnittstelle derzeit zugeordnet ist. Nach der LIF-Migration kann sich der aktuelle Port vom Home Port unterscheiden.

Failover-Richtlinie

Zeigt die Failover-Richtlinie an, die für die Schnittstelle konfiguriert ist.

Routinggruppen

Zeigt den Namen der Routinggruppe an. Sie können weitere Informationen zu den Routen und dem Ziel-Gateway anzeigen, indem Sie auf den Namen der Routinggruppe klicken.

Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt. Daher wird für diese Cluster eine leere Spalte angezeigt.

Failover-Gruppe

Zeigt den Namen der Failover-Gruppe an.

Registerkarte Knoten

Zeigt Informationen zu Nodes im ausgewählten Cluster an. Sie können ausführliche Informationen zu HA-Paaren, Festplatten-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 Übernahmvorgangs wird beispielsweise die folgende Meldung angezeigt: Storage Failover möglich.

Sie können eine Liste der Ereignisse anzeigen, die zum HA-Paar und seiner Umgebung betreffen, z. B. Lüfter, Netzteile, NVRAM-Batterie, Flash-Karten, Serviceprozessor und Verbindung von Festplatten-Shelfs: Sie können auch die Uhrzeit anzeigen, zu der die Ereignisse ausgelöst wurden.

Sie können weitere Node-bezogene Informationen anzeigen, z. B. die Modellnummer.

Bei Single-Node-Clustern können Sie auch Details zu den Nodes anzeigen.

Platten-Shelfs

Zeigt Informationen über die Festplatten-Shelfs im HA-Paar an.

Sie können auch Ereignisse anzeigen, die für die Festplatten-Shelfs und die Umgebungskomponenten generiert wurden, sowie die Zeit, zu der die Ereignisse ausgelöst wurden.

- **Regal-ID**

  Zeigt die ID des Shelf an, in dem sich die Festplatte befindet.

- **Komponentenstatus**

  Zeigt Umgebungsdetails der Festplatten-Shelfs an, z. B. Netzteile, Lüfter, Temperatursensor, aktuelle Sensoren, Festplattenkonnektivität. Und Spannungssensoren. Die Umgebungsdetails werden als Symbole in den folgenden Farben angezeigt:

  - **Grün**

    Die Umgebungskomponenten funktionieren ordnungsgemäß.

  - **Grau**

    Für die Umgebungskomponenten sind keine Daten verfügbar.

  - * Rot*

    Einige Umgebungskomponenten sind nicht verfügbar.

- **Bundesland**

  Zeigt den Status des Festplatten-Shelf an. Mögliche Status sind Offline, Online, kein Status, Initialisierung erforderlich, fehlt, Und Unbekannt.

- **Modell**

  Zeigt die Modellnummer des Festplatten-Shelf an.

- **Lokales Festplatten-Shelf**

  Gibt an, ob sich das Festplatten-Shelf auf dem lokalen Cluster oder dem Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

- * Unique ID*

  Zeigt die eindeutige ID des Festplatten-Shelf an.

- **Firmware-Version**

Zeigt die Firmware-Version des Festplatten-Shelf an.

Ports

Zeigt Informationen zu den zugehörigen FC-, FCoE- und Ethernet-Ports an. Sie können Details zu den Ports und den zugehörigen LIFs anzeigen, indem Sie auf die Port-Symbole klicken.

Sie können auch die für die Ports generierten Ereignisse anzeigen.

Sie können folgende Portdetails anzeigen:

- Port-ID

  Zeigt den Namen des Ports an. Die Port-Namen können beispielsweise E0M, e0a und e0b sein.

- Rolle

  Zeigt die Rolle des Ports an. Mögliche Rollen sind Cluster, Data, Intercluster, Node-Management und Undefined.

- Typ

  Zeigt das Protokoll der physischen Schicht an, das für den Port verwendet wird. Mögliche Typen sind Ethernet, Fibre Channel und FCoE.

- WWPN

  Zeigt den WWPN (World Wide Port Name) des Ports an.

- Firmware-Version

  Zeigt die Firmware-Version des FC/FCoE-Ports an.

- Status

  Zeigt den aktuellen Status des Ports an. Die möglichen Zustände sind auf, ab, Verbindung nicht verbunden oder Unbekannt ( ).

  Sie können die portbezogenen Ereignisse in der Ereignisliste anzeigen. Sie können auch die zugehörigen LIF-Details anzeigen, z. B. LIF-Name, Betriebsstatus, IP-Adresse oder WWPN, Protokolle, den Namen der zu dieser LIF gehörenden SVM, den aktuellen Port, die Failover-Richtlinie und die Failover-Gruppe.

Registerkarte „Festplatten“

Zeigt Details zu den Festplatten im ausgewählten Cluster an. Sie können Festplatten-bezogene Informationen wie die Anzahl der verwendeten Festplatten, Ersatzfestplatten, fehlerhafte Festplatten und nicht zugewiesene Laufwerke anzeigen. Sie können auch weitere Details anzeigen, z. B. den Festplattennamen, den Festplattentyp und den Besitzer-Node der Festplatte.

Disk-Pool: Zusammenfassung

Zeigt die Anzahl der Laufwerke an, die nach effektiven Typen (FCAL, SAS, SATA, MSATA, SSD, NVMe SSD, SSD CAP, Array LUN und VMDISK) und der Zustand der Festplatten. Sie können auch andere Details anzeigen, wie z. B. die Anzahl der Aggregate, gemeinsam genutzte Festplatten, Ersatzfestplatten, fehlerhafte Festplatten, nicht zugewiesene Festplatten, Und nicht unterstützten Festplatten. Wenn Sie auf den Link zur

Anzahl der effektiven Festplattentypen klicken, werden Festplatten mit dem ausgewählten Status und dem effektiven Typ angezeigt. Wenn Sie beispielsweise auf den Zähllink für den Festplattenstatus „beschädigt“ und „effektiver Typ SAS“ klicken, werden alle Festplatten mit dem Festplattenstatus „beschädigt“ und „effektiver Typ „SAS“ angezeigt.

Festplatte

Zeigt den Namen der Festplatte an.

RAID-Gruppen

Zeigt den Namen der RAID-Gruppe an.

Owner-Node

Zeigt den Namen des Node an, zu dem die Festplatte gehört. Wenn die Festplatte nicht zugewiesen ist, wird in dieser Spalte kein Wert angezeigt.

Status

Zeigt den Status der Festplatte an: Aggregate, Shared, Spare, broken, Unassigned, Nicht unterstützt oder Unbekannt. Standardmäßig wird diese Spalte sortiert, um die Status in der folgenden Reihenfolge anzuzeigen: Gebrochen, nicht zugewiesen, nicht unterstützt, Spare, Aggregat, Und Shared IT.

Lokale Festplatte

Zeigt entweder Ja oder Nein an, um anzugeben, ob sich das Laufwerk im lokalen Cluster oder im Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

Position

Zeigt die Position des Laufwerks basierend auf seinem Container-Typ an, z. B. Kopieren, Daten oder Parität. Standardmäßig ist diese Spalte ausgeblendet.

Betroffene Aggregate

Zeigt die Anzahl der Aggregate an, die aufgrund der ausgefallenen Festplatte betroffen sind. Sie können den Mauszeiger über den Zähllink verschieben, um die betroffenen Aggregate anzuzeigen. Klicken Sie dann auf den Aggregatnamen, um Details zum Aggregat anzuzeigen. Sie können auch auf die Aggregatanzahl klicken, um die Liste der betroffenen Aggregate in der Ansicht „Systemzustand: Alle Aggregate“ anzuzeigen.

In dieser Spalte wird für die folgenden Fälle kein Wert angezeigt:

- Für fehlerhafte Festplatten, wenn ein Cluster mit solchen Festplatten zu Unified Manager hinzugefügt wird
- Wenn keine ausgefallenen Festplatten vorhanden sind

Storage-Pool

Zeigt den Namen des Speicherpools an, zu dem die SSD gehört. Sie können den Zeiger über den Speicherpool verschieben, um Details des Speicherpools anzuzeigen.

Speicherbare Kapazität

Zeigt die verfügbare Festplattenkapazität an.

Bruttokapazität

Zeigt die Kapazität der unformatierten RAW-Festplatte vor der richtigen Dimensionierung und RAID-Konfiguration an. Standardmäßig ist diese Spalte ausgeblendet.

Typ

Zeigt die Festplattentypen an, z. B. ATA, SATA, FCAL oder VMDISK.

Effektiver Typ

Zeigt den von ONTAP zugewiesenen Festplattentyp an.

Bestimmte ONTAP-Festplattentypen werden als gleichbedeutend mit dem Erstellen und Hinzufügen zu Aggregaten und mit Ersatzmanagement angesehen. ONTAP weist jedem Festplattentyp einen effektiven Festplattentyp zu.

Spare-Blöcke Verbrauchen %

Zeigt in Prozent die Spare-Blöcke an, die in der SSD-Festplatte verbraucht werden. Diese Spalte ist bei anderen Festplatten als SSD-Festplatten leer.

Bewertete Lebensdauer %

Zeigt prozentual eine Schätzung der verwendeten SSD-Lebensdauer an, basierend auf der tatsächlichen SSD-Nutzung und der Vorhersage der SSD-Lebensdauer des Herstellers. Ein Wert größer als 99 zeigt an, dass die geschätzte Haltbarkeit verbraucht wurde, weist aber möglicherweise nicht auf einen SSD-Ausfall hin. Wenn der Wert unbekannt ist, wird die Platte weggelassen.

Firmware

Zeigt die Firmware-Version der Festplatte an.

U/MIN

Zeigt die Umdrehungen pro Minute (U/min) der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

Modell

Zeigt die Modellnummer der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

Anbieter

Zeigt den Namen des Festplattenanbieters an. Standardmäßig ist diese Spalte ausgeblendet.

Shelf-ID

Zeigt die ID des Shelf an, in dem sich die Festplatte befindet.

Bucht

Zeigt die ID des Einschubschachts an, in dem sich die Festplatte befindet.

Bereich „Verwandte Anmerkungen“

Hiermit können Sie die mit dem ausgewählten Cluster verknüpften Anmerkungsdetails anzeigen. Die Details umfassen den Anmerkungsnamen und die auf das Cluster angewandten Anmerkungswerte. Sie können auch manuelle Anmerkungen aus dem Bereich Verwandte Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Mit dieser Option können Sie Gerätedetails anzeigen, die mit dem ausgewählten Cluster verknüpft sind.

Zu den Details gehören Eigenschaften des mit dem Cluster verbundenen Geräts, wie z. B. Gerätetyp, Größe, Anzahl und Integritätsstatus. Sie können auf den Zähllink klicken, um weitere Analysen zu diesem Gerät durchzuführen.

Mithilfe des Teilfensters MetroCluster können Sie Anzahl und auch Details zum Remote MetroCluster Partner sowie zu den zugehörigen Cluster-Komponenten wie Nodes, Aggregaten und SVMs abrufen. Das Teilfenster „MetroCluster Partner“ wird nur für Cluster in einer MetroCluster-Konfiguration angezeigt.

Im Bereich „Verwandte Geräte“ können Sie die Nodes, SVMs und Aggregate anzeigen und navigieren, die mit dem Cluster in Verbindung stehen:

MetroCluster Partner

Zeigt den Integritätsstatus des MetroCluster Partners an. Über den Link „count“ können Sie weitere Informationen über Zustand und Kapazität der Cluster-Komponenten abrufen.

Knoten

Zeigt die Anzahl, die Kapazität und den Systemzustand der Nodes an, die zum ausgewählten Cluster gehören. Kapazität gibt die nutzbare Gesamtkapazität über die verfügbare Kapazität an.

Storage Virtual Machines

Zeigt die Anzahl der SVMs an, die zum ausgewählten Cluster gehören.

Aggregate

Zeigt die Anzahl, Kapazität und den Systemzustand der Aggregate an, die zum ausgewählten Cluster gehören.

Bereich „Verwandte Gruppen“

Mit können Sie die Liste der Gruppen anzeigen, die den ausgewählten Cluster enthalten.

Bereich „Verwandte Warnungen“

Im Teilfenster „Related Alerts“ können Sie die Liste der Meldungen für das ausgewählte Cluster anzeigen. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Verwandte Informationen

"Volume-Seite" "Anzeigen der Cluster-Liste und der Details"

Registerkarte „Aggregate/Health Details“

Mithilfe der Seite „Aggregat/Systemzustand“ werden ausführliche Informationen über das ausgewählte Aggregat angezeigt, beispielsweise Kapazität, Festplatteninformationen, Konfigurationsdetails und erzeugte Ereignisse. Sie können auch Informationen zu verwandten Objekten und zugehörigen Warnmeldungen für das Aggregat anzeigen.

Befehlsschaltflächen

Bei der Überwachung eines FabricPool-fähigen Aggregats gelten die überzugesund auf dieser Seite überzuschichtenden Werte nur für die lokale Kapazität oder das Performance-Tier. Der auf dem Cloud-Tier verfügbare Speicherplatz wird nicht in den überengagierten Werten dargestellt. Ebenso gelten die Werte für die Aggregatschwellenwerte nur für die lokale Performance-Tier.

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für das ausgewählte Aggregat ausführen:

- **Wechseln Sie zur Leistungsansicht**

  Ermöglicht Ihnen die Navigation zur Seite „Aggregat-/Performance-Details“.

- **Aktionen**
  - Alarm Hinzufügen

    Ermöglicht Ihnen das Hinzufügen einer Warnung zum ausgewählten Aggregat.

  - Schwellenwerte Bearbeiten

    Ermöglicht Ihnen das Ändern der Schwellenwerteinstellungen für das ausgewählte Aggregat.

- **Aggregate Anzeigen**

  Ermöglicht Ihnen die Navigation zur Ansicht „Systemzustand: Alle Aggregate“.

Registerkarte „Kapazität“

Auf der Registerkarte Kapazität werden ausführliche Informationen zum ausgewählten Aggregat, z. B. Kapazität, Schwellenwerte und tägliche Wachstumsrate, angezeigt.

Standardmäßig werden Kapazitätsereignisse nicht für die Root-Aggregate generiert. Darüber hinaus gelten die von Unified Manager verwendeten Schwellenwertwerte nicht für die Root-Aggregate der Nodes. Nur ein Mitarbeiter des technischen Supports kann die Einstellungen für diese zu erstellenden Ereignisse ändern. Wenn die Einstellungen von einem Mitarbeiter des technischen Supports geändert werden, werden die Schwellenwerte auf das Root-Aggregat des Nodes angewendet.

- * Kapazität*

  Zeigt das Datenkapazitätsdiagramm und das Diagramm Snapshot Kopien an, in dem Kapazitätsdetails zum Aggregat angezeigt werden:

  - Genutzter Logischer Speicherplatz

    Die tatsächliche Größe der im Aggregat gespeicherten Daten, ohne dabei die Einsparungen durch die ONTAP Storage-Effizienztechnologien zu verwenden.

- Verwendet

  Die von Daten im Aggregat genutzte physische Kapazität

- Überengagiert

  Wenn der Speicherplatz im Aggregat zu hoch belegt ist, wird im Diagramm ein Flag mit dem überbelegten Betrag angezeigt.

- Warnung

  Zeigt eine gepunktete Linie an der Stelle an, an der der Warnschwellenwert eingestellt ist; Bedeutung der Speicherplatz im Aggregat ist fast voll. Wird diese Schwelle nicht erreicht, wird das Ereignis „Space Fast Full“ generiert.

- Fehler

  Zeigt eine solide Zeile an dem Ort an, an dem der Fehlerschwellenwert festgelegt ist; bedeutet, dass der Speicherplatz im Aggregat voll ist. Wird dieser Schwellenwert nicht erreicht, wird das Ereignis „Space Full“ generiert.

- Diagramm Snapshot Kopien

  Dieses Diagramm wird nur angezeigt, wenn die verwendete Snapshot-Kapazität oder die Snapshot-Reserve nicht null ist.

Beide Diagramme zeigen die Kapazität an, in der die Snapshot-Kapazität die Snapshot-Reserve überschreitet, wenn die genutzte Snapshot-Kapazität die Snapshot-Reserve überschreitet.

- * Cloud Tier*

  Zeigt den Speicherplatz an, der für Daten im Cloud-Tier für FabricPool-fähige Aggregate verwendet wird. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

  Wenn die Cloud-Ebene zu einem anderen Cloud-Provider (die “mMirror Tier”) gespiegelt wird, werden hier beide Cloud-Tiers angezeigt.

- **Details**

  Zeigt detaillierte Informationen zur Kapazität an.

  - Gesamtkapazität

    Zeigt die Gesamtkapazität im Aggregat an.

  - Datenkapazität

    Zeigt den vom Aggregat (genutzte Kapazität) verwendeten Speicherplatz und die Menge des verfügbaren Speicherplatzes im Aggregat an (freie Kapazität).

  - Snapshot-Reserve

    Zeigt die verwendete und freie Snapshot Kapazität des Aggregats an.

  - Überzuviel Kapazität

Zeigt die Überbelegung des Aggregats an. Aufgrund einer Überbelegung von Aggregaten bieten Sie mehr Storage, als tatsächlich in einem bestimmten Aggregat verfügbar ist, sofern nicht alle Storage-Ressourcen derzeit verwendet werden. Bei Nutzung von Thin Provisioning kann die Gesamtgröße der Volumes im Aggregat die Gesamtkapazität des Aggregats überschreiten.

Wenn Sie Ihr Aggregat zu hoch ansetzen, müssen Sie den verfügbaren Speicherplatz sorgfältig überwachen und Storage nach Bedarf hinzufügen, um Schreibfehler aufgrund von unzureichendem Speicherplatz zu vermeiden.

- Cloud-Tier

  Zeigt den Speicherplatz an, der für Daten im Cloud-Tier für FabricPool-fähige Aggregate verwendet wird. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein. Wenn der Cloud-Tier zu einem anderen Cloud-Provider (der Spiegeltier) gespiegelt wird, werden hier beide Cloud-Tiers angezeigt

- Cache-Speicherplatz Insgesamt

  Zeigt den gesamten Speicherplatz der Solid State-Laufwerke (SSDs) bzw. Zuweisungseinheiten an, die einem Flash Pool Aggregat hinzugefügt werden. Wenn Sie Flash Pool für ein Aggregat aktiviert, aber keine SSDs hinzugefügt haben, wird der Cache-Speicherplatz als 0 KB angezeigt.

  Dieses Feld ist ausgeblendet, wenn Flash Pool für ein Aggregat deaktiviert ist.

- Schwellenwerte Für Aggregate

  Zeigt die folgenden Kapazitätsschwellenwerte für das Aggregat an:

  - Nahezu Vollständig. Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Aggregat fast voll ist.

  - Vollständiger Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Aggregat voll ist.

  - Nahezu Überbeanspruchung Des Schwellenwerts

    Gibt den Prozentsatz an, mit dem ein Aggregat fast überbelegt ist.

  - Überbeanspruchung Des Schwellenwerts

    Gibt den Prozentsatz an, zu dem ein Aggregat überengagiert ist.

- Weitere Details: Tägliche Wachstumsrate

  Zeigt den im Aggregat verwendeten Festplattenspeicher an, wenn die Änderungsrate zwischen den letzten beiden Proben 24 Stunden andauert.

  Wenn ein Aggregat beispielsweise 10 GB Festplattenspeicher bei 2:00 Uhr und 12 GB bei 6:00 Uhr nutzt, beträgt die tägliche Wachstumsrate (GB) für dieses Aggregat 2 GB.

- Volume-Verschiebung

  Zeigt die Anzahl der aktuell laufenden Volume-Move-Vorgänge an:

- Volumes Aus

  Zeigt die Anzahl und Kapazität der Volumes an, die aus dem Aggregat verschoben werden.

  Über den Link können Sie weitere Details anzeigen, beispielsweise den Volume-Namen, die Aggregate, zu denen das Volume verschoben wird, den Status der Verschiebung eines Volumes und die geschätzte Endzeit.

- Volumes In

  Zeigt die Anzahl und die verbleibende Kapazität der Volumes an, die in das Aggregat verschoben werden.

  Über den Link können Sie weitere Details anzeigen, beispielsweise den Volume-Namen, das Aggregat, aus dem das Volume verschoben wird, den Status der Verschiebung des Volumes und die geschätzte Endzeit.

- Geschätzte genutzte Kapazität nach der Verschiebung eines Volumes

  Zeigt den geschätzten belegten Speicherplatz (in Prozent und in KB, MB, GB usw.) im Aggregat an, nachdem die Verschiebevorgänge des Volumes abgeschlossen sind.

- **Kapazitätsüberblick - Volumen**

  Zeigt Diagramme an, die Informationen zur Kapazität der Volumes im Aggregat enthalten sind. Es wird die Menge an Speicherplatz angezeigt, die vom Volume (genutzte Kapazität) und die Menge des verfügbaren Speicherplatzes (freie Kapazität) im Volume verwendet wird. Wenn ein Risikoereignis für Thin Provisioning Volume für Volumes mit Thin Provisioning erstellt wird, wird die vom Volume verwendete Menge an Speicherplatz (genutzte Kapazität) und die Menge an Speicherplatz, die im Volume verfügbar ist, jedoch nicht verwendet werden kann (nicht nutzbare Kapazität), da die Kapazität des Aggregats angezeigt wird.

  Sie können das anzuangezeigte Diagramm in den Dropdown-Listen auswählen. Sie können die im Diagramm angezeigten Daten sortieren, um Details wie die genutzte Größe, die bereitgestellte Größe, die verfügbare Kapazität, die schnellste tägliche Wachstumsrate und die langsamste Wachstumsrate anzuzeigen. Sie können die Daten auf Grundlage der Storage Virtual Machines (SVMs) filtern, die die Volumes im Aggregat enthalten. Sie können auch Details zu Volumes anzeigen, die über Thin Provisioning bereitgestellt wurden. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den Bereich von Interesse positionieren. Standardmäßig werden im Diagramm die Top 30 der gefilterten Volumes im Aggregat angezeigt.

Registerkarte „Festplatteninformationen“

Zeigt detaillierte Informationen zu den Festplatten im ausgewählten Aggregat an, einschließlich RAID-Typ und -Größe sowie Typ der im Aggregat verwendeten Festplatten. Auf der Registerkarte werden auch die RAID-Gruppen und die verwendeten Festplatten (z. B. SAS, ATA, FCAL, SSD oder VMDISK) grafisch dargestellt. Weitere Informationen, wie z. B. der Schacht, das Shelf und die Drehgeschwindigkeit der Festplatte, können Sie mit dem Cursor über die Parity-Festplatten und die Daten-Festplatten anzeigen.

- * Daten*

  Grafische Anzeige von Details zu dedizierten Datenträgern, freigegebenen Datenträgern oder beidem. Wenn die Datenfestplatten freigegebene Laufwerke enthalten, werden grafische Details der freigegebenen Laufwerke angezeigt. Wenn die Datenfestplatten dedizierte Laufwerke und freigegebene Festplatten enthalten, werden grafische Details sowohl der dedizierten Datenlaufwerke als auch der freigegebenen Datenträger angezeigt.

- **RAID Details**

  RAID-Details werden nur für dedizierte Festplatten angezeigt.

  - Typ

    Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

  - Gruppengröße

    Zeigt die maximale Anzahl an Laufwerken an, die in der RAID-Gruppe zulässig sind.

  - Gruppen

    Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

- **Verwendete Festplatten**
  - Effektiver Typ

    Zeigt die Typen der Datenfestplatten an (z. B. ATA, SATA, FCAL, SSD, Oder VMDISK) im Aggregat.

  - Datenfestplatten

    Zeigt die Anzahl und Kapazität der Datenfestplatten an, die einem Aggregat zugewiesen sind. Details zur Datenfestplatte werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Festplatten enthält.

  - Parity-Festplatten

    Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat zugewiesen werden. Details zur Parity-Festplatte werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Festplatten enthält.

  - Gemeinsame Festplatten

    Zeigt die Anzahl und Kapazität der freigegebenen Datenfestplatten an, die einem Aggregat zugewiesen sind. Details zu gemeinsam genutzten Festplatten werden nur angezeigt, wenn das Aggregat freigegebene Festplatten enthält.

- **Ersatzfestplatten**

  Zeigt den effektiven Typ, die Nummer und die Kapazität der Ersatzfestplatten an, die für den Knoten im ausgewählten Aggregat verfügbar sind.

  Bei einem Failover eines Aggregats an den Partner-Node zeigt Unified Manager nicht alle freien Festplatten an, die mit dem Aggregat kompatibel sind.

- **SSD Cache**

  Enthält Details zu dedizierten Cache-SSD-Festplatten und Shared Cache SSD-Festplatten.

  Für die dedizierten Cache-SSD-Festplatten werden folgende Details angezeigt:

  - **RAID Details**

- Typ

  Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

- Gruppengröße

  Zeigt die maximale Anzahl an Laufwerken an, die in der RAID-Gruppe zulässig sind.

- Gruppen

  Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

◦ **Verwendete Festplatten**

- Effektiver Typ

  Gibt an, dass die Festplatten, die für den Cache im Aggregat verwendet werden, vom Typ SSD sind.

- Datenfestplatten

  Zeigt die Anzahl und Kapazität der Datenfestplatten an, die einem Aggregat für den Cache zugewiesen werden.

- Parity-Festplatten

  Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat für den Cache zugewiesen werden.

◦ **Ersatzfestplatten**

Zeigt den effektiven Typ, die Nummer und die Kapazität der Ersatzfestplatten an, die für den Knoten im ausgewählten Aggregat für den Cache verfügbar sind.

Bei einem Failover eines Aggregats an den Partner-Node zeigt Unified Manager nicht alle freien Festplatten an, die mit dem Aggregat kompatibel sind.

Enthält die folgenden Details für den gemeinsamen Cache:

◦ **Speicherpool**

Zeigt den Namen des Speicherpools an. Sie können den Zeiger über den Speicherpool-Namen verschieben, um folgende Details anzuzeigen:

- Status

  Zeigt den Status des Speicherpools an, der gesund oder ungesund sein kann.

- Gesamtzuweisungen

  Zeigt die Gesamtzuordnungseinheiten und die Größe im Speicherpool an.

- Größe Der Zuordnungseinheit

  Zeigt den minimalen Speicherplatz im Speicherpool an, der einem Aggregat zugewiesen werden kann.

        - Festplatten

          Zeigt die Anzahl der Laufwerke an, die zum Erstellen des Speicherpools verwendet werden. Wenn die Anzahl der Laufwerke in der Spalte „Speicherpool“ und die Anzahl der Festplatten, die auf der Registerkarte „Laufwerksinformationen“ für diesen Speicherpool angezeigt werden, nicht übereinstimmen, zeigt dies an, dass eine oder mehrere Festplatten beschädigt sind und der Speicherpool ungesund ist.

        - Zuweisung Verwendet

          Zeigt Anzahl und Größe der von den Aggregaten verwendeten Zuordnungseinheiten an. Sie können auf den Aggregatnamen klicken, um Details zum Aggregat anzuzeigen.

        - Verfügbare Zuweisung

          Zeigt die Anzahl und Größe der für die Nodes verfügbaren Zuweisungseinheiten an. Sie können auf den Node-Namen klicken, um weitere Details zum Aggregat anzuzeigen.

    - **Zugewiesener Cache**

      Zeigt die Größe der vom Aggregat verwendeten Zuordnungseinheiten an.

    - **Zuordnungseinheiten**

      Zeigt die Anzahl der vom Aggregat verwendeten Zuordnungseinheiten an.

    - **Festplatten**

      Zeigt die Anzahl der Festplatten im Speicherpool an.

    - **Details**
        - Storage-Pool

          Zeigt die Anzahl der Speicherpools an.

        - Gesamtgröße

          Zeigt die Gesamtgröße der Speicherpools an.

- * Cloud Tier*

  Zeigt den Namen der Cloud-Tier an, sofern Sie ein FabricPool-fähiges Aggregat konfiguriert haben und den insgesamt verwendeten Speicherplatz anzeigt. Wenn der Cloud-Tier zu einem anderen Cloud-Provider (der Spiegeltier) gespiegelt wird, werden hier die Details für beide Cloud-Tiers angezeigt

Registerkarte Konfiguration

Auf der Registerkarte Konfiguration werden Details zum ausgewählten Aggregat angezeigt, z. B. hinsichtlich seines Cluster-Nodes, des Blocktyps, des RAID-Typs, der RAID-Größe und der Anzahl der RAID-Gruppen:

- **Übersicht**
    - Knoten

      Zeigt den Namen des Node an, der das ausgewählte Aggregat enthält.

- Blocktyp

  Zeigt das Blockformat des Aggregats an: Entweder 32-Bit oder 64-Bit.

- RAID-Typ

  Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP, RAID-TEC oder gemischtes RAID).

- RAID-Größe

  Zeigt die Größe der RAID-Gruppe an.

- RAID-Gruppen

  Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

- SnapLock-Typ

  Zeigt den SnapLock-Typ des Aggregats an.

- * Cloud Tier*

  Wenn es sich um ein FabricPool-fähiges Aggregat handelt, werden die Details für die Cloud-Tier angezeigt. Einige Felder sind je nach Speicheranbieter unterschiedlich. Wenn die Cloud-Ebene zu einem anderen Cloud-Provider (die “mMirror Tier”) gespiegelt wird, werden hier beide Cloud-Tiers angezeigt.

  - Anbieter

    Zeigt den Namen des Storage-Providers an, z. B. StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud, Google Cloud Storage oder Alibaba Cloud Object Storage.

  - Name

    Zeigt den Namen des Cloud-Tiers an, als er von ONTAP erstellt wurde.

  - Server

    Zeigt den FQDN der Cloud-Tier an.

  - Port

    Der Port, der für die Kommunikation mit dem Cloud-Provider verwendet wird.

  - Auf Schlüssel oder Konto zugreifen

    Zeigt den Zugriffsschlüssel oder das Konto für die Cloud-Tier an.

  - Containername

    Zeigt den Bucket- oder Container-Namen des Cloud-Tiers an.

  - SSL

    Zeigt an, ob die SSL-Verschlüsselung für die Cloud-Ebene aktiviert ist.

Historienbereich

Im Bereich Verlauf werden Diagramme angezeigt, die Informationen über die Kapazität des ausgewählten Aggregats enthalten. Außerdem können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie anzeigen.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Fenster Verlauf auswählen. Sie können Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Verlaufsdiagramme können Ihnen bei der Identifizierung von Trends helfen: Wenn beispielsweise die Aggregatnutzung konsistent den Schwellenwert „nahezu voll“ überschreitet, können Sie die entsprechenden Maßnahmen ergreifen.

Verlaufsdiagramme zeigen folgende Informationen an:

- **Verwendete Aggregatskapazität (%)**

  Zeigt die verwendete Kapazität im Aggregat und den Trend in der Art und Weise an, wie die aggregierte Kapazität basierend auf dem Nutzungsverlauf als Liniendiagramme in Prozentsätzen auf der vertikalen (y) Achse verwendet wird. Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Kapazität verwendet“ klicken, wird die Diagramm-Zeile mit der verwendeten Kapazität ausgeblendet.

- **Verwendete Aggregatskapazität vs Gesamtkapazität**

  Zeigt den Trend in der Verwendung der Aggregatskapazität basierend auf dem Nutzungsverlauf sowie der verwendeten Kapazität und der Gesamtkapazität als Liniendiagramme in Byte, Kilobyte, Megabyte, Und so weiter, auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „verwendete Trend-Kapazität“ klicken, wird das Diagramm „verwendete Trendkapazität“ ausgeblendet.

- **Verwendete Aggregatskapazität (%) gegenüber dem Einsatz (%)**

  Zeigt den Trend an, wie die aggregierte Kapazität basierend auf dem Nutzungsverlauf verwendet wird, sowie den belegten Speicherplatz als Liniendiagramme in Prozent auf der vertikalen Achse (y). Der Zeitraum wird auf der horizontalen Achse (x) angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details zu bestimmten Punkten im Diagramm anzeigen, indem Sie den Cursor auf einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Space engagierte“ klicken, wird die Zeile „Space engagierte“ ausgeblendet.

Ereignisliste

In der Ereignisliste werden Details zu neuen und bestätigten Ereignissen angezeigt:

- **Severity**

  Zeigt den Schweregrad des Ereignisses an.

- **Veranstaltung**

  Zeigt den Ereignisnamen an.

- **Auslösezeit**

  Zeigt die Zeit an, die seit der Erzeugung des Ereignisses verstrichen ist. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel für den Zeitpunkt angezeigt, zu dem das Ereignis generiert wurde.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie den Clusterknoten, Volumes und Festplatten anzeigen, die mit dem Aggregat in Verbindung stehen:

- **Knoten**

  Zeigt die Kapazität und den Integritätsstatus des Node an, der das Aggregat enthält. Kapazität gibt die nutzbare Gesamtkapazität über die verfügbare Kapazität an.

- **Aggregate im Knoten**

  Zeigt die Anzahl und Kapazität aller Aggregate im Cluster-Node an, der das ausgewählte Aggregat enthält. Auf der Grundlage des höchsten Schweregrads wird der Systemzustand der Aggregate ebenfalls angezeigt. Wenn z. B. ein Cluster-Node zehn Aggregate enthält, von denen fünf den Warnstatus und die verbleibenden fünf den kritischen Status anzeigen, ist der angezeigte Status „kritisch“.

- **Bände**

  Zeigt die Anzahl und Kapazität der FlexVol Volumes und FlexGroup Volumes im Aggregat an. Die Anzahl umfasst keine FlexGroup-Komponenten. Auf der Grundlage des höchsten Schweregrades wird zudem der Integritätsstatus der Volumes angezeigt.

- **Ressourcen-Pool**

  Zeigt die mit dem Aggregat verbundenen Ressourcen-Pools an.

- **Festplatten**

  Zeigt die Anzahl der Festplatten im ausgewählten Aggregat an.

Bereich „Verwandte Warnungen“

Im Bereich „Related Alerts“ können Sie die Liste der Warnmeldungen anzeigen, die für das ausgewählte Aggregat erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link Warnung hinzufügen klicken oder eine vorhandene Warnung bearbeiten, indem Sie auf den Alarmnamen klicken.

Verwandte Informationen

"Anzeigen von Details zum Speicherpool"

Sichern und Wiederherstellen von Daten

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. Die Replizierung von einer 9.1 Quelle auf ein 9.0 Ziel wird nicht unterstützt, da auf dem Ziel eine frühere Hauptversion ausgeführt wird.

SnapMirror Asynchronous Protection mit versionsflexibler Replizierung

SnapMirror Asynchronous Schutz mit versionsflexibler Replizierung bietet einen logischen Spiegelschutz zwischen Quell- und Ziel-Volumes, auch wenn diese Volumes unter verschiedenen Versionen von ONTAP 8.3 oder höher ausgeführt werden (z. B. Version 8.3 auf 8.3.1, 8.3 zu 9.1 oder 9.2.2 zu 9.2).

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 Unified Replication (Spiegelung und Vault)

Dank der einheitlichen Replizierung mit SnapMirror können Disaster Recovery und Archivierung auf demselben Ziel-Volume konfiguriert werden. Wie bei SnapMirror führt die einheitliche Datensicherung beim ersten Aufruf einen Basistransfer durch. Ein Basistransfer unter der standardmäßigen, einheitlichen Datenschutzrichtlinie von „`MirrorAndVault`“ erstellt eine Snapshot Kopie des Quell-Volume, dann werden diese Kopie und die Datenblöcke übertragen, auf die sie auf das Ziel-Volume verweist. Wie bei SnapVault umfasst auch die Unified Datensicherung keine älteren Snapshot Kopien in der Basiskonfiguration.

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 von der Ansicht „Zustand: Alle Volumes“ oder der Seite „Volume / Health Details“ überwacht werden.

SnapMirror Active Sync

Die Funktion für die aktive Synchronisierung von SnapMirror ist mit ONTAP 9.8 und höher verfügbar und dient zum Schutz von Applikationen mit LUNs, sodass Applikationen transparent ein Failover durchführen können, sodass für den Fall, dass es zu einem Ausfall kommt, Business Continuity sichergestellt wird.

Damit können Sie die synchronen SnapMirror Beziehungen für Konsistenzgruppen (CGS) erkennen und überwachen, die auf Clustern und Storage Virtual Machines von Unified Manager verfügbar sind. SnapMirror Active Sync wird auf AFF Clustern oder auf All-SAN-Array (ASA) Clustern unterstützt, bei denen die primären und sekundären Cluster entweder AFF oder ASA sein können. SnapMirror Active Sync sichert Applikationen mit iSCSI- oder FCP-LUNs.

Wenn Sie die durch die SnapMirror Active Sync Beziehung geschützten Volumes und LUNs anzeigen, erhalten Sie eine einheitliche Ansicht für Sicherungsbeziehungen, Konsistenzgruppen in der Volume-Inventarisierung,

Sicherungstopologie für Konsistenzgruppenbeziehungen, Anzeigen von Verlaufsdaten für Konsistenzgruppenbeziehungen bis zu einem Jahr. Sie können den Bericht auch herunterladen. Sie können auch die Zusammenfassung der Konsistenzgruppenbeziehungen anzeigen, die Unterstützung von Konsistenzgruppenbeziehungen suchen und Informationen zu Volumes erhalten, die von der Konsistenzgruppe geschützt sind.

Auf der Seite „Beziehungen“ können Sie auch den Schutz der Quell- und Ziel-Storage-Objekte und ihre Beziehung, die durch die Konsistenzgruppe geschützt sind, sortieren, filtern und erweitern.

Weitere Informationen zu SnapMirror Active Sync finden Sie unter "ONTAP 9 Dokumentation für SnapMirror Active Sync (ehemals SM-BC)".

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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ 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.

Was Sie brauchen

- Die installierte Version von Workflow Automation muss 5.1 oder höher sein.

Das „`WFA Paket für das Management von Clustered Data ONTAP`“ ist in WFA 5.1 enthalten, sodass Sie dieses Paket nicht mehr aus dem NetApp Storage Automation Store herunterladen und es je nach Anforderung separat auf Ihrem WFA Server installieren müssen. "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 „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Workflow Automation**.
2. Wählen Sie im Bereich **Datenbankbenutzer** der Seite **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 **Workflow Automation Credentials** der Seite den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) sowie den Benutzernamen und das Passwort für das Workflow Automation Setup ein.

   Sie müssen den Unified Manager-Serverport verwenden (Port 443).

4. Klicken Sie Auf **Speichern**.
5. Wenn Sie ein selbstsigniertes Zertifikat verwenden, klicken Sie auf **Ja**, um das Sicherheitszertifikat zu autorisieren.

   Die Seite Workflow Automation wird angezeigt.

6. Klicken Sie auf **Ja**, um die Web-Benutzeroberfläche neu zu laden, und fügen Sie die Workflow-Automation-Funktionen hinzu.

Verwandte Informationen

"NetApp Dokumentation: OnCommand Workflow Automation (aktuelle Versionen)"

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.

Was Sie brauchen

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.

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.

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.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsfenster im linken Einrichtungsmenü auf **Allgemein** > **Workflow-Automatisierung**.
2. Klicken Sie auf der Seite **Workflow Automation** auf **Setup entfernen**.

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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ 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.

Eine SnapMirror Beziehung von der Seite „Volume/Health Details“ abbrechen

Sie können eine Sicherungsbeziehung von der Seite Volume / Health Details brechen 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Registerkarte **Schutz** der Seite **Volumen / Gesundheit** 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.

Rückkehrschutzbeziehungen auf der Seite Volume/Health 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ 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.
- 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 **Protection**-Registerkarte der **Volume / Health**-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 „Volume/Health Details“ wird ein Job-Link angezeigt.

4. **Optional:** Klicken Sie auf **Jobs anzeigen** auf der Seite **Volumen / Gesundheit** Details, um den Status jedes umgekehrten Neusynchronisierung zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.

5. **Optional:** Klicken Sie auf den Pfeil **Zurück** in Ihrem Browser, um zur Detailseite **Volumen / Gesundheit** zurückzukehren.

   Nach erfolgreichem Abschluss aller Jobaufgaben ist die Neusynchronisierung bei umgekehrter Neusynchronisierung abgeschlossen.

Entfernen einer Schutzbeziehung von der Seite Volume / Health 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Registerkarte **Protection** der Seite **Volume / Health** 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 Volume / Health Details entfernt.

Sicherungsbeziehungen von der Seite Volume / Health Details neu synchronisieren

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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Suchen Sie auf der Registerkarte **Schutz** der Seite **Volumen / Gesundheit** Details 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 auf die Seite Volume / Health Details zurückgeschickt und oben auf der Seite wird ein Link zu Jobs angezeigt.

9. **Optional:** Klicken Sie auf **Jobs anzeigen** auf der Seite **Volume / Health Details**, um den Status jedes Resynchronisierung Jobs zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.

10. **Optional:** Klicken Sie auf den Pfeil **Zurück** in Ihrem Browser, um zur Detailseite **Volumen / Gesundheit** 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.

Was Sie brauchen

Da für einige Aufgaben in diesem Workflow eine Anmeldung über die Administratorrolle erforderlich ist, müssen Sie mit den Rollen vertraut sein, die für die Verwendung verschiedener Funktionen erforderlich sind.

In diesem Szenario greifen Sie auf die Dashboard-Seite zu, um festzustellen, ob es Probleme mit Ihren Schutzaufgaben 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 im Bereich ungelöste Vorfälle und Risiken auf das Ereignis * Schutz Job fehlgeschlagen*.

   Der verknüpfte Text für das Ereignis wird in der Form geschrieben `object_name:/object_name - Error Name`, wiez. 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. Fahren Sie dann zur Seite Volume / Health Details, um weitere Informationen zu erhalten.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

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.

  Bei dem Job handelt es sich um eine Schutzbeziehung zwischen dem Quell-Volume `cluster2_src_vol2` `cluster2_src_svm` auf dem virtuellen Server und dem Ziel-Volume `managed_svc2_vol3` auf dem virtuellen Server mit dem Namen `cluster3_dst_svm`.

- Ein Snapshot Kopierauftrag für auf dem Quell-Volume `cluster2_src_svm:/cluster2_src_vol2` ist fehlgeschlagen `0426cluster2_src_vol2snap`.

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.

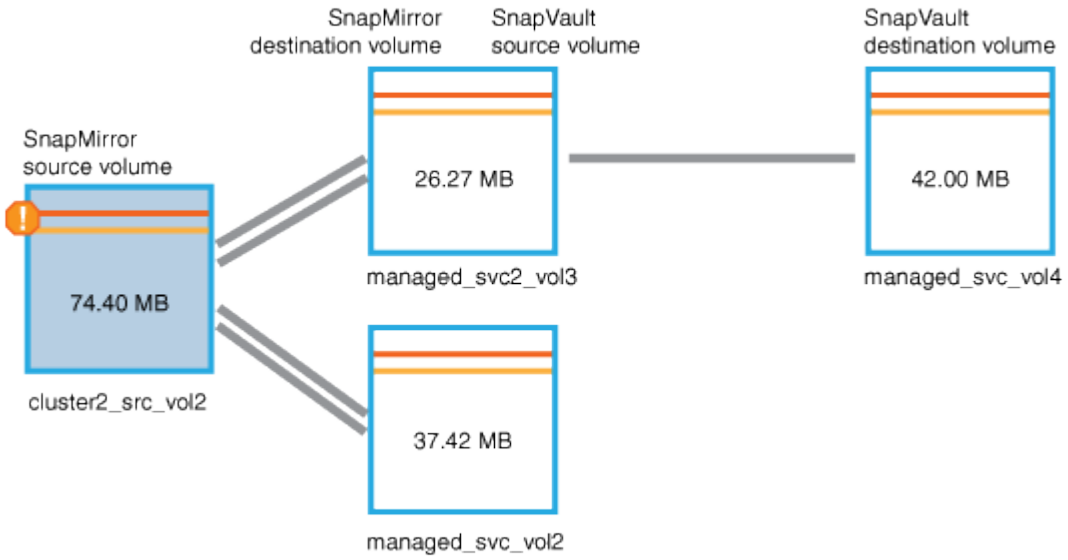
2. Sie entscheiden, dass Sie versuchen möchten, das Ereignis zu lösen, so gehen Sie wie folgt vor:
   a. Klicken Sie auf die Schaltfläche **Zuweisen zu** und wählen Sie im Menü die Option **ME** aus.
   b. Klicken Sie auf die Schaltfläche **Bestätigen**, damit Sie keine wiederholten Warnmeldungen erhalten, 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 Volume / Health Details wird für angezeigt, auf der der Inhalt der Registerkarte Protection angezeigt `cluster2_src_vol2` wird.

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` werden angezeigt.

7. Im Fenster **Kapazität** sehen Sie, 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. Unter dem Übersichtsbereich werden vorgeschlagene 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. Schauen Sie sich das übergeordnete Aggregat, `cluster2_src_aggr1`, im Bereich **Verwandte Geräte** an.

       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 Option zu aktivieren `volume autogrow`.

    Notieren Sie sich die Namen des Volumes und des Aggregats, sodass Sie sie bei der Aktivierung von Autogrow zur Verfügung haben.

15. Kehren Sie nach der Behebung des Kapazitätsproblem zur Detailseite für Unified Manager **Event** zurück, und markieren Sie 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 ManagerDashboard zu, um zu sehen, ob Probleme mit Ihren Schutzbeziehungen auftreten und, falls sie vorhanden sind, Lösungen zu finden.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Auf der Dashboard-Seite 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 **Protection** auf der Seite **Dashboard** den Fehler bezüglich SnapMirror Beziehung lag und klicken Sie darauf.

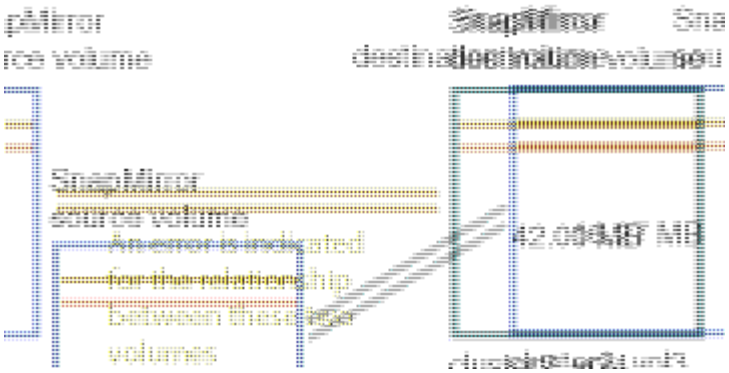
   Es wird die Seite Ereignisdetails für das Ereignis lag-Fehler angezeigt.

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 Volume / Health 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.

Managen und Überwachen von Sicherungsbeziehungen

Mit Active IQ Unified Manager können Sie Sicherungsbeziehungen erstellen, SnapMirror und SnapVault Beziehungen auf gemanagten Clustern überwachen und Fehler beheben und Daten beim Überschreiben oder Verlust wiederherstellen.

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.

Anzeigen des Volume-Sicherungsstatus

Die Seite Datensicherung bietet eine ganzheitliche Übersicht über die Datensicherungsdetails für alle geschützten Volumes in einem einzelnen Cluster oder alle

Cluster eines Datacenters.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Je nachdem, ob Sie den Datenschutzstatus für alle überwachten Cluster oder für einen einzelnen Cluster anzeigen möchten, wählen Sie **Alle Cluster** oder wählen Sie einen einzelnen Cluster aus dem Dropdown-Menü aus.
3. Klicken Sie auf den Rechtspfeil oben im Bereich Datenschutz. Die Seite **Datenschutz** wird angezeigt.

Je nachdem, ob Sie ein einzelnes oder alle Cluster im Datacenter ausgewählt haben, wird auf dieser Seite der Datensicherungsstatus der durch Snapshot Kopien oder SnapMirror Richtlinien geschützten Volumes angezeigt. Außerdem wird die Anzahl der nicht geschützten Volumes angezeigt.

Durch Auswahl eines Clusters aus der Liste **individueller Cluster** werden die Snapshot-Sicherung und der SnapMirror Beziehungsstatus der geschützten Volumes in diesem Cluster angezeigt.

Wenn Sie auf dieser Seite auf die Ereignisse klicken, gelangen Sie zur Seite mit den Veranstaltungsdetails. Sie können auf den Link * Alle anzeigen* klicken, um alle aktiven Schutzereignisse auf der Seite Ereignisverwaltung Inventar anzuzeigen. Sie können mit der Maus die entsprechenden Zählungen und Legenden anzeigen. Klicken Sie auf:

- Die Balkendiagramme für nicht geschützte Volumes und durch Snapshot-Kopien geschützte Volumes sind, werden zur Seite „Volumes“ und zur Ansicht der Details angezeigt.
- Die Balkendiagramme für alle Beziehungen werden auf die Seite „Beziehungen“ angezeigt, auf der die Details nach dem Quellcluster gefiltert werden.

Anzeige des Sicherungsstatus von durch Snapshot Kopien geschützten Volumes

Snapshot Kopien Übersicht: Eine Übersicht über die durch Snapshot Kopien geschützten Volumes, wie z. B.:

- Die Gesamtzahl der geschützten und nicht durch Snapshot Kopien geschützten Volumes.
- Die Gesamtzahl der Volumes, die den Reservespeicherplatz für die Snapshot Kopien nutzen oder übersteigen.

Snapshot Kopien Analysis enthält folgende Informationen:

- Einzelne Ereignisse für Snapshot-Kopien, einschließlich der in den letzten 24 Stunden aufgeworfenen Ereignisse
- Detaillierte Tabelle für Volumes, die geschützt sind und nicht durch Snapshot-Kopien geschützt sind.
- Volumes verwenden, nicht verwenden und durchbrechen die Kapazität der reservierten Snapshot-Kopie.
- Die Aufsplits der Volumes in Bezug auf die Anzahl ihrer Snapshot-Kopien.

Verweist auf die Anmerkung für Snapshot-Kopien

- Zur Zählung der durch Snapshot Kopien geschützten Volumes werden sowohl Quell- als auch Ziel-Volumes berücksichtigt.
- Die Anzahl der zurückgegebenen Snapshot-Kopien gilt nur für die Volumes, die online und verfügbar sind.
- Der Diagrammbereich für die Anzahl der Snapshot Kopien ist dynamisch. Sie wird auf Basis der Anzahl der Snapshots generiert, die im ausgewählten Cluster vorhanden sind.
- Wenn Sie ein Volume als gesichert betrachten, sollte der Zeitplan für die Snapshot-Kopie des Volumes

aktiviert sein.

- Der Wert für den reservierten Speicherplatz für Snapshot-Kopien ist wichtig, um zu sehen, wie viel Speicherplatz genutzt wird, oder um den Speicherplatz zu berechnen, der zurückgewonnen werden kann, wenn eine oder mehrere Snapshot-Kopien gelöscht werden.

Anzeige des Sicherungsstatus von SnapMirror Beziehungen

SnapMirror Overview: Eine Übersicht über die durch SnapMirror-Richtlinien geschützten Volumes, wie z. B.:

- Anzahl der Volumes, die durch die jeweiligen SnapMirror Richtlinien gesichert werden, z. B. Volume-SnapMirror Beziehungen, Disaster Recovery für Storage VMs (SVM-DR) und ihre Kombinationen aus diesen Ressourcen.
- Die Gesamtzahl der SnapMirror Beziehungen, die bezüglich der Verzögerung des Recovery Point Objective (RPO) liegen, basierend auf dem Verzögerungsstatus.

SnapMirror Analysis enthält folgende Informationen:

- Einzelne Ereignisse für SnapMirror Beziehungen, einschließlich der in den letzten 24 Stunden aufgeworfenen Ereignisse
- Die Anzahl der durch jeden Typ der SnapMirror-Richtlinie geschützten Volumes.
- Die Anzahl der durch die SnapMirror-Beziehungstypen geschützten Beziehungen, z. B. Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StricxtSync, SnapMirror Active Sync Consistency Group und Sync.
- Die Anzahl der gesunden und ungesunden Beziehungen.
- Aufbrechen der Anzahl der Volume-Beziehungen Sie können die Diagramme nach RPO-Verzögerungszeit und Status umschalten.
- Lag-Schwellenwerte für nicht gemanagte Beziehungen. Sie können auf das Einstellungssymbol () klicken , um die Verzögerungsschwellenwerteinstellungen zu konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren von Verzögerungsschwellenwerten für nicht verwaltete Schutzbeziehungen".

Punkte, die für SnapMirror Beziehungen zu beachten sind

- Beim Zählen von SnapMirror Beziehungen werden die Quell-Volumes gezählt, die zum Lesen und Schreiben aktiviert sind. Ziel- und Root-Volumes werden nicht berücksichtigt.
- Für die SnapMirror Beziehung werden die Ereignisse für das Quell-Cluster angezeigt.
- Die Anzahl der SnapMirror Beziehung umfasst die Anzahl der Volumes mit Quellen und Zielen im selben oder verschiedenen Cluster.
- Die Verzögerungsdauer der RPO-Verzögerung bei der Datenreplizierung basiert auf der SnapMirror-Beziehung. Der Status wird basierend auf dem Beziehungsschwellenwert als, `warning` oder `error`, kategorisiert. `ok` Sie können den Status überprüfen, um zu bestimmen, ob die Parameter wie erwartet funktionieren oder ob Sie Probleme beheben müssen.
- Wenn ein Volume über mehrere SnapMirror-Beziehungen verfügt, wird jeder Beziehungstyp auf die RPO-Verzögerung gezählt.
- Volume-Beziehungen werden als ungesund betrachtet, wenn bei der Datenreplizierung zwischen Quelle und Ziel Probleme auftreten, beispielsweise wenn die Beziehung unterbrochen ist.

Zeigen Sie durch die MetroCluster-Konfiguration geschützte Cluster an

Im Fenster **MetroCluster-Schutz** auf der Seite **Datenschutz** wird die Anzahl der durch MetroCluster über FC oder IP geschützten Cluster an Ihrem Standort angezeigt. Wenn Sie auf die Balkendiagramme in diesem Bereich klicken, gelangen Sie zur Seite Cluster, auf der die Cluster-Details basierend auf den geschützten oder ungeschützten Clustern gefiltert werden. Informationen zum Monitoring Ihrer MetroCluster-Konfiguration finden Sie unter "Monitoring der MetroCluster Konfigurationen".

Anzeigen von Volume-Sicherungsbeziehungen

Aus der Ansicht „Beziehungen“: Alle Beziehungen und auf der Seite „Volume-Beziehungen“ können Sie den Status vorhandener Volume SnapMirror und SnapVault Beziehungen anzeigen. Sie können auch Details zu Sicherungsbeziehungen unter anderem hinsichtlich Transfer- und lag-Status, Quell- und Zieldetails, Zeitplan- und Richtlinieninformationen usw. prüfen.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können auch Beziehungsbefehle von dieser Seite aus initiieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Beziehung** > **Alle Beziehungen**.

   Die Ansicht „Beziehung: Alle Beziehungen“ wird angezeigt.

3. Es gibt folgende Möglichkeiten, die Details zur Volume-Sicherung anzuzeigen:

   - Um aktuelle Informationen über alle Volume-Beziehungen anzuzeigen, bleiben Sie auf der Standard **Alle Beziehungen** Seite.
   - Um detaillierte Informationen zu den Trends der Volume-Übertragung über einen bestimmten Zeitraum anzuzeigen, wählen Sie im Menü Ansicht die Option Beziehung: Status der letzten 1 Monate übertragen.
   - Um detaillierte Informationen über die Aktivität der Volume-Übertragung auf Tagesbasis anzuzeigen, wählen Sie im Menü Ansicht die Option Beziehung: Letzte 1 Monat Transferrate.

   Die Volume-Transferansichten zeigen Informationen zu Volumes nur in asynchronen Beziehungen an - Volumes in synchronen Beziehungen werden nicht angezeigt.

Überwachung von LUNs in einer Konsistenzgruppe

Wenn Ihre ONTAP Umgebung SnapMirror Active Sync unterstützt, um Applikationen mit LUNs zu schützen, können Sie diese LUNs auf Active IQ Unified Manager anzeigen und überwachen.

SnapMirror Active Sync sorgt für null Recovery Time Objective (RTO) während des Failovers in SAN-Umgebungen. In einer typischen Bereitstellung, die SnapMirror Active Sync unterstützt, sind die LUNs auf Volumes durch Beziehungen zu Konsistenzgruppen geschützt.

Diese primären und sekundären LUNs sind zusammengesetzte LUNs oder ein LUN-Replikatpaar mit derselben UUID und Seriennummer. Die I/O-Vorgänge (sowohl Lese- als auch Schreibvorgänge) werden über die Quell- und Zielstandorte auf diesen zusammengesetzten LUNs multipliziert, wodurch Transparenz gewährleistet wird.

Zur Anzeige zusammengesetzter LUNs sollten sowohl die primären als auch die sekundären Cluster mit den LUNs, die Teil der Consistency Group-Beziehung sind, hinzugefügt und in Unified Manager entdeckt werden. Es werden nur iSCSI- und FCP-LUNs unterstützt.

Informationen über SnapMirror Active Sync finden Sie unter "ONTAP 9 Dokumentation für SnapMirror Active Sync (ehemals SM-BC)".

Um sich zusammengesetzte LUNs in Ihrer Umgebung anzusehen, folgen Sie den folgenden Schritten:

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **LUNs**.
2. Wählen Sie im Menü Ansicht die Option **Beziehung** > **Alle LUNs**.

   Die Beziehung: Alle LUNs-Ansicht wird angezeigt.

Sie können die LUN-Details anzeigen, z. B. den LUN-Namen, das Volume, eine Storage-VM mit LUN, Cluster, Konsistenzgruppe und der Partner-LUN. Sie können auf jede dieser Komponenten klicken, um eine detaillierte Ansicht aufzurufen. Wenn Sie auf die Konsistenzgruppe klicken, gelangen Sie zur Seite Beziehungen.

Durch Klicken auf die Partner-LUN können Sie die Konfigurationsdetails auf der Registerkarte SAN auf der Seite Storage VM Details der Storage VM anzeigen, auf der die Partner-LUN gehostet wird. Informationen wie die Initiatoren, Initiatorgruppen und andere Aspekte der Partner-LUN werden angezeigt.

Sie können die standardmäßigen Funktionen auf Grid-Ebene zum Sortieren, Filtern, Erstellen und Hochladen von Berichten für die geschützten LUNs in Ihrer Umgebung ausführen.

Erstellen einer SnapVault-Schutzbeziehung aus der Ansicht „Systemzustand: Alle Volumes“

Sie können die Ansicht Systemzustand: Alle Volumes verwenden, um SnapVault-Beziehungen für ein oder mehrere Volumes auf derselben Storage-VM zu erstellen, um Daten-Backups zu Sicherungszwecken zu ermöglichen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

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 besteht und der Ziel-Cluster noch nicht erkannt wurde

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.

2. Wählen Sie in der Ansicht **Gesundheit: Alle Volumen** ein Volumen aus, das Sie schützen möchten, und klicken Sie auf **schützen**.

   Wenn Sie mehrere Sicherungsbeziehungen auf derselben virtuellen Speichermaschine (SVM) erstellen möchten, wählen Sie in der Ansicht Systemzustand: Alle Volumes ein oder mehrere Volumes aus, und klicken Sie in der Symbolleiste auf **schützen**.

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 werden wieder in die Ansicht „Health: All Volumes“ angezeigt.

8. Klicken Sie oben in der Ansicht **Gesundheit: Alle Volumes** auf den Link für die Schutzkonfiguration.

   Wenn Sie nur eine Schutzbeziehung erstellen, wird die Seite 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 „Volume/Health Details“

Sie können eine SnapVault-Beziehung auf der Seite Volume / Health Details erstellen, so dass Daten-Backups für Sicherungszwecke auf Volumes aktiviert sind.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten, um diese Aufgabe auszuführen.

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 besteht und der Ziel-Cluster noch nicht erkannt wurde

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Volumen / Gesundheit** 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 Volume / Health Details.
7. Klicken Sie oben auf der Seite **Volumen / Gesundheit** Details auf den Link für die Schutzkonfiguration.

   Die Seite 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 Volume / Health Details angezeigt.

Erstellen einer SnapMirror Schutzbeziehung aus der Ansicht „Systemzustand: Alle Volumes“

Nutzung der Ansicht „Systemzustand“: Alle Volumes ermöglichen das Erstellen mehrerer SnapMirror Sicherungsbeziehungen gleichzeitig, indem Sie mehrere Volumes auf derselben Storage-VM auswählen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

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 besteht und der Ziel-Cluster

noch nicht erkannt wurde

Schritte

1. Wählen Sie in der Ansicht **Gesundheit: Alle Volumes** ein Volume aus, das Sie schützen möchten.

   Wenn Sie mehrere Sicherungsbeziehungen auf derselben SVM erstellen möchten, wählen Sie in der Ansicht Systemzustand: Alle Volumes ein oder mehrere Volumes aus, und klicken Sie in der Symbolleiste auf **schützen** > **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 werden wieder in die Ansicht „Health: All Volumes“ angezeigt.

6. Klicken Sie oben in der Ansicht **Gesundheit: Alle Volumen** auf den Link für die Schutzkonfiguration.

   Wenn Sie nur eine Schutzbeziehung erstellen, wird die Seite 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.

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.
- Falls Sie eine Ziel-SVM angegeben haben, die im Vergleich zur Version des Quell-Volumes unter derselben oder einer neueren Version von ONTAP läuft, jedoch in den erweiterten Einstellungen versionsflexible Replizierung aktiviert wurde, ist das Ergebnis eine SnapMirror Beziehung mit versionsflexibler Replizierung.

- Wenn Sie eine Ziel-SVM angegeben haben, die unter einer früheren Version von ONTAP ausgeführt wird als jene des Quell-Volume, und die frühere Version unterstützt versionsflexible Replizierung. Das automatische Ergebnis ist eine SnapMirror Beziehung mit versionsflexibler Replizierung.

Erstellen einer SnapMirror Schutzbeziehung auf der Seite „Volume/Health Details“

Sie können auf der Seite Volume-/Integritätsdetails eine SnapMirror Beziehung erstellen, sodass die Datenreplizierung zu Sicherungszwecken aktiviert wird. Die SnapMirror Replizierung ermöglicht Ihnen die Wiederherstellung von Daten vom Ziel-Volume im Falle eines Datenverlusts auf dem Quellsystem.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

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 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 **Volumen / Gesundheit** 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 Volume / Health Details.

7. Klicken Sie oben auf der Seite **Volumen / Gesundheit** Details auf den Link für die Schutzkonfiguration.

   Die Aufgaben und Details des Jobs werden auf der Seite Jobdetails angezeigt.

8. Klicken Sie auf der Seite **Job** Details auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und bestimmen Sie, wann der Job abgeschlossen ist.

9. Wenn die Aufgaben abgeschlossen sind, klicken Sie auf **Zurück** in Ihrem Browser, um zur Detailseite **Volumen / Gesundheit** zurückzukehren.

   Die neue Beziehung wird auf der Topologieansicht Volume / Health Details angezeigt.

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.
- Falls Sie eine Ziel-SVM angegeben haben, die im Vergleich zur Version des Quell-Volumes unter derselben oder einer neueren Version von ONTAP läuft, jedoch in den erweiterten Einstellungen versionsflexible Replizierung aktiviert wurde, ist das Ergebnis eine SnapMirror Beziehung mit versionsflexibler Replizierung.
- Wenn Sie eine Ziel-SVM angegeben haben, die unter einer früheren Version von ONTAP 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ 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.

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 der Seite Volume / Health Details anzeigen, klicken Sie mit der rechten Maustaste in die Topologieansicht, die den Namen eines Volumes hat, das Sie schützen möchten, und wählen Sie im Menü **Protect** > **SnapMirror** aus.
   - Wenn Sie die Ansicht Health: All Volumes anzeigen, suchen Sie ein Volume, das Sie schützen möchten, und klicken Sie mit der rechten Maustaste darauf; wählen Sie dann aus dem Menü **schützen** > **SnapMirror**. 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 Volume / Health Details.

6. Klicken Sie oben auf der Seite **Volumen / Gesundheit** Details auf den Link für die Schutzkonfiguration.

   Die Aufgaben und Details der Aufträge werden auf der Seite Job Details angezeigt.

7. Klicken Sie auf der Seite **Job** Details auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und bestimmen Sie, wann der Job abgeschlossen ist.
8. Wenn die Aufgaben abgeschlossen sind, klicken Sie auf **Zurück** in Ihrem Browser, um zur Detailseite **Volumen / Gesundheit** zurückzukehren.

   Die neue Beziehung wird auf der Topologieansicht Volume / Health 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ 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 von ONTAP ausgeführt werden, die eine versionsflexible Replizierung unterstützt.

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 auf der Seite Volume / Health Details die Registerkarte Schutz anzeigen, klicken Sie mit der rechten Maustaste in die Topologieansicht auf den Namen eines Volumes, das Sie schützen möchten, und wählen Sie im Menü **Protect** > **SnapMirror** aus.
- Wenn Sie die Ansicht Health: All Volumes anzeigen, suchen Sie ein Volume, das Sie schützen möchten, und klicken Sie mit der rechten Maustaste darauf; wählen Sie dann aus dem Menü **schützen** > **SnapMirror**. 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 Volume / Health Details.

8. Klicken Sie oben auf der Seite **Volumen / Gesundheit** Details auf den Link für die Schutzkonfiguration.

   Die Aufgaben und Details der Aufträge werden auf der Seite Job Details angezeigt.

9. Klicken Sie auf der Seite **Job** Details auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und bestimmen Sie, wann der Job abgeschlossen ist.
10. Wenn die Aufgaben abgeschlossen sind, klicken Sie auf **Zurück** in Ihrem Browser, um zur Detailseite **Volumen / Gesundheit** zurückzukehren.

    Die neue Beziehung wird auf der Topologieansicht Volume / Health 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.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ 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.

Sie können die Sicherung auf Volumes mithilfe der Konsistenzgruppe erweitern. Hierbei handelt es sich um einen Container mit mehreren Volumes, sodass Sie alle Volumes als eine Einheit verwalten können. Sie können die SnapMirror Active Sync Konsistenzgruppe und die synchrone Konsistenzgruppenbeziehung auf der Seite Beziehungen von Unified Manager anzeigen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Klicken Sie Auf **Schutz** > **Beziehungen**. Alternativ können Sie die Beziehungen auf der Seite Volume Details anzeigen.
2. Wählen Sie auf der Seite **Volume Relationships** 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** abhängig von der Art der Schutzbeziehung, die Sie erstellen.

   Das Dialogfeld **Schutz konfigurieren** wird angezeigt.

   Dies kann auf der Seite Unified Relationship / Volume Relationship und Volume / Health Details erreicht werden.

6. Füllen Sie die Informationen aus, wie im Dialogfeld **Schutz konfigurieren** angegeben.

Bearbeiten von Schutzbeziehungen auf der Seite Volume Relationships

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.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

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 **Volume Relationships** in den Volumes eine 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 Volume / Health Details

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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Workflow Automation muss installiert und konfiguriert sein.

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 **Schutz**-Registerkarte der Seite **Volumen / Gesundheit** 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 „Beziehung 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ 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. **Optional:** 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 Datensicherung wird von der Seite „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.

Sie können Volume-Beziehungen, die von der Konsistenzgruppe geschützt sind, nicht abbrechen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

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 **Volume Relationships** 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 Volume-Beziehungen angezeigt, zusammen mit einem Link zu den Jobdetails.

4. **Optional:** Klicken Sie auf den Link **Details anzeigen**, um zur Seite **Job** Details weitere Details zu gelangen und den Fortschritt der Aufträge anzuzeigen.

Aktive Datensicherung wird von der Seite Volume / Health 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.

Sie können Volume-Beziehungen, die von der Konsistenzgruppe geschützt sind, nicht abbrechen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

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 **Volumen / Gesundheit** mit der rechten Maustaste auf die Beziehung in der Topologieansicht für die Datenübertragung, die Sie abbrechen möchten, und wählen Sie **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 Abbruchvorgangs wird oben auf der Seite Volume / Health Details sowie ein Link zu den Jobdetails angezeigt.

4. **Optional:** Klicken Sie auf den Link **Details anzeigen**, um zur Seite **Job** Details weitere Details zu gelangen und den Fortschritt der Aufträge anzuzeigen.
5. Klicken Sie auf jeden Job, um seine Details anzuzeigen.
6. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Detailseite **Volumen / Gesundheit** zurückzukehren.

   Der Abbruchvorgang ist abgeschlossen, wenn alle Aufgabenstellungen erfolgreich abgeschlossen wurden.

Eine Schutzbeziehung wird auf der Seite Volume Relationships stillgelegt

Auf der Seite „Volume Relationships“ können Sie 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 des Snapshot Kopiervorgangs stabil ist.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

- Sie müssen Workflow Automation einrichten.

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 besteht 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 **Volume Relationships** eine 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 Volume / Health Details angezeigt, zusammen mit einem Link zu den Jobdetails.

3. Klicken Sie auf den Link **Details anzeigen**, um zur Seite **Job**-Details weitere Details und den Job-Fortschritt aufzurufen.
4. **Optional:** Klicken Sie auf den Pfeil **Zurück** auf Ihrem Browser, um zur Seite **Volume Relationships** zurückzukehren.

   Der quiesce-Job ist abgeschlossen, wenn alle Arbeitsaufgaben erfolgreich abgeschlossen wurden.

Eine Schutzbeziehung wird auf der Seite „Volume/Health 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

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 der 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 **Volumen / Gesundheit** 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 Volume / Health Details angezeigt, zusammen mit einem Link zu den Jobdetails.

4. Klicken Sie auf den Link **Details anzeigen**, um zur Seite **Job**-Details weitere Details und den Job-Fortschritt aufzurufen.
5. **Optional:** Klicken Sie auf den Zurück-Pfeil in Ihrem Browser, um zur Detailseite **Volumen / Gesundheit** zurückzukehren.

   Der quiesce-Job ist abgeschlossen, wenn alle Arbeitsaufgaben erfolgreich abgeschlossen wurden.

Brechen einer SnapMirror Beziehung von der Seite „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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Seite **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 **Volume Relationships** in der Spalte **Relationship State**, ob die Beziehung unterbrochen ist.

   Die Spalte „Beziehungsstatus“ ist standardmäßig ausgeblendet, daher müssen Sie sie möglicherweise in der Spaltenliste ein-/ausblenden auswählen  .

Entfernen einer Schutzbeziehung von der Seite Volume Relationships

Auf der Seite Volume Relationships können Sie eine Schutzbeziehung entfernen, um eine vorhandene 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Seite **Volume Relationships** 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 Volume Relationships entfernt.

Wiederaufnahme geplanter Transfers für eine stillgelegte Beziehung von der Seite Volume-Beziehungen

Nachdem Sie eine Beziehung stillgelegt haben, um geplante Transfers zu stoppen, können Sie **Resume** verwenden, um geplante Transfers wieder zu aktivieren, damit Daten auf dem Quell- oder Primärvolume geschützt sind. Transfers werden im nächsten geplanten Transferintervall von einem Kontrollpunkt fortgesetzt, falls vorhanden.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Sie können maximal 10 stillgelegene Beziehungen auswählen, auf denen die Übertragung fortgesetzt werden soll.

Schritte

1. Wählen Sie auf der Seite Volume **Relationships** ein oder mehrere Volumes mit stillgelegten Beziehungen aus, und klicken Sie in der Symbolleiste auf **Fortsetzen**.
2. Klicken Sie im Dialogfeld **Fortsetzen** auf **Weiter**.

   Sie werden zur Seite Volume Relationships zurückkehren.

3. Um die zugehörigen Aufgaben anzuzeigen und deren Fortschritt zu verfolgen, klicken Sie auf den Job-Link, der oben auf der Seite **Volume Relationships** angezeigt wird.
4. Führen Sie einen der folgenden Schritte aus:
   - Wenn nur ein Job angezeigt wird, klicken Sie auf der Seite Jobdetails auf **Aktualisieren**, um die Aufgabenliste und die mit dem Konfigurationsauftrag für den Schutz verknüpften Aufgaben zu aktualisieren und zu bestimmen, wann der Job abgeschlossen ist.
   - Wenn mehrere Jobs angezeigt werden,
     i. Klicken Sie auf der Seite Jobs auf den Job, für den Sie die Details anzeigen möchten.
     ii. Klicken Sie auf der Seite 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 Volume / Health Details

Nachdem Sie eine Beziehung stillgelegt haben, um geplante Transfers zu stoppen, können Sie **Resume** auf der Seite Volume / Health 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Volumen / Gesundheit** 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 Volume / Health Details.

3. Um die zugehörigen Aufgaben anzuzeigen und deren Fortschritt zu verfolgen, klicken Sie auf den Job-Link, der oben auf der Seite **Volumen / Gesundheit** Details angezeigt wird.
4. Klicken Sie auf der Seite **Job** Details auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Konfigurationsauftrag für den Schutz verknüpft sind, und bestimmen Sie, wann der Job abgeschlossen ist.

   Nach Abschluss der Jobs werden die Datenübertragungen im nächsten geplanten Übertragungsintervall fortgesetzt.

Schutzbeziehungen werden auf der Seite Volume-Beziehungen initialisiert oder aktualisiert

Auf der Seite Volume Relationships können Sie eine erste Baseline-Übertragung 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.

Sie können Volumes, die durch Konsistenzgruppen geschützt sind, nicht initialisieren oder aktualisieren.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Klicken Sie auf der Seite **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 zurück 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 Updatejob wird gestartet, Sie gelangen wieder zur Seite Volume-Beziehungen und oben auf der Seite wird ein Link zu Jobs angezeigt.

8. **Optional:** Klicken Sie auf **Jobs anzeigen** in der Ansicht **Gesundheit: Alle Volumes**, um den Status jedes Initialisierungs- oder Aktualisierungs-Jobs zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.

9. **Optional:** Klicken Sie auf jeden Job, um seine Details anzuzeigen.
10. **Optional:** Klicken Sie auf den Pfeil **Zurück** auf Ihrem Browser, um zur Seite **Volume Relationships** zurückzukehren.

    Der Initialisierungs- oder Aktualisierungsvorgang ist abgeschlossen, wenn alle Aufgaben erfolgreich abgeschlossen wurden.

Initialisierung oder Aktualisierung von Schutzbeziehungen auf der Seite Volume / Health 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.

HINWEIS: Sie können Volumes, die durch Consistency Groups geschützt sind, nicht initialisieren oder

aktualisieren.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Suchen Sie auf der Registerkarte **Schutz** der Seite **Volume / Health** 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 Updatejob wird gestartet, Sie gelangen wieder zur Seite Volume / Health Details und oben auf der Seite wird ein Link Jobs angezeigt.
9. **Optional:** Klicken Sie auf **Jobs anzeigen** auf der Seite **Volumen / Gesundheit** Details, um den Status jedes Initialisierungs- oder Aktualisierungs-Jobs zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.
10. **Optional:** Klicken Sie auf jeden Job, um seine Details anzuzeigen.
11. **Optional:** Klicken Sie auf den Zurück-Pfeil in Ihrem Browser, um zur Detailseite **Volumen / Gesundheit** zurückzukehren.

    Der Initialisierungs- oder Aktualisierungsvorgang ist abgeschlossen, wenn alle Aufgabenstellungen erfolgreich abgeschlossen wurden.

Sicherungsbeziehungen von der Seite Volume Relationships neu synchronisieren

Auf der Seite Volume Relationships 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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Seite **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 Neusynchronisierung Job wurde gestartet, Sie werden zur Seite Volume Relationships zurückgegeben und ein Link für Jobs wird oben auf der Seite angezeigt.

8. **Optional:** Klicken Sie auf **Jobs anzeigen** auf der Seite **Volume Relationships**, um den Status jedes Resynchronisierung Jobs zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.

9. **Optional:** Klicken Sie auf den Pfeil **Zurück** auf Ihrem Browser, um zur Seite **Volume Relationships** zurückzukehren.

   Die Neusynchronisierung ist nach erfolgreichem Abschluss aller Aufgabenstellungen abgeschlossen.

Schutzbeziehungen auf der Seite Volume Relationships rückgängig machen

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.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ 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.
- 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 **Volume Relationships** ein oder mehrere Volumes mit Beziehungen aus, die Sie umkehren möchten, und klicken Sie in der Symbolleiste auf **Resync rückwärts**.

   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**.

   Der Vorgang der umgekehrten Neusynchronisierung wird gestartet, Sie werden zur Seite Volume Relationships zurückkehren und ein Link zu Jobs wird oben auf der Seite angezeigt.

3. **Optional:** Klicken Sie auf **Jobs anzeigen** auf der Seite **Volume Relationships**, um den Status jedes Reverse Resynchronisierung Jobs zu verfolgen.

   Eine gefilterte Liste der Jobs, die mit diesem Vorgang in Verbindung stehen, wird angezeigt.

4. **Optional:** Klicken Sie auf den Pfeil **Zurück** auf Ihrem Browser, um zur Seite **Volume Relationships** zurückzukehren.

   Nach erfolgreichem Abschluss aller Jobaufgaben ist die Neusynchronisierung bei umgekehrter Neusynchronisierung abgeschlossen.

Wiederherstellen von Daten mithilfe der Seiten Volume- und Volume-/Health-Details

Sie können überschreibte oder gelöschte Dateien, Verzeichnisse oder ein gesamtes Volume anhand einer Snapshot Kopie wiederherstellen. Hierzu verwenden Sie die Wiederherstellungsfunktion auf den Seiten „Volume and Volume/Health Details“.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Beachten Sie folgende Punkte:

- 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 für die synchrone SnapMirror Replizierung konfiguriert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherung > Volumes**.
2. Wählen Sie die Lautstärke aus und klicken Sie auf die Schaltfläche **Wiederherstellen**. Klicken Sie alternativ auf das Volume, um zu **Volume / Health Details > Aktionen > Wiederherstellen** zu wechseln. Das Dialogfeld Wiederherstellen wird angezeigt. Informationen zu dieser Seite finden Sie unter "Dialogfeld „Wiederherstellen“".
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 wiederhergestellt werden sollen, z. B. die Quell-LUN.

   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 Ziel-Cluster, die Storage VM (SVM) und das Volume aus, das Sie wiederherstellen möchten.
     ii. Wählen Sie in der Tabelle Name einen Verzeichnisnamen aus, der wiederhergestellt werden soll.
     iii. Klicken Sie Auf **Verzeichnis Auswählen**.
7. Klicken Sie Auf **Wiederherstellen**.

   Der Wiederherstellungsprozess beginnt. Zum Abschluss des Wiederherstellungsprozesses wird im Backend ein Job erstellt.

8. Wenn Sie den Job-Fortschritt anzeigen möchten, navigieren Sie im linken Navigationsbereich zu **Schutz > Jobs**, um den Status des Wiederherstellungsjobs aus der Liste der Jobs anzuzeigen.

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 diese Konfiguration mithilfe von BlueXP aus.

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.

Erstellen von Ressourcenpools

Sie können das Dialogfeld Ressourcen-Pool erstellen verwenden, um Aggregate für Bereitstellungszwecke zu gruppieren.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

Ressourcen-Pools können Aggregate von verschiedenen Clustern enthalten, aber das gleiche Aggregat kann nicht zu verschiedenen Ressourcen-Pools gehören.

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcen-Pools**.
2. Klicken Sie auf der Seite **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.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

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 „Ressourcen-Pools“ können Sie den Ressourcenpoolbestand anzeigen und die verbleibende Kapazität für jeden Ressourcenpool überwachen.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritt

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.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

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.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

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.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

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.

Monitoring der Disaster-Recovery-Sicherungsbeziehungen für Storage VMs

Active IQ Unified Manager unterstützt das Monitoring von Disaster-Recovery-Beziehungen für Storage-VMs, sodass Disaster Recovery auf Ebene einer Storage-VM möglich ist. Die Disaster Recovery für Storage-VMs ermöglicht die Wiederherstellung der vorhandenen Daten in den zusammengehörigen Volumes der Storage-VM und der Wiederherstellung der Storage-VM-Konfiguration.

Zur Gewährleistung eines asynchronen Disaster Recoverys wird eine DR-Beziehung zwischen Storage und einer Storage VM auf der Quell-Storage-VM der Ziel-Storage-VM erstellt. Sie können entweder die gesamte Storage-VM-Konfiguration oder den Teil der Storage-VM-Konfiguration replizieren (außer Netzwerk- und Protokollkonfiguration) und die Daten-Volumes basierend auf dem Cluster-Setup.

Nachdem die Disaster Recovery-Beziehung für die Storage-VM konfiguriert ist und die Storage-Quell-VM aufgrund eines Hardware-Ausfalls oder eines Umweltausfalls nicht mehr verfügbar ist, wird die Ziel-Storage-VM gestartet, die den Zugriff auf die Daten mit minimalen Unterbrechungen ermöglicht. Auf ähnliche Weise wird die Quell-Storage-VM erneut mit der Ziel-Storage-VM synchronisiert, sodass die Quelle dann neu startet, um Daten bereitzustellen. Mit SnapMirror Befehlen können Sie die Disaster-Recovery-Beziehung für Storage-VMs konfigurieren und managen.

Überwachung von Storage VMs mithilfe der Seite „Beziehungen“

Sie können Ihre Disaster-Recovery-Beziehungen für Storage-VMs von der Seite „Beziehungen“ im ABSCHNITT „SCHUTZ“ des BESTANDS aus überwachen. Standardmäßig werden auf der Seite „Beziehungen“ nur die Beziehungen auf der obersten Ebene aufgeführt, wenn der Filter „Bestandbeziehungen“ angewendet wird.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Mithilfe von Filtern können Sie die Disaster-Recovery-Beziehungen zwischen Storage-VMs anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **SCHUTZ** > **Beziehungen**.

   Auf der Seite werden alle Arten von Beziehungen angezeigt: Volume, Consistency Group und Storage VM

Relationships.

2. Klicken Sie auf **Filter** und wählen Sie dann **Relationship Object Type** und **Storage VM** aus, um nur Disaster Recovery-Beziehungen zu Storage VM anzuzeigen.
3. Klicken Sie Auf **Filter Anwenden**.

> Sie sollten den Filter für konstituierende Beziehungen löschen, um alle Sicherungsbeziehungen anzuzeigen.

Auf der Seite werden nur Disaster-Recovery-Beziehungen für Storage-VMs angezeigt.

Anzeigen von Sicherungsbeziehungen von der Seite Storage VMs

Auf der Seite Storage VMs können Sie den Status vorhandener Storage-VMs' Disaster-Recovery-Beziehungen anzeigen.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Auch Details zu den Sicherungsbeziehungen einschließlich Transfer- und Verzögerungsstatus, Quelle- und Zieldetails können Sie überprüfen. Sie können Berichte planen oder vorhandene Berichte in dem erforderlichen Format herunterladen. Mit der Schaltfläche **ein-/Ausblenden** können Sie die erforderlichen Spalten zu den Berichten hinzufügen, da diese standardmäßig nicht angezeigt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **STORAGE** > **Storage VMs**.
2. Wählen Sie im Menü **ANSICHT** die Option **Beziehung** > **Alle Beziehungen**.

   Die Beziehungsansicht: Alle Beziehungen wird mit allen konfigurierten Speicher-VMs angezeigt.

Anzeigen von Storage VMs basierend auf dem Sicherungsstatus

Sie können auf der Seite Storage VMs im Inventar alle Storage VMs in Active IQ Unified Manager anzeigen und die Storage-VMs anhand ihres Sicherungsstatus filtern.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Eine neue Spalte Sicherungsrolle wird der Storage VMs-Ansicht hinzugefügt. Sie enthält Informationen darüber, ob die Storage-VM geschützt oder ungesichert ist.

> Wenn ein Quell-Cluster nicht zu Active IQ Unified Manager hinzugefügt wird, sind alle Informationen zu diesem Cluster nicht in den Grids verfügbar.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **STORAGE** > **Storage VMs**.
2. Wählen Sie im Menü **ANSICHT** die Option **Systemzustand** > **Alle Storage VMs**.

Der Status: Alle Speicher-VMs wird angezeigt.

3. Klicken Sie auf **Filter**, um eine der folgenden Speicher-VMs anzuzeigen.

Um sie anzuzeigen	Filterwert
• Geschützte Storage-VMs*	**Schutzrolle** ist **geschützt**
Ungeschützte Storage VMs	**Schutzrolle** ist **ungeschützt**

Sie können die geschützten und nicht geschützten Storage VMs nicht gleichzeitig anzeigen. Sie müssen den vorhandenen Filter löschen, um eine neue Filteroption erneut anzuwenden.

4. Klicken Sie Auf **Filter Anwenden**.

In der nicht gespeicherten Ansicht werden alle Storage-VMs angezeigt, die entweder gesichert oder ungeschützt sind, basierend auf Ihrer Filterauswahl durch die Disaster Recovery der Storage-VM.

Allgemeines zu Storage VM-Zuordnungen

Zuordnungen von Storage Virtual Machines (Storage VM) sind Zuordnungen von einer Quell-Storage-VM zu einer Ziel-Storage-VM, die von den Partnerapplikationen zur Ressourcenauswahl und Bereitstellung von sekundären Volumes verwendet werden.

Zwischen einer Quell-Storage-VM und einer Ziel-Storage-VM werden Zuordnungen erstellt, unabhängig davon, ob die Ziel-Storage-VM ein sekundäres Ziel oder ein tertiäres Ziel ist. Sie können keine sekundäre Ziel-Storage-VM als Quelle verwenden, um eine Zuordnung zu einer tertiären Ziel-Speicher-VM zu erstellen.

Als Anwendungsadministrator oder Speicheradministrator können Sie die Speicher-VM-Zuordnungen in Ihrer Umgebung auf der Seite **Sicherung** > **Storage-VM-Verknüpfungen** anzeigen.

SVMs können auf drei Arten zugeordnet werden:

- **Zuweisen einer Storage-VM**: Sie können eine Verknüpfung zwischen einer beliebigen primären Quell-Storage-VM 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.
- **Zuweisen einer bestimmten Storage-VM**: Sie können eine Verknüpfung zwischen einer bestimmten Quell-Storage-VM 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-Storage-VM einer bestimmten Ziel-Storage-VM zu zuordnen, die nur diesem Client zugewiesen ist.
- **Verknüpfung mit einer externen Speicher-VM**: Sie können eine Verknüpfung zwischen einer Quell-Speicher-VM und einem externen flexiblen Volume einer Ziel-Speicher-VM erstellen.

Erstellen von Storage-VM-Zuordnungen

Mit dem Assistenten zur Erstellung von Storage Virtual Machines können Partnersicherungsapplikationen eine Quell-Storage-VM zur Verwendung mit SnapMirror und SnapVault Beziehungen mit einer Ziel-Storage-VM verknüpfen. Partnerapplikationen verwenden diese Verknüpfungen zum Zeitpunkt der Erstbereitstellung der

Ziel-Volumes, um zu ermitteln, welche Ressourcen ausgewählt werden sollen.dd

Was Sie brauchen

- Die Storage-VM, die Sie verknüpfen, muss bereits vorhanden sein.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Für jede Quell-Storage-VM und jeden Beziehungstyp können Sie nur eine Ziel-Storage-VM 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** > **Storage VM Associations**.
2. Klicken Sie auf der Seite **Storage VM Associations** auf **Erstellen**.

   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 Speicher-VM-Quelle zu einer oder mehreren Ziel-Speicher-VM erstellen möchten. Das heißt, alle bestehenden Storage-VMs, die derzeit gesichert werden müssen, sowie jede zukünftig erstellte Storage-VM sind mit der angegebenen Ziel-Storage-VM verknüpft. Beispielsweise kann es sinnvoll sein, dass Applikationen aus verschiedenen Quellen an verschiedenen Standorten auf einer oder mehreren Ziel-Storage-VM an einem Standort gesichert werden.

   - **Single**

     Wählen Sie diese Option, wenn Sie eine bestimmte Quell-Storage-VM auswählen möchten, die einer oder mehreren Ziel-Storage-VM zugeordnet ist. Wenn Sie beispielsweise vielen Clients Storage-Services bereitstellen, deren Daten voneinander getrennt sein müssen, wählen Sie diese Option, um eine bestimmte Storage-VM-Quelle einem bestimmten Storage-VM-Ziel zu zuordnen, das nur diesem Client zugewiesen ist.

   - **Keine (Extern)**

     Wählen Sie diese Option, wenn Sie eine Zuordnung zwischen einer Quell-Speicher-VM und einem externen flexiblen Volume einer Ziel-Speicher-VM 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 Storage-VM-Schutzziele aus.
7. Klicken Sie Auf **Fertig Stellen**.

Löschen der Storage-VM-Zuordnungen

Sie können Storage-VM-Zuordnungen für Partnerapplikationen löschen, um die sekundäre Bereitstellungsbeziehung zwischen Quell- und Ziel-Storage-VM zu entfernen. So kann dies beispielsweise geschehen, wenn die Ziel-Storage-VM voll ist und Sie neue Storage-VM-Sicherungsverknüpfungen erstellen möchten.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die Schaltfläche **Löschen** ist deaktiviert, bis mindestens eine Speicher-VM-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** > **Storage VM Associations**.
2. Wählen Sie mindestens eine Speicher-VM-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 Speicher-VM-Zuordnung wird aus der Liste entfernt.

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.

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 diese erfolgreich abgeschlossen wurden.

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 starten, können Sie die Seite Jobs und die Seite Jobdetails verwenden, um den Job und den Fortschritt der zugeordneten Job-Aufgaben zu überwachen.

Überwachen von Jobs

Auf der Seite Jobs können Sie den Jobstatus überwachen und Jobeigenschaften wie Speicherservicetyp, Status, Abges. Zeit und Abgeschlossene Zeit anzeigen, um zu bestimmen, ob ein Job erfolgreich abgeschlossen wurde oder nicht.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Jobs**.

   Die Seite 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 Jobdetails wird angezeigt.

Anzeigen von Jobdetails

Nachdem Sie einen Job gestartet haben, können Sie den Fortschritt auf der Seite Jobdetails verfolgen und die zugehörigen Aufgaben auf mögliche Fehler überwachen.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Jobs**.
2. Klicken Sie auf der Seite 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 Jobs verwenden, um einen Job abzubrechen, wenn er zu lange 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.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ 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.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

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. Über die entsprechende Seite „Health Schwellen“ können Sie globale Grenzwerte für den Systemzustand für Aggregate, Volumes und Beziehungen konfigurieren.

Seite „Ressourcen-Pools“

Auf der Seite „Ressourcenpools“ werden vorhandene Ressourcen-Pools und ihre Mitglieder angezeigt. Hier können Sie Ressourcen-Pools zu Bereitstellungszwecken 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 (), Fehler ( ), Warnung ( ) oder Normal ( ) sein.

- **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 sind 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 (), Fehler ( ), Warnung ( ) oder Normal ( ) sein.

  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 Jobs

Auf der Seite „Jobs“ können Sie den aktuellen Status und weitere Informationen zu allen aktuell ausgeführten Partneranwendungen 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 Error () oder Normal ( )✅ sein❗.

- **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.

Jobdetails

Auf der Seite Job Details können Sie den Status und weitere Informationen zu bestimmten 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
- Status
- 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 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 ausgeführt wird als jene des Quell-Volume.

  - 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
  - None + zum Beispiel, Sie können ein 200 GB-Volumen, das Dateien mit einer Gesamtmenge von 50 GB enthält, aber diese Dateien enthalten 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.

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
- 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. Wenn Sie auf einen Pfad klicken  , werden Sie in der Verzeichnisstruktur um 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 zu dem Ort, an dem die Daten wiederhergestellt werden sollen, oder Sie können den Pfad manuell über das 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. Wenn Sie auf einen Ordner klicken  , werden Sie in der Verzeichnisstruktur um 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. Beim Erstellen der Beziehung wird ein Suffix zwischen 001 und 999 an den Zielnamen angehängt, wobei die im Vorschautext angezeigte nn ersetzt wird, 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.

  - 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. Beim Erstellen der Beziehung wird ein Suffix zwischen 001 und 999 an den sekundären Namen angehängt, wobei die im Vorschautext angezeigte nn ersetzt wird, 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.

  - 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 eine neue Snapshot Kopie erstellt wird, bevor ein Transfer neu gestartet wird. Falls vorhanden, wird der Transfer 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:

▪ Hinzufügung

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 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.

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.
Aktualisieren	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.
Aktualisieren	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.
Aktualisieren	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.
Aktualisieren	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-Volume vor einer Resynchronisierung

- **Zielvolumen**

  Name und Standort des Ziel-Volumes vor einer Resynchronisierung

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.

Beziehung: Ansicht aller Beziehungen

Die Beziehung: Die Ansicht „Alle Beziehungen“ zeigt Informationen über Sicherungsbeziehungen auf dem Storage-System an.

Wenn Sie auf die Seite Beziehungen zugreifen, enthält der angezeigte Bericht standardmäßig die obersten Sicherungsbeziehungen für Volumes und Storage-VMs. Mit den Steuerelementen oben auf der Seite können Sie eine bestimmte Ansicht auswählen, nach bestimmten Objekten suchen, Filter erstellen und anwenden, um die Liste der angezeigten Daten einzugrenzen, Spalten auf der Seite hinzuzufügen/zu entfernen/neu zu sortieren und die Daten auf der Seite in .csv, .pdf zu exportieren. Oder .xlsx-Datei. Nachdem Sie die Seite angepasst haben, können Sie die Ergebnisse als benutzerdefinierte Ansicht speichern und anschließend einen Bericht dieser Daten erstellen und regelmäßig per E-Mail senden. Wenn Sie das Menü **Relationships** auswählen, enthält der angezeigte Bericht standardmäßig Schutzbeziehungen sowohl für Volumes als auch für Speicher-VMs in Ihrem Datacenter. Mit der Option **Filter** können nur ausgewählte Speichersysteme wie nur Volumes oder nur Storage VMs angezeigt werden. Derselbe Bericht wird auf der Seite Speicher und nur für die ausgewählte Speichereinheit angezeigt. Wenn Sie Volume- oder Storage-VM-Beziehungen anzeigen möchten, können Sie entweder auf die Seite **Storage** > **Volumes** > **Beziehung: Alle Beziehungen** oder auf **Schutz** > **Beziehungen** > **Beziehung: Alle Beziehungen**, und verwenden Sie die Option **Relationship Object Type** im **Filter**, um nur Volumes oder Speicher-VM-Daten herauszufiltern.

Die Beziehungsseite, auf der alle Schutzbeziehungen aufgelistet sind, enthält den Link **Anzeigen in System Manager** für den Ziel-Cluster, mit dem Sie dieselben Objekte in ONTAP System Manager anzeigen können.

- **Status**

  Zeigt den aktuellen Status der Schutzbeziehung an.

  Der Status kann als Fehler (), Warnung ( ) oder OK ( ) angegeben werden.

- **Quell-Storage-VM**

  Zeigt den Namen der Quell-SVM an. Weitere Details zur Quell-SVM können Sie anzeigen, indem Sie auf den Namen der SVM klicken.

  Wenn im Cluster eine SVM vorhanden, aber noch nicht zum Unified Manager-Inventar hinzugefügt wurde oder die SVM nach der letzten Aktualisierung des Clusters erstellt wurde, ist dieses Feld leer. Sie müssen sicherstellen, dass die SVM existiert, oder eine erneute Erkennung im Cluster durchführen, um die Liste der Ressourcen zu aktualisieren.

- **Quelle**

  Zeigt das Quell-Volume oder die Quell-Storage-VM an, die basierend auf Ihrer Auswahl geschützt wird. Weitere Details zum Quell-Volume oder der Storage-VM können Sie anzeigen, indem Sie auf den Namen

des Volume oder der Storage-VM klicken.

Wenn die Meldung `Resource-key not discovered` angezeigt wird, gibt dies möglicherweise an, dass das Volume im Cluster vorhanden ist, jedoch noch nicht zum Unified Manager-Inventar 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-Storage-VM**

  Zeigt den Namen der Ziel-SVM an. Weitere Details zur Ziel-SVM können Sie anzeigen, indem Sie auf den Namen der SVM klicken.

- **Ziel**

  Zeigt den Namen des Ziel-Volumes oder der Storage-VM basierend auf Ihrer Auswahl an. Weitere Details zum Ziel-Volume oder Storage-VM können Sie anzeigen, indem Sie auf den entsprechenden Objektnamen klicken.

- **Beziehungsobjekt Typ**

  Zeigt den Objekttyp an, der in der Beziehung verwendet wird, z. B. Storage-VM, Volume und Konsistenzgruppe. Für Objekte in einer Konsistenzgruppe werden die Konsistenzgruppe aus der Beziehungsquelle und Zielen angezeigt. Wenn Sie auf diese klicken, werden Sie zur Seite LUNs weitergeleitet, um die Beziehung anzuzeigen.

- **Richtlinien**

  Zeigt den Namen der Sicherungsrichtlinie für die SnapMirror Beziehung 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.

- Aufbewahrungseinstellung

  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 Retention Warnungsschwellenwert

  Gibt das Limit für die Snapshot Kopie an, bei dem eine Warnung gesendet wird, um anzugeben, dass das maximale Aufbewahrungslimit fast erreicht ist.

- **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.

- **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.

  - OK

    Die Verzögerungsdauer liegt innerhalb der normalen Grenzwerte.

  - Keine Angabe

    Der lag-Status gilt nicht für synchrone Beziehungen, da ein Zeitplan nicht konfiguriert werden kann.

- **Letzte Erfolgreiche Aktualisierung**

  Zeigt die Zeit des letzten erfolgreichen SnapMirror oder SnapVault Vorgangs an.

  Die letzte erfolgreiche Aktualisierung gilt nicht für synchrone Beziehungen.

- **Konstituierende Beziehungen**

  Zeigt an, ob Volumes im ausgewählten Objekt vorhanden sind.

- **Beziehungstyp**

  Zeigt den Beziehungstyp an, mit dem ein Volume repliziert wird. Beziehungstypen:

  - Asynchrones Spiegeln
  - Asynchroner Vault
  - Asynchroner MirrorVault
  - StrictSync
  - Synchron

- **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.

- **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.

- **Mediatoren**

  Zeigt den Mediatorstatus an.

  - Keine Angabe

    Wenn der Cluster die aktive SnapMirror Synchronisierung nicht unterstützt.

  - Nicht Konfiguriert

    Wenn er nicht konfiguriert ist oder konfiguriert ist, sondern nur das Ziel-Cluster hinzugefügt wird und das Quell-Cluster nicht in Unified Manager hinzugefügt wird.

  - Mediator-IP-Adresse

Wenn er konfiguriert ist, und Quell- und Ziel-Cluster werden im Unified Manager hinzugefügt.

- **Bundesland**

  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.

- **Gesundheit Der Beziehung**

  Zeigt den Systemzustand der Beziehung des Clusters an.

- * Ungesunde Gründe*

  Der Grund, warum die Beziehung in einem ungesunden Zustand ist.

- * 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.

- **Zeitplan**

  Zeigt den Namen des Schutzplans an, der der Beziehung zugeordnet ist.

  Der Zeitplan gilt nicht für synchrone Beziehungen.

- **Version Flexible Replikation**

  Zeigt entweder Ja, Ja mit Sicherungsoption oder Keine an.

- * Quellcluster*

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Quellclusters für die SnapMirror-Beziehung an.

- **Quellcluster FQDN**

  Zeigt den Namen des Quell-Clusters für die SnapMirror Beziehung an.

- **Quellknoten**

  Zeigt den Namen des Links mit dem Namen des Quell-Nodes für die SnapMirror Beziehung eines Volumes an und zeigt den Link zur Anzahl der SnapMirror Beziehungs-Nodes an, wenn es sich um eine Storage-VM oder eine Konsistenzgruppe handelt.

Wenn Sie in der benutzerdefinierten Ansicht auf den Link Node-Name klicken, können Sie den Schutz für Storage-Objekte anzeigen und erweitern, auf denen die Volumes dieser Konsistenzgruppen zu einer aktiven SnapMirror Synchronisierungsbeziehung gehören.

Wenn Sie auf den Link Knotenanzahl klicken, gelangen Sie zur Knotenseite mit den entsprechenden Knoten, die dieser Beziehung zugeordnet sind. Wenn die Knotenanzahl 0 ist, wird kein Wert angezeigt, da der Beziehung keine Knoten zugeordnet sind.

- **Zielknoten**

  Zeigt den Namen des Links mit dem Ziel-Node-Namen für die SnapMirror Beziehung eines Volumes an und zeigt den Link zur Anzahl der SnapMirror Beziehungs-Nodes an, wenn es sich um eine Storage-VM oder eine Konsistenzgruppe handelt.

  Wenn Sie auf den Link Knotenanzahl klicken, gelangen Sie zur Knotenseite mit den entsprechenden Knoten, die dieser Beziehung zugeordnet sind. Wenn die Knotenanzahl 0 ist, wird kein Wert angezeigt, da der Beziehung keine Knoten zugeordnet sind.

- **Zielcluster**

  Zeigt den Namen des Ziel-Clusters für die SnapMirror Beziehung an.

- **Zielcluster FQDN**

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Zielclusters für die SnapMirror-Beziehung an.

- * Geschützt Durch*

  Zeigt die verschiedenen Beziehungen an. In dieser Spalte können Sie Volume- und Konsistenzgruppenbeziehungen für Cluster und Storage Virtual Machines in der Reihenfolge anzeigen, darunter:

  - SnapMirror
  - DR von Storage-VMs
  - SnapMirror, Storage VM DR
  - Konsistenzgruppe
  - SnapMirror, Konsistenzgruppe.

Verwandte Informationen

- Für Informationen über **Beziehung: MetroCluster** Ansicht, siehe "Monitoring der MetroCluster Konfigurationen".
- Informationen zu **Beziehung: Letzte 1 Monat Transferstatus** Ansicht, siehe "Beziehung: Letzte 1 Monat Transfer Status Ansicht".
- Für Informationen über **Beziehung: Alle Beziehungen** Ansicht, siehe "Beziehung: Letzte 1 Monat Transferrate Ansicht".

Beziehung: Letzte 1 Monat Transfer Status Ansicht

Die Beziehung: Die Ansicht „Transferstatus der letzten 1 Monate“ ermöglicht Ihnen die Analyse der Übertragungstrends für Volumes und Storage VMs in asynchronen Beziehungen. Auf dieser Seite wird außerdem angezeigt, ob die Übertragung erfolgreich oder fehlgeschlagen ist.

Mit den Steuerelementen oben auf der Seite können Sie Suchen durchführen, um bestimmte Objekte zu finden, Filter zu erstellen und anzuwenden, um die Liste der angezeigten Daten einzugrenzen, Spalten auf der Seite hinzuzufügen/zu entfernen/neu anzuordnen und die Daten auf der Seite in eine, oder `.xlsx` - `.pdf`Datei zu exportieren `.csv`. Nachdem Sie die Seite angepasst haben, können Sie die Ergebnisse als benutzerdefinierte Ansicht speichern und anschließend einen Bericht dieser Daten erstellen

und regelmäßig per E-Mail senden. Mit der Option **Filter** können Sie nur ausgewählte Speichersysteme wie nur Volumes oder nur Storage VMs anzeigen. Derselbe Bericht wird auf der Seite Speicher und nur für die ausgewählte Speichereinheit angezeigt. Wenn Sie beispielsweise Volume-Beziehungen anzeigen möchten, können Sie entweder auf den Relationship: Last 1 Month Transfer Status Report for the Storage VMs entweder aus dem Menü **Storage** > **Storage VMs** > **Relationship: Last 1 month Transfer Status** oder aus **Protection** > **Relationships** > **Relationship: Im Menü „Transferstatus** des letzten Monats“ können Sie mit dem **Filter** nur Daten für Volumes anzeigen.

- **Quellvolumen**

  Zeigt den Namen des Quell-Volumes an.

- **Zielvolumen**

  Zeigt den Namen des Zieldatenträgers an.

- **Operationstyp**

  Zeigt den Typ der Volume-Übertragung 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.

- **Quell-SVM**

  Zeigt den Namen der Storage Virtual Machine (SVM) an.

- * Quellcluster*

  Zeigt den Quellcluster-Namen an.

- **Ziel-SVM**

  Zeigt den Namen der Ziel-SVM an.

- **Zielcluster**

  Zeigt den Ziel-Cluster-Namen an.

Verwandte Informationen

- Für Informationen über **Beziehung: Alle Beziehungen** Ansicht, siehe "Beziehung: Ansicht aller Beziehungen".
- Informationen zur Ansicht **Beziehung:MetroCluster** finden Sie unter "Monitoring der MetroCluster Konfigurationen".
- Für Informationen über **Beziehung: Alle Beziehungen** Ansicht, siehe "Beziehung: Letzte 1 Monat Transferrate Ansicht".

Beziehung: Letzte 1 Monat Transferrate Ansicht

Die Beziehung: Die Ansicht der letzten 1 Monate Transferrate ermöglicht Ihnen, die Menge des Datenvolumen, das täglich für Volumes in asynchronen Beziehungen übertragen wird, zu analysieren. Diese Seite bietet auch Details zu täglichen Transfers und die Zeit, die für den Transfer von Volumes und Storage VMs erforderlich ist.

Mit den Steuerelementen oben auf der Seite können Sie Suchen durchführen, um bestimmte Objekte zu finden, Filter zu erstellen und anzuwenden, um die Liste der angezeigten Daten einzugrenzen, Spalten auf der Seite hinzuzufügen/zu entfernen/neu zu sortieren und die Daten auf der Seite in eine .csv-, .pdf- oder .xlsx-Datei zu exportieren. Nachdem Sie die Seite angepasst haben, können Sie die Ergebnisse als benutzerdefinierte Ansicht speichern und anschließend einen Bericht dieser Daten erstellen und regelmäßig per E-Mail senden. Wenn Sie beispielsweise Volume-Beziehungen anzeigen möchten, können Sie entweder auf das Menü **Storage** > **Volumes** > **Beziehung: Letzte 1 Monat Transferrate** oder auf **Schutz** > **Beziehungen** > **Beziehungen:Letzte 1 Monat Transferrate** zugreifen und mit **Filter** nur Daten für Volumes anzeigen.

- **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.

Verwandte Informationen

- Informationen zur Ansicht **Beziehung:MetroCluster** finden Sie unter "Monitoring der MetroCluster Konfigurationen".
- Informationen zu **Beziehung: Letzte 1 Monat Transferstatus** Ansicht, siehe "Beziehung: Letzte 1 Monat Transfer Status Ansicht".
- Informationen zur Ansicht **Beziehung: Alle Beziehungen** finden Sie unter "Beziehung: Letzte 1 Monat Transferrate Ansicht"

Erstellen benutzerdefinierter Berichte

Unified Manager Berichterstellung

Active IQ Unified Manager (ehemals OnCommand Unified Manager) bietet die Möglichkeit, Berichte für Ihre ONTAP Storage-Systeme anzuzeigen, anzupassen, herunterzuladen und zu planen. Die Berichte können Details zur Kapazität, zum Zustand, zur Performance, Sicherheit und zum Schutz des Storage-Systems enthalten.

Die neue Active IQ Unified Manager 9.6 Funktion für Reporting und Planung von Unified Manager ersetzt die bisherige Reporting Engine, die in Unified Manager Version 9.5 außer Betrieb genommen wurde.

Mit der Berichterstellung erhalten Sie verschiedene Ansichten Ihres Netzwerks und können so nützliche Informationen zu Kapazitäts-, Zustand-, Performance-, Sicherheits- und Sicherungsdaten erhalten. Sie können Ihre Ansichten anpassen, indem Sie Spalten anzeigen, ausblenden und neu anordnen, Daten filtern, Daten sortieren, Und die Ergebnisse zu durchsuchen. Sie können benutzerdefinierte Ansichten zur Wiederverwendung speichern, sie als Berichte herunterladen und als wiederkehrende Berichte über E-Mails verteilen.

Sie können Ansichten im Microsoft® Excel-Format herunterladen und anpassen. Sie können erweiterte Excel-Funktionen wie komplexe Sortierungen, mehrstufige Filter, Pivot-Tabellen und Diagramme verwenden. Wenn Sie mit dem resultierenden Excel-Bericht zufrieden sind, können Sie die Excel-Datei bei jeder Planung und Freigabe des Berichts hochladen.

Zusätzlich zum Generieren von Berichten aus der Benutzeroberfläche können Sie mit den folgenden zusätzlichen Methoden Gesundheits-, Sicherheits- und Performancedaten aus Unified Manager extrahieren:

- Verwenden der Open Database Connectivity (ODBC)- und ODBC-Tools für den direkten Zugriff auf die Datenbank für Clusterinformationen
- Ausführung von Unified Manager REST-APIs zur Rückgabe der Informationen, für die Sie interessiert sind, zu überprüfen

Ab dieser Version von Active IQ Unified Manager wurden die Berichte um die folgenden Verbesserungen erweitert:

- E-Mail wird für einen Bericht gemäß dem konfigurierten Zeitplan gesendet. Selbst wenn Sie einen On-Demand-Bericht erstellen, erhalten Sie per E-Mail.
- Der Dateiname des Berichts und der Metadaten des Berichts enthält den Hostnamen, aus dem der Bericht erstellt wurde. Selbst wenn jemand den Dateinamen ändert, können Sie dennoch den Hostnamen identifizieren, aus dem der Bericht aufgrund dieser Verbesserung generiert wurde.

Access Points zur Erstellung von Berichten

Sie können Informationen in Unified Manager über die Cluster erfassen und Berichte von der UI, MySQL-Datenbankabfragen und REST-APIs erstellen.

In diesen Abschnitten werden die Berichterstellung und Planung von Unified Manager über die UI beschrieben.

Es gibt drei Möglichkeiten, wie Sie auf die Reporting-Funktionen von Unified Manager zugreifen können:

- Daten direkt aus den Bestandsseiten in der Benutzeroberfläche extrahieren

- Verwenden der Open Database Connectivity (ODBC)- und ODBC-Tools, um auf alle verfügbaren Objekte zuzugreifen.
- Ausführung von Unified Manager REST APIs zur Rückgabe der Informationen, die Sie überprüfen möchten.

In diesen Abschnitten werden die Berichterstellung und Planung von Unified Manager über die UI beschrieben.

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.

Alle Tabellendaten aus den folgenden Datenbanken sind verfügbar:

Datenbank	Beschreibung
netapp_Modell	Daten zu den Objekten auf ONTAP Controllern.
netapp_Modell_Ansicht	Daten zu den Objekten auf ONTAP Controllern, geeignet für die Nutzung von Berichtstools.
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	Ansichten für Bestandskonfiguration und kapazitätsbezogene Daten, geeignet für den Einsatz von Berichtstools.
opm	Einstellungen für Performance-Konfiguration und Schwellenwertinformationen.
Skalemonitor	Daten zu Zustand- und Performance-Problemen der Unified Manager Applikation
vmware_Modell	VMware Objektdaten für Datastores, die auf NetApp Storage gehostet werden.
vmware_model_view	Ansichten für VMware Objektdaten für Datastores, die auf NetApp Storage gehostet werden und sich für die Nutzung von Berichtstools eignen.

Datenbank	Beschreibung
vmware_Performance	Daten der VMware Performance für Datastores, die auf NetApp Storage gehostet werden.

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.

Unified Manager REST-APIs, die für die Berichterstellung verwendet werden können

Über REST-APIs können Sie Ihre Cluster managen, indem Sie die von Unified Manager erfassten Daten zu Zustand, Kapazität, Performance und Sicherheit abrufen.

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. Klicken Sie in der Web-UI von Unified Manager in der Menüleiste auf die Schaltfläche **Hilfe** und wählen Sie dann **API-Dokumentation** aus. Weitere Informationen zu Unified Manager REST-APIs finden Sie unter "Erste Schritte mit Active IQ Unified Manager REST APIs".

Sie müssen über die Operator-, Storage Administrator- oder Anwendungsadministratorrolle verfügen, um auf DIE REST-APIs zuzugreifen.

Allgemeines zu Berichten

In Berichten werden detaillierte Informationen zu Storage, Netzwerk, Servicequalität und Sicherungsbeziehungen angezeigt, sodass Sie potenzielle Probleme erkennen und beheben können, bevor sie auftreten.

Wenn Sie eine Ansicht anpassen, können Sie diese mit einem eindeutigen Namen für die zukünftige Verwendung speichern. Sie können einen Bericht auf Basis dieser Ansicht so planen, dass er regelmäßig ausgeführt und an andere weitergegeben wird. Sie können die Ansicht auch in Excel herunterladen, um sie mithilfe erweiterter Excel-Funktionen anzupassen, und diese Datei anschließend wieder in Unified Manager hochladen. Wenn Sie einen Bericht über diese Ansicht planen, wird er die hochgeladene Excel-Datei verwenden, um zuverlässige Berichte zu erstellen, die Sie freigeben können.

Sie können alle Berichte verwalten, die geplant wurden, über die Seite „Berichtszeitpläne“.

Zum Verwalten von Berichten müssen Sie über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können Berichte als kommagetrennte Werte (CSV), Excel oder PDF-Dateien herunterladen.

Verständnis der Ansichten und der Berichtsbeziehung

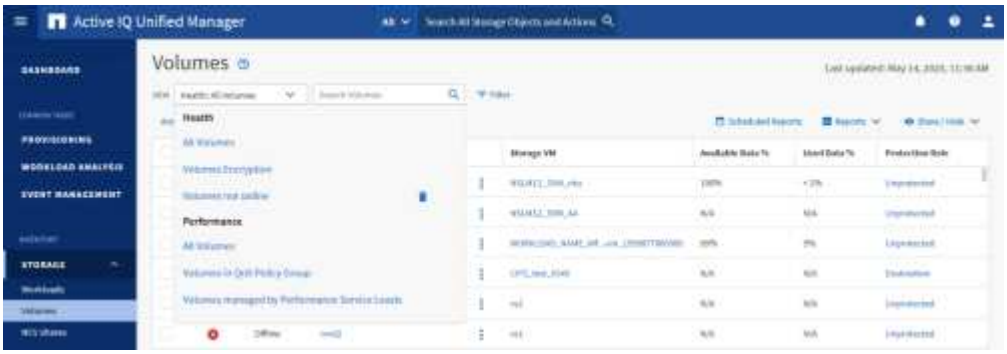
Ansichten und Bestandsseiten werden zu Berichten, wenn Sie sie herunterladen oder planen.

Sie können Ansichten und Bestandsseiten zur Wiederverwendung anpassen und speichern. Nahezu alle Daten, die in Unified Manager angezeigt werden, können gespeichert, wiederverwendet, individuell, geplant

und als Bericht freigegeben werden.

In der Dropdown-Ansicht sind Elemente mit dem Löschsymbol bereits vorhandene benutzerdefinierte Ansichten, die Sie oder ein anderer Benutzer erstellt haben. Elemente ohne Symbol sind Standardansichten, die in Unified Manager bereitgestellt werden. Standardansichten können nicht geändert oder gelöscht werden.

- Wenn Sie eine benutzerdefinierte Ansicht aus der Liste löschen, werden auch alle Excel-Dateien oder geplanten Berichte gelöscht, die diese Ansicht verwenden.
- Wenn Sie eine benutzerdefinierte Ansicht ändern, werden Berichte, die diese Ansicht verwenden, die Änderung beim nächsten Generieren und Versenden des Berichts per E-Mail entsprechend dem Berichtsplan widerspiegeln. Wenn Sie Ansichten ändern, stellen Sie sicher, dass Ihre Änderungen mit den zugehörigen Excel-Anpassungen funktionieren, die für die Berichte verwendet werden. Sie können die Excel-Datei bei Bedarf aktualisieren, indem Sie sie herunterladen, die erforderlichen Änderungen vornehmen und als neue Excel-Anpassung für die Ansicht hochladen.



Nur Benutzer mit der Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ können das Löschsymbol anzeigen, eine Ansicht ändern oder löschen oder einen geplanten Bericht ändern oder löschen.

Berichtstypen

Diese Tabelle enthält eine umfassende Liste der Ansichten und Inventarseiten, die als Berichte zur Verfügung stehen, die Sie anpassen, herunterladen und planen können.

Active IQ Unified Manager Berichte

Typ	Storage oder Netzwerkobjekt
Kapazität	Cluster Aggregate Volumes Qtrees

Typ	Storage oder Netzwerkobjekt
Systemzustand	Cluster Knoten Aggregate Storage-VMs Volumes SMB/CIFS-Freigaben NFS-Freigaben
Performance	Cluster Knoten Aggregate Storage-VMs Volumes LUNs NVMe Namespaces Netzwerkschnittstellen (LIFs) Ports
Quality of Service	Herkömmliche QoS-Richtliniengruppen Adaptive QoS-Richtliniengruppen Richtliniengruppen für Performance-Service-Level
Volume-Sicherungsbeziehungen (verfügbar auf der Seite Volumes)	Alle Beziehungen Transferstatus der letzten 1 Monate Letzte 1 Monat Transferrate
Sicherheit	Storage-VMs Cluster

Einschränkungen bei der Berichterstellung

Es gibt einige Einschränkungen bei der neuen Active IQ Unified Manager-Berichtsfunktion, die Sie beachten sollten.

Vorhandene Berichte aus früheren Versionen von Unified Manager

Sie können den Zeitplan und die Empfänger nur für vorhandene Berichte bearbeiten, die in Unified Manager 9.5 und früheren Versionen erstellt und importiert wurden (als .rptdesign-Dateien). Wenn Sie einen der Standardberichte, die mit Unified Manager 9.5 oder früher bereitgestellt wurden, angepasst haben, werden diese benutzerdefinierten Berichte nicht in das neue Reporting-Tool importiert.

Wenn Sie vorhandene Berichte bearbeiten müssen, die aus .rptdesign-Dateien importiert wurden, führen Sie einen der folgenden Schritte aus, und entfernen Sie den importierten Bericht:

- Erstellen einer neuen Ansicht und Planen eines Berichts aus dieser Ansicht (bevorzugt)
- Bewegen Sie den Mauszeiger über den Bericht, kopieren Sie den SQL, und ziehen Sie die Daten mit einem externen Tool

Die Standardansichten können als Berichte erstellt werden, ohne dass eine Anpassung erforderlich ist. Sie können die neue Berichtslösung verwenden, um benutzerdefinierte Berichte neu zu erstellen.

Planen und berichten von Beziehungen

Sie können für jeden gespeicherten Bericht viele verschiedene Zeitpläne mit einer beliebigen Kombination von Empfängern erstellen. Sie können den Zeitplan jedoch nicht für mehrere Berichte wiederverwenden.

Berichtsschutz

Jeder Benutzer mit den entsprechenden Berechtigungen kann Berichte bearbeiten oder löschen. Es gibt keine Möglichkeit, andere Benutzer daran zu hindern, gespeicherte Ansichten oder Zeitpläne zu entfernen oder zu ändern.

Ereignisberichte

Sie können die Ereignisansicht anpassen und den resultierenden Bericht im CSV-Format herunterladen, jedoch können Sie keine wiederkehrenden Ereignisberichte für die Erstellung und Verteilung planen.

Berichtsanhänge

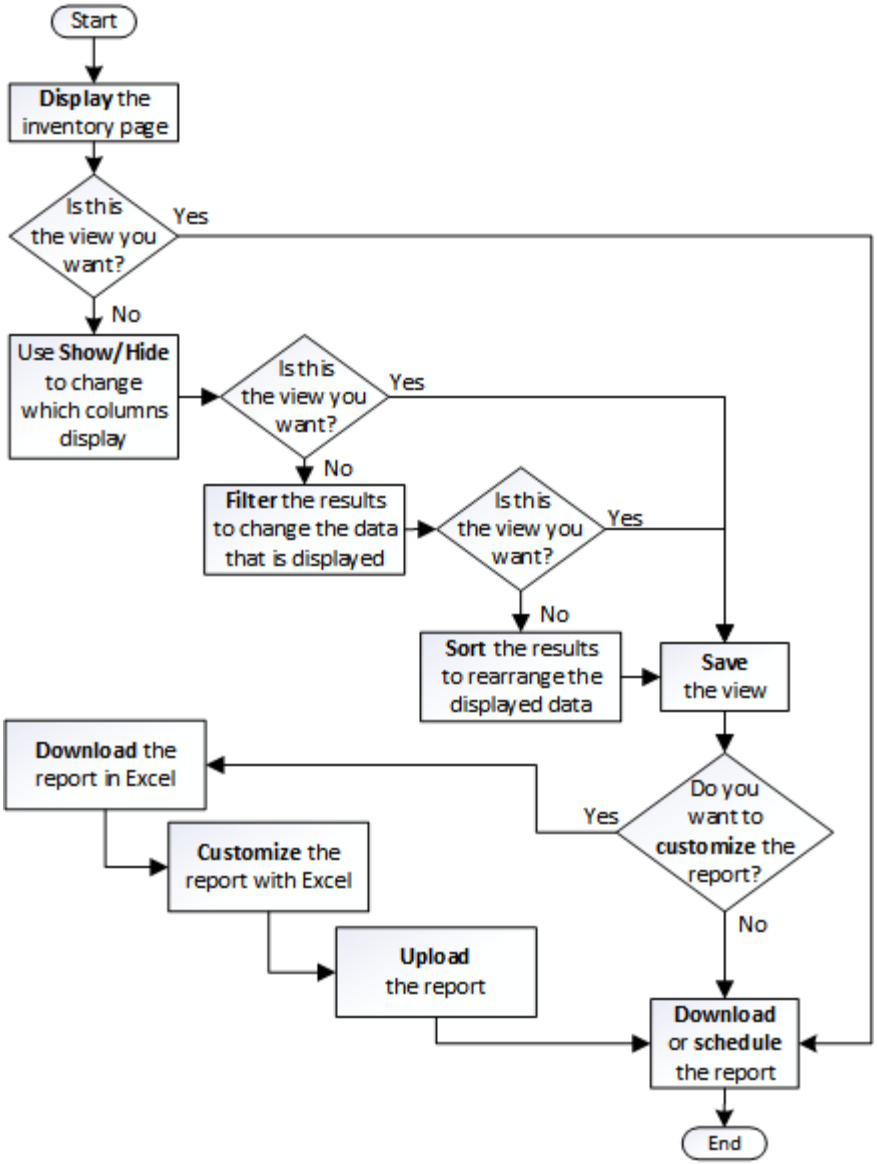
Berichte können nicht im Text einer E-Mail gesendet werden. Stattdessen werden Berichte nur als PDF-, Excel- oder CSV-Anlagen versendet.

Arbeiten mit Berichten

Erfahren Sie, wie Sie Bestandsseite-Ansichten in gemeinsam nutzbare, geplante Berichte suchen und anpassen.

Berichtsworkflow zu erstellen

Entscheidungsbaum, in dem der Berichtworkflow beschrieben wird.



Schnellstartanleitung für die Berichterstellung

Erstellen Sie einen benutzerdefinierten Beispielbericht, um Ansichten zu untersuchen und Berichte zu planen. Dieser Schnellstart-Bericht enthält eine Liste der Volumes, die Sie möglicherweise auf das Cloud-Tier verschieben möchten, da es eine Menge inaktiver (kalter) Daten gibt. Sie öffnen die Ansicht „Leistung: Alle Volumes“, passen die Ansicht mit Filtern und Spalten an, speichern die benutzerdefinierte Ansicht als Bericht und planen den Bericht für die Freigabe einmal pro Woche.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen FabricPool Aggregate konfiguriert haben und Volumes auf diesen Aggregaten haben.

Befolgen Sie die nachstehenden Schritte:

- Öffnen Sie die Standardansicht

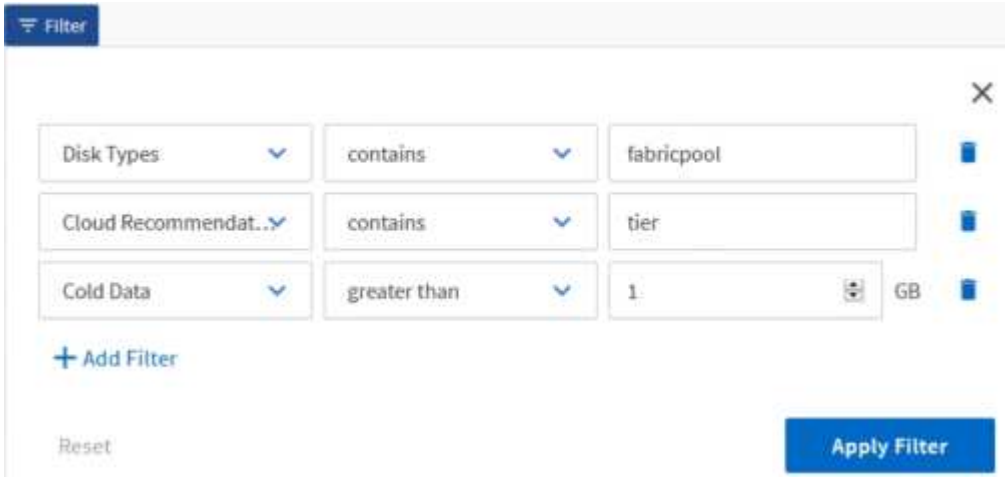
- Passen Sie die Spalten an, indem Sie die Daten filtern und sortieren
- Speichern Sie die Ansicht
- Planen eines Berichts für die benutzerdefinierte Ansicht

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Leistung** > **Alle Volumes**.
3. Klicken Sie auf **ein-/Ausblenden**, um sicherzustellen, dass die Spalte “DFestplatten-Typen” in der Ansicht angezeigt wird.

   Fügen Sie weitere Spalten hinzu oder entfernen Sie diese, um eine Ansicht zu erstellen, die die für Ihren Bericht wichtigen Felder enthält.

4. Ziehen Sie die Spalte „`Disk types`“ neben der Spalte „`Cloud Recommendation`“.
5. Klicken Sie auf das Filtersymbol, um die folgenden drei Filter hinzuzufügen, und klicken Sie dann auf **Filter anwenden**:
   - Festplattentypen enthalten FabricPool
   - Cloud-Empfehlung enthält Tier
   - Kalte Daten größer als 10 GB



   Beachten Sie, dass jeder Filter mit einem logischen verbunden ist, damit alle zurückgegebenen Volumes alle Kriterien erfüllen müssen. Sie können maximal fünf Filter hinzufügen.

6. Klicken Sie oben in der Spalte „kalte Daten“, um die Ergebnisse so zu sortieren, dass die Volumes mit den meisten kalten Daten oben in der Ansicht angezeigt werden.
7. Wenn die Ansicht angepasst ist, ist der Ansichtsname nicht gespeicherte Ansicht. Benennen Sie die Ansicht, mit der die Ansicht dargestellt wird, z. B. „`Vols change Tiering Policy`“. Wenn Sie fertig sind, klicken Sie auf das Häkchen oder drücken Sie **Enter**, um die Ansicht mit dem neuen Namen zu speichern.

8. Laden Sie den Bericht als **CSV**-, **Excel**- oder **PDF**-Datei herunter, um die Ausgabe anzuzeigen, bevor Sie sie planen oder freigeben.

   Öffnen Sie die Datei mit einer installierten Anwendung, z. B. Microsoft Excel (CSV oder Excel) oder Adobe

Acrobat (PDF), oder speichern Sie die Datei.

> Sie können Ihren Bericht mithilfe komplexer Filter, Sortierungen, Pivot-Tabellen oder Diagramme weiter anpassen, indem Sie die Ansicht als Excel-Datei herunterladen. Nachdem Sie die Datei in Excel geöffnet haben, können Sie den Bericht mithilfe der erweiterten Funktionen anpassen. Wenn Sie zufrieden sind, laden Sie die Excel-Datei hoch. Diese Datei mit den zugehörigen Anpassungen wird bei der Ausführung des Berichts auf die Ansicht angewendet.

Weitere Informationen zum Anpassen von Berichten mithilfe von Excel finden Sie unter *Beispiel Microsoft Excel-Berichte*.

9. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**. Alle geplanten Berichte, die sich auf das Objekt beziehen, werden in diesem Fall in der Liste angezeigt.

10. Klicken Sie auf **Zeitplan hinzufügen**, um eine neue Zeile zur Seite „Berichtszeitpläne“ hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
11. Geben Sie einen Namen für den Bericht ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

    Der folgende Beispielbericht ist im CSV-Format verfügbar:

    Der folgende Beispielbericht ist im PDF-Format verfügbar:

Basierend auf den im Bericht gezeigten Ergebnissen sollten Sie möglicherweise ONTAP System Manager oder die ONTAP CLI verwenden, um die Tiering-Richtlinie in „`Auto`“ oder „`all`“ zu ändern, damit bestimmte Volumes weniger häufig benötigte Daten auf Cloud-Tier verlagern.

Suche nach einem geplanten Bericht

Sie können nach geplanten Berichten nach Name, Ansichtsname, Objekttyp oder Empfänger suchen.

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Berichtspläne**.
2. Verwenden Sie das Textfeld **geplante Berichte suchen**.

Um Berichte von …	Versuchen Sie …
Name des Zeitplans	Geben Sie einen Teil des Berichtszeitplans ein.
Name anzeigen	Geben Sie einen Teil des Namens für die Berichtsansicht ein. Standardansichten und benutzerdefinierte Ansichten werden in der Ansichtsliste angezeigt.

Um Berichte von …	Versuchen Sie …
Empfänger	Geben Sie einen Teil der E-Mail-Adresse ein.
Dateityp	Geben Sie „PDF“, „CSV“ oder „XLSX“ ein.

3. Sie können auf eine Spaltenüberschrift klicken, um Berichte in aufsteigender oder absteigender Reihenfolge nach dieser Spalte zu sortieren, z. B. Name oder Format des Zeitplans.

Anpassen von Berichten

Sie können Ansichten auf verschiedene Weise anpassen, um einen Bericht zu erstellen, der alle für das Management Ihrer ONTAP Cluster erforderlichen Informationen enthält.

Beginnen Sie mit einer Standardinventarseite oder einer benutzerdefinierten Ansicht, und passen Sie sie an, indem Sie Spalten hinzufügen oder entfernen, die Spaltenreihenfolge ändern, die Daten filtern oder eine bestimmte Spalte in aufsteigender oder absteigender Reihenfolge sortieren.

Ab Unified Manager 9.8 können Sie die Ansicht auch in Excel herunterladen, um sie mithilfe erweiterter Funktionen anzupassen. Laden Sie anschließend die angepasste Excel-Datei hoch. Wenn Sie einen Bericht über diese Ansicht planen, verwendet er die angepasste Excel-Datei, um robuste Berichte zu erstellen, die Sie freigeben können.

Weitere Informationen zum Anpassen von Berichten mithilfe von Excel finden Sie unter *Beispiel Microsoft Excel-Berichte*.

Zum Verwalten von Berichten müssen Sie über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Anpassen von Spalten

Wählen Sie mit **ein-/Ausblenden** die Spalten aus, die Sie in Ihrem Bericht verwenden möchten. Ziehen Sie die Spalten auf der Bestandsseite, um sie neu anzuordnen.

Schritte

1. Klicken Sie auf **ein-/Ausblenden**, um Spalten hinzuzufügen oder zu entfernen.
2. Ziehen Sie auf der Bestandsseite Spalten, um sie in der gewünschten Reihenfolge in Ihrem Bericht neu anzuordnen.
3. Benennen Sie die nicht gespeicherte Ansicht, um Ihre Änderungen zu speichern.

Filtern von Daten

Filtern Sie die Daten, um sicherzustellen, dass die Ergebnisse Ihren Berichtsanforderungen entsprechen. Durch Filtern können Sie nur die Daten anzeigen, für die Sie sich interessieren.

Schritte

1. Klicken Sie auf das Filtersymbol, um Filter hinzuzufügen, um die gewünschten Ergebnisse zu fokussieren,

und klicken Sie dann auf **Filter anwenden**.

2. Benennen Sie die nicht gespeicherte Ansicht, um Ihre Änderungen zu speichern.

Daten sortieren

Um die Ergebnisse zu sortieren, klicken Sie auf eine Spalte und zeigen eine aufsteigende oder absteigende Reihenfolge an. Beim Sortieren von Daten werden die für den Bericht erforderlichen Informationen priorisiert.

Schritte

1. Klicken Sie oben in einer Spalte, um die Ergebnisse so zu sortieren, dass oben in der Ansicht die wichtigsten Informationen angezeigt werden.
2. Benennen Sie die nicht gespeicherte Ansicht, um Ihre Änderungen zu speichern.

Mit der Suche können Sie Ihre Ansicht verfeinern

Nachdem Sie über die gewünschte Ansicht verfügen, können Sie die Ergebnisse mithilfe des Feldes „Suchen“ weiter verfeinern, um sich auf die Ergebnisse zu konzentrieren, die in den Bericht einbezogen werden sollen.

Schritte

1. Öffnen Sie die benutzerdefinierte oder Standardansicht, die Sie als Grundlage Ihres Berichts verwenden möchten.
2. Geben Sie das Suchfeld ein, um die in der Ansicht aufgeführten Daten zu verfeinern. Sie können Teildaten in eine der angezeigten Spalten eingeben. Wenn Sie beispielsweise nach Knoten suchen möchten, die den Namen „US_East“ enthalten, können Sie die vollständige Liste der Knoten verfeinern.

   Die Ergebnisse Ihrer Suche werden in der benutzerdefinierten Ansicht gespeichert und in den resultierenden geplanten Bericht verwendet.

3. Benennen Sie die nicht gespeicherte Ansicht, um Ihre Änderungen zu speichern.

Verwenden von Excel zum Anpassen des Berichts

Nachdem Sie die Ansicht gespeichert haben, können Sie sie im Excel-Workbook-Format (.xlsx) herunterladen. Wenn Sie die Excel-Datei öffnen, können Sie den Bericht mithilfe erweiterter Excel-Funktionen anpassen.

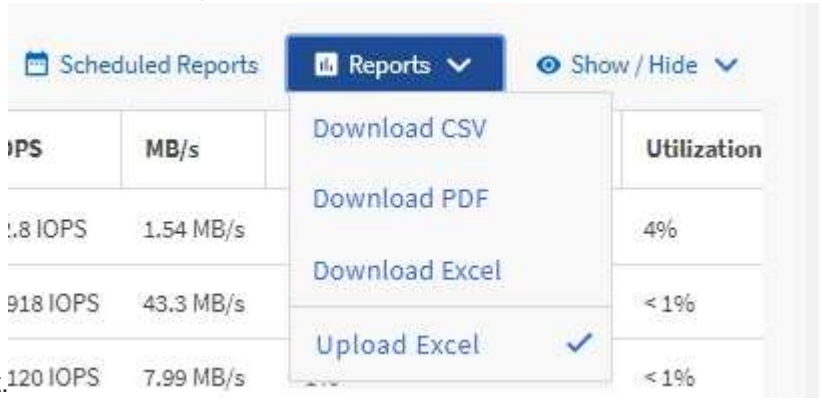
Was Sie brauchen

Sie können nur eine Excel-Arbeitsmappe mit der Erweiterung .xlsx hochladen.

Einige der erweiterten Excel-Funktionen können Sie beispielsweise in Ihrem Bericht verwenden:

- Sortieren mehrerer Spalten
- Komplexe Filterung
- Pivot-Tabellen
- Diagramme

- Die heruntergeladene Excel-Datei verwendet den Standarddateinamen für die Ansicht und nicht den gespeicherten Namen.
  - Das Format lautet `<View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx`.
  - Beispielsweise hat eine benutzerdefinierte gespeicherte Ansicht mit dem Namen einen Dateinamen, der den zu diesem Tag und zu dieser Zeit gespeicherten Namen `Volumes-not online` hat `health-volumes-05-May-2020-19-18-00.xlsx`.
- Sie können Blätter zur Excel-Datei hinzufügen, aber vorhandene Blätter nicht ändern.
  - Ändern Sie die vorhandenen Blätter, Daten und Informationen nicht. Kopieren Sie stattdessen die Daten auf eine neue Seite, die Sie erstellen.
  - Eine Ausnahme der obigen Regel ist, dass Sie Formeln auf der Seite "data" erstellen können. Verwenden Sie die Formeln der Datenseite, um Diagramme auf neuen Seiten zu erstellen.
  - Benennen Sie keine neuen Bogendaten oder Informationen.
- Wenn eine angepasste Excel-Datei vorhanden ist, wird neben dem Menüpunkt **Berichte** > **Excel hochladen** ein Häkchen angezeigt. Wenn Sie die Excel-Datei herunterladen, wird die Version mit den Anpassungen



verwendet.

Schritte

1. Öffnen Sie die Standard-, benutzerdefinierte oder gespeicherte Ansicht, die Sie als Grundlage Ihres Berichts verwenden möchten.
2. Wählen Sie **Berichte** > **Excel Herunterladen**.
3. Speichern Sie die Datei. Die Datei wird in Ihrem Download-Ordner gespeichert.
4. Öffnen Sie die gespeicherte Datei in Excel. Verschieben Sie die Datei nicht an einen neuen Speicherort, oder speichern Sie die Datei vor dem Hochladen mit dem ursprünglichen Dateinamen an einem anderen Speicherort zurück, wenn Sie an einem anderen Speicherort arbeiten.
5. Passen Sie die Datei mithilfe von Excel-Funktionen an, z. B. komplexe Sortierungen, mehrstufige Filter, Pivot-Tabellen oder Diagramme. Weitere Informationen finden Sie in der Microsoft® Excel-Dokumentation.
6. Wählen Sie **Berichte** > **Excel hochladen** und wählen Sie die Datei aus, die Sie geändert haben. Die zuletzt heruntergeladene Datei wird vom selben Dateispeicherort hochgeladen.
7. Senden Sie sich einen Testbericht mit der Funktion **geplante Berichte**.

Berichte werden heruntergeladen

Sie können Berichte herunterladen und die Daten als CSV-Datei (Comma Separated

Values), als Microsoft Excel (.XLSX)-Datei oder als PDF-Datei auf einem lokalen oder Netzwerklaufwerk speichern. Sie können CSV- und XLSX-Dateien mit Tabellenkalkulationsanwendungen wie Microsoft Excel und PDF-Dateien mit Lesern wie Adobe Acrobat öffnen.

Schritte

1. Klicken Sie auf die Schaltfläche **Berichte**, um den Bericht wie folgt herunterzuladen:

Wählen	An…
CSV herunterladen	Speichern Sie den Bericht als kommagetrennte Datei (CSV).
PDF herunterladen	Speichern Sie den Bericht als PDF-Datei.
Excel Herunterladen	Speichern Sie den Bericht als XLSX-Datei (Microsoft Excel).

Planen von Berichten

Nachdem Sie eine Ansicht haben, die Sie wiederverwenden und als Bericht freigeben möchten, können Sie sie mithilfe von Active IQ Unified Manager planen. Sie können geplante Berichte verwalten und die Empfänger und die Verteilfrequenz für jeden Berichtsplan ändern.

Sie können die meisten Ansichten oder Bestandsseiten in Unified Manager planen. Ausnahmen sind Ereignisse, die Berichte sind, die Sie als CSV-Dateien herunterladen können, aber Sie können keine Ereignisse für die Regeneration und Freigabe planen. Außerdem können Sie die Dashboards, Favoriten oder Konfigurationsseiten nicht herunterladen oder planen.

Ab Active IQ Unified Manager 9.8 können Sie Ansichten im Microsoft® Excel-Format herunterladen und anpassen. Sie können erweiterte Excel-Funktionen wie komplexe Sortierungen, mehrstufige Filter, Pivot-Tabellen und Diagramme verwenden. Wenn Sie mit dem resultierenden Excel-Bericht zufrieden sind, können Sie die Excel-Datei bei jeder Planung und Freigabe des Berichts hochladen.

Sie können die integrierten Ansichten oder Ansichten planen, die Sie anpassen. Sie können wählen, welcher Dateityp gesendet werden soll, entweder CSV, PDF oder XSLX. Wenn Sie einen Bericht zum ersten Mal planen, können Sie ihn herunterladen und sich als einzigen Empfänger zuweisen, der den Bericht sieht, da der Empfänger ihn sieht.

Planen eines Berichts

Nachdem Sie über eine Ansicht oder eine Excel-Datei verfügen, die Sie für die regelmäßige Erstellung und Verteilung planen möchten, können Sie den Bericht planen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die SMTP-Servereinstellungen auf der Seite **Allgemein** > **Benachrichtigungen** konfiguriert

haben, damit die Reporting-Engine Berichte als E-Mail-Anhänge an die Empfängerliste des Unified Manager-Servers senden kann.

- Der E-Mail-Server muss so konfiguriert sein, dass Anhänge mit den generierten E-Mails gesendet werden können.

Führen Sie die folgenden Schritte aus, um einen Bericht für eine Ansicht zu testen und zu planen. Wählen Sie die gewünschte Ansicht aus oder passen Sie sie an. Im folgenden Verfahren wird eine Netzwerkansicht verwendet, die die Leistung Ihrer Netzwerkschnittstellen zeigt, aber Sie können jede beliebige Ansicht verwenden.

Schritte

1. Öffnen Sie Ihre Ansicht. Dieses Beispiel verwendet die Standardansicht, die die LIF-Performance zeigt. Klicken Sie im linken Navigationsbereich auf **Netzwerk > Netzwerkschnittstellen**.
2. Die Ansicht wird mithilfe der integrierten Unified Manager Funktionen nach Bedarf angepasst.
3. Nachdem Sie die Ansicht angepasst haben, können Sie im Feld **Ansicht** einen eindeutigen Namen angeben und auf das Häkchen klicken, um sie zu speichern.
4. Sie können die erweiterten Funktionen von Microsoft® Excel verwenden, um Ihren Bericht anzupassen. Weitere Informationen finden Sie unter "Verwenden von Excel zum Anpassen des Berichts".
5. So sehen Sie die Ausgabe, bevor Sie sie planen oder teilen:

Option	Beschreibung
Wenn Sie Excel zum Anpassen des Berichts verwendet haben	Zeigen Sie die vorhandene heruntergeladene Excel-Datei an.
Wenn Sie Excel nicht zum Anpassen des Berichts verwendet haben	Laden Sie den Bericht als **CSV**-, **PDF**- oder **XLSX** -Datei herunter.

   Öffnen Sie die Datei mit einer installierten Anwendung, z. B. Microsoft Excel (CSV/XSLX) oder Adobe Acrobat (PDF).

6. Wenn Sie mit dem Bericht zufrieden sind, klicken Sie auf **geplante Berichte**.
7. Klicken Sie auf der Seite Berichtspläne auf **Zeitplan hinzufügen**.
8. Akzeptieren Sie den Standardnamen, der eine Kombination aus dem Ansichtsnamen und der Frequenz ist, oder passen Sie den **Terminplannamen** an.
9. Um den geplanten Bericht zum ersten Mal zu testen, fügen Sie sich nur als **Empfänger** hinzu. Wenn Sie zufrieden sind, fügen Sie die E-Mail-Adressen für alle Berichtsempfänger hinzu.
10. Geben Sie an, wie oft der Bericht erstellt und an die Empfänger gesendet wird. Sie können **Daily**, **Weekly** oder **Monthly** wählen.
11. Wählen Sie das Format aus, entweder **PDF**, **CSV** oder **XSLX**.

    Wählen Sie für Berichte, in denen Sie Excel zum Anpassen des Inhalts verwendet haben, immer **XSLX** aus.

12. Klicken Sie auf das Häkchen (✓), um den Berichtsplan zu speichern.

Der Bericht wird sofort als Test gesendet. Danach wird der Bericht unter Verwendung der geplanten Häufigkeit generiert und per E-Mail an die Empfänger gesendet.

Planen importierter .rptdesign-Berichte

Sie können vorhandene Berichte planen, die in einer früheren Version von Unified Manager erstellt und importiert wurden.

Die Planung importierter Berichte erfordert Folgendes:

- Importierte BIRT-Datei erstellt .rptdesign-Berichte in einer früheren Unified Manager-Version
- Verfügbar beim Upgrade auf Unified Manager 9.6 GA oder höher

Nach dem Upgrade auf Unified Manager 9.6 GA oder höher werden auf der Seite „Berichtszeitpläne“ die importierten Berichte aufgeführt. Sie können den Zeitplan für diese Berichte bearbeiten, um die E-Mail-Adressen, die Häufigkeit und das Format (PDF oder CSV) des Empfängers anzugeben. Andernfalls können diese Berichte nicht in der Benutzeroberfläche von Unified Manager bearbeitet oder angezeigt werden.

Schritte

1. Öffnen Sie die Seite Berichtszeitpläne. Wenn Sie Berichte importiert haben, wird eine Meldung angezeigt.
2. Klicken Sie auf den Namen **Ansicht**, um die SQL-Abfrage anzuzeigen, die zur Generierung des Berichts verwendet wird.
3. Klicken Sie auf das Symbol Mehr , klicken Sie auf **Bearbeiten**, definieren Sie die Details des Berichtplans und speichern Sie den Bericht.

   Sie können auch alle unerwünschten Berichte aus dem Mehr-Symbol löschen .

Verwalten von Berichtzeitplänen

Sie können Ihre Berichtspläne auf der Seite Berichtspläne verwalten. Sie können vorhandene Zeitpläne anzeigen, ändern oder löschen.

Was Sie brauchen

Sie können keine neuen Berichte über die Seite „Berichtszeitpläne“ planen. Sie können nur geplante Berichte von den Objektbestandsseiten hinzufügen.

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Berichtspläne**.
2. Auf der Seite Berichtspläne:

Ihr Ziel ist	Dann…
Vorhandenen Zeitplan anzeigen	Blättern Sie mithilfe der Bildlaufleisten und Seitensteuerungen durch die Liste der vorhandenen Berichte.
Einen vorhandenen Zeitplan bearbeiten	a. Klicken Sie auf das Symbol Mehr ⋮ für den gewünschten Zeitplan. b. Klicken Sie Auf **Bearbeiten**. c. Nehmen Sie die erforderlichen Änderungen vor. d. Klicken Sie auf das Häkchen, um die Änderungen zu speichern.
Einen vorhandenen Zeitplan löschen	a. Klicken Sie auf das Symbol Mehr ⋮ für den gewünschten Zeitplan. b. Klicken Sie Auf **Löschen**. c. Bestätigen Sie Ihre Entscheidung.

Bearbeiten von geplanten Berichten

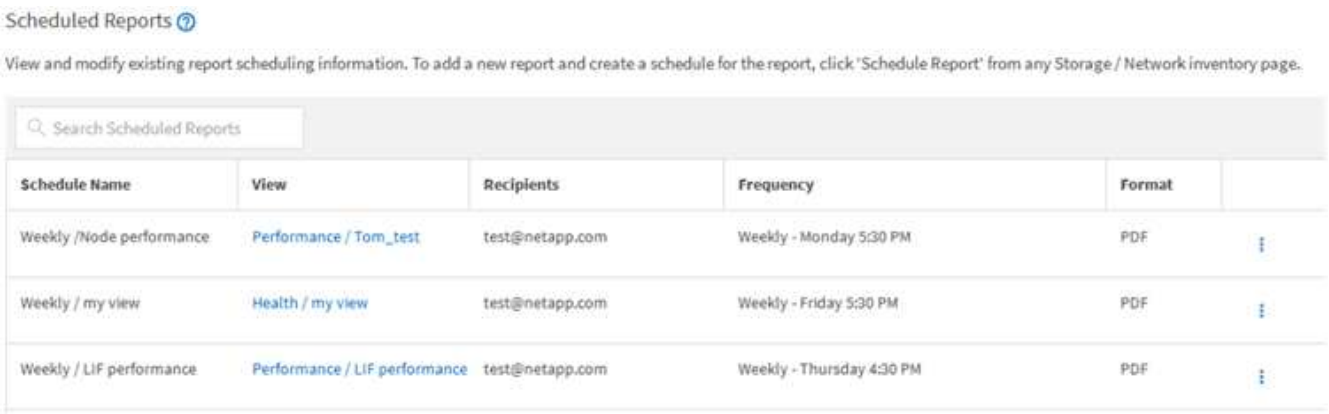
Nach der Planung von Berichten können Sie diese auf der Seite „Berichtszeitpläne“ bearbeiten.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Berichtspläne**.



Wenn Sie über die entsprechenden Berechtigungen verfügen, können Sie jeden Bericht und seinen Zeitplan im System ändern.

2. Klicken Sie auf das Symbol Mehr ⋮ für den Zeitplan, den Sie ändern möchten.

3. Klicken Sie Auf **Bearbeiten**.
4. Sie können die Liste **Terminplanname**, **Empfänger**, **Frequenz** und **Format** für den Berichtsplan ändern.
5. Wenn Sie fertig sind, klicken Sie auf das Häkchen, um Ihre Änderungen zu speichern.

Löschen geplanter Berichte

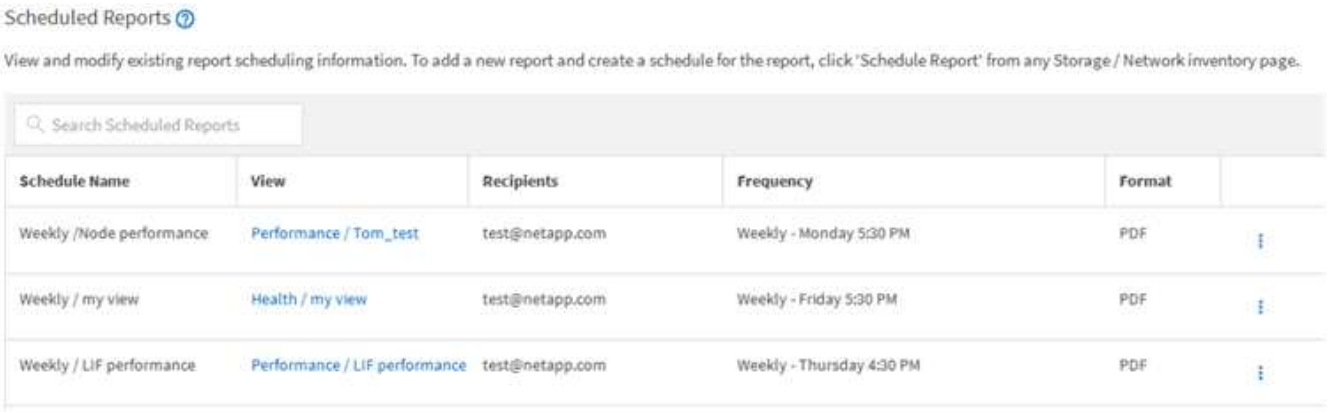
Nach der Planung von Berichten können Sie diese auf der Seite „Berichtszeitpläne“ löschen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Berichtspläne**.



> Wenn Sie über die entsprechenden Berechtigungen verfügen, können Sie alle Berichte und deren Zeitplan im System entfernen.

2. Klicken Sie auf das Symbol Mehr ⋮ für den Zeitplan, den Sie entfernen möchten.
3. Klicken Sie Auf **Löschen**.
4. Bestätigen Sie Ihre Entscheidung.

   Der geplante Bericht wird aus der Liste entfernt und wird nicht mehr im festgelegten Zeitplan erstellt und verteilt.

> Wenn Sie eine benutzerdefinierte Ansicht auf der Bestandsseite löschen, werden auch alle benutzerdefinierten Excel-Dateien oder geplanten Berichte, die diese Ansicht verwenden, gelöscht.

Beispiel für benutzerdefinierte Berichte

Benutzerdefinierte Beispielberichte werden üblicherweise verwendet, um Ihnen dabei zu helfen, potenzielle Probleme zu identifizieren und auf potenzielle Probleme zu reagieren, bevor sie auftreten.

Die Liste der Berichte in diesem Abschnitt ist nicht vollständig und wird mit der Zeit wachsen. Sie können vorschlagen, benutzerdefinierte Berichte zu diesem Abschnitt hinzuzufügen, indem Sie Feedback zur Dokumentation geben.

Zum Verwalten von Berichten müssen Sie über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Anpassen von Berichten zu Cluster-Storage

Die Beispiel-Berichte für Cluster-Storage in diesem Abschnitt sind nur Beispiele für das Verständnis, wie Berichte zur Cluster-Kapazität erstellt werden können, die Ihnen helfen, die Storage-Systemressourcen zu überwachen.

Erstellen eines Berichts zur Anzeige der Kapazität nach Clustermodell

Sie können einen Bericht erstellen, um die Storage-Kapazität und Auslastung von Clustern auf der Grundlage des Storage-Systemmodells zu analysieren.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Mit den folgenden Schritten erstellen Sie eine benutzerdefinierte Ansicht, die Kapazität nach Cluster-Modell anzeigt und dann einen Bericht für diese Ansicht erstellt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Cluster**.
2. Wählen Sie im Menü Ansicht die Option **Kapazität** > **Alle Cluster**.
3. Wählen Sie **ein-/Ausblenden** aus, um Spalten wie „`Cluster FQDN`“ und „`OS Version`“ zu entfernen, die Sie im Bericht nicht wünschen.
4. Ziehen Sie die „`Gesamt-Rohkapazität`“, die „`Model/Family`“ und die drei Aggregat-Spalten in der Nähe der Spalte „`Cluster`“.
5. Klicken Sie oben in der Spalte „`Model/Family`“, um die Ergebnisse nach Cluster-Typ zu sortieren.
6. Speichern Sie die Ansicht mit einem spezifischen Namen, der die Anzeige beschreibt, z. B. „`Capacity by Cluster Model`“.
7. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
8. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtspläne** eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
9. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf der Grundlage der im Bericht gezeigten Ergebnisse möchten Sie möglicherweise bestimmte Cluster um mehr Kapazität erweitern oder ältere Cluster-Modelle aktualisieren.

Erstellen eines Berichts, um Cluster mit der am meisten nicht zugewiesenen LUN-Kapazität zu identifizieren

Sie können einen Bericht erstellen, um die Cluster mit der am meisten nicht zugewiesenen LUN-Kapazität zu finden. Dieser Wert liegt bei über 0,5 TB. Damit können Sie ermitteln, wo Sie zusätzliche Workloads hinzufügen können.

Was Sie benötigen * Sie müssen die Rolle „Application Administrator“ oder „Storage Administrator“ haben.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, in der Cluster mit der am meisten nicht zugewiesenen LUN-Kapazität angezeigt werden. Anschließend können Sie einen Bericht so planen, dass er für diese Ansicht erstellt wird.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Cluster**.
2. Wählen Sie im Menü Ansicht die Option **Kapazität** > **Alle Cluster**.
3. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
4. Ziehen Sie die Spalte „`Unzugewiesene LUN Capacity`“ in die Spalte „`HA Pair`“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Nicht zugewiesene LUN-Kapazität größer als 0.5 TB
6. Klicken Sie oben in der Spalte „`Unzugewiesene LUN Capacity`“, um die Ergebnisse nach der größten Menge nicht zugewiesener LUN-Kapazität zu sortieren.
7. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige der Ansicht wiedergibt, z. B. „`Most Unalloked LUN Capacity`“, und klicken Sie auf das Häkchen (✓).
8. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite Berichtspläne eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
10. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf Grundlage der im Bericht gezeigten Ergebnisse möchten Sie möglicherweise die nicht zugewiesene LUN-Kapazität des Clusters verwenden.

Erstellen eines Berichts zur Anzeige von HA-Paaren mit der höchsten verfügbaren Kapazität

Sie können einen Bericht erstellen, um zu ermitteln, welche Hochverfügbarkeitspaare (HA) mit der größten Kapazität zur Bereitstellung neuer Volumes und LUNs bestehen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Mit den folgenden Schritten erstellen Sie eine benutzerdefinierte Ansicht, in der HA-Paare angezeigt werden, die nach der meisten verfügbaren Kapazität zur Bereitstellung neuer Volumes und LUNs sortiert sind.

Anschließend können Sie einen Bericht für diese Ansicht erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Cluster**.
2. Wählen Sie im Menü Ansicht die Option **Kapazität** > **Alle Cluster**.
3. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
4. Ziehen Sie die Spalte „`Aggregate unused Capacity`“ nahe der Spalte „`HA Pair`“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Ungenutzte Kapazität aggregieren über 0.5 TB
6. Klicken Sie oben in der Spalte „`Aggregate Unused Capacity`“, um die Ergebnisse nach der größten Menge an ungenutzter Aggregatskapazität zu sortieren.
7. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige der Ansicht wiedergibt, z. B. „`Least Used Aggregate Capacity`“, und klicken Sie auf das Häkchen (✓).
8. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite Berichtspläne eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
10. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf Grundlage der im Bericht gezeigten Ergebnisse sollten Sie basierend auf der Aggregatskapazität den Ausgleich der HA-Paare schaffen.

Erstellen eines Berichts zum Anzeigen von Nodes, auf denen ältere Versionen von ONTAP ausgeführt werden

Sie können einen Bericht erstellen, um die Version der ONTAP Software anzuzeigen, die auf allen Cluster-Nodes installiert ist. So können Sie sehen, welche Nodes Sie aktualisieren sollten.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, in der Nodes mit älteren ONTAP-Versionen angezeigt werden, und planen Sie anschließend einen Bericht für diese Ansicht zu erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherung** > **Knoten**.
2. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
3. Ziehen Sie die Spalte „`OS Version`“ in die Spalte „`Node`“.
4. Klicken Sie oben in der Spalte „`OS Version`“, um die Ergebnisse nach der ältesten Version von ONTAP zu sortieren.

5. Speichern Sie die Ansicht mit einem bestimmten Namen, der angibt, was die Ansicht zeigt, z. B. „`Knoten nach ONTAP-Version`“.
6. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
7. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite Berichtspläne eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
8. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf der Grundlage der im Bericht gezeigten Ergebnisse sollten Sie möglicherweise ein Upgrade auf Nodes durchführen, auf denen ältere Versionen von ONTAP laufen.

Anpassung der Berichte zur Aggregatskapazität

Anhand dieser individuellen Beispielberichte können Sie potenzielle Probleme im Zusammenhang mit der Aggregat-Storage-Kapazität identifizieren und darauf reagieren.

Die Berichte in diesem Abschnitt sind nur Beispiele, die Ihnen dabei helfen, Berichte über Aggregatskapazität zu erstellen, damit Sie die Storage-Systemressourcen überwachen können.

Erstellen eines Berichts, um Aggregate anzuzeigen, die voll ausgelastet sind

Sie können einen Bericht erstellen, um die volle Kapazität der Aggregate zu ermitteln, damit Sie mehr Kapazität hinzufügen oder Workloads zu anderen Aggregaten verschieben können.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Mit den folgenden Schritten erstellen Sie eine benutzerdefinierte Ansicht, auf der Aggregate vollständig ausgelastet sind. Planen Sie dann einen Bericht, der für diese Ansicht erstellt werden soll.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Aggregate**.
2. Wählen Sie im Menü Ansicht die Option **Kapazität** > **Alle Aggregate**.
3. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
4. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Tage bis zur vollen Zeit weniger als 45 Tage
5. Klicken Sie oben in der Spalte „`Dzu voll`“, um die Ergebnisse nach der verbleibenden Anzahl an Tagen zu sortieren, um die volle Kapazität zu erreichen.
6. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige der Ansicht wiedergibt, z. B. „`Tage zur vollen Aggregatkapazität`“, und klicken Sie auf das Häkchen (✓).
7. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.

8. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtspläne** eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
9. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Basierend auf den im Bericht gezeigten Ergebnissen sollten Sie den Storage für Aggregate erhöhen, die die volle Kapazität erreichen. Außerdem können Sie die Tage bis zur vollständigen Kapazitätsgrenze auf mehr als die standardmäßigen 7 Tage erhöhen, sodass Sie Ereignisse erhalten, die mehr Zeit bieten, um auf den bei Aggregaten niedrig zu reagieren.

Erstellen eines Berichts, um Aggregate zu sehen, die zu 80 % oder mehr voll sind

Sie können einen Bericht erstellen, um die Aggregate zu markieren, die zu 80 % oder mehr voll sind.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Erstellen Sie mithilfe der folgenden Schritte eine benutzerdefinierte Ansicht, in der Aggregate angezeigt werden, die zu 80 % oder mehr voll sind. Planen Sie dann einen Bericht, der für diese Ansicht erstellt werden soll.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Aggregate**.
2. Wählen Sie im Menü Ansicht die Option **Kapazität** > **Alle Aggregate**.
3. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
4. Ziehen Sie die Spalten „`Available Data %`“ und „`used Data %`“ in die Nähe der Spalte „`Aggregate`“.
5. Klicken Sie auf das Filtersymbol, fügen Sie die folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Verwendete Daten % sind größer als 80 %
6. Klicken Sie oben in der Spalte „`Used Data %`“, um die Ergebnisse nach Capacity prozentual zu sortieren.
7. Speichern Sie die Ansicht mit einem bestimmten Namen, der das anzeigt, was die Ansicht zeigt, zum Beispiel “Aggregate nearing full”, und klicken Sie auf das Häkchen (✓) .
8. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite Berichtspläne eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
10. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Möglicherweise möchten Sie auf der Grundlage der im Bericht gezeigten Ergebnisse einige Daten von bestimmten Aggregaten verschieben.

Erstellen eines Berichts, um überzugesetzte Aggregate anzuzeigen

Sie können einen Bericht erstellen, um die Storage-Kapazität und die Verwendung von Aggregaten zu analysieren und überzugesetzte Aggregate anzuzeigen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, in der Aggregate angezeigt werden, die den überdefinierten Schwellenwert überschreiten. Planen Sie dann einen Bericht für diese Ansicht zu erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Aggregate**.
2. Wählen Sie im Menü Ansicht die Option **Kapazität** > **Alle Aggregate**.
3. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
4. Ziehen Sie die Spalte „`overovered Capacity %`“ nahe der Spalte „`Aggregate`“.
5. Klicken Sie auf das Filtersymbol, fügen Sie die folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Überzuviel Kapazität % ist größer als 100 %
6. Klicken Sie oben in der Spalte „`overed Capacity %`“, um die Ergebnisse nach Capacity prozentual zu sortieren.
7. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige der Ansicht wiedergibt, z. B. „`Aggregate overcommitted`“, und klicken Sie auf das Häkchen (✓).
8. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite Berichtspläne eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
10. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Basierend auf den im Bericht gezeigten Ergebnissen möchten Sie möglicherweise zusätzliche Kapazitäten zu Aggregaten hinzufügen oder einige Daten von bestimmten Aggregaten verschieben.

Anpassen der Berichte zur Volume-Kapazität

Anhand dieser individuellen Berichte können Sie potenzielle Probleme im Zusammenhang mit Volume-Kapazität und Performance identifizieren und beheben.

Erstellen eines Berichts, um Volumes zu identifizieren, die sich der vollen Kapazität nähern, für die die automatische Löschung von Snapshot deaktiviert ist

Sie können einen Bericht erstellen, der die Liste der Volumes enthält, die sich mit deaktiviertem Snapshot Autodelete fast voll ausgelastet sind. Die Ergebnisse können dabei helfen, Volumes zu identifizieren, in denen Sie Snapshot Autodelete konfigurieren

möchten.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, in der die erforderlichen Spalten in der richtigen Reihenfolge angezeigt werden, und planen Sie dann einen Bericht, der für diese Ansicht erstellt werden soll.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Kapazität** > **Alle Volumes**.
3. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
4. Ziehen Sie die Spalten „`Snapshot Autodelete`“ und „`Ds to Full`“ in die Nähe der Spalte „`Available Data Capacity`“.
5. Klicken Sie auf das Filtersymbol, fügen Sie die folgenden beiden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Tage bis zur vollen Zeit weniger als 30 Tage
   - Snapshot Autodelete ist deaktiviert
6. Klicken Sie oben in der Spalte **Tage bis voll**, damit die Volumes mit den wenigsten verbleibenden Tagen oben in der Liste angezeigt werden.
7. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige beschreibt, z. B. „`Vols near Capacity`“.
8. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
9. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf der Grundlage der im Bericht gezeigten Ergebnisse möchten Sie möglicherweise das automatische Löschen von Snapshots auf den Volumes aktivieren oder den verfügbaren Speicherplatz erweitern.

Erstellen eines Berichts zur Ermittlung des von Volumes mit deaktiviertem Thin Provisioning genutzten Speicherplatzes

Ist kein Thin Provisioning auf einem Volume möglich, nimmt dies den gesamten Speicherplatz auf der Festplatte ein, wie zum Zeitpunkt der Erstellung des Volume definiert. Wenn Sie Volumes mit deaktiviertem Thin Provisioning festlegen, können Sie entscheiden, ob Sie Thin Provisioning auf bestimmten Volumes aktivieren möchten.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, in der die erforderlichen Spalten in der richtigen Reihenfolge angezeigt werden, und planen Sie dann einen Bericht, der

für diese Ansicht erstellt werden soll.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Kapazität** > **Alle Volumes**.
3. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
4. Ziehen Sie die Spalten „`Used Data %`“ und „`Thin Provisioning`“ in die Nähe der Spalte „`Available Data Capacity`“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu: **Thin Provisioning** ist **Nein** und klicken Sie dann auf **Filter anwenden**.
6. Klicken Sie oben in der Spalte „`Used Data %`“, um die Ergebnisse zu sortieren, sodass die Volumes mit dem höchsten Prozentsatz oben in der Liste angezeigt werden.
7. Speichern Sie die Ansicht mit einem Namen, um die Anzeige abzuspiegeln, z. B. „`Vols no Thin Provisioning`“.
8. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtspläne** eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
10. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Basierend auf den im Bericht gezeigten Ergebnissen sollten Sie Thin Provisioning auf bestimmten Volumes aktivieren.

Erstellen eines Berichts zur Ermittlung von Volumes in FabricPool Aggregaten, die Daten in das Cloud-Tier verschieben sollten

Sie können einen Bericht mit einer Liste der Volumes erstellen, die sich derzeit in FabricPool Aggregaten befinden, über eine Cloud-Empfehlung von Tiers verfügen und über eine große Menge an kalten Daten. In diesem Bericht können Sie entscheiden, ob Sie die Tiering-Richtlinie für bestimmte Volumes in „`Auto`“ oder „`all`“ ändern sollten, um mehr kalte (inaktive) Daten auf die Cloud-Tier zu verlagern.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen FabricPool Aggregate konfiguriert haben und Volumes auf diesen Aggregaten haben.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, in der die erforderlichen Spalten in der richtigen Reihenfolge angezeigt werden, und planen Sie dann einen Bericht, der für diese Ansicht erstellt werden soll.

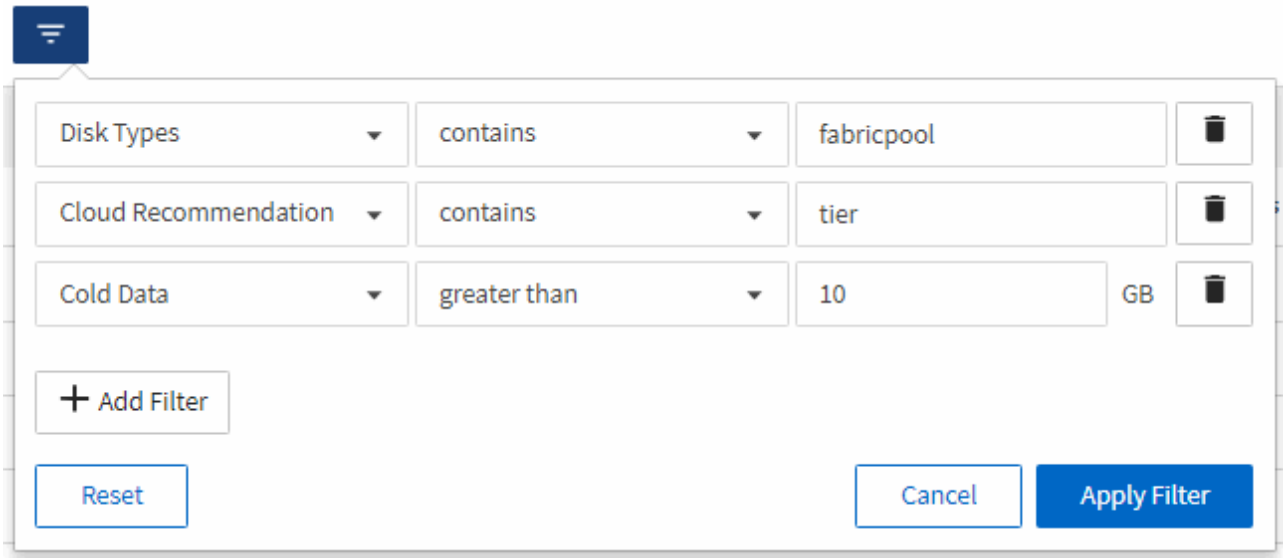
Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Leistung** > **Alle Volumes**.

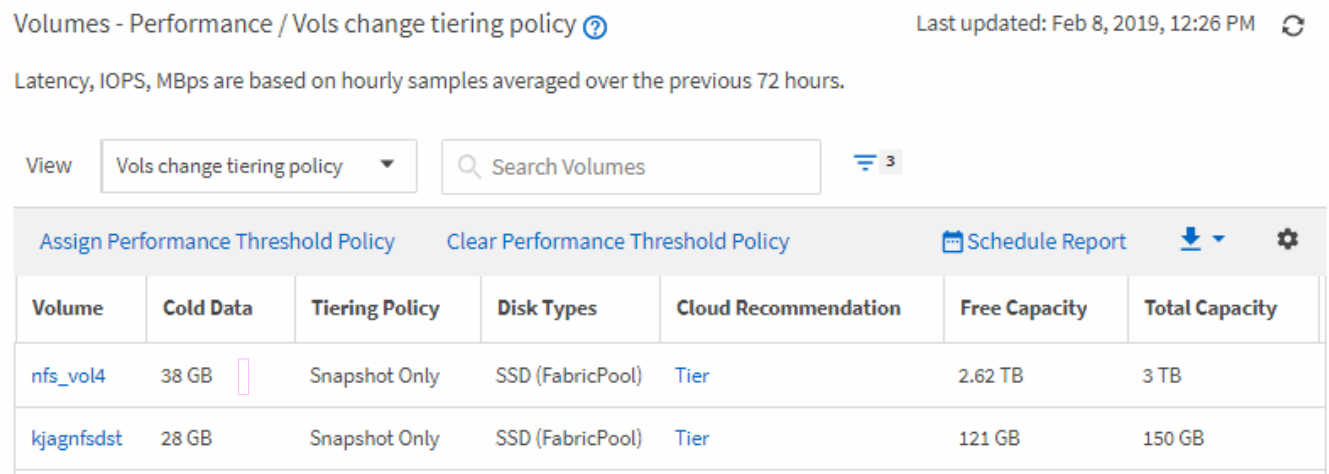
3. Stellen Sie in der Spaltenauswahl sicher, dass die Spalte „`DFestplatten-Typ`“ in der Ansicht angezeigt wird.

   Fügen Sie weitere Spalten hinzu oder entfernen Sie diese, um eine für Ihren Bericht wichtige Ansicht zu erstellen.

4. Ziehen Sie die Spalte „`Disk Type`“ in die Spalte „`Cloud Recommendation`“.
5. Klicken Sie auf das Filtersymbol, fügen Sie die folgenden drei Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Der Festplattentyp enthält FabricPool
   - Cloud-Empfehlung enthält Tier
   - Kalte Daten größer als 10 GB



6. Klicken Sie oben in der Spalte „kalte Daten“, damit die Volumes mit den meisten kalten Daten oben in der Ansicht angezeigt werden.
7. Speichern Sie die Ansicht mit einem Namen, um die Anzeige der Ansicht widerzuspiegeln, z. B. „`Vols change Tiering Policy`“.



8. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite Berichtspläne eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.

10. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Basierend auf den im Bericht gezeigten Ergebnissen sollten Sie möglicherweise System Manager oder die ONTAP CLI verwenden, um die Tiering-Richtlinie in „`Auto`“ oder „`all`“ zu ändern, damit bestimmte Volumes mehr „kalte“ Daten auf die Cloud-Tier verlagern.

Qtree Anpassung der Kapazitätsberichte

Anhand dieser individuellen Beispielberichte können Sie potenzielle Probleme im Zusammenhang mit qtree-Kapazität identifizieren und darauf reagieren.

Erstellung eines Berichts zur Anzeige von fast vollen qtrees

Sie können einen Bericht erstellen, um die Storage-Kapazität und -Auslastung von qtrees zu analysieren und nahezu volle qtrees anzuzeigen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Erstellen Sie mit den folgenden Schritten eine benutzerdefinierte Ansicht, in der fast vollständige qtrees angezeigt werden, und planen Sie dann einen Bericht, der für diese Ansicht erstellt werden soll.

Schritte

1. Klicken Sie im linken Navigationsfenster auf **Storage** > **Qtrees**.
2. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
3. Ziehen Sie die Spalte „`Disk used %`“ in die Spalte „`Qtrees`“.
4. Klicken Sie auf das Filtersymbol, fügen Sie die folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
    - Verwendete Festplatten % sind größer als 75 %
5. Klicken Sie oben in der Spalte „`Disk used %`“, um die Ergebnisse nach Kapazitätsanteil zu sortieren.
6. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige der Ansicht wiedergibt, z. B. „`Qtrees nearing full`“, und klicken Sie auf das Häkchen (✓).
7. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
8. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtspläne** eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
9. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Basierend auf den im Bericht gezeigten Ergebnissen sollten Sie möglicherweise die Festplatten- und Soft-Limits (sofern vorhanden) anpassen oder die Daten in qtrees ausgleichen.

Anpassen von Berichten zur NFS-Freigabe

Sie können NFS-Share-Berichte anpassen, um Informationen zu NFS-Exportrichtlinien und Regeln für Volumes auf Ihren Storage-Systemen zu analysieren. Sie können Berichte beispielsweise anpassen, um Volumes mit nicht zugänglichen Mount-Pfaden und Volumes mit der Standard-Exportrichtlinie anzuzeigen.

Erstellen eines Berichts zum Anzeigen von Volumes mit einem nicht zugänglichen Bereitstellungspfad

Sie können einen Bericht erstellen, um nach Volumes zu suchen, die über einen nicht zugänglichen Bereitstellungspfad verfügen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht für Volumes zu erstellen, die über einen nicht zugänglichen Mount-Pfad verfügen, und planen Sie dann einen Bericht, der für diese Ansicht erstellt werden soll.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **NFS Shares**.
2. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
3. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Mount Path Active ist Nein
4. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige der Ansicht wiedergibt, z. B. „`Volumes mit einem unzugänglichen Mount-Pfad`“, und klicken Sie auf das Häkchen (✓).
5. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
6. Klicken Sie auf **Zeitplan hinzufügen**, um eine neue Zeile zur Seite „Berichtszeitpläne“ hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
7. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Anhand der im Bericht gezeigten Ergebnisse möchten Sie möglicherweise die nicht zugänglichen Mount-Pfade korrigieren.

Erstellen eines Berichts, um Volumes anzuzeigen, die die Standard-Exportrichtlinie verwenden

Sie können einen Bericht erstellen, um nach Volumes zu suchen, die die Standard-Exportrichtlinie verwenden.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht für Volumes zu erstellen, die die Standard-Exportrichtlinie verwenden, und planen Sie dann einen Bericht für diese Ansicht zu erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **NFS Shares**.
2. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
3. Ziehen Sie die Spalte „`Export Policy`“ in die Spalte „`Volume`“.
4. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Exportrichtlinie enthält den Standardwert
5. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige der Ansicht wiedergibt, z. B. „`Volumes mit einer Standardexportrichtlinie`“, und klicken Sie auf das Häkchen (✓).
6. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
7. Klicken Sie auf **Zeitplan hinzufügen**, um eine neue Zeile zur Seite „Berichtszeitpläne“ hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
8. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf der Grundlage der im Bericht gezeigten Ergebnisse möchten Sie möglicherweise eine benutzerdefinierte Exportrichtlinie konfigurieren.

Anpassung von Storage-VM-Berichten

Sie können Storage-VM-Berichte erstellen, um Volume-Informationen zu analysieren und den Gesamtzustand und die Storage-Verfügbarkeit anzuzeigen. Sie können beispielsweise Berichte erstellen, um SVMs die maximale Volume-Anzahl zu erreichen und beendete SVMs zu analysieren.

Erstellen eines Berichts, um Storage-VMs anzuzeigen, die die maximale Volume-Grenze erreichen

Sie können einen Bericht erstellen, um SVMs zu finden, die die maximale Volume-Obergrenze erreichen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Mit den folgenden Schritten erstellen Sie eine benutzerdefinierte Ansicht, die Storage-VMs anzeigt, die die maximale Volume-Grenze erreichen. Anschließend können Sie einen Bericht planen, der für diese Ansicht erstellt werden soll.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Storage VMs**.
2. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.

3. Ziehen Sie die Spalten „`Datenträgeranzahl`“ und „`Maximum allowed Volumes`“ in der Nähe der Spalte „`Storage VM`“.
4. Klicken Sie oben in der Spalte „`Maximum allowed Volumes`“, um die Ergebnisse nach der höchsten Anzahl von Volumes zu sortieren.
5. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Ansicht wiedergibt, z. B. „`SVMs reaching max Volumes`“, und klicken Sie auf das Häkchen (✓).
6. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
7. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtspläne** eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
8. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf Grundlage der im Bericht gezeigten Ergebnisse sollten Sie möglicherweise die Volumes, die Storage VMs zugewiesen sind, ausgleichen oder – falls möglich – mit ONTAP System Manager die maximal zulässigen Volumes ändern.

Erstellen eines Berichts, um angehalten Storage-VMs anzuzeigen

Sie können einen Bericht erstellen, um eine Liste aller angehalten SVMs anzuzeigen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die angehörte Storage-VMs anzeigt, und planen Sie dann einen Bericht für diese Ansicht zu erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Storage VMs**.
2. Wählen Sie im Menü Ansicht die Option **Systemzustand** > **Alle Storage VMs** aus.
3. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
4. Ziehen Sie die Spalte „`State`“ in der Spalte „`Storage VM`“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Der Status wurde angehalten
6. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige der Ansicht wiedergibt, z. B. „`gestoppte SVMs`“, und klicken Sie auf das Häkchen (✓).
7. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
8. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtspläne** eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
9. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die

Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf der Grundlage der im Bericht gezeigten Ergebnisse sollten Sie möglicherweise untersuchen, warum die SVM angehalten wurde, um zu sehen, ob Sie die angehalten SVMs neu starten möchten.

Anpassen von Berichten 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.

Erstellen eines Berichts, um Volume-Beziehungen nach Fehlerquelle zu gruppieren

Sie können einen Bericht erstellen, in dem Volumes gruppiert werden, weil die Beziehung sich in einem ungesunden Zustand befindet.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die Volumes nach Fehlerquelle gruppiert und dann einen Bericht für diese Ansicht zu erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Beziehung** > **Alle Beziehungen**.
3. Wählen Sie **ein-/Ausblenden** aus, um sicherzustellen, dass die Spalten „`Beziehungsgesundheit`“ und „`ungesunder Grund`“ in der Ansicht angezeigt werden.

   Fügen Sie weitere Spalten hinzu oder entfernen Sie diese, um eine für Ihren Bericht wichtige Ansicht zu erstellen.

4. Ziehen Sie die Spalten „`Relationship Health`“ und „`ungesunder Grund`“ in die Nähe der Spalte „`State`“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Gesundheit der Beziehung ist schlecht
6. Klicken Sie oben in der Spalte „`ungesunder Grund`“, um die Volume-Beziehungen nach Fehlerquelle zu gruppieren.
7. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige beschreibt, z. B. „`Vol Relationships by Failure`“.
8. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
9. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf der Grundlage der im Bericht angezeigten Ergebnisse können Sie die Quelle und die Auswirkungen jeder Art von Fehlern untersuchen.

Erstellen eines Berichts zur Gruppierung von Volume-Beziehungen nach Problem

Sie können einen Bericht erstellen, der Volume-Beziehungen nach Problem gruppiert.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Mit den folgenden Schritten erstellen Sie eine benutzerdefinierte Ansicht, in der Volume-Beziehungen nach Problem gruppiert werden, und planen Sie dann einen Bericht für diese Ansicht zu erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Beziehung** > **Alle Beziehungen**.
3. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
4. Ziehen Sie die Spalte „`ungesunder Grund`“ in die Spalte „`State`“.
5. Klicken Sie oben in der Spalte „`ungesunder Grund`“, um die Volumes nach Problem zu gruppieren.
6. Speichern Sie die Ansicht mit einem bestimmten Namen, der angibt, was die Ansicht zeigt, z. B. „`Vol Relationships by Ausgabe`“.
7. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
8. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf Grundlage der im Bericht angezeigten Ergebnisse können Sie die Quelle und die Auswirkungen jedes Problems untersuchen.

Erstellen eines Berichts zur Anzeige von Trends der Volume-Übertragung in bestimmten Zeitintervallen

Sie können einen Bericht erstellen, in dem die Trends der Volume-Übertragung in bestimmten Zeitintervallen angezeigt werden.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht für Volumes in bestimmten Zeitintervallen zu erstellen und anschließend einen Bericht für diese Ansicht zu planen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Beziehung** > **letzter 1 Monat Transferstatus** aus.
3. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.

4. Ziehen Sie die Spalte Übertragungsdauer in der Spalte „`Operationelles Ergebnis`“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Endzeit der Übertragung in den letzten 7 Tagen
6. Klicken Sie oben in der Spalte „`Transferdauer`“, um die Volumes nach Zeitintervall zu sortieren.
7. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige beschreibt, z. B. „`Volumes nach Dauer`“.
8. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
9. Geben Sie einen Namen für den Berichtsplan ein, legen Sie die Häufigkeit als **wöchentlich** fest, füllen Sie die anderen Berichtsfelder aus, und klicken Sie dann am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Anhand der im Bericht gezeigten Ergebnisse können Sie die Transferzeitintervalle untersuchen.

Erstellen eines Berichts zur Anzeige eines fehlgeschlagenen oder erfolgreichen Volume-Transfers

Sie können einen Bericht erstellen, in dem der Status der Volume-Transfers angezeigt wird. Sie können sowohl fehlgeschlagene als auch erfolgreiche Volume-Transfers in diesem Bericht anzeigen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Verwenden Sie die folgenden Schritte, um eine benutzerdefinierte Ansicht zu erstellen, um anzuzeigen, welche Transfers fehlgeschlagen und welche erfolgreich waren, und einen Bericht für diese Ansicht zu erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Beziehung** > **letzter 1 Monat Transferstatus** aus.
3. Wählen Sie **ein-/Ausblenden** aus, um alle Spalten zu entfernen, die im Bericht nicht benötigt werden.
4. Ziehen Sie die Spalte „`Operation result`“ in die Spalte „`State`“.
5. Klicken Sie oben in der Spalte „`Operation result`“, um die Volumes nach dem Status zu sortieren.
6. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige beschreibt, z. B. „`Volumes nach Transferstatus`“.
7. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
8. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf der Grundlage der im Bericht angezeigten Ergebnisse können Sie den Transferstatus untersuchen.

Erstellen eines Berichts zur Anzeige von Volume-Transfers basierend auf der Übertragungsgröße

Sie können einen Bericht erstellen, um Volume-Transfers basierend auf der Übertragungsgröße anzuzeigen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Mit den folgenden Schritten erstellen Sie eine benutzerdefinierte Ansicht für Volume-Transfers basierend auf der Transfergröße und planen dann einen Bericht, der für diese Ansicht erstellt werden soll.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Beziehung** > **Letzter 1 Monat Transferrate**.
3. Klicken Sie oben in der Spalte „`Total Transfer Size`“, um die Volume-Transfers nach Größe zu sortieren.
4. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige beschreibt, z. B. „`Volumes nach Transfergröße`“.
5. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
6. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf Grundlage der im Bericht gezeigten Ergebnisse können Sie die Volume-Beziehungen anhand der Übertragungsgröße untersuchen.

Erstellen eines Berichts zur Anzeige von Volume-Transfers nach Tag gruppiert

Sie können einen Bericht erstellen, um Volume-Transfers nach Tagen gruppiert anzuzeigen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Mit den folgenden Schritten erstellen Sie eine benutzerdefinierte Ansicht für Volume-Transfers nach Tag gruppiert und planen dann einen Bericht für diese Ansicht zu erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Beziehung** > **Letzter 1 Monat Transferrate**.
3. Klicken Sie oben in der Spalte „`Day`“, um die Volume-Transfers nach Tag zu sortieren.
4. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige beschreibt, z. B. „`Volume Transfers by day`“.
5. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.

6. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf Grundlage der im Bericht gezeigten Ergebnisse können Sie die Volume-Transfers pro Tag untersuchen.

Sie können die Performance-Berichte von Volumes anpassen

Anhand dieser individuellen Berichte können Sie potenzielle Probleme im Zusammenhang mit der Volume-Performance identifizieren und darauf reagieren.

Erstellen eines Berichts, um Volumes mit einer hohen Menge an „kalten“ Daten auf einem Aggregat anzuzeigen, das nicht FabricPool-aktiviert ist

Sie können einen Bericht erstellen, um Volumes mit einer hohen Menge an „kalten“ Daten auf einem nicht-FabricPool-Aggregat anzuzeigen. So können Sie Volumes identifizieren, die in ein FabricPool Aggregat verschoben werden sollten.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Mit den folgenden Schritten erstellen Sie eine benutzerdefinierte Ansicht für Volumes mit einer hohen Menge an kalten Daten auf einem nicht FabricPool-fähigen Aggregat und planen anschließend einen Bericht für diese Ansicht zu erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Leistung** > **Alle Volumes**.
3. Wählen Sie **ein-/Ausblenden** aus, um sicherzustellen, dass die Spalte „`DFestplatten-Typ`“ in der Ansicht angezeigt wird.

   Fügen Sie weitere Spalten hinzu oder entfernen Sie diese, um eine für Ihren Bericht wichtige Ansicht zu erstellen.

4. Ziehen Sie die Spalte „`Disk Type`“ in der Spalte „`Cold Data`“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Kalte Daten größer als 100 GB
   - Der Festplattentyp enthält SSD
6. Klicken Sie oben in der Spalte „`DFestplatten Typ`“, um die Volumes nach Festplattentyp zu sortieren, sodass sich die Festplatte des SSD (FabricPool) unten befindet.
7. Speichern Sie die Ansicht mit einem bestimmten Namen, der die Anzeige wiedergibt, z. B. „`Cold Data Vols not FabricPool`“.
8. Klicken Sie auf der Bestandsseite auf die Schaltfläche **geplante Berichte**.
9. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken

Sie am Ende der Zeile auf das Häkchen (✓).

Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf der Grundlage der im Bericht gezeigten Ergebnisse können Sie die Volumes finden, die gute Kandidaten für die Verschiebung zu FabricPool Aggregaten sind.

Beispiel für Microsoft Excel-Berichte

Diese Beispielberichte von Microsoft Excel dienen der Einführung von Berichtsoptionen, die über die erweiterten Excel-Funktionen verfügbar sind.

Mit den erweiterten Funktionen von Excel können Sie eine Vielzahl von Berichten erstellen, die speziell auf Ihre Bedürfnisse zugeschnitten sind. Ausführliche Informationen zur Verwendung von Excel finden Sie in der Produktdokumentation.

Zum Verwalten von Berichten müssen Sie über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Erstellen eines Berichts zur Anzeige einer aggregierten Kapazitätstabelle und eines Diagramms

Sie können einen Bericht erstellen, um die Kapazität in einer Excel-Datei zu analysieren, indem Sie die summierten Summen und das Format der Cluster-Spaltendiagramme verwenden.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Gehen Sie wie folgt vor, um eine Integritätsansicht zu öffnen: Alle Aggregate, laden Sie die Ansicht in Excel herunter, erstellen Sie ein verfügbares Kapazitätdiagramm, laden Sie die angepasste Excel-Datei hoch und planen Sie den Abschlussbericht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Aggregate**.
2. Wählen Sie **Berichte** > **Excel Herunterladen**.

   Je nach Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.
3. Klicken Sie bei Bedarf auf **Bearbeiten aktivieren**.
4. Öffnen Sie in Excel die heruntergeladene Datei.
5. Erstellen Sie ein neues Blatt (⊕) nach dem `data` Blatt und benennen Sie es **Gesamtdatenkapazität**.
6. Fügen Sie auf der neuen Seite „Gesamtkapazität Daten“ die folgenden Spalten hinzu:
   a. Datenkapazität (GB) insgesamt
   b. Engagierte Kapazität (GB)

c. Genutzte Datenkapazität (GB)

d. Verfügbare Datenkapazität (GB)

7. Geben Sie in der ersten Zeile jeder Spalte die folgende Formel ein, achten Sie darauf, dass sie auf das Datenblatt (Daten!) verweist und die korrekten Spalten- und Zeilenangaben für die erfassten Daten referenziert (die Gesamtkapazität der Daten zieht Daten aus Spalte E, Zeilen 2 bis 20).

   a. =SUM(Daten!E-Dollar 2:Daten!E-20 USD)

   b. =SUM(Data!F €2:Data!F €50)

   c. =SUM(Data!G 2:Data!G 50 USD)

   d. =SUM(Daten!H 2 USD:Daten!H 50 USD)

   Die Formel summensiert jede Spalte basierend auf den aktuellen Daten.

1. Wählen Sie auf dem Datenblatt die Spalten **Gesamtkapazität (GB)** und **Kapazität (GB)** aus.
2. Wählen Sie im Menü * Einfügen* * * * * die Option **geclusterte Spalte** aus.
3. Klicken Sie mit der rechten Maustaste auf das Diagramm, und wählen Sie **Diagramm verschieben**, um das Diagramm auf das Blatt zu verschieben `Total Data Capacity`.
4. Mit den Menüs **Design** und **Format**, die bei der Auswahl des Diagramms zur Verfügung stehen, können Sie die Darstellung des Diagramms anpassen.
5. Wenn Sie zufrieden sind, speichern Sie die Datei mit Ihren Änderungen. Ändern Sie nicht den Dateinamen oder den Speicherort.

6. Wählen Sie in Unified Manager die Option **Berichte** > **Excel hochladen** aus.

   Stellen Sie sicher, dass Sie sich in der gleichen Ansicht befinden, in der Sie die Excel-Datei heruntergeladen haben.

7. Wählen Sie die Excel-Datei aus, die Sie geändert haben.
8. Klicken Sie Auf **Offen**.
9. Klicken Sie Auf **Absenden**.

   Neben dem Menüpunkt **Berichte** > **Excel hochladen** wird ein Häkchen angezeigt.

10. Klicken Sie Auf **Geplante Berichte**.
11. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite Berichtspläne eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.

    Wählen Sie das Format **XLSX** für den Bericht aus.

12. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf der Grundlage der im Bericht gezeigten Ergebnisse sollten Sie möglicherweise untersuchen, wie Sie die verfügbare Kapazität in Ihrem Netzwerk am besten nutzen können.

Erstellen eines Berichts zur Anzeige der insgesamt im Vergleich zu den verfügbaren Kapazitätsdiagrammen

Sie können einen Bericht erstellen, um die Gesamtspeicherkapazität und die Kapazität in einem Excel-Diagrammformat zu analysieren.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Gehen Sie wie folgt vor, um eine Integritätsansicht zu öffnen: Alle Aggregate, laden Sie die Ansicht in Excel herunter, erstellen Sie ein Diagramm mit der Gesamt- und der zugesagt Kapazität, laden Sie die angepasste Excel-Datei hoch und planen Sie den Abschlussbericht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Aggregate**.
2. Wählen Sie **Berichte** > **Excel Herunterladen**.

   Je nach Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.
3. Öffnen Sie in Excel die heruntergeladene Datei.
4. Klicken Sie bei Bedarf auf **Bearbeiten aktivieren**.
5. Klicken Sie auf dem Datenblatt mit der rechten Maustaste auf die Spalte Typ und wählen Sie **Sortieren** > **Sortieren Sie A bis Z** aus.

   Damit werden Ihre Daten nach Storage-Typ angeordnet. Dies umfasst beispielsweise:

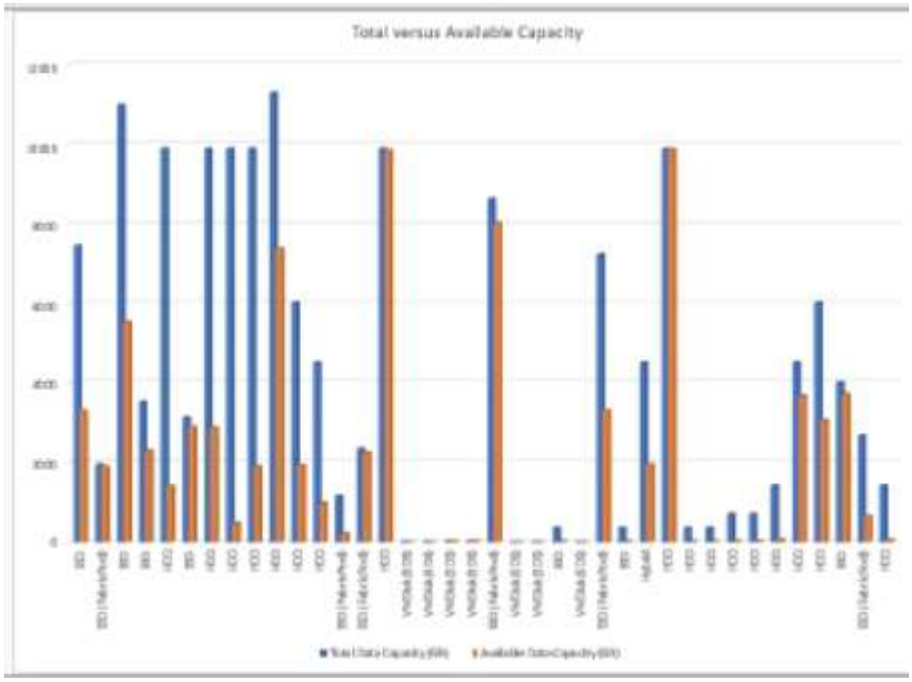
   - HDD
   - Hybrid
   - SSD
   - SSD (FabricPool)
6. Wählen Sie die `Type, Total Data Capacity,` Spalten und `Available Data Capacity` aus.
7. Wählen Sie im Menü **Einfügen** ein `3-D column` Diagramm aus.

   Das Diagramm wird auf dem Datenblatt angezeigt.
8. Klicken Sie mit der rechten Maustaste auf das Diagramm und wählen Sie **Diagramm verschieben**.
9. Wählen Sie **Neues Blatt** und benennen Sie das Blatt **Gesamtspeicherdiagramme**.

   Stellen Sie sicher, dass das neue Blatt nach den Angaben und Datenblättern angezeigt wird.
10. Name des Diagrammtitels **Gesamt im Vergleich zur verfügbaren Kapazität**.
11. Mit den Menüs **Design** und **Format**, die verfügbar sind, wenn das Diagramm ausgewählt ist, können Sie

das Aussehen des Diagramms anpassen.

12. Wenn Sie zufrieden sind, speichern Sie die Datei mit Ihren Änderungen. Ändern Sie nicht den Dateinamen oder den Speicherort.



13. Wählen Sie in Unified Manager die Option **Berichte** > **Excel hochladen** aus.

> Stellen Sie sicher, dass Sie sich in der gleichen Ansicht befinden, in der Sie die Excel-Datei heruntergeladen haben.

14. Wählen Sie die Excel-Datei aus, die Sie geändert haben.
15. Klicken Sie Auf **Offen**.
16. Klicken Sie Auf **Absenden**.

    Neben dem Menüpunkt **Berichte** > **Excel hochladen** wird ein Häkchen angezeigt.

17. Klicken Sie Auf **Geplante Berichte**.
18. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtspläne** eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.

> Wählen Sie das Format **XLSX** für den Bericht aus.

19. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf Grundlage der im Bericht gezeigten Ergebnisse sollten Sie die Last der Aggregate ausgleichen.

Erstellen eines Berichts, um verfügbare Volume-Kapazitätsdiagramme anzuzeigen

Sie können einen Bericht erstellen, um die verfügbare Volume-Kapazität in einem Excel-Diagramm zu analysieren.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Gehen Sie wie folgt vor, um eine Health-Ansicht zu öffnen: Alle Volumes, laden Sie die Ansicht in Excel herunter, erstellen Sie ein verfügbares Kapazitätdiagramm, laden Sie die benutzerdefinierte Excel-Datei hoch und planen Sie den Abschlussbericht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie **Berichte** > **Excel Herunterladen**.

   Je nach Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.
3. Klicken Sie bei Bedarf auf **Bearbeiten aktivieren**.
4. Öffnen Sie in Excel die heruntergeladene Datei.
5. Wählen Sie auf dem `data` Blatt die Daten aus, die Sie in den Spalten und `Available Data` % verwenden möchten `Volume`.
6. Wählen Sie im Menü **Einfügen** A aus `3-D piechart.`

   Das Diagramm zeigt, welche Volumen den größten verfügbaren Platz haben. Das Diagramm wird auf dem Datenblatt angezeigt.

   Je nach Netzwerkkonfiguration kann die Auswahl der gesamten Spalten oder zu vielen Datenzeilen das Kreisdiagramm unlesbar machen. Dieses Beispiel verwendet das 3-D-Kreisdiagramm, aber Sie können jeden Diagrammtyp verwenden. Verwenden Sie das Diagramm, in dem die zu verwendenden Daten am besten angezeigt werden.
7. Name des Diagrammtitels **verfügbare Kapazität**.
8. Klicken Sie mit der rechten Maustaste auf das Diagramm und wählen Sie **Diagramm verschieben**.
9. Wählen Sie **Neues Blatt** und benennen Sie das Blatt **Speichervolumendiagramme**.

   Stellen Sie sicher, dass das neue Blatt nach den Angaben und Datenblättern angezeigt wird.
10. Mit den Menüs **Design** und **Format**, die verfügbar sind, wenn das Diagramm ausgewählt ist, können Sie das Aussehen des Diagramms anpassen.
11. Wenn Sie zufrieden sind, speichern Sie die Datei mit Ihren Änderungen.
12. Wählen Sie in Unified Manager die Option **Berichte** > **Excel hochladen** aus.

    Stellen Sie sicher, dass Sie sich in der gleichen Ansicht befinden, in der Sie die Excel-Datei heruntergeladen haben.

13. Wählen Sie die Excel-Datei aus, die Sie geändert haben.
14. Klicken Sie Auf **Offen**.
15. Klicken Sie Auf **Absenden**.

    Neben dem Menüpunkt **Berichte** > **Excel hochladen** wird ein Häkchen angezeigt.

16. Klicken Sie Auf **Geplante Berichte**.
17. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtspläne** eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
18. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Wählen Sie das Format **XLSX** für den Bericht aus.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf Grundlage der im Bericht gezeigten Ergebnisse sollten Sie die Last auf den Volumes ausgleichen.

Erstellung eines Berichts, um Aggregate mit den meisten verfügbaren IOPS anzuzeigen

Dieser Bericht zeigt, welche Aggregate die meisten verfügbaren IOPS pro Aggregattyp haben, auf dem Sie neue Workloads bereitstellen können.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Gehen Sie wie folgt vor, um eine Health-Ansicht zu öffnen: Alle Volumes, laden Sie die Ansicht in Excel herunter, erstellen Sie ein verfügbares Kapazitätdiagramm, laden Sie die benutzerdefinierte Excel-Datei hoch und planen Sie den Abschlussbericht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Aggregate**.
2. Wählen Sie aus dem Dropdown-Menü **Ansicht** die Option **Performance: Alle Aggregate** aus.
3. Wählen Sie **ein-/Ausblenden**, um die Spalte ein `Available IOPS- Threshold Policy` und auszublenden `Cluster FQDN, Inactive Data Reporting,`.
4. Ziehen Sie die Spalten und `Free Capacity` neben die `Available IOPS` Spalte `Type`.
5. Benennen und speichern Sie die benutzerdefinierte Ansicht `Available IOPS Per Aggr.`
6. Wählen Sie **Berichte** > **Excel Herunterladen**.

    Je nach Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.

7. Klicken Sie bei Bedarf auf **Bearbeiten aktivieren**.
8. Öffnen Sie in Excel die heruntergeladene Datei.

9. Klicken Sie auf dem Datenblatt oben links auf das kleine Dreieck, um das gesamte Blatt auszuwählen.
10. Wählen Sie auf dem Menüband **Data** aus dem die Option **Sortieren** aus `Sort & Filter area.`
11. Legen Sie die folgenden Sortierstufen fest:
    a. Geben Sie die Werte **Sortieren nach** als (IOPS), **Sortieren nach** **`Available IOPS`** als und **Reihenfolge** `Cell Values,` als an `Largest to Smallest.`
    b. Klicken Sie Auf **Stufe Hinzufügen**.
    c. Geben Sie die **Sortieren nach** als, die **Sortieren nach** **`Type`** als `Cell Values,` und die **Reihenfolge** als an `Z to A.`
    d. Klicken Sie Auf **Stufe Hinzufügen**.
    e. Geben Sie die Option **Sortieren nach** als **Sortieren nach** und die Option **Reihenfolge** `Cell Values,` als `Free Capacity (GB),` an `Largest to Smallest.`
    f. Klicken Sie auf **OK**.
12. Speichern und schließen Sie die Excel-Datei.
13. Wählen Sie in Unified Manager die Option **Berichte** > **Excel hochladen** aus.

    Stellen Sie sicher, dass Sie sich in der gleichen Ansicht befinden, in der Sie die Excel-Datei heruntergeladen haben.

14. Wählen Sie in diesem Fall die Excel-Datei aus, die Sie geändert haben `performance-aggregates-<date>.xlsx.`
15. Klicken Sie Auf **Offen**.
16. Klicken Sie Auf **Absenden**.

    Neben dem Menüpunkt **Berichte** > **Excel hochladen** wird ein Häkchen angezeigt.

17. Klicken Sie Auf **Geplante Berichte**.
18. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite Berichtspläne eine neue Zeile hinzuzufügen, damit Sie die Terminplaneigenschaften für den neuen Bericht definieren können.
19. Geben Sie einen Namen für den Berichtsplan ein, füllen Sie die anderen Berichtsfelder aus, und klicken Sie am Ende der Zeile auf das Häkchen (✓).

    Wählen Sie das Format **XLSX** für den Bericht aus.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und per E-Mail an die Empfänger gesendet, die unter der angegebenen Häufigkeit aufgeführt sind.

Auf der Grundlage der im Bericht gezeigten Ergebnisse sollten Sie möglicherweise neue Workloads auf den Aggregaten bereitstellen, die über die höchsten verfügbaren IOPS verfügen.

Management von Storage über REST-APIs

Erste Schritte mit Active IQ Unified Manager REST APIs

Active IQ Unified Manager stellt einen Satz von APIs bereit, um Ihre Storage-Ressourcen auf den unterstützten Storage-Systemen über eine RESTful Web Service-Schnittstelle für eine beliebige Integration von Lösungen anderer Hersteller zu managen.

In diesen Themen finden Sie Informationen zu Unified Manager APIs, Beispiele für Workflows zur Behebung bestimmter Probleme sowie einige Beispielcodes. Anhand dieser Informationen können Sie RESTful Clients von NetApp Manageability Software-Lösungen für das Management von NetApp Systemen erstellen. Die APIs basieren auf dem Rest-Architekturstil (Representational State Transfer). Alle vier REST-Vorgänge Erstellen, Lesen, Aktualisieren und Löschen (auch CRUD genannt) werden unterstützt.

Unter finden "Active IQ Unified Manager" Sie weitere Ressourcen und Details zu den Vorteilen der Active IQ Unified Manager REST-API.

Zielgruppe für diesen Inhalt

Die folgenden Themen sind für Entwickler bestimmt, die Applikationen erstellen, die über REST-APIs mit der Active IQ Unified Manager Software interface sind.

Storage-Administratoren und -Architekten. Diese Informationen bieten grundlegende Informationen dazu, wie die Unified Manager REST APIs verwendet werden können, um Client-Applikationen zum Managen und Überwachen von NetApp Storage-Systemen zu erstellen.

Sie sollten diese Informationen verwenden, wenn Sie den Storage-Provider, den ONTAP Cluster und Management-Administrations-APIs für das Management Ihres Storage verwenden möchten.

> Sie müssen eine der folgenden Rollen haben: Operator, Storage Administrator oder Application Administrator. Sie müssen die IP-Adresse oder den vollqualifizierten Domänennamen des Unified Manager Servers kennen, auf dem Sie die REST APIs ausführen möchten.

Active IQ Unified Manager API-Zugriff und Kategorien

Die Active IQ Unified Manager APIs ermöglichen Ihnen das Management und die Bereitstellung von Storage-Objekten in Ihrer Umgebung. Sie können auch auf die Web-Benutzeroberfläche von Unified Manager zugreifen, um einige dieser Funktionen auszuführen.

Bauen einer URL für den direkten Zugriff AUF REST-APIs

Sie können die REST-APIs direkt über eine Programmiersprache wie Python, C#, C++, JavaScript, Und so weiter. Geben Sie den Hostnamen oder die IP-Adresse und die URL ein, um auf DIE REST-APIs im Format zuzugreifen

https://<hostname>/API

> Der Standardport ist 443. Sie können den Port wie für Ihre Umgebung erforderlich konfigurieren.

Zugriff auf die Online-API-Dokumentationsseite

Sie können auf die Seite *API Documentation* Referenzinhalt zugreifen, die zusammen mit dem Produkt verpackt ist, um die API-Dokumentation anzuzeigen, sowie manuell einen API-Aufruf (z. B. Swagger) auszuführen. Sie können diese Dokumentation über das Klicken auf die **Menüleiste** > **Hilfe-Schaltfläche** > **API-Dokumentation** aufrufen

Alternativ geben Sie den Hostnamen oder die IP-Adresse und die URL ein, um auf die REST-API-Seite im Format zuzugreifen

https://<hostname>/docs/API/

Kategorien

Die API-Aufrufe werden basierend auf den Bereichen oder Kategorien in funktionale Funktionen organisiert. Um eine bestimmte API zu finden, klicken Sie auf die entsprechende API-Kategorie.

DIE REST-APIs von Unified Manager helfen Ihnen bei der Durchführung von Administrations-, Monitoring- und Provisionierungsfunktionen. Die APIs sind in die folgenden Kategorien unterteilt.

- **Rechenzentrum**

  Diese Kategorie enthält die APIs, die Sie bei Datacenter-Storage-Management und -Analyse mit Tools wie Work Flow Automation und Ansible unterstützen. Die REST-APIs aus dieser Kategorie liefern Informationen über die Cluster, Nodes, Aggregate, Volumes, LUNs. File Shares, Namespaces und andere Elemente im Datacenter.

- * Management-Server*

  Die APIs unter der Kategorie **Management-Server** enthalten die `jobs, system,` APIs und `events`. Aufträge sind Vorgänge, die für die asynchrone Ausführung im Zusammenhang mit dem Management von Storage-Objekten oder Workloads auf Unified Manager geplant werden. Die `events` API gibt Ereignisse in Ihrem Rechenzentrum zurück, und die `system` API gibt die Details der Unified Manager-Instanz zurück.

- * Storage-Anbieter*

  Diese Kategorie enthält alle Bereitstellungs-APIs, die Sie für das Management und die Bereitstellung von File Shares, LUNs, Performance Service Levels und Richtlinien zur Storage-Effizienz benötigen. Die APIs ermöglichen außerdem die Konfiguration von Zugriffendpunkten, aktiven Verzeichnissen sowie die Zuweisung von Performance-Service-Leveln und Storage-Effizienzrichtlinien für Storage-Workloads.

- * Verwaltung*

  Diese Kategorie enthält die APIs, die für die Ausführung von Administrationsaufgaben verwendet werden, z. B. zum Verwalten von Backup-Einstellungen, zum Anzeigen von Vertrauenswürdigkeit-Speicherzertifikaten für die Daten von Unified Manager und zum Verwalten von ONTAP-Clustern als Datenquellen für Unified Manager.

- * Gateway*

  Mit Unified Manager können ONTAP REST-APIs über die APIs der Kategorie Gateway genutzt und die Storage-Objekte im Datacenter gemanagt werden.

- **Sicherheit**

Diese Kategorie enthält APIs zum Verwalten von Unified Manager Benutzern.

REST-Services in Active IQ Unified Manager angeboten

Vor der Verwendung der Active IQ Unified Manager-APIs sollten Sie sich über DIE REST-Services und -Vorgänge im Klaren sein, die angeboten werden.

Die Bereitstellungs- und Administrations-APIs, die für die Konfiguration des API-Servers verwendet werden, unterstützen die Vorgänge beim Lesen (ABRUFEN) oder Schreiben (POST, PATCH, LÖSCHEN). Im Folgenden sind einige Beispiele für GET-, PATCH-, POST- und LÖSCHVORGÄNGE aufgeführt, die von den APIs unterstützt werden:

- Beispiel für GET: `GET /datacenter/cluster/clusters` Ruft Clusterdetails in Ihrem Rechenzentrum ab. Die maximale Anzahl von Datensätzen, die durch den Vorgang zurückgegeben werden `GET`, beträgt 1000.

  Mithilfe der APIs können Sie die Datensätze nach unterstützten Attributen filtern, sortieren und sortieren.

- Beispiel für den POST-Test: `POST /datacenter/svm/svms` Erstellt eine benutzerdefinierte Storage Virtual Machine (SVM).
- Beispiel für EINEN PATCH: `PATCH /datacenter/svm/svms/{key}` Ändert die Eigenschaften einer SVM mithilfe des eindeutigen Schlüssels.
- Beispiel für DAS LÖSCHEN: `DELETE /storage-provider/access-endpoints/{key}` Löscht einen Zugriffs-Endpunkt aus einer LUN, SVM oder Dateifreigabe mithilfe des eindeutigen Schlüssels.

DIE REST-Vorgänge, die mit den APIs ausgeführt werden können, hängen von der Rolle des Operators, des Storage-Administrators oder des Applikationsadministrators ab.

Benutzerrolle	Unterstützte REST-Methode
Operator	Schreibgeschützter Zugriff auf Daten. Benutzer mit dieser Rolle können alle GET-Anforderungen ausführen.
Storage-Administrator	Lesezugriff auf alle Daten. Benutzer mit dieser Rolle können alle GET-Anforderungen ausführen. Zudem verfügen sie über Schreibzugriff (zur Ausführung VON ANFRAGEN ZU PATCHES und NACH DEM POSTEN und LÖSCHEN), um bestimmte Aktivitäten wie das Management von Storage-Serviceobjekten und Storage-Management-Optionen durchzuführen.
Applikationsadministrator	Lese- und Schreibzugriff auf alle Daten Benutzer mit dieser Rolle können Anfragen FÜR alle Funktionen ABRUFEN, PATCHEN, VERÖFFENTLICHEN und LÖSCHEN.

Weitere Informationen zu allen REST-Vorgängen finden Sie in der Dokumentation_Online API_.

API-Version in Active IQ Unified Manager

DIE REST-API-URIs in Active IQ Unified Manager geben eine Versionsnummer an. Die Versionsnummer `v2` in `/v2/datacenter/svm/svms` gibt beispielsweise `/v2/datacenter/svm/svms.` die API-Version an, die in einem bestimmten Release verwendet wird. Die Versionsnummer minimiert die Auswirkungen von API-Änderungen auf die Client-Software durch das Senden einer Antwort, die der Client verarbeiten kann.

Der numerische Teil dieser Versionsnummer ist in Bezug auf Releases inkrementell. URIs mit einer Versionsnummer bieten eine konsistente Schnittstelle, die die Abwärtskompatibilität in zukünftigen Versionen beibehalten. Sie finden auch die gleichen APIs ohne eine Version, zum Beispiel, `/datacenter/svm/svms`, die die Basis-APIs ohne eine Version angeben. Die Basis-APIs sind immer die neueste Version der APIs.

> In der rechten oberen Ecke der Swagger-Schnittstelle können Sie die Version der zu verwendenden API auswählen. Die höchste Version ist standardmäßig ausgewählt. Es wird empfohlen, die höchste Version einer bestimmten API (im Hinblick auf die inkrementelle Ganzzahl) zu verwenden, die in der Unified Manager-Instanz verfügbar ist.

Für alle Anforderungen müssen Sie explizit die API-Version anfordern, die Sie verwenden möchten. Wenn die Versionsnummer angegeben ist, gibt der Dienst keine Antwortelemente zurück, die von Ihrer Anwendung nicht behandelt werden sollen. IM RUHEZUSTAND sollten Sie den Versionsparameter enthalten. Die früheren Versionen der APIs sind schließlich nach ein paar Releases veraltet. In dieser Version ist die `v1` Version der APIs veraltet.

Storage-Ressourcen in ONTAP

Die Storage-Ressourcen in ONTAP können grob in *physische Storage-Ressourcen* und *logische Storage-Ressourcen eingeteilt werden.* um Ihre ONTAP Systeme mit den in Active IQ Unified Manager zur Verfügung gestellten APIs effizient zu managen, müssen Sie das Storage-Ressourcenmodell und die Beziehung zwischen den verschiedenen Storage-Ressourcen kennen.

- **Physische Speicherressourcen**

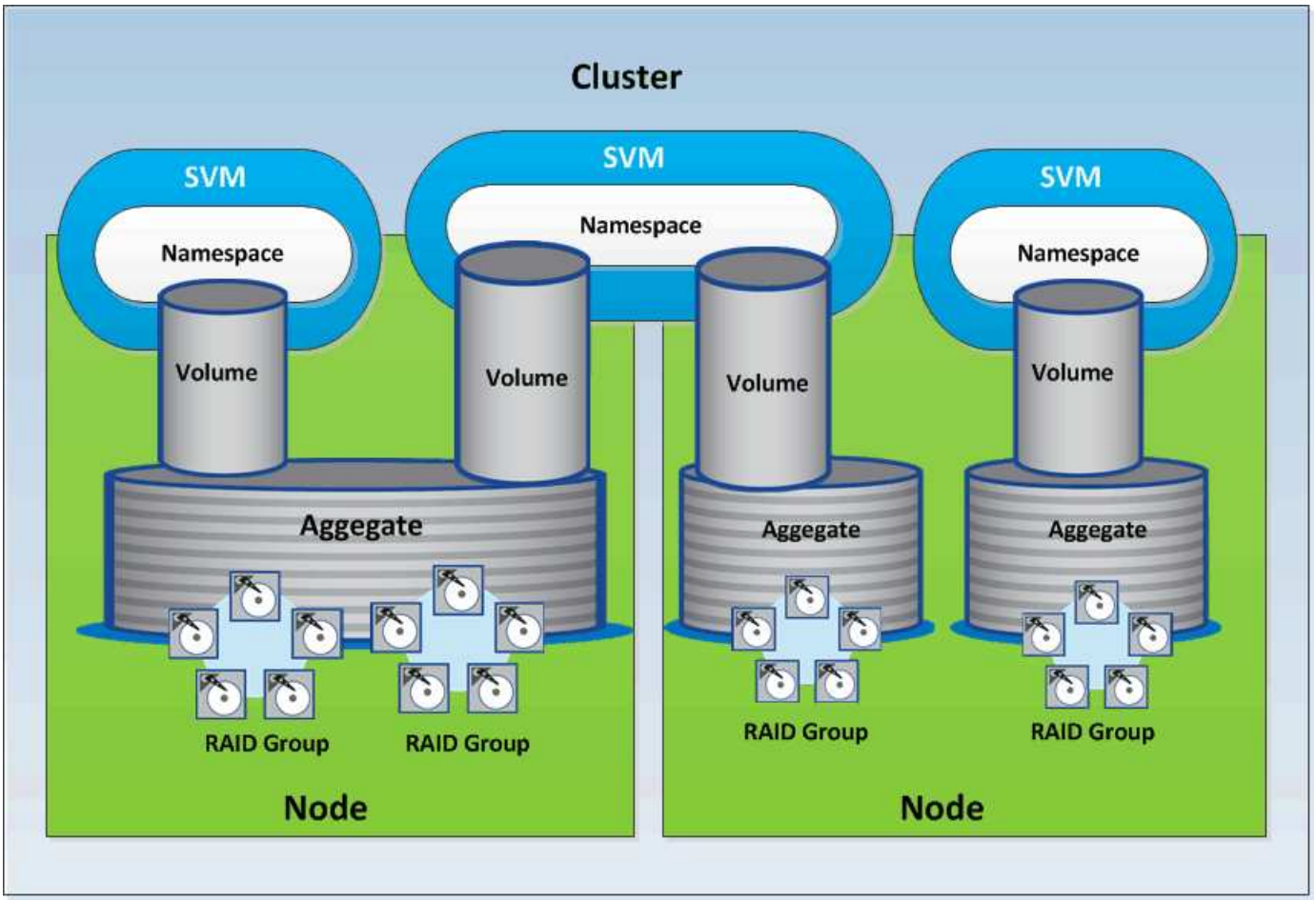
  Bezieht sich auf die von ONTAP zur Verfügung gestellten physischen Speicherobjekte. Physische Storage-Ressourcen umfassen Festplatten, Cluster, Storage Controller, Nodes und Aggregate.

- **Logische Speicherressourcen**

  Bezieht sich auf die von ONTAP bereitgestellten Storage-Ressourcen, die nicht an eine physische Ressource gebunden sind. Diese Ressourcen werden einer Storage Virtual Machine (SVM, ehemals Vserver) zugewiesen. Sie stehen unabhängig von spezifischen physischen Storage-Ressourcen wie Festplatten, Array-LUNs oder Aggregaten zur Verfügung.

  Zu den logischen Storage-Ressourcen zählen Volumes aller Typen und qtrees sowie die Funktionen und Konfigurationen, die in diesen Ressourcen verwendet werden können, beispielsweise Snapshot Kopien, Deduplizierung, Komprimierung und Kontingente.

Die folgende Abbildung zeigt die Storage-Ressourcen in einem 2-Node Cluster:



REST-API-Zugriff und Authentifizierung in Active IQ Unified Manager

Auf die Active IQ Unified Manager REST API kann über jeden REST-Client oder jede Programmierplattform zugegriffen werden, die HTTP-Anfragen mit einem grundlegenden HTTP-Authentifizierungsmechanismus ausgeben kann.

Beispielanfrage und -Antwort:

- **Anfrage**

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

- **Antwort**

```
{
  "records": [
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
```

```
00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "name": "fas8040-206-21",
      "uuid": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "contact": null,
      "location": null,
      "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33
UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
      },
      "isSanOptimized": false,
      "management_ip": "10.226.207.25",
      "nodes": [
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb",
          "uuid": "12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
          "name": "fas8040-206-21-01",
          "_links": {
            "self": {
              "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb"
            }
          },
          "location": null,
          "version": {
            "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
            "generation": 9,
            "major": 5,
            "minor": 0
          },
          "model": "FAS8040",
          "uptime": 13924095,
          "serial_number": "701424000157"
        },
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7",
          "uuid": "1ed606ed-2e3a-11e9-a270-00a0985bb9b7",
          "name": "fas8040-206-21-02",
```

```
          "_links": {
            "self": {
              "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7"
            }
          },
          "location": null,
          "version": {
            "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
            "generation": 9,
            "major": 5,
            "minor": 0
          },
          "model": "FAS8040",
          "uptime": 14012386,
          "serial_number": "701424000564"
        }
      ],
      "_links": {
        "self": {
          "href": "/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-
00a0985badbb"
        }
      }
    },
```

- *IP address/hostname* Ist die IP-Adresse oder der vollständig qualifizierte Domänenname (FQDN) des API-Servers.
- Anschluss 443

  Der Standard-HTTPS-Port 443 ist. Sie können den HTTPS-Port bei Bedarf anpassen.

Um HTTP-Anfragen von einem Webbrowser zu stellen, müssen Sie REST API Browser-Plugins verwenden. Sie können auch über Skripting-Plattformen wie Curl und Perl auf DIE REST-API zugreifen.

Authentifizierung

Unified Manager unterstützt das grundlegende HTTP-Authentifizierungsschema für APIs. Für einen sicheren Informationsfluss (Anfrage und Antwort) sind die REST-APIs nur über HTTPS zugänglich. Der API-Server stellt allen Clients ein selbstsigniertes SSL-Zertifikat zur Server-Überprüfung zur Verfügung. Dieses Zertifikat kann durch ein benutzerdefiniertes Zertifikat (oder ein CA-Zertifikat) ersetzt werden.

Sie müssen den Benutzerzugriff auf den API-Server konfigurieren, um die REST-APIs zu aufrufen. Die Benutzer können lokale Benutzer (Benutzerprofile, die in der lokalen Datenbank gespeichert sind) oder LDAP-Benutzer (wenn Sie den API-Server für die Authentifizierung über LDAP konfiguriert haben) sein. Sie können

den Benutzerzugriff verwalten, indem Sie sich an der Benutzeroberfläche der Unified Manager Administration Console anmelden.

In Active IQ Unified Manager verwendete HTTP-Statuscodes

Bei Ausführung der APIs oder bei der Fehlerbehebung sollten Sie die verschiedenen HTTP-Statuscodes und -Fehlercodes kennen, die von Active IQ Unified Manager-APIs verwendet werden.

In der folgenden Tabelle sind die Fehlercodes für die Authentifizierung aufgeführt:

HTTP-Statuscode	Titel des Statuscodes	Beschreibung
200	OK	Wird bei der erfolgreichen Ausführung von synchronen API-Aufrufen zurückgegeben.
201	Erstellt	Erstellung neuer Ressourcen durch synchrone Anrufe, wie z. B. Konfiguration von Active Directory.
202	Akzeptiert	Wird bei der erfolgreichen Ausführung von asynchronen Aufrufen für Bereitstellungsfunktionen zurückgegeben, z. B. Erstellen von LUNs und File Shares.
400	Ungültige Anforderung	Zeigt Fehler bei der Eingabevalidierung an. Der Benutzer muss die Eingaben korrigieren, z. B. gültige Schlüssel in einem Anforderungskörper.
401	Nicht autorisierte Anforderung	Sie sind nicht berechtigt, die Ressource/Unbefugte anzuzeigen.
403	Anfrage verweigert	Der Zugriff auf die Ressource, die Sie erreichen wollten, ist verboten.
404	Ressource nicht gefunden	Die Ressource, die Sie erreichen wollten, wurde nicht gefunden.
405	Methode Nicht Zulässig	Methode nicht zulässig.
429	Zu Viele Anfragen	Dieser Wert wird zurückgegeben, wenn der Benutzer zu viele Anfragen innerhalb eines bestimmten Zeitraums sendet.

HTTP-Statuscode	Titel des Statuscodes	Beschreibung
500	Interner Serverfehler	Interner Serverfehler. Fehler beim Abrufen der Antwort vom Server. Dieser interne Serverfehler ist möglicherweise permanent oder nicht permanent. Wenn Sie beispielsweise einen oder- `GET ALL`Vorgang ausführen `GET` und diesen Fehler erhalten, wird empfohlen, diesen Vorgang mindestens fünf Wiederholungen zu wiederholen. Wenn es sich um einen permanenten Fehler handelt, ist der zurückgegebene Statuscode weiterhin 500. Wenn der Vorgang erfolgreich ist, wird der zurückgegebene Statuscode 200 zurückgegeben.

Empfehlungen für die Verwendung der APIs für Active IQ Unified Manager

Bei Verwendung der APIs in Active IQ Unified Manager sollten Sie bestimmte empfohlene Methoden befolgen.

- Alle Arten von Antwortinhalten müssen für eine gültige Ausführung das folgende Format aufweisen:

```
application/json
```

- Die API-Versionsnummer steht nicht zur Produktversionsnummer. Sie sollten die neueste Version der für Ihre Unified Manager Instanz verfügbaren API verwenden. Weitere Informationen zu den Unified Manager API-Versionen finden Sie im Abschnitt „`reST API Versionierung in Active IQ Unified Manager`“.
- Beim Aktualisieren der Array-Werte mithilfe einer Unified Manager API müssen Sie die gesamte Zeichenfolge von Werten aktualisieren. Sie können einem Array keine Werte anhängen. Sie können nur ein vorhandenes Array ersetzen.
- Filteroperatoren wie Pipe („) und Wild Card (*) können für alle Abfrageparameter verwendet werden, mit Ausnahme von doppelten Werten, z. B. IOPS und Performance in den Kennzahlen-APIs.
- Vermeiden Sie das Abfragen von Objekten, indem Sie eine Kombination aus Wildcard (*) und Rohr () des Filterbedieners verwenden. Es kann eine falsche Anzahl von Objekten abrufen.
- Wenn Sie Werte für Filter verwenden, stellen Sie sicher, dass der Wert kein Zeichen enthält `?`. Dies soll die Risiken der SQL-Injektion mindern.
- Beachten Sie, dass die `GET` (alle)-Anforderung für eine beliebige API maximal 1000 Datensätze zurückgibt. Selbst wenn Sie die Abfrage durch Setzen des Parameters auf einen Wert über 1000 ausführen `max_records`, werden nur 1000 Datensätze zurückgegeben.
- Für administrative Aufgaben wird empfohlen, die Unified Manager-Benutzeroberfläche zu verwenden.

Protokolle für die Fehlerbehebung

Mithilfe von Systemprotokollen können Sie die Ursachen eines Ausfalls und die Behebung von Problemen analysieren, die bei der Ausführung der APIs auftreten können.

Rufen Sie die Protokolle vom folgenden Speicherort ab, um Probleme im Zusammenhang mit den API-Aufrufen zu beheben.

Speicherort protokollieren	Nutzung
`/var/log/ocie/access_log.log`	Enthält alle API-Anrufdetails, z. B. den Benutzernamen des Benutzers, der die API aufruft, Startzeit, Ausführungszeit, Status und URL. In dieser Protokolldatei können Sie die häufig verwendeten APIs überprüfen oder einen Fehler in jedem GUI-Workflow beheben. Sie können die Analyse auch anhand der Ausführungszeit skalieren.
`/var/log/ocum/ocumserver.log`	Enthält alle API-Ausführungsprotokolle. Sie können diese Protokolldatei zur Fehlerbehebung und Fehlersuche bei API-Aufrufen verwenden.
`/var/log/ocie/server.log`	Enthält alle WildFly-Server-Bereitstellungen und Start/Stop-Service-bezogene Protokolle. Sie können diese Protokolldatei verwenden, um die Ursache von Problemen zu finden, die während des Starts, Stoppens oder der Bereitstellung des WildFly-Servers auftreten.
`/var/log/ocie/au.log`	Enthält Protokolle für die Erfassungseinheit. Sie können diese Protokolldatei verwenden, wenn Sie Objekte in ONTAP erstellt, geändert oder gelöscht haben, sie sich jedoch nicht für die Active IQ Unified Manager REST-APIs wiederspiegeln.

Auftragsobjekte asynchrone Prozesse

Active IQ Unified Manager stellt die API bereit `jobs`, die Informationen über die Jobs abruft, die während der Ausführung anderer APIs ausgeführt werden. Sie müssen wissen, wie die asynchrone Verarbeitung mit dem Job-Objekt funktioniert.

Einige der API-Aufrufe, insbesondere solche, die zum Hinzufügen oder Ändern von Ressourcen verwendet werden, können länger dauern als andere Anrufe. Unified Manager verarbeitet diese langfristigen Anforderungen asynchron.

Asynchrone Anforderungen, die mit Job Object beschrieben werden

Nach einem API-Aufruf, der asynchron ausgeführt wird, weist der HTTP-Antwortcode 202 darauf hin, dass die Anforderung erfolgreich validiert und akzeptiert, aber noch nicht abgeschlossen wurde. Die Anforderung wird als Hintergrundaufgabe verarbeitet, die nach der ersten HTTP-Antwort auf den Client weiter ausgeführt wird. Die Antwort umfasst das Job-Objekt, das die Anfrage einschließlich der eindeutigen Kennung anverankert.

Abfragen des mit einer API-Anforderung verknüpften Jobobjekts

Das in der HTTP-Antwort zurückgegebene Job-Objekt enthält mehrere Eigenschaften. Sie können die Statuseigenschaft abfragen, um festzustellen, ob die Anfrage erfolgreich abgeschlossen wurde. Ein Job-Objekt kann einen der folgenden Status haben:

- `NORMAL`
- `WARNING`
- `PARTIAL_FAILURES`
- `ERROR`

Es gibt zwei Verfahren, die Sie beim Abfragen eines Jobobjekts verwenden können, um einen Terminalstatus für die Aufgabe zu erkennen: Erfolg oder Fehler:

- Standard-Abfrage: Der aktuelle Job-Status wird sofort zurückgegeben.
- Lange Abfrage: Wenn der Jobstatus in oder `PARTIAL_FAILURES`. verschoben wird `NORMAL, ERROR,`

Schritte in einer asynchronen Anforderung

Sie können den folgenden grundlegenden Vorgang verwenden, um einen asynchronen API-Aufruf abzuschließen:

1. Geben Sie den asynchronen API-Aufruf aus.
2. Sie erhalten eine HTTP-Antwort 202, die darauf hinweist, dass die Anfrage erfolgreich angenommen wurde.
3. Extrahieren Sie die Kennung für das Job-Objekt aus dem Antwortkörper.
4. Warten Sie innerhalb einer Schleife, bis das Objekt Job den Terminalstatus oder `PARTIAL_FAILURES`. erreicht hat `NORMAL, ERROR,`
5. Überprüfen Sie den Terminalstatus des Jobs, und rufen Sie das Jobergebnis ab.

Hallo API Server

Der *Hello API-Server* ist ein Beispielprogramm, das zeigt, wie eine REST-API in Active IQ Unified Manager mit einem einfachen REST-Client aufgerufen wird. Das Beispielprogramm enthält grundlegende Details zum API-Server im JSON-Format (der Server unterstützt nur das `application/json` Format).

Der verwendete URI ist: `https://<hostname>/api/datacenter/svm/svms`. Dieser Beispielcode nimmt die folgenden Eingabeparameter ein:

- Die IP-Adresse oder FQDN des API-Servers

- Optional: Portnummer (Standard: 443)
- Benutzername
- Passwort
- Antwortformat (`application/json`)

Um REST-APIs aufzurufen, können Sie auch andere Skripte wie Jersey und RESTEasy verwenden, um einen Java REST-Client für Active IQ Unified Manager zu schreiben. Beachten Sie die folgenden Überlegungen zum Beispielcode:

- Verwendet eine HTTPS-Verbindung zu Active IQ Unified Manager, um den angegebenen REST-URI aufzurufen
- Ignoriert das von Active IQ Unified Manager bereitgestellte Zertifikat
- Überspringt die Überprüfung des Host-Namens während des Handshakes
- Verwendet `javax.net.ssl.HttpsURLConnection` für eine URI-Verbindung
- Verwendet eine Bibliothek eines Drittanbieters (`org.apache.commons.codec.binary.Base64`) zum Erstellen des Base64-kodierten Strings, der in der HTTP-Basisauthentifizierung verwendet wird

Um den Beispielcode kompilieren und ausführen zu können, müssen Sie Java Compiler 1.8 oder höher verwenden.

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpsURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import org.apache.commons.codec.binary.Base64;

public class HelloApiServer {

    private static String server;
    private static String user;
    private static String password;
    private static String response_format = "json";
    private static String server_url;
    private static String port = null;

    /*
     * * The main method which takes user inputs and performs the *
necessary steps
     * to invoke the REST URI and show the response
```

```
     */ public static void main(String[] args) {
        if (args.length < 2 || args.length > 3) {
            printUsage();
            System.exit(1);
        }
        setUserArguments(args);
        String serverBaseUrl = "https://" + server;
        if (null != port) {
            serverBaseUrl = serverBaseUrl + ":" + port;
        }
        server_url = serverBaseUrl + "/api/datacenter/svm/svms";
        try {
            HttpsURLConnection connection =
getAllTrustingHttpsUrlConnection();
            if (connection == null) {
                System.err.println("FATAL: Failed to create HTTPS
connection to URL: " + server_url);
                System.exit(1);
            }
            System.out.println("Invoking API: " + server_url);
            connection.setRequestMethod("GET");
            connection.setRequestProperty("Accept", "application/" +
response_format);
            String authString = getAuthorizationString();
            connection.setRequestProperty("Authorization", "Basic " +
authString);
            if (connection.getResponseCode() != 200) {
                System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
                        + connection.getResponseMessage());
                System.exit(1);
            }
            BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
            String response;
            System.out.println("Response:");
            while ((response = br.readLine()) != null) {
                System.out.println(response);
            }
            connection.disconnect();
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    /* Print the usage of this sample code */ private static void
```

```
printUsage() {
        System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
        System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
        System.out.println("\tHelloApiServer 10.22.12.34:8320 admin
password");
        System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
        System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
        System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
    }

    /* * Set the server, port, username and password * based on user
inputs. */ private static void setUserArguments(
            String[] args) {
        server = args[0];
        user = args[1];
        password = args[2];
        if (server.contains(":")) {
            String[] parts = server.split(":");
            server = parts[0];
            port = parts[1];
        }
    }

    /*
     * * Create a trust manager which accepts all certificates and * use
this trust
     * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
     * SSL Context and skip * server hostname verification during SSL
handshake. * *
     * Note: Trusting all certificates or skipping hostname verification *
is not
     * required for API Services to work. These are done here to * keep
this sample
     * REST Client code as simple as possible.
     */ private static HttpsURLConnection
getAllTrustingHttpsUrlConnection()    {        HttpsURLConnection conn =
null;        try {            /* Creating a trust manager that does not
validate certificate chains */            TrustManager[]
trustAllCertificatesManager = new                    TrustManager[]{new
X509TrustManager(){
```

```
     public X509Certificate[] getAcceptedIssuers(){return  null;}
     public void checkClientTrusted(X509Certificate[]
certs, String authType){}
     public void checkServerTrusted(X509Certificate[]
certs, String authType){}            }};            /* Initialize the
SSLContext with the all-trusting trust manager */
     SSLContext sslContext = SSLContext.getInstance("TLS");
sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
HttpsURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));            URL url = new URL(server_url);            conn =
(HttpsURLConnection) url.openConnection();           /* Do not perform an
actual hostname verification during SSL Handshake.            Let all
hostname pass through as verified.*/
conn.setHostnameVerifier(new HostnameVerifier() {               public
boolean verify(String host, SSLSession                        session) {
return true;               }           });        } catch (Exception e)
{            e.printStackTrace();        }        return conn;    }

    /*
     * * This forms the Base64 encoded string using the username and
password *
     * provided by the user. This is required for HTTP Basic
Authentication.
     */ private static String getAuthorizationString() {
        String userPassword = user + ":" + password;
        byte[] authEncodedBytes =
Base64.encodeBase64(userPassword.getBytes());
        String authString = new String(authEncodedBytes);
        return authString;
    }

}
```

Unified Manager REST-APIs

DIE REST-APIs für Active IQ Unified Manager sind in diesem Abschnitt basierend auf ihren Kategorien aufgeführt.

Sie können die Online-Dokumentationsseite von Ihrer Unified Manager Instanz aus einsehen, die alle Einzelheiten zu jedem REST-API-Aufruf enthält. Dieses Dokument wiederholt die Details der Online-Dokumentation nicht. Jeder API-Aufruf, der in diesem Dokument aufgeführt oder beschrieben wird, enthält nur die Informationen, die Sie benötigen, um den Anruf auf der Dokumentationsseite zu finden. Nach dem Auffinden eines bestimmten API-Aufrufs können Sie die vollständigen Details dieses Anrufs überprüfen, einschließlich der Eingabeparameter, Ausgabeformate, HTTP-Statuscodes und der Anforderungstypen.

Für jeden API-Aufruf in einem Workflow sind folgende Informationen enthalten, um den Anruf auf der

Dokumentationsseite zu finden:

- Kategorie

  Die API-Aufrufe werden auf der Dokumentationsseite in funktional bezogene Bereiche oder Kategorien unterteilt. Um einen bestimmten API-Aufruf zu finden, scrollen Sie nach unten auf der Seite und klicken Sie dann auf die entsprechende API-Kategorie.

- HTTP-Verb (Anruf)

  Das HTTP-Verb identifiziert die Aktion, die für eine Ressource durchgeführt wird. Jeder API-Aufruf wird über ein einziges HTTP-Verb ausgeführt.

- Pfad

  Der Pfad bestimmt die spezifische Ressource, die die Aktion als Teil der Durchführung eines Anrufs verwendet. Der Pfadstring wird an die Core-URL angehängt, um die vollständige URL zur Identifizierung der Ressource zu bilden.

Management von Storage-Objekten in einem Datacenter mithilfe von APIs

Mithilfe der REST-APIs unter der `datacenter` Kategorie können Sie die Storage-Objekte in Ihrem Datacenter managen, wie z. B. Cluster, Nodes, Aggregate, Storage-VMs, Volumes, LUNs, Dateifreigaben und Namespaces. Diese APIs sind für das Abfragen der Konfiguration der Objekte verfügbar, während einige von ihnen es Ihnen ermöglichen, diese Objekte hinzuzufügen, zu löschen oder zu ändern.

Die meisten dieser APIs sind GET-Aufrufe, die Cluster-übergreifende Aggregation mit Filter-, Sortier- und Paginierungsunterstützung bieten. Wenn sie diese APIs ausführen, geben sie Daten aus der Datenbank zurück. Daher müssen die neu erstellten Objekte durch den nächsten Erfassungszyklus entdeckt werden, damit sie in der Antwort angezeigt werden.

Wenn Sie die Details eines bestimmten Objekts abfragen möchten, müssen Sie die eindeutige ID dieses Objekts eingeben, um dessen Details anzuzeigen. Informationen zu Metriken und Analyseinformationen der Storage-Objekte finden Sie beispielsweise unter "Anzeigen von Performance-Metriken".

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-
2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

Die CURL-Befehle, Beispiele, Anfragen und Antworten auf die APIs sind auf Ihrer Swagger API-Schnittstelle verfügbar. Sie können die Ergebnisse nach bestimmten Parametern filtern und sortieren, wie auf Swagger angegeben. Diese APIs ermöglichen die Filterung der Ergebnisse nach spezifischen Storage-Objekten wie Cluster, Volume oder Storage VM.

APIs für Storage-Objekte in Ihrem Datacenter

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}	Mit dieser Methode können Sie Details zu den ONTAP Clustern im gesamten Datacenter anzeigen. Die API gibt Informationen zurück, z. B. die IPv4- oder IPv6-Adresse des Clusters, Informationen über den Node, z. B. Systemzustand, Performance-Kapazität und HA-Paar (Hochverfügbarkeit), und gibt an, ob es sich bei dem Cluster um das All-SAN-Array handelt.
GET	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	Gibt die Details der auf den Clustern in Ihrem Rechenzentrum installierten Lizenzen zurück. Sie können Ihre Ergebnisse nach den erforderlichen Kriterien filtern. Informationen wie Lizenzschlüssel, Cluster-Schlüssel, Ablaufdatum und Umfang der Lizenz werden zurückgegeben. Sie können einen Lizenzschlüssel eingeben, um die Details einer bestimmten Lizenz abzurufen.
GET	/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}	Mit dieser Methode können Sie die Details der Nodes im Datacenter anzeigen. Sie können Informationen über das Cluster, den Zustand der Nodes, die Performance-Kapazität und das HA-Paar (Hochverfügbarkeit) für den Node anzeigen.
GET	/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}	Mit dieser Methode können Sie Details zu den CIFS-Freigaben im Datacenter anzeigen. Neben Cluster-, SVM- und Volume-Details werden auch Informationen über Access Control List (ACL) zurückgegeben.

HTTP-Verb	Pfad	Beschreibung

GET	`/datacenter/protocols/nfs/export-policies`
	
	`/datacenter/protocols/nfs/export-policies/{key}`
		Sie können diese Methode verwenden, um die Details der Exportrichtlinien für die unterstützten NFS-Dienste anzuzeigen.
		
		Sie können die Exportrichtlinien für eine Cluster- oder Storage-VM abfragen und den Richtlinienschlüssel für den Export zur Bereitstellung von NFS-Dateifreigaben verwenden. Weitere Informationen über das Zuweisen und erneute Verwenden von Exportrichtlinien für Workloads finden Sie unter „`Provisioning von CIFS- und NFS-Dateifreigaben`“.

GET	`/datacenter/storage/aggregates`
	
	`/datacenter/storage/aggregates/{key}`
		Mit dieser Methode können Sie die Erfassung von Aggregaten im Datacenter oder ein bestimmtes Aggregat für die Bereitstellung von Workloads auf diesen oder das Monitoring anzeigen. Informationen wie Details zu Clustern und Nodes, die genutzte Performance-Kapazität, verfügbarer und genutzter Speicherplatz sowie Storage-Effizienz werden zurückgegeben.

GET	`/datacenter/storage/luns`
	
	`/datacenter/storage/luns/{key}`
		Mit dieser Methode können Sie die Erfassung von LUNs im gesamten Datacenter anzeigen. Hier können Informationen zur LUN angezeigt werden, beispielsweise Angaben zu Cluster und SVM, QoS-Richtlinien und Initiatorgruppen.

GET	`/datacenter/storage/qos/policies`
	
	`/datacenter/storage/qos/policies/{key}`
		Mit dieser Methode können Sie Details zu allen QoS-Richtlinien anzeigen, die für die Storage-Objekte im Datacenter gelten. Informationen wie Details zu Cluster und SVM, Details zu festen oder anpassungsfähigen Richtlinien und die Anzahl der für diese Richtlinie anwendbaren Objekte werden zurückgegeben.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	Mit dieser Methode können Sie die qtree-Details im gesamten Datacenter für alle FlexVol Volumes oder FlexGroup Volumes anzeigen. Informationen wie Details zu Cluster und SVM, FlexVol Volume und Exportrichtlinie werden zurückgegeben.
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	Mit dieser Methode können Sie die Volume-Sammlungen im Datacenter anzeigen. Informationen zu Volumes, wie z. B. Angaben zu SVM und Cluster, QoS und Exportrichtlinien, ob für das Volume Lese-, Datensicherungs- oder Load-Sharing-Typen vorhanden sind, werden zurückgegeben. Für FlexVol und FlexClone Volumes erhalten Sie Informationen zu den jeweiligen Aggregaten. Bei einem FlexGroup Volume liefert die Abfrage die Liste der zusammengehörigen Aggregate zurück.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/protocols/san/igroups`
	
	`/datacenter/protocols/san/igroups/{key}`
		Sie können Initiatorgruppen zuweisen, die für den Zugriff auf bestimmte LUN-Ziele autorisiert sind. Wenn eine vorhandene Initiatorgruppe vorhanden ist, können Sie sie zuweisen. Sie können auch Initiatorgruppen erstellen und sie den LUNs zuweisen.
		
		Sie können diese Methoden zum Abfragen, Erstellen, Löschen und Ändern von Initiatorgruppen verwenden.
		
		Hinweise:
		
		• `POST`: Beim Erstellen einer Initiatorgruppe können Sie die Storage-VM festlegen, auf der Sie Zugriff zuweisen möchten.
		• `DELETE`: Zum Löschen einer bestimmten Initiatorgruppe müssen Sie den igroup-Schlüssel als Eingabeparameter angeben. Wenn Sie einer LUN bereits eine Initiatorgruppe zugewiesen haben, können Sie diese Initiatorgruppe nicht löschen.
		• `PATCH`: Sie müssen den igroup-Schlüssel als Eingabeparameter angeben, um eine bestimmte Initiatorgruppe zu ändern. Sie müssen auch die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/svm/svms`
	
	`/datacenter/svm/svms/{key}`
		Sie können diese Methoden verwenden, um Storage Virtual Machines (Storage VMs) anzuzeigen, zu erstellen, zu löschen und zu ändern.
		
		• `POST`: Sie müssen das Storage-VM-Objekt eingeben, das Sie als Eingabeparameter erstellen möchten. Sie können eine benutzerdefinierte Storage-VM erstellen und anschließend erforderliche Eigenschaften zuweisen.
		• `DELETE`: Sie müssen den Storage-VM-Schlüssel angeben, um eine bestimmte Storage-VM zu löschen.
		• `PATCH`: Sie müssen den Storage-VM-Schlüssel angeben, um eine bestimmte Storage-VM zu ändern. Sie müssen außerdem die Eigenschaften eingeben, die Sie aktualisieren möchten, zusammen mit ihren Werten.

Hinweise:

Wenn Sie die SLO-basierte Workload-Bereitstellung in Ihrer Umgebung aktiviert und gleichzeitig die Storage-VM erstellt haben, müssen Sie sicherstellen, dass alle Protokolle unterstützt werden, die für die Bereitstellung von LUNs und File Shares auf ihnen erforderlich sind, z. B. CIFS oder SMB, NFS, FCP Und iSCSI. Die Bereitstellungs-Workflows können fehlschlagen, wenn die Storage-VM die erforderlichen Services nicht unterstützt. Es wird empfohlen, auf der Storage-VM auch die Services für die jeweiligen Workload-Typen zu aktivieren.

Wenn Sie die SLO-basierte Workload-Bereitstellung in Ihrer Umgebung aktiviert haben, kann diese Storage-VM nicht gelöscht werden, auf der Storage-Workloads bereitgestellt wurden. Wenn Sie eine Speicher-VM löschen, auf der ein CIFS- oder SMB-Server konfiguriert wurde, löscht diese API auch den CIFS- oder SMB-Server sowie die lokale Active Directory-Konfiguration. Der CIFS- oder SMB-Servername befindet sich jedoch weiterhin in der Active Directory-Konfiguration, die Sie manuell vom Active Directory-Server löschen müssen.

APIs für Netzwerkelemente in Ihrem Datacenter

Mit den folgenden APIs in der Datacenter-Kategorie werden Informationen über die Ports und Netzwerkschnittstellen in Ihrer Umgebung abgerufen, insbesondere die FC-Ports, FC-Schnittstellen, ethernet-Ports und IP-Schnittstellen.

HTTP-Verb	Pfad	Beschreibung

GET	`/datacenter/network/ethernet/ports`
	
	`/datacenter/network/ethernet/ports/{key}`
		Informationen zu allen ethernet-Ports in Ihrer Datacenter-Umgebung werden abgerufen. Wenn ein Port-Schlüssel als Eingabeparameter liegt, können Sie die Informationen dieses spezifischen Ports anzeigen. Informationen, z. B. Cluster-Details, Broadcast-Domain, Port-Details, z. B. Status, Geschwindigkeit Und geben Sie ein, und ob der Port aktiviert ist, wird abgerufen.

GET	`/datacenter/network/fc/interfaces`
	
	`/datacenter/network/fc/interfaces/{key}`
		Mit dieser Methode können Sie die Details der FC-Schnittstellen in Ihrer Rechenzentrumsumgebung anzeigen. Wenn ein Schnittstellenschlüssel als Eingabeparameter ist, können Sie die Informationen dieser spezifischen Schnittstelle anzeigen. Informationen wie Cluster-Details, Home Node-Details und Home Port-Details werden abgerufen.

GET	`/datacenter/network/fc/ports`
	
	`/datacenter/network/fc/ports/{key}`
		Informationen zu allen FC-Ports, die in den Nodes in Ihrer Datacenter-Umgebung verwendet werden, werden abgerufen. Wenn ein Port-Schlüssel als Eingabeparameter liegt, können Sie die Informationen dieses spezifischen Ports anzeigen. Informationen, wie z. B. Cluster-Details, Port-Beschreibung, unterstütztes Protokoll und der Status des Ports, werden abgerufen.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	Mit dieser Methode können Sie die Details der IP-Schnittstellen in Ihrer Rechenzentrumsumgebung anzeigen. Wenn ein Schnittstellenschlüssel als Eingabeparameter ist, können Sie die Informationen dieser spezifischen Schnittstelle anzeigen. Informationen wie Cluster-Details, IPspace-Details, Home Node-Details, ob das Failover aktiviert ist, werden abgerufen.

Zugriff auf ONTAP-APIs über Proxy-Zugriff

Die Gateway-APIs bieten den Vorteil, dass Sie die Active IQ Unified Manager-Zugangsdaten verwenden können, um ONTAP REST-APIs und das Management von Storage-Objekten auszuführen. Diese APIs sind verfügbar, wenn die API-Gateway-Funktion über die Web-UI von Unified Manager aktiviert ist.

Unified Manager REST-APIs unterstützen nur einen ausgewählten Satz von Aktionen, die auf den Daten von Unified Manager ausgeführt werden sollen, d. h. ONTAP Cluster. Sie können die anderen Funktionen über ONTAP APIs nutzen. Durch die Gateway-APIs ist Unified Manager eine Pass-Through-Schnittstelle zum Tunneln aller API-Anfragen, die auf dem verwalteten ONTAP-Cluster ausgeführt werden, ohne sich einzeln an die einzelnen Datacenter-Cluster anzumelden. Sie arbeitet als zentraler Managementpunkt bei der Ausführung der APIs auf den ONTAP Clustern, die von Ihrer Unified Manager Instanz gemanagt werden. Dank der API Gateway-Funktion kann Unified Manager als zentrale Managementoberfläche eingerichtet werden, über die Sie diverse ONTAP Cluster managen können, ohne sich dabei individuell anmelden zu müssen. Die Gateway-APIs ermöglichen es Ihnen, bei Unified Manager angemeldet zu bleiben und die ONTAP-Cluster zu managen, indem Sie ONTAP REST-API-Vorgänge ausführen.

Alle Benutzer können eine Abfrage mithilfe der GET-Operation ausführen. Applikationsadministratoren können alle REST-Operationen für ONTAP ausführen.

Das Gateway fungiert als Proxy, um die API-Anforderungen zu Tunneln, indem die Header- und Body-Anfragen im gleichen Format wie in den ONTAP-APIs beibehalten werden. Kunden können ihre Unified Manager Anmeldedaten verwenden und bestimmte Vorgänge ausführen, um ohne die individuellen Cluster-Anmeldedaten zuzugreifen und das Management der ONTAP Cluster durchzuführen. Die Cluster-Authentifizierung und das Cluster-Management werden weiterhin gemanagt, allerdings werden die API-Anfragen umgeleitet, damit sie direkt auf dem spezifischen Cluster ausgeführt werden. Die Antwort der APIs ist die gleiche wie die Antwort, die von den jeweiligen ONTAP REST APIs zurückgegeben wird, die direkt von ONTAP ausgeführt werden.

HTTP-Verb	Pfad (URL)	Beschreibung
GET	/gateways	Diese GET-Methode ruft die Liste aller von Unified Manager verwalteten Cluster ab, die Rest-Aufrufe von ONTAP unterstützen. Sie können die Cluster-Details überprüfen und auswählen, ob andere Methoden auf Basis der Cluster-UUID oder Universal Unique Identifier (UUID) ausgeführt werden sollen. Die Gateway-APIs rufen nur die von ONTAP 9.5 oder höher unterstützten Cluster ab und sind über HTTPS zu Unified Manager hinzugefügt.

HTTP-Verb	Pfad (URL)	Beschreibung

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
 	
`OPTIONS` (Nicht verfügbar bei Swagger)
 	
`HEAD` (Nicht verfügbar bei Swagger)
	`/gateways/{uuid}/{path}`
	
	Der Wert für {UUID} muss durch die Cluster-UUID ersetzt werden, für die der REST-Vorgang ausgeführt wird. Stellen Sie außerdem sicher, dass die UUID des Clusters enthält, das von ONTAP 9.5 oder höher unterstützt und über HTTPS zu Unified Manager hinzugefügt wird. {path} muss durch die ONTAP REST-URL ersetzt werden. Sie müssen aus der URL entfernen `/api/`.
		Dies ist eine Single-Point-Proxy-API, die DEN POST- und LÖSCHVORGANG sowie DEN PATCH-Betrieb und DEN ZUGRIFF auf alle ONTAP REST-APIs unterstützt. Es gelten keine Einschränkungen für die API, sofern sie von ONTAP unterstützt wird. Die Tunneling- oder Proxy-Funktion kann nicht deaktiviert werden.
		
		Die `OPTIONS` Methode gibt alle von einer ONTAP-REST-API unterstützten Vorgänge zurück. Wenn z. B. eine ONTAP-API nur den Vorgang unterstützt `GET`, gibt das Ausführen der `OPTIONS` Methode mithilfe dieser Gateway-API als Antwort zurück `GET`. Diese Methode wird auf Swagger nicht unterstützt, kann aber auf anderen API-Tools ausgeführt werden.
		
		Die `OPTIONS` Methode bestimmt, ob eine Ressource verfügbar ist. Mit diesem Vorgang können die Metadaten zu einer Ressource in den HTTP-Antwortheadern angezeigt werden. Diese Methode wird auf Swagger nicht unterstützt, kann aber auf anderen API-Tools ausgeführt werden.

Allgemeines zum API-Gateway-Tunneling

Mithilfe der Gateway-APIs können Sie ONTAP-Objekte über Unified Manager managen. Unified Manager verwaltet die Cluster- und Authentifizierungsdetails und leitet die Anfragen an den REST-Endpunkt von ONTAP weiter. Die Gateway-API wandelt die URL und Hypermedia als Engine of Application State (HATEOAS)-Links im Header und Response Body mit der API-Gateway-Basis-URL um. Die Gateway-API fungiert als Proxy-Basis-URL, an die Sie die ONTAP-REST-URL anhängen und den erforderlichen ONTAP-REST-Endpunkt ausführen.

Damit eine ONTAP API erfolgreich über das API-Gateway ausgeführt werden kann, muss die API von dieser Version des ONTAP-Clusters unterstützt werden, auf dem sie ausgeführt wird. Die Ausführung einer API, die nicht auf dem ONTAP-Cluster unterstützt wird, liefert keine Ergebnisse.

In diesem Beispiel lautet die Gateway-API (Proxy-Basis-URL): `/gateways/{uuid}/`

Die ONTAP API genommen ist: `/storage/volumes`. Sie müssen die Rest-URL der ONTAP-API als Wert für

den Pfadparameter hinzufügen.

> Stellen Sie beim Hinzufügen des Pfads sicher, dass Sie „` add `storage/volumes.` entfernt haben/" `symbol at the beginning of the URL. For the API` `/storage/volumes,`

Die angehängte URL lautet: `/gateways/{uuid}/storage/volumes`

Beim Ausführen des `GET` Vorgangs ist die generierte URL wie folgt:
`GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes`

Das `/api` Tag der ONTAP-REST-URL wird in der angehängten URL entfernt und für die Gateway-API beibehalten.

Befehl zum Curl-Beispiel

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes" -H "accept: application/hal+json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

Die API gibt die Liste der Storage Volumes in diesem Cluster zurück. Das Antwortformat entspricht dem, das Sie erhalten, wenn Sie dieselbe API von ONTAP ausführen. Die zurückgegebenen Statuscodes sind die ONTAP-REST-Statuscodes.

API-Umfang wird festgelegt

Alle APIs weisen einen Kontext im Umfang des Clusters auf. APIs, die auf Storage-VMs basieren, haben auch den Cluster als Umfang, das heißt, die API-Vorgänge werden auf einer bestimmten Storage-VM innerhalb eines gemanagten Clusters ausgeführt. Stellen Sie beim Ausführen der `/gateways/{uuid}/{path}` API sicher, dass Sie die Cluster-UUID (Unified Manager Datasource UUID) für das Cluster eingeben, auf dem Sie den Vorgang ausführen. Geben Sie zum Festlegen des Kontexts für eine bestimmte Storage-VM innerhalb dieses Clusters den Storage-VM-Schlüssel als X-Dot-SVM-UUID Parameter oder den Storage-VM-Namen als Parameter X-Dot-SVM-Name ein. Der Parameter wird als Filter im String-Header hinzugefügt und der Vorgang wird im Rahmen dieser Storage-VM innerhalb dieses Clusters ausgeführt.

Befehl zum Curl-Beispiel

```
curl -X GET "https://<hostname>/api/gateways/e4f33f90-f75f-11e8-9ed9-
00a098e3215f/storage/volume" -H "accept: application/hal+json" -H "X-Dot-
SVM-UUID: d9c33ec0-5b61-11e9-8760-00a098e3215f"
-H "Authorization: Basic <Base64EncodedCredentials>"
```

Weitere Informationen zur Verwendung von ONTAP REST-APIs finden Sie unter "ONTAP REST-API-AUTOMATISIERUNG"

Durchführen administrativer Aufgaben mithilfe von APIs

Sie können die APIs unter der Kategorie verwenden `administration`, um Backup-

Einstellungen zu ändern, die Informationen zu Sicherungsdateien und Clusterzertifikate zu überprüfen und ONTAP-Cluster auch als Active IQ Unified Manager-Datenquellen zu verwalten.

Sie müssen die Anwendungsadministratorrolle besitzen, um diese Vorgänge ausführen zu können. Sie können diese Einstellungen auch über die Web-Benutzeroberfläche von Unified Manager konfigurieren.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`PATCH`
	`/admin/backup-settings`
	
	`/admin/backup-settings`
		Sie können die Methode verwenden `GET`, um die Einstellungen des in Unified Manager konfigurierten Backup-Zeitplans standardmäßig anzuzeigen. Sie können Folgendes überprüfen:
		• Gibt an, ob der Zeitplan aktiviert oder deaktiviert ist
		• Häufigkeit des geplanten Backups (täglich oder wöchentlich)
		• Zum Zeitpunkt des Backups
		• Maximale Anzahl an Backup-Dateien, die in der Applikation aufbewahrt werden sollen
		
		Die Zeit des Backups befindet sich in der Server-Zeitzone.
		
		Die Backup-Einstellungen für die Datenbank sind standardmäßig in Unified Manager verfügbar, und Sie können keinen Backup-Zeitplan erstellen. Sie können jedoch die Methode verwenden `PATCH`, um die Standardeinstellungen zu ändern.

`GET`	`/admin/backup-file-info`	Eine Backup Dump-Datei wird jedes Mal erzeugt, wenn der Backup-Zeitplan für Unified Manager geändert wird. Mit dieser Methode können Sie überprüfen, ob die Sicherungsdatei gemäß den geänderten Backup-Einstellungen generiert wird und ob die Informationen in der Datei mit den geänderten Einstellungen übereinstimmen.

HTTP-Verb	Pfad	Beschreibung
GET	/admin/datasource-certificate	Sie können diese Methode verwenden, um das Datasource (Cluster)-Zertifikat aus dem Trust Store anzuzeigen. Bevor Sie ein ONTAP Cluster als Unified Manager-Datenquelle hinzufügen, ist eine Überprüfung des Zertifikats erforderlich.
GET POST PATCH DELETE	/admin/datasources/clusters /admin/datasources/clusters/{key}	Mit dieser Methode können GET Sie die Details der von Unified Manager verwalteten Datenquellen (ONTAP-Cluster) abrufen. Sie können auch ein neues Cluster zu Unified Manager als Datenquelle hinzufügen. Zum Hinzufügen eines Clusters müssen Sie seinen Host-Namen, seinen Benutzernamen und sein Passwort kennen. Verwenden Sie den ONTAP-Clusterschlüssel zum Ändern und Löschen eines von Unified Manager als Datenquelle gemanagten Clusters.

Management von Benutzern mithilfe von APIs

Sie können die APIs in der Kategorie verwenden `security`, um den Benutzerzugriff auf ausgewählte Clusterobjekte in Active IQ Unified Manager zu steuern. Sie können lokale Benutzer oder Datenbankbenutzer hinzufügen. Sie können auch Remote-Benutzer oder -Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Basierend auf den Berechtigungen der Rollen, die Sie den Benutzern zuweisen, können sie die Speicherobjekte verwalten oder die Daten in Unified Manager anzeigen.

Sie müssen die Anwendungsadministratorrolle besitzen, um diese Vorgänge ausführen zu können. Sie können diese Einstellungen auch über die Web-Benutzeroberfläche von Unified Manager konfigurieren.

Die APIs unter der `security` Kategorie verwenden den Parameter Users, also den Benutzernamen und nicht den Schlüsselparameter als eindeutige Kennung für die Benutzereinheit.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`POST`
	`/security/users`
	
	`/security/users`
		Sie können diese Methoden verwenden, um Details zu Benutzern anzuzeigen oder neue Benutzer zu Unified Manager hinzuzufügen.
		
		Sie können den Benutzern basierend auf ihren Benutzertypen bestimmte Rollen hinzufügen. Beim Hinzufügen von Benutzern müssen Sie Passwörter für den lokalen Benutzer, den Wartungbenutzer und den Datenbankbenutzer bereitstellen.

`GET`
 	
`PATCH`
 	
`DELETE`
	`/security/users/{name}`	Mit DER GET-Methode können Sie alle Details eines Benutzers abrufen, z. B. Name, E-Mail-Adresse, Rolle und Berechtigungstyp. Mit der PATCH-Methode können Sie die Details aktualisieren. Mit der LÖSCHMETHODE können Sie den Benutzer entfernen.

Anzeigen von Performance-Metriken mithilfe von APIs

Active IQ Unified Manager stellt Ihnen unter der Kategorie APIs zur Verfügung `/datacenter`, mit denen Sie die Performance-Daten der Cluster und Storage-Objekte in einem Datacenter anzeigen können. Diese APIs rufen Performance-Daten der unterschiedlichen Storage-Objekte wie Cluster, Nodes, LUNs, Volumes, Aggregate, ab. Storage-VMs, FC-Schnittstellen, FC-Ports, Ethernet-Ports und IP-Schnittstellen.

Die `/metrics` APIs und `/analytics` bieten unterschiedliche Ansichten der Performance-Metriken. Dabei lassen sich diverse Detailebenen für die folgenden Storage-Objekte im Datacenter anzeigen:

- Cluster
- Knoten
- Storage-VMs
- Aggregate
- Volumes
- LUNs
- FC-Schnittstellen
- FC-Ports
- Ethernet-Ports

- IP-Schnittstellen

In der folgenden Tabelle wird ein Vergleich zwischen dem und `/analytics` APIs hinsichtlich der Angaben zu den abgerufenen Leistungsdaten erstellt `/metrics`.

Metriken	Analysen
Performance-Details für ein einzelnes Objekt. Zur API muss beispielsweise der `/datacenter/cluster/clusters/{key}/metrics` Cluster-Schlüssel als Pfadparameter zum Abrufen der Kennzahlen für dieses spezifische Cluster eingegeben werden.	Performance-Details für mehrere Objekte desselben Typs in einem Datacenter. Die API ruft beispielsweise `/datacenter/cluster/clusters/analytics` die kollektiven Kennzahlen aller Cluster in einem Rechenzentrum ab.
Beispiel für Performance-Kennzahlen für ein Storage-Objekt auf Basis des Zeitungsintervalls für den Abruf.	Der aggregierte Nutzwert der Performance auf hoher Ebene für einen bestimmten Storage-Typ für einen bestimmten Zeitraum (über 72 Stunden).
Grundlegende Details des Objekts werden abgerufen, z. B. Details zu einem Node oder Cluster.	Es werden keine Details abgerufen.
Akkumulierte Zähler, wie z. B. Minimum, Maximum, 95. Perzentil und die durchschnittlichen Performance-Werte über einen Zeitraum, werden für ein einzelnes Objekt wie Lesen, Schreiben, gesamt und andere Zähler abgerufen.	Für alle Objekte desselben Typs wird ein einzelner aggregierter Wert angezeigt.

Metriken	Analysen
Der Zeitbereich und die Probendaten basieren auf dem folgenden Zeitplan: Dem Zeitbereich für die Daten. Beispiele können 1 h, 12 h, 1d, 2d, 3d, 15 D, 1 w, 1 m, 2 m, 3 m, 6 m Sie erhalten 1 Stunde Proben, wenn der Bereich mehr als 3 Tage (72 Std.), sonst sind es 5 Minuten Proben. Der Zeitraum für jeden Zeitbereich ist wie folgt: • 1h: Kennzahlen der letzten Stunde, die über 5 Minuten erfasst wurden. • 12h: Kennzahlen über die letzten 12 Stunden, die über 5 Minuten erfasst wurden. • 1d: Kennzahlen des letzten Tages, abgetastet über 5 Minuten • 2d: Kennzahlen der letzten 2 Tage, die über 5 Minuten abgetastet wurden. • 3d: Kennzahlen der letzten 3 Tage, die über 5 Minuten abgetastet wurden. • 15d: Kennzahlen der letzten 15 Tage, die über eine Stunde abgetastet wurden. • 1w: Kennzahlen in der letzten Woche, die über 1 Stunde erfasst wurden. • 1M: Kennzahlen im letzten Monat, die über 1 Stunde abgetastet wurden. • 2m: Kennzahlen der letzten 2 Monate, die über 1 Stunde abgetastet wurden. • 3m: Kennzahlen der letzten 3 Monate, die über 1 Stunde abgetastet wurden. • 6m: Kennzahlen der letzten 6 Monate, die über 1 Stunde abgetastet wurden. Verfügbare Werte : 1h, 12h, 1d, 2d, 3d, 15 D, 1 w, 1 m, 2 m, 3 m, 6 m Standardwert : 1h	Über 72 Stunden. Die Dauer, über die diese Probe berechnet wird, wird im ISO-8601-Standardformat dargestellt.

Ausgabebeispiel für Kennzahlen-APIs

Die API ruft beispielsweise `/datacenter/cluster/nodes/{key}/metrics` die folgenden Details (unter anderem) für einen Knoten ab:

Das 95 Perzentil im Zusammenfassungswert zeigt an, dass 95 % der für den Zeitraum erfassten Proben einen Zählerwert haben, der unter dem als 95 Perzentil angegebenen Wert liegt.

```
{
```

```
      "iops": {
        "local": {
          "other": 100.53,
          "read": 100.53,
          "total": 100.53,
          "write": 100.53
        },
        "other": 100.53,
        "read": 100.53,
        "total": 100.53,
        "write": 100.53
      },
      "latency": {
        "other": 100.53,
        "read": 100.53,
        "total": 100.53,
        "write": 100.53
      },
      "performance_capacity": {
        "available_iops_percent": 0,
        "free_percent": 0,
        "system_workload_percent": 0,
        "used_percent": 0,
        "user_workload_percent": 0
      },
      "throughput": {
        "other": 100.53,
        "read": 100.53,
        "total": 100.53,
        "write": 100.53
      },
      "timestamp": "2018-01-01T12:00:00-04:00",
      "utilization_percent": 0
    }
  ],
  "start_time": "2018-01-01T12:00:00-04:00",
  "summary": {
    "iops": {
      "local_iops": {
        "other": {
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        },
        "read": {
```

```
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        },
        "total": {
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        },
        "write": {
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        }
      },
```

Ausgabebeispiel für Analyse-APIs

Die API ruft beispielsweise `/datacenter/cluster/nodes/analytics` die folgenden Werte (unter anderem) für alle Knoten ab:

```
{     "iops": 1.7471,
     "latency": 60.0933,
     "throughput": 5548.4678,
     "utilization_percent": 4.8569,
     "period": 72,
     "performance_capacity": {
       "used_percent": 5.475,
       "available_iops_percent": 168350
     },
     "node": {
       "key": "37387241-8b57-11e9-8974-
00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a",
       "uuid": "95f94e8d-8b4e-11e9-8974-00a098e0219a",
       "name": "ocum-infinity-01",
       "_links": {
         "self": {
           "href": "/api/datacenter/cluster/nodes/37387241-8b57-11e9-8974-
00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a"
         }
       }
     },
     "cluster": {
       "key": "37387241-8b57-11e9-8974-
00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a",
       "uuid": "37387241-8b57-11e9-8974-00a098e0219a",
       "name": "ocum-infinity",
       "_links": {
         "self": {
           "href": "/api/datacenter/cluster/clusters/37387241-8b57-11e9-
8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a"
         },
     "_links": {
       "self": {
         "href": "/api/datacenter/cluster/nodes/analytics"
       }
     }
   },
```


Liste der verfügbaren APIs

In der folgenden Tabelle werden Details zum und `/analytics` APIs beschrieben `/metrics`.

Die durch diese APIs zurückgegebenen IOPS- und Performance-Metriken sind beispielsweise doppelte Werte `100.53`. Das Filtern dieser Float-Werte durch die Pfeife („) und die Platzhalter (*)-Zeichen wird nicht unterstützt.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/cluster/clusters/{key}/metrics	Ruft die Performance-Daten (Beispiel und Zusammenfassung) für ein Cluster ab, das vom Eingabeparameter des Cluster-Schlüssels angegeben wurde. Informationen wie der Cluster-Schlüssel und die UUID, der Zeitbereich, IOPS, Durchsatz und die Anzahl der Proben werden zurückgegeben.
GET	/datacenter/cluster/clusters/analytics	Ruft Performance-Kennzahlen auf hoher Ebene für alle Cluster in einem Datacenter ab. Sie können Ihre Ergebnisse nach den erforderlichen Kriterien filtern. Werte wie aggregierte IOPS, Durchsatz und Erfassungszeitraum (in Stunden) werden zurückgegeben.
GET	/datacenter/cluster/nodes/{key}/metrics	Ruft Performance-Daten (Beispiel und Zusammenfassung) für einen Node ab, der durch den Eingabeparameter des Node-Schlüssels angegeben wurde. Informationen wie Node-UUID, Zeitbereich, Zusammenfassung der IOPS, Durchsatz, Latenz und Performance, die Anzahl der erfassten Proben und der verwendete Prozentsatz werden zurückgegeben.
GET	/datacenter/cluster/nodes/analytics	Ruft High-Level-Performance-Metriken für alle Nodes im Datacenter ab. Sie können Ihre Ergebnisse nach den erforderlichen Kriterien filtern. Informationen wie Node- und Cluster-Schlüssel und Werte wie aggregierte IOPS, Durchsatz und Erfassungszeitraum (in Stunden) werden zurückgegeben.

HTTP-Verb	Pfad	Beschreibung
GET	`/datacenter/storage/aggregates/{key}/metrics`	Ruft Performance-Daten (Probe und Zusammenfassung) für ein Aggregat ab, das durch den Eingabeparameter des Aggregatschlüssels angegeben wurde. Informationen wie z. B. Zeitraum, Zusammenfassung der IOPS, Latenz, Durchsatz und Performance-Kapazität, die Anzahl der für jeden Zähler gesammelten Proben und der Prozentsatz der genutzten Kapazität werden zurückgegeben.
GET	`/datacenter/storage/aggregates/analytics`	Ruft Performance-Kennzahlen auf höchster Ebene für alle Aggregate in einem Datacenter ab. Sie können Ihre Ergebnisse nach den erforderlichen Kriterien filtern. Informationen wie Aggregat- und Cluster-Schlüssel und Werte wie aggregierte IOPS, Durchsatz und Erfassungszeitraum (in Stunden) werden zurückgegeben.

GET	`/datacenter/storage/luns/{key}/metrics`
	
	`/datacenter/storage/volumes/{key}/metrics`
		Ruft Performance-Daten (Beispiel und Zusammenfassung) für eine LUN oder eine Dateifreigabe (Volume) ab, die vom Eingabeparameter der LUN- oder Volume-Taste angegeben wurde. Informationen, z. B. eine Zusammenfassung des minimalen, maximalen und durchschnittlichen Lese-, Schreib- und Gesamt-IOPS, der Latenz und des Durchsatzes Und die Anzahl der Proben, die für jeden Zähler gesammelt wurden, wird zurückgegeben.

GET	`/datacenter/storage/luns/analytics`
	
	`/datacenter/storage/volumes/analytics`
		Ruft Performance-Kennzahlen auf höchster Ebene für alle LUNs oder Volumes eines Datacenters ab. Sie können Ihre Ergebnisse nach den erforderlichen Kriterien filtern. Informationen wie Storage-VM- und Cluster-Schlüssel und Werte wie aggregierte IOPS, Durchsatz und Erfassungszeitraum (in Stunden) werden zurückgegeben.

HTTP-Verb	Pfad	Beschreibung
GET	`/datacenter/svm/svms/{key}/metrics`	Ruft die Performance-Daten (Beispiel und Zusammenfassung) für eine Storage-VM ab, die durch den Eingabeparameter des Storage-VM-Schlüssels angegeben wurde. Zusammenfassung der IOPS basierend auf jedem unterstützten Protokoll, wie `nvmf, fcp, iscsi,` und `nfs`, Durchsatz, Latenz und die Anzahl der erfassten Proben werden zurückgegeben.
GET	`/datacenter/svm/svms/analytics`	Abruf von Performance-Metriken auf höchster Ebene für alle Storage VMs in einem Datacenter Sie können Ihre Ergebnisse nach den erforderlichen Kriterien filtern. Informationen wie Storage-VM-UUID, aggregierte IOPS, Latenz, Durchsatz und der Erfassungszeitraum (in Stunden) werden zurückgegeben.
GET	`/datacenter/network/ethernet/ports/{key}/metrics`	Ruft die Leistungskennzahlen für einen bestimmten ethernet-Port ab, der durch den Eingabeparameter des Portschlüssels angegeben wird. Wenn ein Intervall (Zeitraum) aus dem unterstützten Bereich angegeben wird, gibt die API die kumulierten Zähler zurück, z. B. Minimum, Maximum und die durchschnittlichen Leistungswerte über den Zeitraum.
GET	`/datacenter/network/ethernet/ports/analytics`	Ruft die grundlegenden Performance-Kennzahlen für alle ethernet-Ports in Ihrer Datacenter-Umgebung ab. Informationen wie der Cluster- und Node-Schlüssel und die UUID, Durchsatz, Erfassungszeitraum und Prozentsatz der Auslastung für die Ports werden zurückgegeben. Sie können das Ergebnis nach den verfügbaren Parametern filtern, wie z. B. Portschlüssel, Auslastungsgrad, Cluster- und Node-Name und UUID.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/network/fc/interfaces/{key}/metrics	Ruft die Leistungskennzahlen für eine bestimmte Netzwerk-FC-Schnittstelle ab, die vom Eingabeparameter des Interface Key angegeben wird. Wenn ein Intervall (Zeitraum) aus dem unterstützten Bereich angegeben wird, gibt die API die kumulierten Zähler zurück, z. B. Minimum, Maximum und die durchschnittlichen Leistungswerte über den Zeitraum.
GET	/datacenter/network/fc/interfaces/analytics	Ruft die grundlegenden Performance-Kennzahlen für alle ethernet-Ports in Ihrer Datacenter-Umgebung ab. Informationen wie der Schlüssel für die Cluster- und FC-Schnittstelle und die UUID, Durchsatz, IOPS, Latenz und Storage VM werden zurückgegeben. Sie können das Ergebnis nach den verfügbaren Parametern filtern, z. B. dem Namen des Clusters und der FC-Schnittstelle und der UUID, Storage VM, Durchsatz usw.
GET	/datacenter/network/fc/ports/{key}/metrics	Ruft die Performance-Metriken für einen bestimmten FC-Port ab, der durch den Eingabeparameter des Port-Schlüssels angegeben wurde. Wenn ein Intervall (Zeitraum) aus dem unterstützten Bereich angegeben wird, gibt die API die kumulierten Zähler zurück, z. B. Minimum, Maximum und die durchschnittlichen Leistungswerte über den Zeitraum.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/network/fc/ports/analytics	Ruft die grundlegenden Performance-Metriken für alle FC Ports in Ihrer Datacenter-Umgebung ab. Informationen wie der Cluster- und Node-Schlüssel und die UUID, Durchsatz, Erfassungszeitraum und Prozentsatz der Auslastung für die Ports werden zurückgegeben. Sie können das Ergebnis nach den verfügbaren Parametern filtern, wie z. B. Portschlüssel, Auslastungsgrad, Cluster- und Node-Name und UUID.
GET	/datacenter/network/ip/interfaces/{key}/metrics	Ruft die Leistungskennzahlen für eine Netzwerk-IP-Schnittstelle ab, die durch den Eingabeparameter des Schnittstellenschlüssels festgelegt wurden. Wenn ein Intervall (Zeitraum) aus dem unterstützten Bereich bereitgestellt wird, gibt die API Informationen zurück, wie z. B. die Anzahl der Proben, angesammelte Zähler, Durchsatz und die Anzahl der empfangenen und übertragenen Pakete.
GET	/datacenter/network/ip/interfaces/analytics	Ruft die Performance-Kennzahlen auf hoher Ebene für alle Netzwerk-IP-Schnittstellen in Ihrer Datacenter-Umgebung ab. Informationen wie der Schlüssel zum Cluster und die IP-Schnittstelle und die UUID, Durchsatz, IOPS und Latenz werden zurückgegeben. Sie können das Ergebnis nach den verfügbaren Parametern filtern, z. B. den Namen der Cluster- und IP-Schnittstelle und die UUID, IOPS, Latenz, Durchsatz usw.

Anzeigen von Jobs und Systemdetails

Sie können die API unter der `management-server` Kategorie verwenden `jobs`, um die Ausführungsdetails asynchroner Vorgänge anzuzeigen. Über die `system` API unter der `management-server` Kategorie können Sie Details zur Instanz in Ihrer Active IQ Unified

Manager-Umgebung anzeigen.

Anzeigen Von Jobs

In Active IQ Unified Manager werden Vorgänge wie das Hinzufügen und Ändern von Ressourcen durch synchrone und asynchrone API-Aufrufe durchgeführt. Aufrufe, die für die asynchrone Ausführung geplant sind, können von einem für diesen Aufruf erstellten Jobobjekt nachverfolgt werden. Jedes Jobobjekt verfügt über einen eindeutigen Schlüssel zur Identifizierung. Jedes Job-Objekt gibt die Job-Objekt-URI zurück, mit der Sie auf den Fortschritt des Jobs zugreifen und diesen verfolgen können. Sie können diese API zum Abrufen der Details jeder Ausführung verwenden.

Mithilfe dieser API können Sie alle Job-Objekte für Ihr Rechenzentrum abfragen, einschließlich historischer Daten. Standardmäßig gibt das Abfragen aller Jobs die Details der letzten 20 Jobs zurück, die über die Web-Benutzeroberfläche und die API-Schnittstelle ausgelöst wurden. Verwenden Sie die integrierten Filter, um bestimmte Jobs anzuzeigen. Sie können auch die Job-Taste verwenden, um die Details eines bestimmten Jobs abzufragen und die nächsten Operationen für die Ressourcen auszuführen.

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/jobs`	Gibt die Jobdetails aller Jobs zurück. Ohne Sortierreihenfolge wird das zuletzt eingereichte Jobobjekt oben zurückgegeben.
Management-Server	GET	`/management-server/jobs/{key}` Geben Sie den Job-Schlüssel des Jobobjekts ein, um die spezifischen Details dieses Jobs anzuzeigen.	Gibt die Details des spezifischen Jobobjekts zurück.

Anzeigen von Systemdetails

Mithilfe der `/management-server/system` API können Sie die instanzspezifischen Details Ihrer Unified Manager Umgebung abfragen. Die API liefert Informationen zum Produkt und zu Services, z. B. zur Version von Unified Manager, die auf Ihrem System installiert ist, UUID, Anbietername, Host OS und Name, beschreibung und Status der auf der Unified Manager-Instanz ausgeführten Services.

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/system`	Für die Ausführung dieser API ist kein Eingabeparameter erforderlich. Die Systemdetails der aktuellen Unified Manager Instanz werden standardmäßig zurückgegeben.

Verwalten von Ereignissen und Warnmeldungen mithilfe von APIs

Mit den `events` APIs , `alerts` und `scripts` unter der `management-server` Kategorie können Sie die Ereignisse, Warnungen und Skripte verwalten, die den Warnmeldungen in Ihrer Active IQ Unified Manager-Umgebung zugeordnet sind.

Anzeigen und Ändern von Ereignissen

Unified Manager erhält die Ereignisse, die auf ONTAP für die durch Unified Manager überwachten und verwalteten Cluster generiert werden. Mit diesen APIs können Sie die für Ihre Cluster generierten Ereignisse anzeigen und sie lösen und aktualisieren.

Wenn Sie die Methode für die `/management-server/events` API ausführen `GET`, können Sie die Ereignisse in Ihrem Rechenzentrum abfragen, einschließlich historischer Daten. Verwenden Sie die eingebauten Filter, z. B. Name, Aufprallgrad, Aufprallbereich, Schweregrad, Status, Ressourcenname und Ressourcentyp, um bestimmte Ereignisse anzuzeigen. Die Ressourcentyp- und Flächenparameter geben Informationen über das Speicherobjekt zurück, auf dem das Ereignis aufgetreten ist, und der Einwirkungsbereich gibt die Informationen über das Problem zurück, für das das Ereignis erhöht wird, wie z. B. Verfügbarkeit, Kapazität, Konfiguration, Sicherheit, Sicherung und Performance.

Durch Ausführen des PATCH-Vorgangs für diese API können Sie den Auflösungsworkflow für das Ereignis aktivieren. Sie können sich selbst oder einem anderen Benutzer ein Ereignis zuweisen und den Empfang der Veranstaltung bestätigen. Wenn Sie die Schritte auf den Ressourcen ausführen, um das Problem, das das Ereignis ausgelöst hat, zu beheben, können Sie diese API verwenden, um das Ereignis als gelöst zu markieren.

Weitere Informationen zu Veranstaltungen finden Sie unter "Verwalten von Ereignissen".

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/events` `/management-server/events/{key}`	Wenn Sie die Methode „Alle abrufen“ ausführen, besteht der Response Body aus den Ereignisdetails aller Ereignisse in Ihrem Datacenter. Wenn Sie die Ereignisdetails mit einem bestimmten Schlüssel abrufen, können Sie die Details zu einem bestimmten Ereignis anzeigen und die nächsten Vorgänge auf den Ressourcen ausführen. Der Antwortkörper besteht aus den Details dieses Ereignisses.
Management-Server	PATCH	`management-server/events/{key}`	Führen Sie diese API aus, um ein Ereignis zuzuweisen oder den Status auf „bestätigt“ oder „gelöst“ zu ändern. Sie können diese Methode auch verwenden, um das Ereignis selbst oder einem anderen Benutzer zuzuordnen. Es handelt sich um einen synchronen Vorgang.

Verwalten von Meldungen

Ereignisse werden automatisch und kontinuierlich generiert. Unified Manager generiert eine Meldung nur, wenn ein Ereignis bestimmte Filterkriterien erfüllt. Sie können die Ereignisse auswählen, für die Warnmeldungen generiert werden sollen. Mithilfe der `/management-server/alerts` API können Sie Warnmeldungen so konfigurieren, dass automatisch Benachrichtigungen gesendet werden, wenn bestimmte Ereignisse oder Ereignisse bestimmter Schweregrade auftreten.

Weitere Informationen zu Warnmeldungen finden Sie unter "Verwalten von Meldungen".

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/alerts` `/management-server/alerts/{key}`	Abfragen aller vorhandenen Warnmeldungen in Ihrer Umgebung oder eines bestimmten Alarms mithilfe des Alarmschlüssels. Sie können die Informationen zu den in Ihrer Umgebung erzeugten Warnmeldungen anzeigen, z. B. Alarmbeschreibung, Aktion, E-Mail-ID, an die die Benachrichtigung gesendet wird, Ereignis- und Schweregrad.
Management-Server	POST	`/management-server/alerts`	Mit dieser Methode können Sie Warnmeldungen für bestimmte Ereignisse hinzufügen. Sie müssen den Warnungsnamen, die physische oder logische Ressource oder das Ereignis hinzufügen, auf das die Warnung anwendbar ist, ob die Warnung aktiviert ist und ob Sie SNMP-Traps ausgeben. Sie können weitere Details hinzufügen, für die Sie die Warnmeldung generieren möchten, z. B. Aktion, Benachrichtigungs-E-Mail-ID, Skriptdetails, falls Sie ein Warnungsskript hinzufügen usw.

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	PATCHEN und LÖSCHEN	`management-server/events/{key}`	Sie können diese Methoden verwenden, um bestimmte Warnmeldungen zu ändern und zu löschen. Sie können verschiedene Attribute ändern, z. B. Beschreibung, Name und Aktivieren und Deaktivieren der Warnmeldung. Sie können eine Meldung löschen, wenn die Meldung nicht mehr erforderlich ist.

Beachten Sie beim Auswählen einer Ressource zum Hinzufügen einer Meldung, dass die Auswahl eines Clusters als Ressource nicht automatisch die Speicherobjekte innerhalb des Clusters auswählt. Wenn Sie beispielsweise eine Meldung für alle kritischen Ereignisse für alle Cluster erstellen, erhalten Sie Warnmeldungen nur für kritische Cluster-Ereignisse. Für kritische Ereignisse in Nodes, Aggregaten usw. werden keine Warnmeldungen ausgegeben.

Verwalten von Skripten

Mithilfe der `/management-server/scripts` API können Sie auch eine Warnung mit einem Skript verknüpfen, das beim Auslösen einer Warnmeldung ausgeführt wird. 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. Sie können eine Warnung mit Ihrem Skript verknüpfen, damit das Skript ausgeführt wird, wenn eine Warnung für ein Ereignis in Unified Manager ausgegeben wird.

Weitere Informationen zu Skripten finden Sie unter "Verwalten von Skripten".

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/scripts`	Verwenden Sie diese API, um alle vorhandenen Skripte in Ihrer Umgebung abzufragen. Verwenden Sie den Standardfilter und die Reihenfolge nach Operationen, um nur bestimmte Skripte anzuzeigen.

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	POST	`/management-server/scripts`	Verwenden Sie diese API, um eine Beschreibung für das Skript hinzuzufügen und die mit einer Warnung verknüpfte Skriptdatei hochzuladen.

Management von Workloads mit APIs

Die hier beschriebenen APIs decken verschiedene Funktionen der Storage-Administration ab, z. B. das Anzeigen von Storage Workloads, das Erstellen von LUNs und Dateifreigaben, das Management von Performance Service Levels und Richtlinien für Storage-Effizienz sowie die Zuweisung von Richtlinien zu Storage Workloads.

Anzeigen von Storage-Workloads mithilfe von APIs

Mit den hier aufgeführten APIs können Sie eine konsolidierte Liste von Storage-Workloads für alle ONTAP Cluster im Datacenter anzeigen. Die APIs bieten auch eine Übersicht über die Anzahl der in Ihrer Active IQ Unified Manager Umgebung bereitgestellten Storage Workloads und ihre Kapazitäts- und IOPS-Statistiken (Performance).

Anzeige von Storage-Workloads

Mithilfe der folgenden Methode können Sie alle Storage-Workloads in allen Clustern in Ihrem Datacenter anzeigen. Informationen zum Filtern der Antwort auf der Grundlage bestimmter Spalten finden Sie in der API-Referenzdokumentation, die in Ihrer Unified Manager Instanz verfügbar ist.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/workloads`

Anzeigen der Zusammenfassung der Speicher-Workloads

Anhand der folgenden Methode können Sie die genutzte Kapazität, verfügbare Kapazität, genutzte IOPS, verfügbare IOPS und Anzahl der von den einzelnen Performance-Service-Level gemanagten Storage Workloads bewerten. Die angezeigten Storage Workloads können für jede LUN, jede NFS-Dateifreigabe oder jede CIFS-Freigabe sein. Die API gibt einen Überblick über Storage-Workloads, einen Überblick über die vom Unified Manager bereitgestellten Storage-Workloads, eine Datacenter-Übersicht, eine Übersicht über die Gesamtzahl der verwendeten sowie den verfügbaren Speicherplatz und die IOPS im Datacenter, im Hinblick auf die zugewiesenen Performance-Service-Level. Die als Antwort auf diese API erhaltenen Informationen werden verwendet, um das Dashboard in die Benutzeroberfläche von Unified Manager einzufüllen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/workloads-summary`

Management von Zugriffendpunkten mithilfe von APIs

Zugriffendpunkte oder logische Schnittstellen (LIFs) müssen erstellt werden, die für die Bereitstellung von Storage Virtual Machines (SVMs), LUNs und Dateifreigaben erforderlich sind. Sie können die Zugriffendpunkte für die SVMs, LUNs oder File Shares in der Active IQ Unified Manager Umgebung anzeigen, erstellen, ändern und löschen.

Zugriffendpunkte anzeigen

Sie können eine Liste der Zugriffendpunkte in Ihrer Unified Manager-Umgebung mithilfe der folgenden Methode anzeigen. Um eine Liste der Zugriffendpunkte einer bestimmten SVM, LUN oder Dateifreigabe abzufragen, müssen Sie die eindeutige Kennung für die SVM, die LUN oder die Dateifreigabe eingeben. Sie können auch die eindeutige Taste für den Zugriffendpunkt eingeben, um die Details des jeweiligen Zugriffendpunkts abzurufen.

Kategorie	HTTP-Verb	Pfad

Anbieter von Storage-Lösungen	GET	`/storage-provider/access-endpoints`
		
		`/storage-provider/access-endpoints/{key}`

Fügen Sie Zugriffendpunkte hinzu

Sie können benutzerdefinierte Zugriffendpunkte erstellen und erforderliche Eigenschaften ihm zuweisen. Sie müssen die Details des Zugriffendpunkts eingeben, den Sie als Eingabeparameter erstellen möchten. Sie können diese API oder die System Manager- oder ONTAP-CLI verwenden, um auf jedem Node einen Zugriffsknoten zu erstellen. Für die Erstellung von Zugriffendpunkten werden sowohl IPv4- als auch IPv6-Adressen unterstützt.

> Sie müssen Ihre SVM für die erfolgreiche Bereitstellung von LUNs und Dateifreigaben mit einer Mindestanzahl an Zugriffendpunkten pro Node konfigurieren. Sie sollten Ihre SVM mit mindestens zwei Zugriffendpunkten pro Node konfigurieren, die jeweils ein CIFS- und/oder NFS-Protokoll unterstützen, ein weiteres iSCSI- oder FCP-Protokoll.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	`/storage-provider/access-endpoints`

Zugriffsendpunkte löschen

Sie können einen bestimmten Zugriffendpunkt mithilfe der folgenden Methode löschen. Zum Löschen eines bestimmten Zugriffsparameters muss der Schlüssel für den Zugriffendpunkt als Eingabeparameter

bereitgestellt werden.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	Löschen	`/storage-provider/access-endpoints/{key}`

Zugriffsendpunkte ändern

Sie können einen Zugriffendpunkt ändern und seine Eigenschaften mithilfe der folgenden Methode aktualisieren. Zur Änderung eines bestimmten Zugriffendpunkts müssen Sie den Schlüssel für den Zugriffendpunkt angeben. Sie müssen außerdem die Eigenschaft eingeben, die Sie aktualisieren möchten, zusammen mit ihrem Wert.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	`/storage-provider/access-endpoints/{key}`

Verwalten der Active Directory-Zuordnung mithilfe von APIs

Mithilfe der hier aufgeführten APIs können Sie die Active Directory-Zuordnungen auf der SVM managen, die für die Bereitstellung von CIFS-Freigaben auf den SVMs erforderlich sind. Active Directory-Zuordnungen müssen konfiguriert werden, um die SVMs mit ONTAP zuzuordnen.

Anzeigen von Active Directory-Zuordnungen

Sie können die Konfigurationsdetails der Active Directory-Zuordnungen für eine SVM über die folgende Methode anzeigen. Um die Active Directory-Zuordnungen auf einer SVM anzuzeigen, müssen Sie den SVM-Schlüssel eingeben. Um die Details einer bestimmten Zuordnung abfragen zu können, müssen Sie den Zuordnungsschlüssel eingeben.

Kategorie	HTTP-Verb	Pfad

Anbieter von Storage-Lösungen	GET	`/storage-provider/active-directories-mappings`
		
		`/storage-provider/active-directories-mappings/{key}`

Fügen Sie die Active Directory-Zuordnung hinzu

Sie können Active Directory-Zuordnungen auf einer SVM mit der folgenden Methode erstellen. Sie müssen die Zuordnungsdetails als Eingabeparameter eingeben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	`/storage-provider/active-directories-mappings`

Verwalten von Dateifreigaben mit APIs

Über die API können Sie die `/storage-provider/file-shares` CIFS- und NFS-Dateifreigabevolumes in Ihrer Datacenter-Umgebung anzeigen, hinzufügen, ändern und löschen.

Bevor Sie die DateifreigabVolumes bereitstellen, müssen Sie sicherstellen, dass die SVM mit den unterstützten Protokollen erstellt und bereitgestellt wurde. Wenn Sie während der Bereitstellung Performance Service Levels (PSLs) oder Storage Efficiency Policies (SEPs) zuweisen, sollten vor dem Erstellen der Dateifreigaben die PSLs oder SEPs erstellt werden.

Anzeigen von Dateifreigaben

Mit der folgenden Methode können Sie die in Ihrer Unified Manager-Umgebung verfügbaren DateifreigabemVolumes anzeigen. Wenn Sie ein ONTAP Cluster als Datenquelle auf Active IQ Unified Manager hinzugefügt haben, werden die Storage-Workloads für diese Cluster automatisch Ihrer Unified Manager Instanz hinzugefügt. Diese API ruft die Dateifreigaben automatisch ab und wird Ihrer Unified Manager-Instanz manuell hinzugefügt. Sie können die Details einer bestimmten Dateifreigabe anzeigen, indem Sie diese API mit dem Dateifreigabschlüssel ausführen.

Kategorie	HTTP-Verb	Pfad

Anbieter von Storage-Lösungen	GET	`/storage-provider/file-shares`
		
		`/storage-provider/file-shares/{key}`

Fügen Sie Dateifreigaben hinzu

Mit der folgenden Methode können Sie CIFS- und NFS-Dateifreigaben in Ihre SVM hinzufügen. Als Eingabeparameter müssen Sie die Details der Dateifreigabe eingeben, die Sie erstellen möchten. Sie können diese API nicht zum Hinzufügen von FlexGroup Volumes verwenden.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	`/storage-provider/file-shares`

Je nachdem, ob die Parameter der Zugriffssteuerungsliste (ACL) oder der Parameter für die Exportrichtlinie zur Verfügung gestellt werden, werden CIFS-Shares oder NFS-Dateifreigaben erstellt. Wenn Sie die Werte für die ACL-Parameter nicht angeben, werden CIFS-Shares nicht erstellt und NFS-Shares werden standardmäßig erstellt, um Zugriff auf alle zu ermöglichen.

Erstellen von Data-Protection-Volumes: Wenn Sie File Shares zu Ihrer SVM hinzufügen, ist der Typ des

gemounteten Volumes standardmäßig `rw` (Lesen/Schreiben). Geben Sie zum Erstellen von Datenschutz-Volumes (DP) als Wert für den `type` Parameter an `dp`.

Löschen von Dateifreigaben

Sie können die folgende Methode verwenden, um eine bestimmte Dateifreigabe zu löschen. Zum Löschen einer bestimmten Dateifreigabe müssen Sie den Freigabeschlüssel als Eingabeparameter eingeben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	Löschen	`/storage-provider/file-shares/{key}`

Ändern von Dateifreigaben

Sie können die folgende Methode verwenden, um eine Dateifreigabe zu ändern und deren Eigenschaften zu aktualisieren.

Sie müssen den Dateifreigabschlüssel angeben, um eine bestimmte Dateifreigabe zu ändern. Außerdem müssen Sie die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben.

Beachten Sie, dass Sie nur eine Eigenschaft bei einem einzelnen Aufruf dieser API aktualisieren können. Für mehrere Updates müssen Sie diese API so oft ausführen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	`/storage-provider/file-shares/{key}`

Verwalten von LUNs mithilfe von APIs

Sie können die `/storage-provider/luns` LUNs in Ihrer Datacenter-Umgebung anzeigen, hinzufügen, ändern und löschen.

Vergewissern Sie sich vor der Bereitstellung der LUNs, dass die SVM mit den unterstützten Protokollen erstellt und bereitgestellt wurde. Wenn Sie während der Bereitstellung Performance Service Levels (PSLs) oder Storage Efficiency Policies (SEPs) zuweisen, sollten vor dem Erstellen der LUN die PSLs oder SEPs erstellt werden.

Zeigen Sie LUNs an

Mit der folgenden Methode können Sie die LUNs in Ihrer Unified Manager Umgebung anzeigen. Wenn Sie ein ONTAP Cluster als Datenquelle auf Active IQ Unified Manager hinzugefügt haben, werden die Storage-Workloads für diese Cluster automatisch Ihrer Unified Manager Instanz hinzugefügt. Diese API ruft alle LUNs automatisch ab und wird manuell zu Ihrer Unified Manager Instanz hinzugefügt. Sie können sich die Details einer bestimmten LUN anzeigen lassen, indem Sie diese API mit dem LUN-Schlüssel ausführen.

Kategorie	HTTP-Verb	Pfad

Anbieter von Storage-Lösungen	GET	`/storage-provider/luns`
		
		`/storage-provider/luns/{key}`

Fügen Sie LUNs hinzu

Mit der folgenden Methode können Sie Ihren SVMs LUNs hinzufügen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	`/storage-provider/luns`

Wenn Sie in Ihrer curl-Anforderung einen Wert für den optionalen Parameter Volume_Name_Tag in der Eingabe angeben, wird dieser Wert bei der Benennung des Volumes während der LUN-Erstellung verwendet. Mit diesem Tag kann das Volume einfach durchsucht werden. Wenn Sie den Volume-Schlüssel in der Anforderung angeben, wird das Tagging übersprungen.

LUNs löschen

Sie können eine bestimmte LUN mit der folgenden Methode löschen. Sie müssen den LUN-Schlüssel zum Löschen einer bestimmten LUN angeben.

Wenn Sie ein Volume in ONTAP erstellt und dann über Unified Manager auf diesem Volume bereitgestellt haben, wenn Sie alle LUNs mithilfe dieser API löschen, wird das Volume auch aus dem ONTAP Cluster gelöscht.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	Löschen	`/storage-provider/luns/{key}`

LUNs ändern

Mit der folgenden Methode können Sie eine LUN ändern und ihre Eigenschaften aktualisieren. Sie müssen den LUN-Schlüssel angeben, um eine bestimmte LUN zu ändern. Sie müssen außerdem die LUN-Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben. Für die Aktualisierung von LUN-Arrays mithilfe dieser API sollten Sie die Empfehlungen unter „`Empfehlungen zur Verwendung der APIs`“ überprüfen.

Sie können nur eine Eigenschaft bei einem einzelnen Aufruf dieser API aktualisieren. Für mehrere Updates müssen Sie diese API so oft ausführen.

Kategorie	HTTP-Verb	Pfad

Anbieter von Storage-Lösungen	PATCH	`/storage-provider/luns/{key}`

Management von Performance Service Levels mithilfe von APIs

Sie können Performance-Service-Level mithilfe der Storage-Provider-APIs für auf Ihrer Active IQ Unified Manager anzeigen, erstellen, ändern und löschen.

Zeigen Sie Performance Service Level An

Mit der folgenden Methode können Sie die Performance-Service-Level für die Zuweisung zu Storage-Workloads anzeigen. Die API listet alle systemdefinierten und vom Benutzer erstellten Performance Service Levels auf und ruft die Attribute aller Performance Service Levels ab. Wenn Sie einen bestimmten Performance-Service-Level abfragen möchten, müssen Sie die eindeutige ID des Performance-Service-Levels eingeben, um die entsprechenden Details abzurufen.

Kategorie	HTTP-Verb	Pfad

Anbieter von Storage-Lösungen	GET	`/storage-provider/performance-service-levels`
		
		`/storage-provider/performance-service-levels/{key}`

Performance-Service-Level Hinzufügen

Mithilfe der folgenden Methode können Sie benutzerdefinierte Performance-Service-Level erstellen und diesen Ihren Storage-Workloads zuweisen, wenn die vom System definierten Performance-Service-Level die erforderlichen Service Level-Ziele (SLOs) für die Storage-Workloads nicht erfüllen. Geben Sie die Details für die Leistungsstufe ein, die Sie erstellen möchten. Stellen Sie für die IOPS-Eigenschaften sicher, dass Sie einen gültigen Wertebereich eingeben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	`/storage-provider/performance-service-levels`

Performance-Service-Level Löschen

Sie können die folgende Methode verwenden, um einen bestimmten Leistungsservicelevel zu löschen. Ein Performance-Service-Level kann nicht gelöscht werden, wenn er einem Workload zugewiesen ist oder wenn es das einzige verfügbare Performance-Service-Level ist. Sie müssen die eindeutige ID des Performance Service Levels als Eingabeparameter angeben, um einen bestimmten Performance Service Level zu löschen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	Löschen	`/storage-provider/performance-service-levels/{key}`

Ändern Sie Performance-Service-Level

Sie können die folgende Methode verwenden, um einen Performance-Service-Level zu ändern und seine Eigenschaften zu aktualisieren. Ein Performance-Service-Level, der systemdefiniert oder einem Workload zugewiesen ist, kann nicht geändert werden. Zum Ändern eines bestimmten Performance-Service-Levels müssen Sie die eindeutige ID des angeben. Sie müssen außerdem die IOPS-Eigenschaft, die Sie aktualisieren möchten, sowie einen gültigen Wert eingeben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	`/storage-provider/performance-service-levels/{key}`

Anzeigen von Aggregatfunktionen auf Basis von Performance-Service-Leveln

Sie können die folgende Methode verwenden, um die Aggregatfunktionen auf Basis der Performance-Service-Level abzufragen. Diese API gibt die Liste der in Ihrem Datacenter verfügbaren Aggregate zurück und weist die Funktionen in Bezug auf die Performance-Service-Level an, die in diesen Aggregaten unterstützt werden können. Während Sie Workloads auf einem Volume bereitstellen, können Sie die Funktionen eines Aggregats anzeigen, um ein bestimmtes Performance Service Level zu unterstützen. Zudem können Sie Workloads basierend auf dieser Funktion bereitstellen. Die Angabe des Aggregats ist nur verfügbar, wenn Sie einen Workload mithilfe von APIs bereitstellen. Diese Funktion steht in der Web-Benutzeroberfläche von Unified Manager nicht zur Verfügung.

Kategorie	HTTP-Verb	Pfad

Anbieter von Storage-Lösungen	GET	`/storage-provider/aggregate-capabilities`
		
		`/storage-provider/aggregate-capabilities/{key}`

Management von Richtlinien zur Storage-Effizienz mithilfe von APIs

Sie können Richtlinien zur Storage-Effizienz mithilfe der Storage-Provider-APIs anzeigen, erstellen, ändern und löschen.

Beachten Sie folgende Punkte:

- Beim Erstellen eines Workloads in Unified Manager ist es nicht erforderlich, eine Storage-Effizienz-Richtlinie zuzuweisen.
- Sie können die Zuweisung einer Storage-Effizienzrichtlinie zu einem Workload nicht aufheben, nachdem eine Richtlinie zugewiesen ist.
- Wenn bei einem Workload einige Storage-Einstellungen angegeben sind, die in ONTAP Volumes wie Deduplizierung und Komprimierung angegeben sind, können diese Einstellungen durch die in der Storage-Effizienzrichtlinie festgelegten Einstellungen überschrieben werden. Nach Hinzufügen der Storage Workloads auf Unified Manager sind diese Einstellungen möglich.

Zeigen Sie Richtlinien Zur Storage-Effizienz An

Sie können die folgenden Methoden verwenden, um die Storage-Effizienzrichtlinien anzuzeigen, bevor Sie sie Storage-Workloads zuweisen. Diese API enthält alle systemdefinierten sowie vom Benutzer erstellten Richtlinien zur Storage-Effizienz und ruft die Attribute aller Storage-Effizienzrichtlinien ab. Wenn Sie eine bestimmte Storage-Effizienz-Richtlinie abfragen möchten, müssen Sie die eindeutige ID der Richtlinie eingeben, um deren Details abzurufen.

Kategorie	HTTP-Verb	Pfad

Anbieter von Storage-Lösungen	GET	`/storage-provider/storage-efficiency-policies`
		
		`/storage-provider/storage-efficiency-policies/{key}`

Fügen Sie Storage-Effizienzrichtlinien Hinzu

Mithilfe der folgenden Methode können Sie benutzerdefinierte Storage-Effizienzrichtlinien erstellen und diesen Ihren Storage Workloads zuweisen, wenn die systemdefinierten Richtlinien die Bereitstellungsanforderungen für Ihre Storage-Workloads nicht erfüllen. Geben Sie die Details der Storage-Effizienz-Richtlinie ein, die Sie erstellen möchten, als Eingabeparameter ein.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	`/storage-provider/storage-efficiency-policies`

Storage-Effizienzrichtlinien Löschen

Sie können eine bestimmte Storage-Effizienz-Richtlinie mit der folgenden Methode löschen: Sie können eine Richtlinie zur Storage-Effizienz nicht löschen, wenn sie einem Workload zugewiesen ist oder wenn sie die einzige verfügbare Richtlinie zur Storage-Effizienz ist. Sie müssen die eindeutige ID der Storage-Effizienz-Richtlinie als Eingabeparameter bereitstellen, um eine bestimmte Storage-Effizienz-Richtlinie zu löschen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	Löschen	`/storage-provider/storage-efficiency-policies/{key}`

Sie Können Die Storage-Effizienzrichtlinien Ändern

Sie können die folgende Methode verwenden, um eine Storage Efficiency Policy zu ändern und deren Eigenschaften zu aktualisieren. Sie können eine Storage-Effizienzrichtlinie, die systemdefiniert oder einem Workload zugewiesen ist, nicht ändern. Sie müssen die eindeutige ID der Storage-Effizienz-Richtlinie angeben, um eine bestimmte Storage-Effizienz-Richtlinie zu ändern. Zusätzlich müssen Sie die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert angeben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	`/storage-provider/storage-efficiency-policies/{key}`

Gängige API-Workflows für das Storage-Management

Die üblichen Workflows bieten Entwicklern von Client-Applikationen Beispiele dafür, wie Active IQ Unified Manager APIs von einer Client-Applikation aufgerufen werden können, um allgemeine Storage-Managementfunktionen auszuführen. Dieser Abschnitt enthält einige Beispiele-Workflows.

Die Workflows beschreiben einige der am häufigsten verwendeten Anwendungsfälle für das Storage-Management und geben Ihnen Beispielcodes an. Jede Aufgabe wird mit einem Workflow-Prozess beschrieben, der aus einem oder mehreren API-Aufrufen besteht.

Allgemeines zu den in den Workflows verwendeten API-Aufrufen

Sie können die Online-Dokumentationsseite von Ihrer Unified Manager Instanz aus einsehen, die alle Einzelheiten zu jedem REST-API-Aufruf enthält. Dieses Dokument wiederholt die Details der Online-Dokumentation nicht. Jeder API-Aufruf, der in den Workflow-Proben in diesem Dokument verwendet wird, enthält nur die Informationen, die Sie benötigen, um den Anruf auf der Dokumentationsseite zu finden. Nach dem Auffinden eines bestimmten API-Aufrufs können Sie die vollständigen Details des Anrufs überprüfen, einschließlich der Eingabeparameter, Ausgabeformate, HTTP-Statuscodes und des Aufruftyps.

Für jeden API-Aufruf in einem Workflow sind folgende Informationen enthalten, um den Anruf auf der Dokumentationsseite zu finden:

- Kategorie: Die API-Aufrufe werden auf der Dokumentationsseite in funktional verwandte Bereiche oder Kategorien organisiert. Um einen bestimmten API-Aufruf zu finden, blättern Sie zum unteren Seitenrand und klicken Sie auf die entsprechende API-Kategorie.
- HTTP-Verb (Aufruf): Das HTTP-Verb identifiziert die Aktion, die auf einer Ressource ausgeführt wird. Jeder API-Aufruf wird über ein einziges HTTP-Verb ausgeführt.
- Pfad: Der Pfad bestimmt die spezifische Ressource, auf die die Aktion als Teil der Durchführung eines Anrufs gilt. Der Pfadstring wird an die Core-URL angehängt, um die vollständige URL zur Identifizierung der Ressource zu bilden.

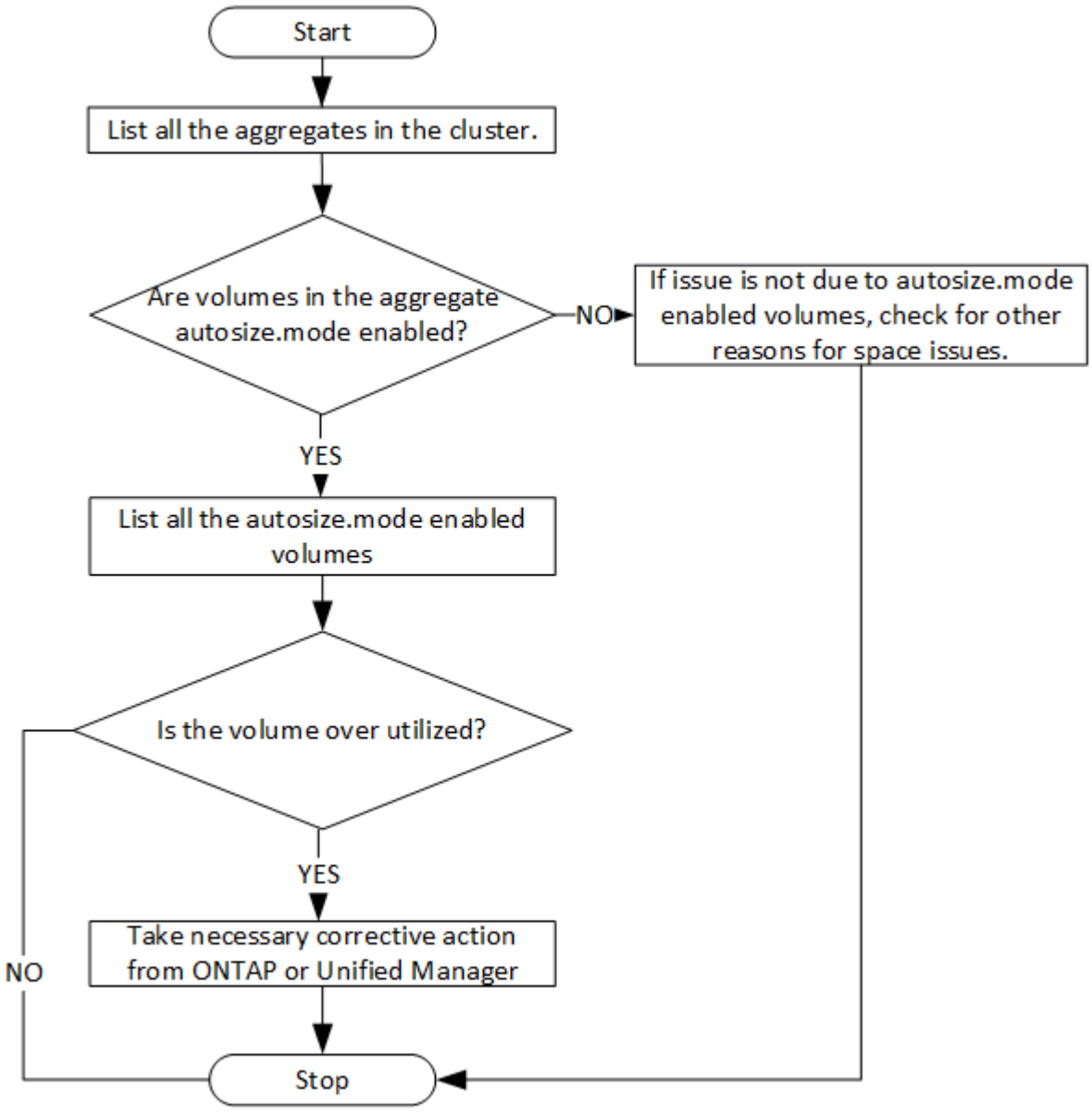
Bestimmen von Platzproblemen in Aggregaten mithilfe von APIs

Mit den Datacenter-APIs in Active IQ Unified Manager können Sie die Verfügbarkeit und Auslastung von Speicherplatz in Ihren Volumes überwachen. Sie können Platzprobleme in Ihrem Volume ermitteln und überlastete oder nicht ausgelastete Storage-Ressourcen identifizieren.

Die Datacenter-APIs für Aggregate rufen die relevanten Informationen über verfügbaren und belegten Speicherplatz sowie Einstellungen zur Speicherplatzersparnis ab. Sie können die abgerufenen Informationen auch anhand bestimmter Attribute filtern.

Eine Methode zur Bestimmung eines Speicherplatzmangels in Ihren Aggregaten ist es, festzustellen, ob in Ihrer Umgebung Volumes mit aktiviertem Autosize-Modus vorhanden sind. Anschließend sollten Sie ermitteln, welche Volumes zu viel genutzt werden, und Sie können Korrekturmaßnahmen vornehmen.

Das folgende Flussdiagramm zeigt den Prozess zum Abrufen von Informationen zu Volumes mit aktiviertem Autosize-Modus:



Es wird vorausgesetzt, dass die Cluster bereits im ONTAP erstellt und zu Unified Manager hinzugefügt wurden.

1. Beziehen Sie den Cluster-Schlüssel, es sei denn, Sie kennen den Wert:

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	`/datacenter/cluster/clusters`

2. Fragen Sie mit dem Cluster Key als Filterparameter die Aggregate auf diesem Cluster ab.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	`/datacenter/storage/aggregates`

3. Analysieren Sie als Antwort den Speicherplatznutzung der Aggregate und bestimmen Sie, welche Aggregate Platzprobleme aufweisen. Beziehen Sie für jedes Aggregat mit einem Platzproblem den Aggregatschlüssel aus der gleichen JSON-Ausgabe.
4. Filtern Sie mit jedem Aggregatschlüssel alle Volumes mit dem Wert für den Parameter autosize.Mode als `grow`.

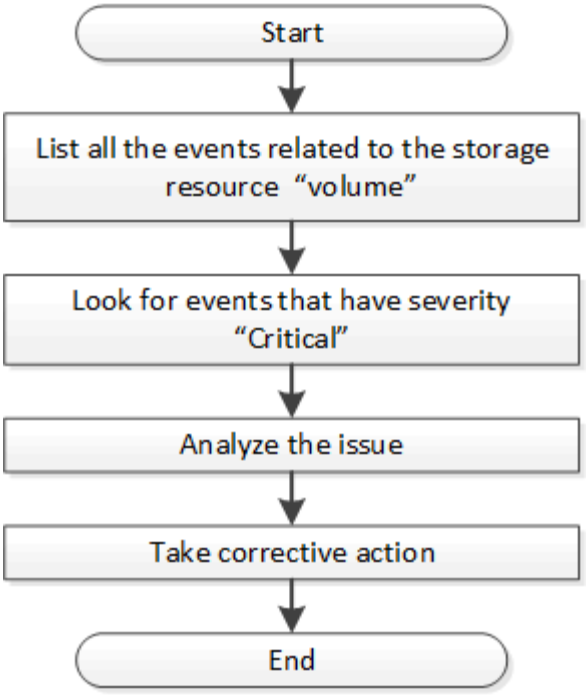
Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	`/datacenter/storage/volumes`

5. Analyse der zu stark ausgelasteten Volumes
6. Führen Sie alle erforderlichen Korrekturmaßnahmen durch, z. B. das Verschieben des Volumes über Aggregate, um die Platzprobleme im Volume zu beheben. Sie können diese Aktionen über die ONTAP- oder die Unified Manager-Weboberfläche ausführen.

Bestimmen von Problemen in Storage-Objekten mithilfe von Ereignis-APIs

Wenn ein Storage-Objekt im Datacenter einen Schwellenwert überschreitet, erhalten Sie eine Benachrichtigung über dieses Ereignis. Mithilfe dieser Benachrichtigung können Sie das Problem analysieren und mithilfe der APIs Korrekturmaßnahmen ergreifen `events`.

Dieser Workflow nimmt das Beispiel eines Volumes als Ressourcenobjekt ein. Sie können die APIs verwenden `events`, um die Liste der Ereignisse in Bezug auf ein Volume abzurufen, die kritischen Probleme für dieses Volume zu analysieren und dann Korrekturmaßnahmen einzuleiten, um das Problem zu beheben.



Führen Sie diese Schritte aus, um die Probleme in Ihrem Volumen zu ermitteln, bevor Sie Schritte zur Problembehebung Unternehmen.

Schritte

1. Analyse der kritischen Active IQ Unified Manager-Ereignisbenachrichtigungen für die Volumes in Ihrem Datacenter
2. Abfragen aller Ereignisse für die Volumes mithilfe der folgenden Parameter in der API /Management-Server/Events:
   `"resource_type": "volume"`
   `"severity": "critical"`

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	/Management-Server/Ereignisse

3. Anzeigen der Ausgabe und Analyse der Probleme in den spezifischen Volumes.
4. Die erforderlichen Aktionen können mithilfe der Unified Manager REST-APIs oder der Web-UI ausgeführt werden, um die Probleme zu beheben.

Fehlerbehebung bei ONTAP Volumes mithilfe von Gateway-APIs

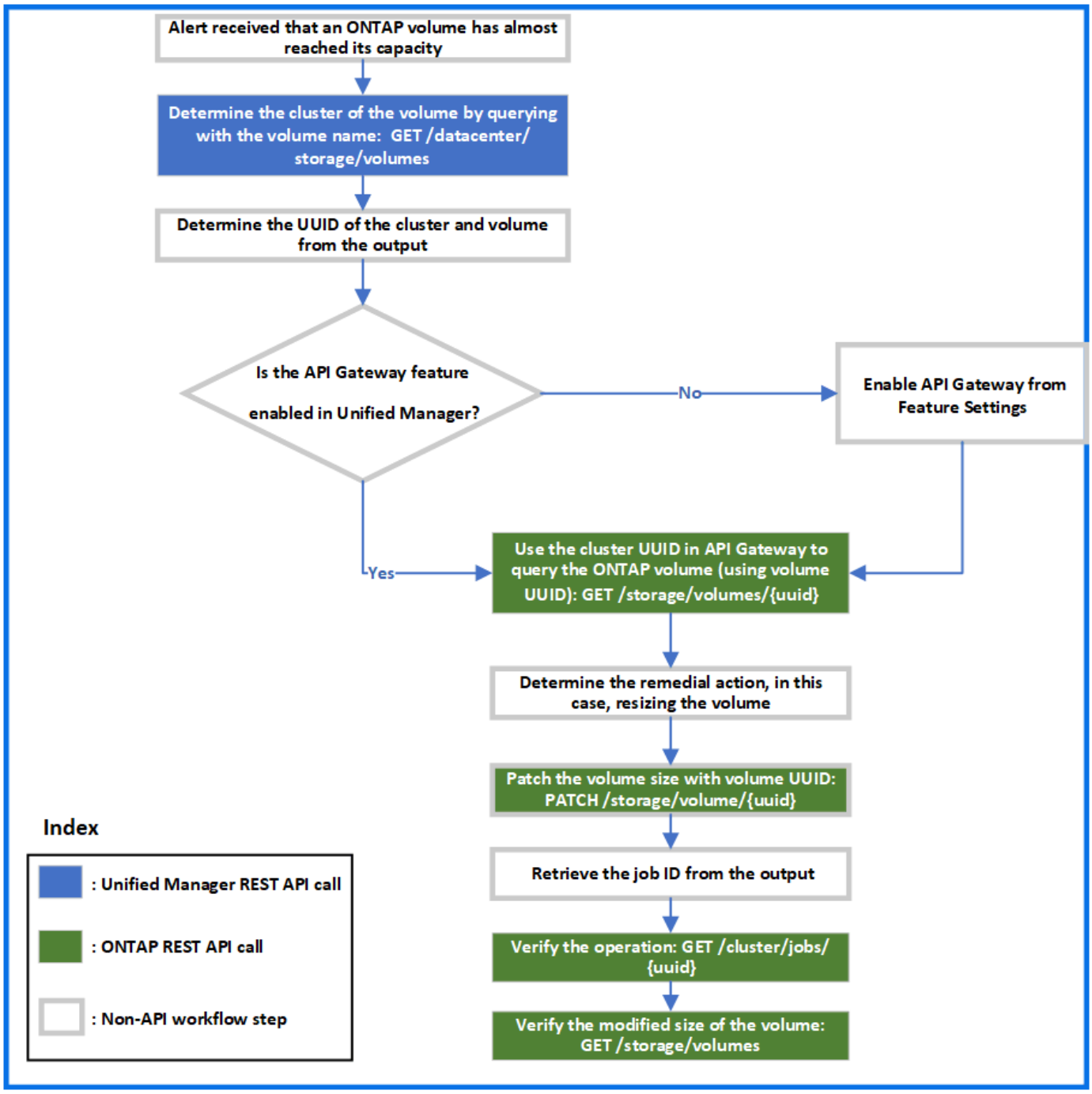
Die Gateway-APIs dienen als Gateway zum Aufrufen von ONTAP APIs, mit denen Informationen über Ihre ONTAP Storage-Objekte abgefragt und Korrekturmaßnahmen ergriffen werden, um die gemeldeten Probleme anzugehen.

Dieser Workflow greift auf einen Beispielfall zurück, in dem ein Ereignis angehoben wird, wenn ein ONTAP-Volume fast seine Kapazität erreicht. Im Workflow wird außerdem gezeigt, wie Sie das Problem beheben können, indem Sie eine Kombination aus Active IQ Unified Manager und ONTAP REST APIs aufrufen.

Bevor Sie die Workflow-Schritte ausführen, stellen Sie Folgendes sicher:

- Sie kennen die Gateway-APIs und deren Nutzung. Weitere Informationen finden Sie unter "Zugriff auf ONTAP-APIs über Proxy-Zugriff".
- Sie sind sich der Nutzung von ONTAP REST-APIs bewusst. Informationen zur Verwendung von ONTAP REST-APIs finden Sie unter "Dokumentation zur ONTAP-Automatisierung".
- Sie sind ein Anwendungsadministrator.
- Das Cluster, auf dem Sie die REST-API-Vorgänge ausführen möchten, wird von ONTAP 9.5 oder höher unterstützt, und das Cluster wird Unified Manager über HTTPS hinzugefügt.

Das folgende Diagramm zeigt jeden Schritt im Workflow zur Fehlerbehebung bei der Verwendung von ONTAP Volume-Kapazität.



Der Workflow umfasst die Anrufinungspunkte sowohl von Unified Manager als auch von ONTAP REST-APIs.

1. Notieren Sie den Volume-Namen aus dem Ereignis, um die Kapazitätsauslastung des Volume zu benachrichtigen.
2. Abfragen Sie das Volume durch Ausführen der folgenden Unified Manager-API, indem Sie den Volume-Namen als Wert im Name-Parameter verwenden.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	`/datacenter/storage/volumes`

3. Abrufen der Cluster-UUID und Volume-UUID von der Ausgabe.
4. Navigieren Sie in der Web-UI von Unified Manager zu **Allgemein** > **Funktionseinstellungen** > **API Gateway**, um zu überprüfen, ob die API-Gateway-Funktion aktiviert ist. Sofern sie nicht aktiviert ist, können Sie die APIs aus der Kategorie Gateway nicht aufrufen. Aktivieren Sie die Funktion, wenn sie deaktiviert ist.
5. Verwenden Sie die Cluster-UUID, um die ONTAP-API über das API-Gateway auszuführen`/storage/volumes/{uuid}`. Die Abfrage gibt die Volume-Details zurück, wenn die Volume-UUID als API-Parameter übergeben wird.

   Zur Ausführung der ONTAP-APIs über das API-Gateway werden die Anmeldeinformationen für den Unified Manager zur internen Authentifizierung übergeben. Sie müssen keinen zusätzlichen Authentifizierungsschritt für den individuellen Cluster-Zugriff ausführen.

Kategorie	HTTP-Verb	Pfad
Unified Manager: Das Gateway ONTAP: Storage	GET	Gateway-API: `/gateways/{uuid}/{path}` ONTAP-API: `/storage/volumes/{uuid}`

> In /Gateways/{UUID}/{Path} muss der Wert für {UUID} durch die Cluster-UUID ersetzt werden, für die der REST-Vorgang ausgeführt werden soll. {path} muss durch die ONTAP REST-URL /Storage/Volumes/{UUID} ersetzt werden.

Die angehängte URL lautet: `/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

Beim Ausführen des GET-Vorgangs lautet die generierte URL: `GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes/{volume_uuid}`

Befehl zum Curl-Beispiel

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

6. Bestimmen Sie von der Ausgabe die zu ergriffende Größe, Nutzung und Abhilfemaßnahme. In diesem Workflow ist die Abhilfemaßnahme die Größe des Volumens.
7. Verwenden Sie die Cluster-UUID, und führen Sie die folgende ONTAP-API über das API-Gateway aus, um die Größe des Volumes zu ändern. Informationen zu den Eingabeparametern für das Gateway und ONTAP APIs finden Sie in Schritt 5.

Kategorie	HTTP-Verb	Pfad

Unified Manager: Das Gateway
 	
ONTAP: Storage
	PATCH	Gateway-API:
		`/gateways/{uuid}/{path}`
		
		ONTAP-API:
		`/storage/volumes/{uuid}`

Zusammen mit der Cluster-UUID und der Volume-UUID müssen Sie einen Wert für den Parameter „Größe“ für die Größenanpassung des Volume eingeben. Stellen Sie sicher, dass Sie den Wert *in Byte* eingeben. Wenn Sie beispielsweise die Größe eines Volumes von 100 GB auf 120 GB erhöhen möchten, geben Sie am Ende der Abfrage den Wert für die Parametergröße ein: `-d {\"size\": 128849018880}"`

Befehl zum Curl-Beispiel

```
curl -X PATCH "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7" -H
    "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
    {\"size\": 128849018880}"
```

Die JSON-Ausgabe gibt eine Job-UUID zurück.

8. Überprüfen Sie, ob der Job erfolgreich ausgeführt wurde, indem Sie die Job-UUID verwenden. Verwenden Sie die Cluster-UUID und Job-UUID, um die folgende ONTAP-API über das API-Gateway auszuführen. Informationen zu den Eingabeparametern für das Gateway und ONTAP APIs finden Sie in Schritt 5.

Kategorie	HTTP-Verb	Pfad

Unified Manager: Das Gateway
 	
ONTAP: Cluster
	GET	Gateway-API:
		`/gateways/{uuid}/{path}`
		
		ONTAP-API:
		`/cluster/jobs/{uuid}`

Die zurückgegebenen HTTP-Codes entsprechen den HTTP-Statuscodes der ONTAP REST-API.

9. Führen Sie die folgende ONTAP API aus, um die Details des Volumes mit der Größe zu abfragen. Informationen zu den Eingabeparametern für das Gateway und ONTAP APIs finden Sie in Schritt 5.

Kategorie	HTTP-Verb	Pfad

Unified Manager: Das Gateway
 	
ONTAP: Storage
	GET	Gateway-API:
		`/gateways/{uuid}/{path}`
		
		ONTAP-API:
		`/storage/volumes/{uuid}`

Die Ausgabe zeigt eine erhöhte Lautstärke von 120 GB an.

API-Workflows für das Workload-Management

Mithilfe von Active IQ Unified Manager können Storage-Workloads (LUNs, NFS-Dateifreigaben und CIFS-Freigaben) bereitgestellt und geändert werden. Die Bereitstellung besteht aus mehreren Schritten: Von der Erstellung der Storage Virtual Machine (SVM) bis zur Anwendung von Performance Service Level- und Storage-Effizienz-Richtlinien auf die Storage Workloads. Das Ändern von Workloads besteht aus den Schritten zum Ändern spezifischer Parameter und zum Aktivieren zusätzlicher Funktionen für diese.

Die folgenden Workflows werden beschrieben:

- Workflow für die Bereitstellung von Storage Virtual Machines (SVMs) in Unified Manager

  Dieser Workflow muss vor der Bereitstellung von LUNs oder File Shares auf Unified Manager durchgeführt werden.

- Bereitstellen von Dateifreigaben:
- Bereitstellung von LUNs:
- Ändern von LUNs und Dateifreigaben (mit dem Beispiel für die Aktualisierung des Parameters für Performance-Service-Level für die Storage-Workloads)
- Ändern einer NFS-Dateifreigabe zur Unterstützung des CIFS-Protokolls
- Änderung von Workloads für das Upgrade von QoS auf AQoS

Stellen Sie für jeden Bereitstellungs-Workflow (LUN und Dateifreigaben) sicher, dass Sie den Workflow zur Überprüfung der SVMs auf den Clustern abgeschlossen haben müssen.

Sie müssen auch die Empfehlungen und Einschränkungen lesen, bevor Sie jede API in den Workflows verwenden. Die relevanten Details der APIs sind in ihren einzelnen Abschnitten in den verwandten Konzepten und Referenzen aufgeführt.

Überprüfung von SVMs auf Clustern mithilfe von APIs

Bevor Sie Dateifreigaben oder LUNs bereitstellen, müssen Sie überprüfen, ob auf den Clustern Storage Virtual Machines (SVMs) erstellt wurden.

Beim Workflow wird vorausgesetzt, dass ONTAP Cluster zu Unified Manager hinzugefügt wurden und der Clusterschlüssel erhalten wurde. Auf Clustern sollten die erforderlichen Lizenzen zur Bereitstellung von LUNs und File Shares vorhanden sein.

1. Überprüfen, ob auf dem Cluster eine SVM erstellt wurde.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	`/datacenter/svm/svms` `/datacenter/svm/svms/{key}`

Stichprobe

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Erstellen Sie die SVM, falls der SVM-Schlüssel nicht zurückgegeben wird. Zum Erstellen der SVMs benötigen Sie den Cluster-Schlüssel, für den Sie die SVM bereitstellen. Sie müssen außerdem den SVM-Namen angeben. Auszuführende Schritte:

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	`/datacenter/cluster/clusters` `/datacenter/cluster/clusters/{key}`

Abrufen des Cluster-Schlüssels.

Stichprobe

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

3. Holen Sie den Cluster-Schlüssel von der Ausgabe, und verwenden Sie ihn als Input für die Erstellung der SVM.

Vergewissern Sie sich bei der Erstellung der SVM, dass sie alle Protokolle unterstützt, die für die Bereitstellung von LUNs und File Shares benötigt werden, zum Beispiel CIFS, NFS, FCP Und iSCSI. Die Bereitstellungs-Workflows können fehlschlagen, wenn die SVM die erforderlichen Services nicht unterstützt. Es wird empfohlen, auch die Services für die jeweiligen Workload-Typen auf der SVM zu aktivieren.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	POST	`/datacenter/svm/svms`

Stichprobe

Geben Sie die Details des SVM-Objekts als Eingabeparameter ein.

```
curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Content-Type: application/json" -H "Authorization:
Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": {},
\"key\": \"1cd8a442-86d1,type=objecttype,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\",
\"name\": \"cluster2\", \"uuid\": \"02c9e252-41be-11e9-81d5-
00a0986138f7\" } ],
\"cifs\": { \"ad_domain\": { \"fqdn\": \"string\", \"password\":
\"string\",
\"user\": \"string\" }, \"enabled\": true, \"name\": \"CIFS1\" },
\"cluster\": { \"key\": \"1cd8a442-86d1-11e0-ae1c-
123478563412,type=object type,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\" },
\"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ],
\"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] },
\"fcp\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true,
\"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" },
\"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\":
\"dataLif1\" } ], \"ipspace\": { \"name\": \"exchange\" },
\"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\",
\"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\",
\"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ]
},
\"name\": \"svm1\", \"nfs\": { \"enabled\": true },
\"nis\": { \"domain\": \"string\", \"enabled\": true,
\"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true },
\"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\",
\"netmask\": \"24\" }, \"gateway\": \"string\" } ],
\"snapshot_policy\": { \"name\": \"default\" },
\"state\": \"running\", \"subtype\": \"default\"}"
```

Die JSON-Ausgabe zeigt einen Objektschlüssel an, mit dem Sie die von Ihnen erstellte SVM überprüfen

können.

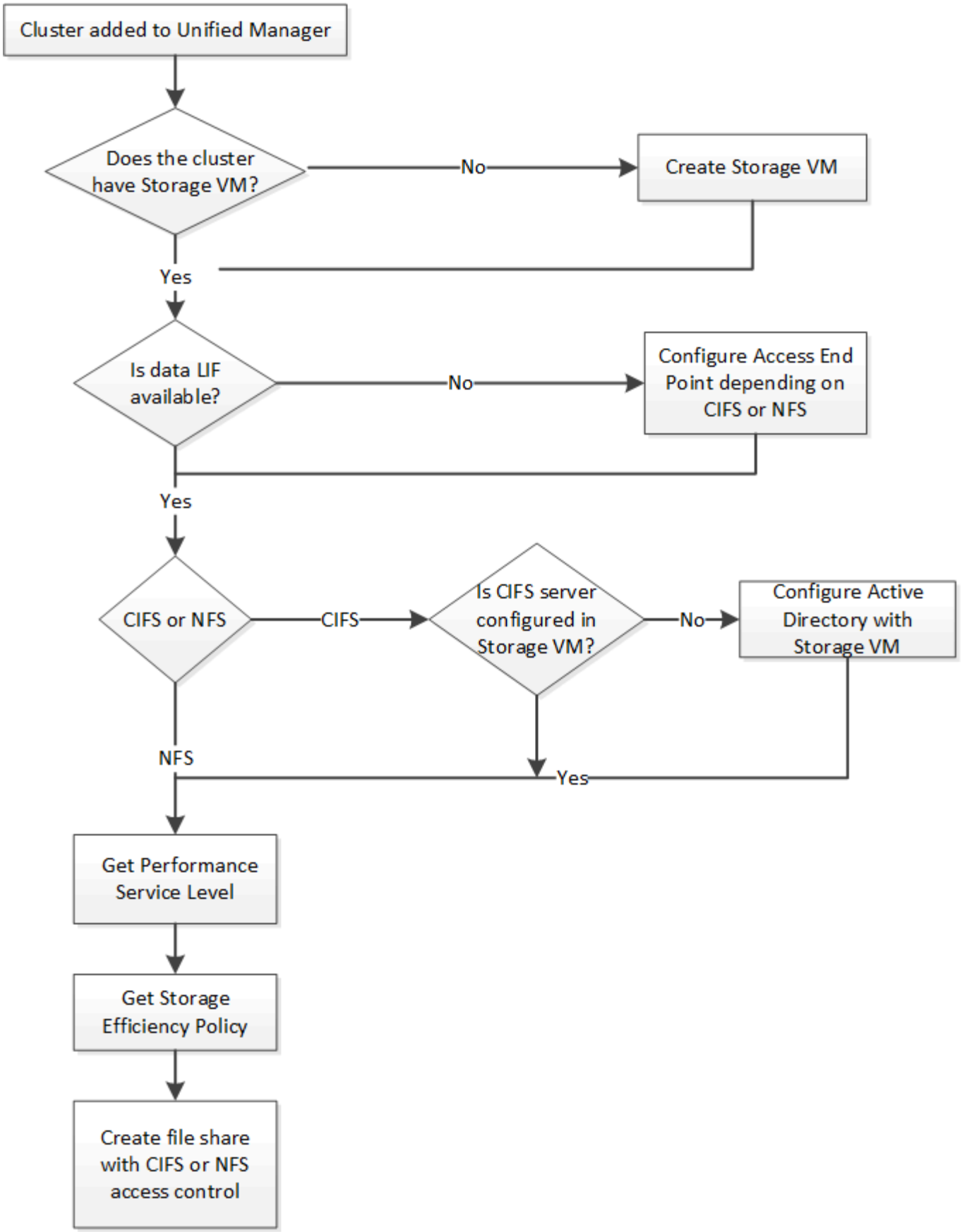
4. Überprüfen Sie die SVM-Erstellung mithilfe des Jobobjektschlüssels für die Abfrage. Wenn die SVM erfolgreich erstellt wurde, wird der SVM-Schlüssel in der Antwort zurückgegeben.

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	`/management-server/jobs/{key}`

Bereitstellen von CIFS- und NFS-Dateifreigaben mithilfe von APIs

Sie können CIFS-Freigaben und NFS-Dateifreigaben auf Ihren Storage Virtual Machines (SVMs) mithilfe der BereitstellungsAPIs, die als Teil von Active IQ Unified Manager bereitgestellt werden, bereitstellen. Dieser Bereitstellungs-Workflow zeigt die Schritte zum Abrufen der Schlüssel der SVMs, Performance Service Levels und Storage-Effizienz-Richtlinien, bevor die Dateifreigaben erstellt werden.

Das folgende Diagramm veranschaulicht die einzelnen Schritte eines Workflows zur Dateifreigabe. Das System umfasst die Bereitstellung von CIFS-Freigaben und NFS-Dateifreigaben.


Cluster added to Unified Manager
Does the cluster have Storage VM?
No
Create Storage VM
Yes
Is data LIF available?
No
Configure Access End Point depending on CIFS or NFS
Yes
CIFS or NFS
CIFS
Is CIFS server configured in Storage VM?
No
Configure Active Directory with Storage VM
NFS
Yes
Get Performance Service Level
Get Storage Efficiency Policy
Create file share with CIFS or NFS access control

Stellen Sie Folgendes sicher:

- Dem Unified Manager wurden ONTAP Cluster hinzugefügt, und der Clusterschlüssel ist abgerufen.
- Auf den Clustern wurden SVMs erstellt.
- Die SVMs unterstützen CIFS- und NFS-Services. Dateifreigaben können möglicherweise fehlschlagen, wenn die SVMs die erforderlichen Services nicht unterstützen.
- Der FCP Port ist online für die Port-Bereitstellung.

1. Ermitteln, ob Daten-LIFs oder Zugriffendpunkte auf der SVM verfügbar sind, auf der Sie die CIFS-Freigabe erstellen möchten. Rufen Sie die Liste der verfügbaren Zugriffendpunkte auf der SVM auf:

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/access-endpoints` `/storage-provider/access-endpoints/{key}`

Stichprobe

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Wenn Ihr Zugriffendpunkt in der Liste verfügbar ist, erhalten Sie den Schlüssel für den Access-Endpunkt, sonst erstellen Sie den Access-Endpunkt.

Stellen Sie sicher, dass Sie Zugriffendpunkte erstellen, auf denen das CIFS-Protokoll aktiviert ist. Die Bereitstellung von CIFS-Freigaben schlägt fehl, es sei denn, Sie haben einen Zugriffendpunkt erstellt, auf dem das CIFS-Protokoll aktiviert ist.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	`/storage-provider/access-endpoints`

Stichprobe

Sie müssen die Details des Zugriffendpunkts, den Sie erstellen möchten, als Eingabeparameter eingeben.

```
curl -X POST "https://<hostname>/api/storage-provider/access-endpoints"
-H "accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
{ \"data_protocols\": \"nfs\",
\"fileshare\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=volume,uuid=f3063d27-2c71-44e5-9a69-a3927c19c8fc\" },
\"gateway\": \"10.132.72.12\",
\"ip\": { \"address\": \"10.162.83.26\",
\"ha_address\": \"10.142.83.26\",
\"netmask\": \"255.255.0.0\" },
\"lun\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=lun,uuid=d208cc7d-80a3-4755-93d4-5db2c38f55a6\" },
\"mtu\": 15000, \"name\": \"aep1\",
\"svm\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a178d39e12:type=vserver,uuid=1d1c3198-fc57-11e8-99ca-00a098d38e12\" },
\"vlan\": 10}"
```

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie den von Ihnen erstellten Zugriffspendpunkt überprüfen können.

3. Überprüfen Sie den Zugriffendpunkt:

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	`/management-server/jobs/{key}`

4. Bestimmen Sie, ob Sie eine CIFS-Freigabe oder eine NFS-Dateifreigabe erstellen müssen. Führen Sie zum Erstellen von CIFS-Freigaben die folgenden Teilschritte aus:

   a. Legen Sie fest, ob der CIFS-Server für Ihre SVM konfiguriert ist, und ermitteln Sie, ob eine Active Directory-Zuordnung auf der SVM erstellt wird.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/active-directories-mappings`

   b. Wenn die Active Directory-Zuordnung erstellt wird, ziehen Sie den Schlüssel, sonst erstellen Sie die Active Directory-Zuordnung auf der SVM.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	`/storage-provider/active-directories-mappings`

Stichprobe

Sie müssen die Details zum Erstellen der Active Directory-Zuordnung als Eingabeparameter eingeben.

```
curl -X POST "https://<hostname>/api/storage-provider/active-
directories-mappings" -H "accept: application/json" -H "Content-Type:
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
{ \"_links\": {},
\"dns\": \"10.000.000.000\",
\"domain\": \"example.com\",
\"password\": \"string\",
\"svm\": { \"key\": \"9f4ddea-e395-11e9-b660-
005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },
\"username\": \"string\"}"
```

+
Dies ist ein synchroner Anruf, und Sie können die Erstellung der Active Directory-Zuordnung in der Ausgabe überprüfen. Im Fehlerfall wird die Fehlermeldung angezeigt, damit Sie die Anfrage beheben und erneut ausführen können.

5. Den SVM-Schlüssel für die SVM erhalten, auf der Sie die CIFS-Freigabe oder die NFS-Dateifreigabe erstellen möchten, wie im Workflow-Thema *ÜberprüfungsSVMs auf Clustern* beschrieben.
6. Erhalten Sie den Schlüssel für den Performance Service Level, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie den Eingabeparameter auf `true` einstellen `system_defined`. Holen Sie in der Ausgabe den Schlüssel des Performance Service Level, den Sie auf die Dateifreigabe anwenden möchten.

7. Sie können optional den Richtlinienschlüssel für die Storage-Effizienz für die Storage-Effizienzrichtlinie abrufen, den Sie auf die Dateifreigabe anwenden möchten, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/storage-efficiency-policies`

8. Erstellen Sie die Dateifreigabe. Sie können eine Dateifreigabe erstellen, die sowohl CIFS als auch NFS unterstützt, indem Sie die Zugriffssteuerungsliste und die Exportrichtlinie angeben. Die folgenden

Teilschritte enthalten Informationen, wenn Sie eine Dateifreigabe erstellen möchten, um nur eines der Protokolle auf dem Volume zu unterstützen. Sie können auch eine NFS-Dateifreigabe aktualisieren, um die Zugriffssteuerungsliste einzuschließen, nachdem Sie die NFS-Freigabe erstellt haben. Informationen hierzu finden Sie im Thema „*Modifizieren von Storage Workloads*“.

a. Wenn Sie nur eine CIFS-Freigabe erstellen möchten, sammeln Sie Informationen über die Zugriffssteuerungsliste (Access Control List, ACL). Geben Sie für die Erstellung der CIFS-Freigabe gültige Werte für die folgenden Eingabeparameter an. Für jede Benutzergruppe, die Sie zuweisen, wird bei der Bereitstellung einer CIFS/SMB-Freigabe eine ACL erstellt. Auf der Grundlage der von Ihnen für die ACL- und Active Directory-Zuordnung eingegebenen Werte werden die Zugriffssteuerung und Zuordnung für die CIFS-Freigabe bei ihrer Erstellung festgelegt.

   Ein Curl-Befehl mit Beispielwerten

   ```
   {
     "access_control": {
       "acl": [
         {
           "permission": "read",
           "user_or_group": "everyone"
         }
       ],
       "active_directory_mapping": {
         "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
       },
   ```

b. Um nur eine NFS-Dateifreigabe zu erstellen, sammeln Sie die Informationen über die Exportrichtlinie. Geben Sie für die Erstellung der NFS-Dateifreigabe gültige Werte für die folgenden Eingabeparameter an. Auf Grundlage Ihrer Werte ist die Exportrichtlinie mit der NFS-Dateifreigabe verbunden, wenn sie erstellt wird.

   > Während Sie die NFS-Freigabe bereitstellen, können Sie entweder eine Exportrichtlinie erstellen, indem Sie alle erforderlichen Werte angeben oder den Schlüssel für die Exportrichtlinie angeben und eine vorhandene Exportrichtlinie wiederverwenden. Wenn Sie eine Exportrichtlinie für die Storage-VM wiederverwenden möchten, müssen Sie den Schlüssel für die Exportrichtlinie hinzufügen. Sofern Sie den Schlüssel nicht kennen, können Sie den Schlüssel für die Exportrichtlinie mithilfe der API abrufen `/datacenter/protocols/nfs/export-policies`. Zum Erstellen einer neuen Richtlinie müssen Sie die Regeln eingeben, die im folgenden Beispiel angezeigt werden. Bei den eingegebenen Regeln versucht die API, nach einer vorhandenen Exportrichtlinie zu suchen, indem sie den Host, die Storage-VM und die Regeln anpasst. Wenn eine Exportrichtlinie vorhanden ist, wird sie verwendet. Andernfalls wird eine neue Exportrichtlinie erstellt.

   Ein Curl-Befehl mit Beispielwerten

```
"export_policy": {
      "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
      "name_tag": "ExportPolicyNameTag",
      "rules": [
        {
          "clients": [
            {
              "match": "0.0.0.0/0"
            }
```

Geben Sie nach der Konfiguration der Zugriffssteuerungsliste und der Exportrichtlinie die gültigen Werte für die obligatorischen Eingabeparameter für CIFS- und NFS-Dateifreigaben ein:

Die Richtlinie zur Storage-Effizienz ist ein optionaler Parameter zum Erstellen von Dateifreigaben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	`/storage-provider/file-shares`

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie die von Ihnen erstellte Dateifreigabe überprüfen können. . Überprüfen Sie die Erstellung der Dateifreigabe, indem Sie den bei der Abfrage des Jobs zurückgegebenen Job-Objektschlüssel verwenden:

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	`/management-server/jobs/{key}`

Am Ende der Antwort sehen Sie den Schlüssel der erstellten Dateifreigabe.

```
    ],
    "job_results": [
        {
            "name": "fileshareKey",
            "value": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
        }
    ],
    "_links": {
        "self": {
            "href": "/api/management-server/jobs/06a6148bf9e862df:-
2611856e:16e8d47e722:-7f87"
        }
    }
}
```

1. Überprüfen Sie die Erstellung der Dateifreigabe, indem Sie die folgende API mit dem zurückgegebenen Schlüssel ausführen:

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/file-shares/{key}`

Beispiel JSON-Ausgabe

Sie sehen, dass die POST-Methode von `/storage-provider/file-shares` intern alle für jede der Funktionen erforderlichen APIs aufruft und das Objekt erstellt. Beispielsweise wird die API aufgerufen, um der `/storage-provider/performance-service-levels/` Dateifreigabe den Performance Service Level zuzuweisen.

```
{
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
    "name": "FileShare_377",
    "cluster": {
        "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
        "name": "AFFA300-206-68-70-72-74",
        "_links": {
            "self": {
                "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-
00a098dcc959"
            }
```

```
        }
    },
    "svm": {
        "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
        "name": "RRT_ritu_vs1",
        "_links": {
            "self": {
                "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-
8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-
00a098dcc959"
            }
        }
    },
    "assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
        }
    },
    "recommended_performance_service_level": {
        "key": null,
        "name": "Idle",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
    },
    "space": {
        "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
        "key": null,
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
```

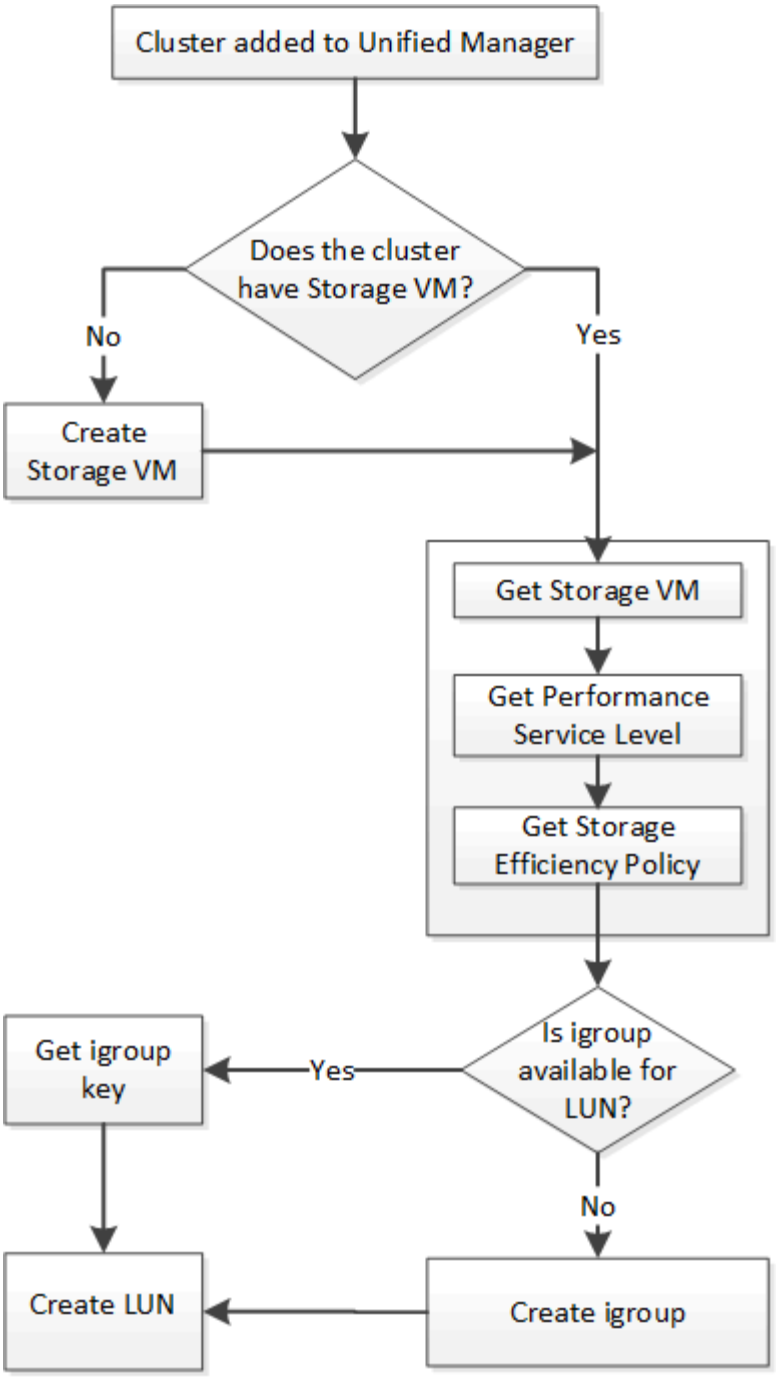
```
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 1,
                    "protocols": [
                        "nfs3",
                        "nfs4"
                    ],
                    "ro_rule": [
                        "sys"
                    ],
                    "rw_rule": [
                        "sys"
                    ],
                    "superuser": [
                        "none"
                    ]
                },
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 2,
                    "protocols": [
                        "cifs"
                    ],
                    "ro_rule": [
                        "ntlm"
                    ],
                    "rw_rule": [
```

```
                        "ntlm"
                    ],
                    "superuser": [
                        "none"
                    ]
                }
            ],
            "_links": {
                "self": {
                    "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
                }
            }
        }
    },
    "_links": {
        "self": {
            "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
        }
    }
}
```

Bereitstellung von LUNs mithilfe von APIs

Sie können LUNs auf Ihren Storage Virtual Machines (SVMs) bereitstellen, indem Sie die BereitstellungsAPIs verwenden, die als Teil von Active IQ Unified Manager zur Verfügung gestellt werden. Dieser Workflow zur Bereitstellung umfasst die Schritte zum Abrufen der Schlüssel der SVMs, Performance Service Levels und Storage-Effizienz-Richtlinien, bevor die LUN erstellt wird.

Im folgenden Diagramm sind die Schritte in einem Workflow zur Bereitstellung von LUNs dargestellt.



Bei diesem Workflow wird vorausgesetzt, dass die ONTAP Cluster zu Unified Manager hinzugefügt wurden und der Clusterschlüssel abgerufen wurde. Beim Workflow wird auch davon ausgegangen, dass die SVMs bereits auf den Clustern erstellt wurden.

1. Den SVM-Schlüssel für die SVM erhalten, auf der Sie die LUN erstellen möchten, wie im Workflow-Thema „*Verifying SVMs on Cluster*“ beschrieben.
2. Erhalten Sie den Schlüssel für den Performance Service Level, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie den Eingabeparameter auf `true` einstellen `system_defined`. Holen Sie von der Ausgabe den Schlüssel des Performance Service Level, den Sie auf der LUN anwenden möchten.

3. Optional können Sie den Richtlinienschlüssel für die Storage-Effizienz für die Storage-Effizienzrichtlinie abrufen, die Sie auf der LUN anwenden möchten, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/storage-efficiency-policies`

4. Legen Sie fest, ob Initiatorgruppen (Initiatorgruppen) erstellt wurden, um Ihnen den Zugriff auf das LUN-Ziel zu gewähren, das Sie erstellen möchten.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	`/datacenter/protocols/san/igroups` `/datacenter/protocols/san/igroups/{key}`

Sie müssen den Parameterwert für die SVM eingeben, für die die Initiatorgruppe über einen autorisierten Zugriff verfügt. Wenn Sie außerdem eine bestimmte Initiatorgruppe abfragen möchten, geben Sie den Initiatorgruppennamen (Schlüssel) als Eingabeparameter ein.

5. Wenn Sie in der Ausgabe die Initiatorgruppe finden, der Sie Zugriff auf gewähren möchten, holen Sie den Schlüssel ein. Erstellen Sie andernfalls die Initiatorgruppe.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	POST	`/datacenter/protocols/san/igroups`

Sie müssen die Details der Initiatorgruppe, die Sie erstellen möchten, als Eingabeparameter eingeben. Dies ist ein synchroner Anruf, und Sie können die igroup-Erstellung in der Ausgabe überprüfen. Im Fehlerfall wird eine Meldung angezeigt, mit der Sie Fehler beheben und die API erneut ausführen können.

6. Erstellen Sie das LUN.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	`/storage-provider/luns`

Stellen Sie zum Erstellen der LUN sicher, dass Sie die abgerufenen Werte als obligatorische Eingabeparameter hinzugefügt haben.

Die Richtlinie zur Storage-Effizienz ist ein optionaler Parameter zum Erstellen von LUNs.

Stichprobe

Sie müssen als Eingabeparameter alle Details der LUN eingeben, die Sie erstellen möchten.

Die JSON-Ausgabe zeigt einen Objektschlüssel an, mit dem Sie die von Ihnen erstellte LUN überprüfen können.

7. Überprüfen Sie die LUN-Erstellung, indem Sie den bei der Abfrage des Jobs zurückgegebenen Job-Objektschlüssel verwenden:

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	`/management-server/jobs/{key}`

Am Ende der Antwort wird der Schlüssel der erstellten LUN angezeigt.

8. Überprüfen Sie die Erstellung der LUN, indem Sie die folgende API mit dem zurückgegebenen Schlüssel ausführen:

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/luns/{key}`

Beispiel JSON-Ausgabe

Sie sehen, dass die POST-Methode von `/storage-provider/luns` intern alle für jede der Funktionen erforderlichen APIs aufruft und das Objekt erstellt. Er ruft beispielsweise die `/storage-provider/performance-service-levels/` API zur Zuweisung des Performance Service Levels auf der LUN auf.

== Fehlerbehebungsschritte für Fehler bei der LUN-Erstellung oder -Zuordnung

Beim Abschließen dieses Workflows wird möglicherweise immer noch ein Fehler bei der LUN-Erstellung angezeigt. Selbst wenn die LUN erfolgreich erstellt wird, schlägt die LUN-Zuordnung mit der Initiatorgruppe möglicherweise fehl, da eine SAN-LIF nicht verfügbar ist oder der Zugriffskpunkt auf dem Node, auf dem Sie die LUN erstellen, nicht verfügbar ist. Bei einem Ausfall wird die folgende Meldung angezeigt:

```
The nodes <node_name> and <partner_node_name> have no LIFs configured with
the iSCSI or FCP protocol for Vserver <server_name>. Use the access-
endpoints API to create a LIF for the LUN.
```

Befolgen Sie diese Schritte zur Fehlerbehebung, um diesen Fehler zu umgehen.

1. Erstellen Sie einen Zugriffssendpunkt, der DAS ISCSI-/FCP-Protokoll auf der SVM unterstützt, auf der Sie die LUN erstellt haben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	`/storage-provider/access-endpoints`

Stichprobe

Sie müssen die Details des Zugriffendpunkts, den Sie erstellen möchten, als Eingabeparameter eingeben.

> Stellen Sie sicher, dass Sie im Eingabeparameter die Adresse hinzugefügt haben, um den Home-Node der LUN und die ha_address anzugeben, um den Partner-Node des Home-Node anzugeben. Bei diesem Vorgang werden sowohl auf dem Home-Node als auch auf dem Partner-Node Zugriffspendpunkte erstellt.

2. Fragen Sie den Job mit dem in der JSON-Ausgabe zurückgegebenen Job-Objektschlüssel ab, um zu überprüfen, ob er erfolgreich ausgeführt wurde, um die Zugriffendpunkte auf der SVM hinzuzufügen und dass die iSCSI/FCP-Dienste auf der SVM aktiviert wurden.

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	`/management-server/jobs/{key}`

Beispiel JSON-Ausgabe

Am Ende der Ausgabe sehen Sie den Schlüssel der erstellten Access-Endpunkte. In der folgenden Ausgabe zeigt der Wert "Name": "AccessEndpointKey" den auf dem Home-Knoten der LUN erstellten Zugriffspendpunkt an, für den der Schlüssel 9c964258-14ef-11ea-9ve2-00a098e32c28 ist. Der Wert "Name": "AccessEndpointHAKey" gibt den Zugriffspendpunkt an, der auf dem Partner-Knoten des Home-Knotens erstellt wurde, für den der Schlüssel 9d347006-14ef-11ea-8760-00a098e3215f ist.

3. Ändern Sie die LUN, um die Initiatorgruppenzuordnung zu aktualisieren. Weitere Informationen zur Änderung von Workflows finden Sie unter „`MModifizieren von Storage-Workloads`“.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	`/storage-provider/lun/{key}`

Geben Sie in der Eingabe den Initiatorgruppenschlüssel an, mit dem Sie die LUN-Zuordnung aktualisieren

möchten, zusammen mit dem LUN-Schlüssel.

Stichprobe

In der JSON-Ausgabe wird ein Objektschlüssel angezeigt, mit dem Sie überprüfen können, ob die Zuordnung erfolgreich ist.

4. Überprüfen Sie die LUN-Zuordnung, indem Sie mit dem LUN-Schlüssel abfragen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/luns/{key}`

Beispiel JSON-Ausgabe

In der Ausgabe sieht man, dass die LUN erfolgreich mit der igroup zugeordnet wurde (Schlüssel d19ec2fa-fec7-11e8-b23d-00a098e32c28), mit der sie ursprünglich bereitgestellt wurde.

Ändern von Storage-Workloads mithilfe von APIs

Das Ändern von Storage-Workloads besteht aus der Aktualisierung von LUNs oder File Shares mit fehlenden Parametern oder der Änderung der vorhandenen Parameter.

Dieser Workflow erläutert beispielhaft die Aktualisierung von Performance Service Levels für LUNs und File Shares.

Beim Workflow wird vorausgesetzt, dass die LUN oder Dateifreigabe mit Performance Service-Leveln bereitgestellt wurde.

Ändern von Dateifreigaben

Während Sie eine Dateifreigabe ändern, können Sie die folgenden Parameter aktualisieren:

- Kapazität oder Größe.
- „Online“- oder „Offline“-Einstellung.
- Storage-Effizienzrichtlinie.
- Performance Service Level:
- Einstellungen für die Zugriffssteuerungsliste (Access Control List, ACL).
- Einstellungen für Exportrichtlinien. Sie können auch die Parameter der Exportrichtlinie löschen und die Standardregeln für den (leeren) Export auf der Dateifreigabe zurücksetzen.

Während einer einzelnen API-Ausführung können Sie nur einen Parameter aktualisieren.

Dieses Verfahren beschreibt das Hinzufügen eines Performance Service Levels zu einer Dateifreigabe. Sie können das gleiche Verfahren zum Aktualisieren einer beliebigen anderen Dateifreigabe-Eigenschaft verwenden.

1. Holen Sie sich den CIFS-Share oder den NFS-Dateifreigabschlüssel der Dateifreigabe, die Sie aktualisieren möchten. Diese API fragt alle Dateifreigaben in Ihrem Datacenter ab. Überspringen Sie

diesen Schritt, wenn Sie den Dateifreigabeconkey bereits kennen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/file-shares`

2. Zeigen Sie die Details der Dateifreigabe an, indem Sie die folgende API mit dem von Ihnen erhaltenen Dateifreigabschlüssel ausführen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/file-shares/{key}`

Zeigen Sie die Details der Dateifreigabe in der Ausgabe an.

```
"assigned_performance_service_level": {
        "key": null,
        "name": "Unassigned",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
      },
```

3. Holen Sie sich den Schlüssel für das Performance Service Level, das Sie für diese Dateifreigabe zuweisen möchten. Derzeit ist keine Richtlinie zugewiesen.

Kategorie	HTTP-Verb	Pfad
Performance Service Level	GET	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie den Eingabeparameter auf `true` einstellen `system_defined`. Holen Sie in der Ausgabe den Schlüssel des Performance Service Level, den Sie auf die Dateifreigabe anwenden möchten.

4. Wenden Sie den Performance Service Level auf der Dateifreigabe an.

Kategorie	HTTP-Verb	Pfad
Storage Provider	PATCH	`/storage-provider/file-shares/{key}`

In der Eingabe müssen Sie nur den Parameter angeben, den Sie aktualisieren möchten, zusammen mit

dem Dateifreigabetschlüssel. In diesem Fall ist es der Schlüssel zum Performance Service Level.

Stichprobe

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares"`-H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{
\"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" },
}"
```

Die JSON-Ausgabe zeigt ein Job-Objekt an, mit dem Sie überprüfen können, ob die Zugriffendpunkte auf den Home- und Partner-Nodes erfolgreich erstellt wurden.

5. Überprüfen Sie, ob der Performance Service Level zur Dateifreigabe hinzugefügt wurde, indem Sie den Job-Objektschlüssel verwenden, der in Ihrer Ausgabe angezeigt wird.

Kategorie	HTTP-Verb	Pfad
Management Server	GET	`/management-server/jobs/{key}`

Wenn Sie mit der ID des Job-Objekts abfragen, sehen Sie, ob die Dateifreigabe erfolgreich aktualisiert wurde. Beheben Sie bei einem Ausfall die Fehlerbehebung, und führen Sie die API erneut aus. Wenn die Datei erfolgreich erstellt wurde, fragen Sie die Dateifreigabe ab, um das geänderte Objekt anzuzeigen:

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/file-shares/{key}`

Zeigen Sie die Details der Dateifreigabe in der Ausgabe an.

```
"assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
        }
```

LUNs werden aktualisiert

Während Sie eine LUN aktualisieren, können Sie die folgenden Parameter ändern:

- Kapazität oder Größe
- „Online“- oder „Offline“-Einstellung
- Storage-Effizienzrichtlinie
- Performance Service Level
- LUN-Zuordnung

Während einer einzelnen API-Ausführung können Sie nur einen Parameter aktualisieren.

Bei diesem Verfahren wird das Hinzufügen eines Performance Service Levels zu einer LUN beschrieben. Sie können dasselbe Verfahren zum Aktualisieren jeder anderen LUN-Eigenschaft verwenden.

1. Holen Sie den LUN-Schlüssel der LUN, die Sie aktualisieren möchten. Diese API gibt Details zu allen LUNS in Ihrem Datacenter zurück. Überspringen Sie diesen Schritt, wenn Sie den LUN-Schlüssel bereits kennen.

Kategorie	HTTP-Verb	Pfad
Storage Provider	GET	`/storage-provider/luns`

2. Zeigen Sie die Details der LUN an, indem Sie die folgende API mit dem erhaltenen LUN-Schlüssel ausführen.

Kategorie	HTTP-Verb	Pfad
Storage Provider	GET	`/storage-provider/luns/{key}`

   Zeigen Sie die Details der LUN in der Ausgabe an. Sie sehen, dass dieser LUN kein Performance-Service-Level zugewiesen ist.

   Beispiel JSON-Ausgabe

```
"assigned_performance_service_level": {
      "key": null,
      "name": "Unassigned",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
```

3. Erhalten Sie den Schlüssel für das Performance Service Level, das Sie der LUN zuweisen möchten.

Kategorie	HTTP-Verb	Pfad
Performance Service Level	GET	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie den Eingabeparameter auf `true` einstellen `system_defined`. Holen Sie von der Ausgabe den Schlüssel des Performance Service Level, den Sie auf der LUN anwenden möchten.

4. Wenden Sie den Performance Service Level auf der LUN an.

Kategorie	HTTP-Verb	Pfad
Storage Provider	PATCH	`/storage-provider/lun/{key}`

Sie müssen in der Eingabe nur den Parameter angeben, den Sie aktualisieren möchten, zusammen mit dem LUN-Schlüssel. In diesem Fall ist es der Schlüssel zum Performance Service Level.

Stichprobe

```
curl -X PATCH "https://<hostname>/api/storage-provider/luns/7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Content-Type: application/json" H "Authorization: Basic <Base64EncodedCredentials>" -d "{ \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-fa163e82bbf2\" }"
```

In der JSON-Ausgabe wird ein Objektschlüssel angezeigt, mit dem Sie die aktualisierte LUN überprüfen können.

5. Zeigen Sie die Details der LUN an, indem Sie die folgende API mit dem erhaltenen LUN-Schlüssel ausführen.

Kategorie	HTTP-Verb	Pfad
Storage Provider	GET	`/storage-provider/luns/{key}`

Zeigen Sie die Details der LUN in der Ausgabe an. Sie sehen, dass dieser LUN das Performance-Service-Level zugewiesen ist.

Beispiel JSON-Ausgabe

```
     "assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
```

Ändern einer NFS-Dateifreigabe mithilfe von APIs zur Unterstützung von CIFS

Sie können eine NFS-Dateifreigabe ändern, um CIFS-Protokoll zu unterstützen. Während der Erstellung von Dateifreigabe können sowohl ACL-Parameter (Access Control List) als auch Richtlinienregeln für den Export für dieselbe Dateifreigabe festgelegt werden. Wenn Sie jedoch CIFS auf demselben Volume aktivieren möchten, auf dem Sie eine NFS-Dateifreigabe erstellt haben, können Sie die ACL-Parameter auf dieser Dateifreigabe aktualisieren, um CIFS zu unterstützen.

Was Sie brauchen

1. Eine NFS-Dateifreigabe muss nur mit den Details der Exportrichtlinie erstellt worden sein. Informationen hierzu finden Sie unter „*Managen von Dateifreigaben*“ und „ Ändern von Storage-Workloads_“.
2. Sie müssen über den Dateifreigabschlüssel verfügen, um diesen Vorgang ausführen zu können. Informationen zum Anzeigen von Details zur Dateifreigabe und zum Abrufen des Dateifreigabschlüssels mithilfe der Job-ID finden Sie unter *Provisioning CIFS and NFS File Shares*.

Dies gilt für eine NFS-Dateifreigabe, die Sie erstellt haben, indem Sie nur Richtlinien für den Export hinzufügen und nicht die ACL-Parameter. Sie ändern die NFS-Dateifreigabe, um die ACL-Parameter einzubeziehen.

Schritte

1. Führen Sie auf der NFS-Dateifreigabe einen `PATCH` Vorgang mit den ACL-Details durch, um CIFS-Zugriff zu ermöglichen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	`/storage-provider/file-shares`

Stichprobe

Basierend auf den Zugriffsberechtigungen, die Sie der Benutzergruppe zuweisen, wird wie im folgenden Beispiel angezeigt eine ACL erstellt und der Dateifreigabe zugewiesen.

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
```

Beispiel JSON-Ausgabe

Der Vorgang gibt die Job-ID des Jobs zurück, der das Update ausführt.

2. Überprüfen Sie, ob die Parameter korrekt hinzugefügt wurden, indem Sie die Details zur Dateifreigabe für dieselbe Dateifreigabe abfragen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	`/storage-provider/file-shares/{key}`

Beispiel JSON-Ausgabe

```
"access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
```

```
                    "index": 1,
                    "protocols": [
                        "nfs3",
                        "nfs4"
                    ],
                    "ro_rule": [
                        "sys"
                    ],
                    "rw_rule": [
                        "sys"
                    ],
                    "superuser": [
                        "none"
                    ]
                },
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 2,
                    "protocols": [
                        "cifs"
                    ],
                    "ro_rule": [
                        "ntlm"
                    ],
                    "rw_rule": [
                        "ntlm"
                    ],
                    "superuser": [
                        "none"
                    ]
                }
            ],
            "_links": {
                "self": {
                    "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
                }
            }
        }
    },
```

```
    "_links": {
        "self": {
            "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
        }
    }
```

Sie können die ACL sehen, die zusammen mit der Exportrichtlinie in die gleiche Dateifreigabe zugewiesen wurde.

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

Informationen über das Urheberrecht und die Lizenzen Dritter, die in diesem Produkt verwendet werden.

"Hinweis für Active IQ Unified Manager 9.14"